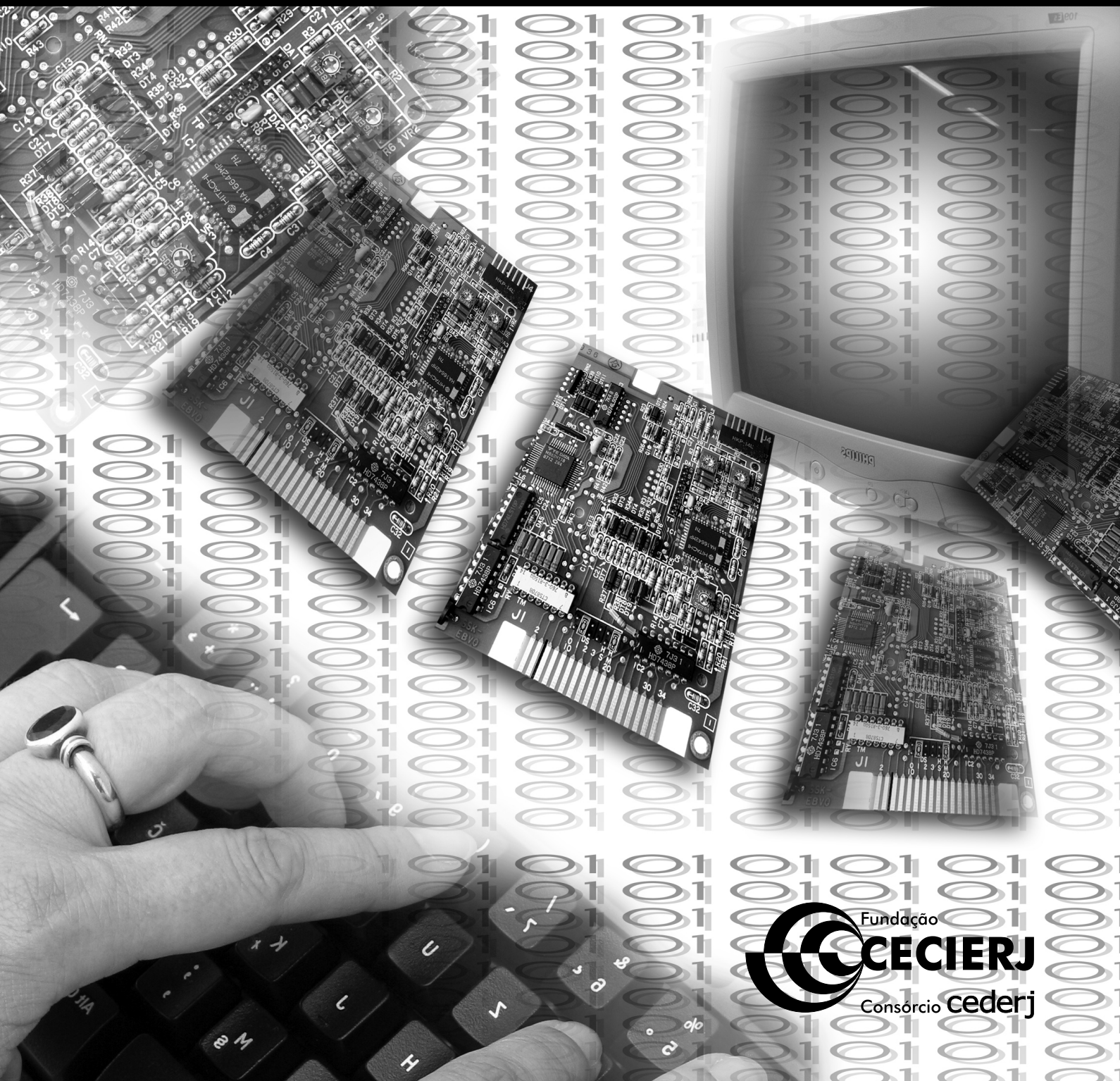
Módulo 2

Volume | 2

Luiz Manoel Figueiredo

Introdução à Criptografia



Fundação CECIERJ
Consórcio cederj

Fundação CECIERJ

Consórcio cederj

Centro de Educação Superior a Distância do Estado do Rio de Janeiro

Introdução à Criptografia

Volume 2 - Módulo 2

Luiz Manoel Figueiredo

UFF – Instituto de Matemática
Celso José da Costa

EB – Centro de Estudos de Pessoal
Antônio Carlos Guelfi

O material constante desta disciplina foi produzido sob o auspício de Convênio de cooperação técnico-acadêmica entre o Exército Brasileiro e a Universidade Federal Fluminense.

GOVERNO DO Rio de Janeiro
SECRETARIA DE CIÊNCIA E TECNOLOGIA

UAB UNIVERSIDADE ABERTA DO BRASIL

Ministério da Educação

BRASIL UM PAÍS DE TODOS
GOVERNO FEDERAL

Apoio:

FAPERJ
Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro

Fundação Cecierj / Consórcio Cederj

Rua Visconde de Niterói, 1364 – Mangueira – Rio de Janeiro, RJ – CEP 20943-001
Tel.: (21) 2334-1569 Fax: (21) 2568-0725

Presidente
Masako Oya Masuda

Vice-presidente
Mirian Crapez

Coordenação do Curso de Matemática
UFF - Regina Moreth
UNIRIO - Luiz Pedro San Gil Jutuca

Material Didático

ELABORAÇÃO DE CONTEÚDO
Luiz Manoel Figueiredo

CAPA
Eduardo Bordoni

PRODUÇÃO GRÁFICA
Oséias Ferraz
Patricia Seabra

972m

Figueiredo, Luiz Manoel.
Introdução à Criptografia. v. 2 / Luiz Manoel Figueiredo.
– Rio de Janeiro: UFF / CEP – EB, 2010.
172p.; 21 x 29,7 cm.

ISBN: 85-7648-331-9

1. Algoritmo de Euclides. 2. Teorema de Fermat.
3. Teorema de Euler. 4. Teorema chinês. I. Título.

CDD: 510

2010/1

Governo do Estado do Rio de Janeiro

Governador
Sérgio Cabral Filho

Secretário de Estado de Ciência e Tecnologia
Alexandre Cardoso

Universidades Consorciadas

UENF - UNIVERSIDADE ESTADUAL DO NORTE FLUMINENSE DARCY RIBEIRO
Reitor: Almy Junior Cordeiro de Carvalho

UERJ - UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
Reitor: Ricardo Vieiralves

UFF - UNIVERSIDADE FEDERAL FLUMINENSE
Reitor: Roberto de Souza Salles

UFRJ - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
Reitor: Aloísio Teixeira

UFRRJ - UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
Reitor: Ricardo Motta Miranda

UNIRIO - UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
Reitora: Malvina Tania Tuttman

SUMÁRIO

Programa da disciplina

Ementa

Aritmética dos inteiros: números primos, algoritmo da divisão, mdc e mmc, algoritmo de Euclides. Aritmética modular: congruência módulo, soma e produto de classes, inversa de uma classe módulo n. Teoremas de Fermat, Euler e o teorema chinês dos restos. Testes de primalidade: teste das divisões sucessivas, teste de Fermat, teste de Rabin-Miller, números de Charmichael.

Criptografia de chave pública: princípios, o algoritmo RSA, assinatura digital. O problema do logaritmo discreto, teste de Lucas, esquema de troca de chaves de Diffie-Hellman, ElGamal e o algoritmo de assinatura digital. Criptografia com o uso de curvas Elípticas: curvas elípticas, grupo de uma curva elíptica e aplicações.

Carga horária

60 horas

Objetivo

Apresentar a área da Matemática chamada Teoria dos Números, abordando os resultados utilizados em criptografia.

Metodologia

O conteúdo programático será apresentado na forma de textos e exemplos, com atividades a serem realizadas. Para complementar seu estudo, serão sugeridos livros e websites.

Avaliação

Prova escrita ao final da disciplina e avaliação a distância (atividades online).

Plano de Aulas

Unidade 1 – Teoria dos Números

Conteúdo	Onde encontrar
Aula 1 – Números Primos Teoria dos Números Divisores Números perfeitos	Textos 1 a 5
Aula 2 – Algoritmo da Divisão Axioma de Eudoxius Algoritmo da divisão Máximo divisor comum e mínimo múltiplo comum	Textos 6 a 11
Aula 3 – Algoritmo de Euclides Cálculo do mdc e do mmc através da fatoração Convergência do Algoritmo de Euclides	Textos 12 a 16
Aula 4 – Testes de Primalidade Primeiro teste de primalidade Teorema dos números primos	Textos 17 e 18
Aula 5 – Aritmética Modular Relações Congruência módulo n Classes de equivalência Classes de congruência	Textos 19 a 22
Aula 6 – Operações com classes de congruência Definição de soma e de produto de classes Tabelas de soma e de multiplicação Divisibilidade e potências	Textos 23 a 26
Aula 7 – Divisão modular Inversa de uma classe de congruência módulo n MDC de dois inteiros como combinação linear	Textos 27 a 30

Conteúdo	Onde encontrar
Aula 8 – Teorema de Fermat Aplicação do teorema de Fermat Equações diofantinas	Textos 31 a 35

Carga horária: 25 h

Unidade 2 – Criptografia de Chave Pública

Conteúdo	Onde encontrar
Aula 9 – Teste de Primalidade de Fermat Testes de primalidade Teste de Fermat Números de Carmichael Teste de Miller-Rabin	Textos 36 a 39
Aula 10 – Teorema de Euler Função ϕ de Euler	Textos 40 a 42
Aula 11 – Teorema Chinês dos Restos Exemplo com duas e três equações Aplicações à criptografia Partilha de um segredo com o teorema	Textos 43 a 47
Aula 12 – RSA Criptografia de chave pública GP/Pari Assinatura digital Segurança do RSA	Textos 48 a 54
Aula 13 – Logaritmo Discreto Raízes primitivas módulo n Grupos e subgrupos Logaritmos discretos	Textos 55 a 57
Aula 14 – Aplicações à Criptografia Teste de Lucas Esquema de troca de chaves de Diffie-Hellman ElGamal Algoritmo de assinatura digital	Textos 58 a 61

Conteúdo	Onde encontrar
Aula 15 – Criptografia com o uso de Curvas Elípticas Corpos finitos Grupo de uma curva elíptica Criptografia de curvas elípticas	Textos 62 a 65

Carga horária: 35 h

Unidade 1

Teoria dos Números

Caro aluno, seja bem-vindo à disciplina *Números primos e criptografia de chave pública*.

Nesta primeira unidade, você vai estudar os conceitos e resultados matemáticos que são a base das aplicações em criptografia de chave pública.

Bom estudo!

Aula 1 – Números Primos

Nesta primeira aula, você vai conhecer os números primos, que são a base para o estudo dos inteiros.

A grande importância dos números primos está em que todo inteiro pode ser escrito de maneira essencialmente única como produto de primos, como veremos a seguir.

Texto 1 - Teoria dos Números

A Teoria dos Números é a área da Matemática que estuda as propriedades dos números inteiros e os problemas que aparecem naturalmente neste estudo. O termo “aritmética” também é utilizado para se referir à Teoria dos Números.

Este campo de estudo da Matemática possui muitos problemas em aberto — problemas não resolvidos — fáceis de serem compreendidos, mas de difícil solução. Ao longo desta unidade você conhecerá alguns deles.

A Teoria dos Números se divide em seis ramos principais.

1. **Teoria elementar dos números**

   É a parte que estuda os inteiros e suas propriedades sem utilizar técnicas derivadas de outros campos da Matemática. Inclui também o estudo de divisibilidade, máximo divisor comum, fatoração em números primos, algoritmo de Euclides e congruência.

2. **Teoria analítica dos números**

   Este ramo emprega técnicas do cálculo e da análise para o estudo de problemas de inteiros. Esta área inclui o famoso teorema dos números primos e a hipótese de Riemann.

3. **Teoria algébrica dos números**

   Aqui o conceito de número é estendido para o de número algébrico e o conceito de inteiro para o de inteiro algébrico. Números algébricos são raízes de polinômios com coeficiente racionais. Muitas propriedades elementares dos inteiros não valem para os inteiros algébricos.

4. **Teoria combinatória dos números**

Estuda as propriedades de inteiros empregando técnicas da área da Matemática chamada Combinatória. O principal fundador desta área é o matemático húngaro **Paul Erdös** (1913 – 1996).

> Paul Erdös mostrou desde cedo aptidão para a Matemática. Com quatro anos descobriu algumas propriedades dos números primos. Fez numerosas e variadas contribuições e tinha fascínio em resolver problemas, como os de análise combinatória, teoria dos grafos e teoria dos números. Sempre queria resolvê-los de forma simples e elegante.

5. Teoria geométrica dos números

Também chamada de geometria dos números, usa técnicas geométricas para o estudo de números inteiros.

6. Teoria computacional dos números

Estuda algoritmos computacionais na Teoria dos Números.

Há dois grupos de algoritmos de grande importância em criptografia:

- **testes de primalidade** - são algoritmos que determinam se um dado inteiro é ou não primo;
- **algoritmos de fatoração de inteiros** - determinam a fatoração em primos de um dado inteiro.

> A Teoria dos Números tem, talvez como nenhuma outra área, a propriedade de incorporar métodos de outros campos de estudo, tornando-a um belo e complexo conjunto de conhecimentos e técnicas.

Texto 2 - Divisores

Agora vamos apresentar nosso primeiro tópico em Teoria dos Números: os divisores.

Sejam a e b inteiros.

Dizemos que a divide b quando existir um inteiro c tal que $b=ac$. Usamos a notação $a|b$, para indicar que a divide b e escrevemos $a\nmid b$ quando a não divide b. Quando $a|b$, dizemos também que b é múltiplo de a.

Exemplos: $6|12$, $23|115$, mas $4\nmid 21$.

Algumas propriedades imediatas são:

1. $n|n$

   Significa que todo inteiro divide a si mesmo. Isto segue da definição. Observe que $n=1\cdot n$.

2. $1|n$

   Isto é, 1 divide qualquer inteiro. Segue da definição, observando que $n=n\cdot 1$.

3. $n|0$

   Todo inteiro é divisor de 0. Basta observar que $0=n\cdot 0$.

Vamos examinar outras propriedades um pouco mais elaboradas.

Proposição 1: $a|b \;\; e \;\; b|a \;\Rightarrow\; |a|=|b|$

Demonstração

Como $a|b$ e $b|a$, então existem inteiros k_1 e k_2, tais que $a=k_1\cdot b$ e $b=k_2\cdot a$.

Substituindo uma expressão na outra, resulta que

$$a = k_1 \cdot (k_2 \cdot a) \Rightarrow a = (k_1 \cdot k_2)\, a \Rightarrow k_1 \cdot k_2 = 1$$

Como k_1 e k_2 são inteiros e $k_1 \cdot k_2 = 1$, então $k_1 = k_2 = 1$ ou $k_1 = k_2 = -1$.

De $a = k_1 \cdot b$, concluímos que $a = \pm b$, ou seja, $|a| = |b|$.

Proposição 2. Sejam a, b e c inteiros. Se $a|b$ e $b|c$, então $a|c$.

Demonstração.

Como $a|b$ e $b|c$, então existem inteiros k_1 e k_2 tais que

$$b = k_1 \cdot a \quad e \quad c = k_2 \cdot b$$

Substituindo o valor de b da primeira equação na segunda, resulta que

$$c = k_2 \cdot b = k_2 \cdot (k_1 \cdot a) = (k_2 \cdot k_1) \cdot a .$$

Portanto, c é múltiplo de a, isto é, $a|c$.

Exemplo: $3|15$ e $15|45$, logo $3|45$.

Proposição 3. Sejam a, b e c inteiros. Se $c|a$ e $c|b$, então $c|(ma + nb)$, para quaisquer inteiros m e n.

Demonstração.

Como $c|a$ e $c|b$, então existem inteiros k_1 e k_2, tais que $a = k_1 \cdot c$ e $b = k_2 \cdot c$.

Substituindo em $ma + nb$, temos:

$$ma + nb = m \cdot (k_1 \cdot c) + n \cdot (k_2 \cdot c) = mk_{1c} + nk_{2c} = (mk_1 + nk_2)\, c .$$

Portanto, $c|(ma+nb)$.

Exemplo: $7|21$ e $7|14$, logo $7|(21\mathrm{m}+14\mathrm{n})$ para quaisquer inteiros m e n.

Chamaremos $D(n)$ ao conjunto de todos os divisores de n.

Exemplo: $D(12)=\{\pm1,\pm2,\pm3,\pm4,\pm6,\pm12\}$

Observe que se d é divisor de n, então $-d$ também é divisor de n, pois, se $d|n$, então existe inteiro k, tal que

$$n=k\cdot d \;\Rightarrow\; n=(-k)\cdot(-d) \;\Rightarrow\; (-d)|n.$$

Assim, os divisores de um inteiro vêm sempre em pares de inteiros simétricos.

Chamamos $D^{+}(n)$ ao conjunto dos divisores positivos de n.

Exemplo: $D^{+}(12)=\{1,2,3,4,6,12\}$ e $D^{+}(6)=\{1,2,3,4,6\}$.

Se $d|n$ e $d\neq n$, então dizemos que d é divisor próprio de n.

Por exemplo, os divisores próprios de 6 são os inteiros ±1, ±2 e ±3.

Observe que 6 é a soma de seus divisores próprios positivos: $6=1+2+3$. Curioso, não? No próximo texto voltaremos a essa questão.

Veja, a seguir, mais algumas propriedades sobre divisores.

Proposição 4. Sejam a e b inteiros. Então $a|b$ se, e somente se, $D(a)\subset D(b)$.

Demonstração

Suponha que $a|b$. Para provar a inclusão $D(a)\subset D(b)$, basta mostrar que $x\in D(a)\Rightarrow x\in D(b)$, isto é, todo elemento de $D(a)$ também é elemento de $D(b)$.

Vamos lá! Se $x \in D(a)$, então $x|a$. Mas $a|b$ por hipótese. Logo, $x|a \ e \ a|b \Rightarrow x|b \Rightarrow x \in D(b)$.

Vamos supor agora que $D(a) \subset D(b)$. Como $a \in D(a)$ (todo inteiro é divisor de si mesmo) e $D(a) \subset D(b)$, então $a \in D(b)$, isto é, $a|b$.

Provamos então que $a|b \Leftrightarrow D(a) \subset D(b)$, isto é, $a|b$ é o mesmo que $D(a) \subset D(b)$, mostrando que a relação de divisibilidade entre dois inteiros $(a|b)$ é equivalente à relação de inclusão entre os conjuntos dos divisores destes inteiros $(D(a) \subset D(b))$.

Quando falarmos de máximo divisor comum (mdc) e mínimo múltiplo comum (mmc) de dois inteiros, retornaremos a essa analogia entre os inteiros e o conjunto de seus divisores.

Texto 3 - Números Perfeitos

Você viu que o inteiro 6 tem a propriedade de ser a soma de seus divisores próprios positivos: $6=1+2+3$.

Como é chamado um inteiro com esta característica? Um inteiro que é a soma de seus divisores próprios positivos é chamado de número perfeito.

Agora, pense em outros inteiros que são números perfeitos. O próximo na lista é o número 28.

Veja:

$D^+(28)=\{1,2,4,7,14,28\}$ e temos que $28=1+2+4+7+14$.

Os quatro primeiros números perfeitos são $6, 28, 496$ e 8128 . Estes quatro inteiros eram os únicos números perfeitos que os antigos gregos conheciam.

Euclides descobriu que estes quatro números são gerados pela fórmula

$$2^{n-1}(2^n-1)$$

para valores de $n=2,3,5 \ e \ 7$.

Então:

$$n=2 \rightarrow\ 2^{2-1}(2^2-1)\ =\ 2(4-1)=2\cdot 3=6$$
$$n=3 \rightarrow\ 2^{3-1}(2^3-1)\ =\ 2^2(8-1)=4\cdot 7=28$$
$$n=5 \rightarrow\ 2^{5-1}(2^5-1)\ =\ 2^4(32-1)=16\cdot 31=496$$
$$n=7 \rightarrow\ 2^{7-1}(2^7-1)\ =\ 2^6(128-1)=64\cdot 127=8128$$

Observe que nos quatro casos, (2^n-1) é um inteiro primo. **Euclides** mostrou que $2^{n-1}(2^n-1)$ é um número perfeito quando (2^n-1) é primo.

> Para saber quem foi Euclides de Alexandria, leia a seção "Saiba mais" ao final desta aula.

Como os inteiros $n=2,3,5\ e\ 7$ são exatamente os quatro primeiros números primos, os gregos naturalmente imaginaram que o quinto número perfeito seria obtido com $n=11$.

No entanto, o número $2^{11}-1$ não é primo. De fato, $2^{11}-1=2047=23\times 89$. Logo, $2^{11-1}(2^{11}-1)$ não é número perfeito.

Na verdade, o quinto número perfeito é o número $2^{12}(2^{13}-1)=33.550.336$, que é o inteiro $2^{n-1}(2^n-1)$, para $n=13$.

No século XVIII, Euler mostrou que a fórmula $2^{n-1}(2^n-1)$ fornece todos os números perfeitos pares.

Como você viu, nem todo inteiro $2^{n-1}(2^n-1)$ é número perfeito (por exemplo, não é perfeito para $n=11$). Mas todo número perfeito par é da forma $2^{n-1}(2^n-1)$. Este inteiro é perfeito exatamente quando 2^n-1 é primo.

Portanto, há uma associação entre números perfeitos e primos da forma 2^n-1 . Estes são chamados primos de Mersenne, em homenagem ao monge **Marin Mersenne** (1588-1648). Há uma busca mundial por primos grandes, em parte devido ao uso destes em criptografia.

Há algoritmos rápidos para testar a primalidade de inteiros da forma 2^n-1, razão pela qual os maiores primos conhecidos são os primos de Mersenne.

O 42° primo de Mersenne é o maior primo conhecido atualmente, descoberto em 14 de fevereiro de 2005. Trata-se do número $2^{25.964.951}-1$, que é um primo com 7.816.230 algarismos.

Há muito ainda o que investigar nesta área de estudo. Por exemplo, não se sabe se há infinitos primos de Mersenne. Mas vamos deixar este assunto para uma outra hora e voltar a falar de números primos e fatoração única.

O francês Marin Mersenne ficou conhecido por seu trabalho na Teoria dos Números e por se corresponder com outros matemáticos, possibilitando assim a comunicação do conhecimento pela Europa em uma época que os jornais científicos não existiam.

Texto 4 - Números Primos

Os números primos desempenham um papel fundamental no estudo dos inteiros e nas técnicas de criptografia.

Um inteiro $p \neq \pm 1$ é um número primo quando seus únicos divisores são ± 1 e $\pm p.$

Exemplo: $p = 2,3,5,7,11,13,17,19,23\, e\, 29$ são os 10 primeiros números primos positivos.

Observe que se p é primo, então $-p$ também é. Assim, são primos $p = -2,-3,-5,-7,-11,-13,-17,-19,-23$ e -29 .

Um número $N \neq \pm 1$ que não é primo é chamado composto. Assim, 12 é um número composto. Observe que ± 1 não é primo nem composto.

Os números primos sempre estiveram no centro da preocupação dos matemáticos que estudam os inteiros. Como você verá a seguir, todo inteiro fatora-se como produto de primos. Isto faz com

que os primos sejam uma espécie de bloco com os quais são construídos os inteiros, assim como todas as moléculas são feitas de átomos.

Vale destacar que a fatoração de inteiros em produtos de primos é, essencialmente, única. Lembre-se que fatorar um inteiro N é escrevê-lo como produto de primos.

Veja um exemplo.

O inteiro 60 pode ser escrito como $60=2^2\times3\times5.$ Esta é a fatoração de 60 em produto de primos. Dizemos que 2, 3 e 5 são os fatores primos de 60.

Mas o que significa dizer que a fatoração é única?

Podemos, por exemplo, escrever 60 também como:

$$60=3\times5\times2^2 \quad 60=5\times3\times2^2 \quad 60=2\times3\times2\times5.$$

O que todas estas fatorações têm em comum? É fácil ver que todas usam os mesmos primos, apenas mudando a ordem. Em todas, o primo 2 aparece duas vezes, o primo 3 aparece uma vez e o primo 5 aparece uma vez.

É neste sentido que dizemos que a fatoração é única: os mesmos primos aparecem o mesmo número de vezes, apenas a ordem difere duas fatorações de um inteiro.

O fato de que todo inteiro pode ser escrito de maneira única com produto de fatores primos é um teorema muito importante, chamado Teorema da Fatoração Única ou Teorema Fundamental da Aritmética.

Teorema da Fatoração Única

Dado um inteiro positivo $n\geq2$, podemos escrevê-lo de modo único na forma:

$$n=p_1^{e_1}\times\cdots\times p_k^{e_k},$$

onde $1<p_1<p_2<\cdots<p_k$ são primos distintos e $e_1,\cdots,e_k$ são inteiros positivos.

Os primos $p_1,\cdots,p_k$ são chamados fatores primos de n, enquanto os expoentes $e_1,\cdots,e_k$ são

chamados multiplicidades dos primos $p_{1,}\cdots,p_k$, respectivamente, na fatoração de n.

Exemplo: No caso de $72=2^3\times3^{2.}$, o primo 2 tem multiplicidade 3 na fatoração de 72, e o primo 3 tem multiplicidade 2.

Texto 5 – A infinitude dos Números Primos

Você estudou que os primos são os blocos fundamentais, os átomos, que constituem os inteiros. Uma primeira questão que se coloca naturalmente é a seguinte:

Existe um número finito ou infinito de primos?

Euclides respondeu a esta pergunta há 2.300 anos. A resposta é que existe um número infinito de primos. Esta resposta aparece como a Proposição 20 do livro IX dos Elementos de Euclides.

O método utilizado na demonstração é o de redução ao absurdo ou demonstração por contradição. Este tipo de prova é feita assumindo-se como verdade o oposto do que queremos provar e chegando-se a uma contradição. O fato de obter uma sentença falsa mostra que a proposição não pode ser negada, sendo por isso verdadeira.

Proposição 5. Existe um número infinito de números primos.

Demonstração

Vamos supor o contrário, isto é, que haja apenas um número finito de inteiros primos. Seja

$$p_1<p_2<\cdots<p_k$$

a lista de todos os inteiros primos. Seja agora $p^{\#}$ o produto de todos eles:

$$p^{\#}=p_1.p_2.\cdots.p_{k.}$$

Considere $N=p^{\#}+1.$ Nenhum dos primos $p_{1,}p_{2,}\cdots,p_k$ pode ser divisor de N, pois, para todo primo p_i, $p_i|p^{\#}.$ Se $p_i|N$, então $p_i\mid(N-p^{\#})=1,$ o que não pode acontecer, pois

$p_i > 1$.

Como nenhum p_i pode dividir N , então N não tem nenhum divisor primo. Portanto N deve ser um inteiro primo. Mas $N > p_k$ é maior que todos os primos da lista $p_1, \cdots, p_k$, o que é uma contradição, pelo fato de que esta é a lista de todos os primos.

Nesta aula você identificou algumas propriedades fundamentais dos números primos e aprendeu que um inteiro é chamado número perfeito quando é a soma de seus divisores próprios positivos. Na próxima aula, você estudará o algoritmo de divisão.

Saiba mais: Euclides de Alexandria

Euclides foi um matemático grego que viveu entre 325 e 265 a.C., tendo lecionado em Alexandria, no Egito. Sua obra mais famosa é a coleção de 13 livros chamados Elementos. Nela, Euclides apresenta uma coleção de definições, postulados (axiomas) e proposições (teoremas) e as provas destes teoremas, abordando os campos da Geometria e da Teoria dos Números.

Essa obra pode ser considerada o livro-texto mais bem sucedido da história da humanidade: foi um dos primeiros livros a serem impressos e é superada apenas pela Bíblia em número de edições – mais de mil já foram feitas. Até o início do século XX, era utilizado como livro-texto em muitas escolas.

Uma das grandes virtudes dos “Elementos” é apresentar de forma lógica e estruturada boa parte do conhecimento matemático conhecido à época de Euclides. Embora a maior parte dos resultados não tenha sido descoberta por ele, muitas das demonstrações foram feitas por Euclides.

A obra de Euclides teve um papel importante, ao legar à posteridade o conhecimento matemático grego. A estrutura lógica influenciou o desenvolvimento de toda a Matemática.

Atividades

1) Determine $D(10) e D(20)$. Verifique que $D(10) \subset D(20)$.

2) Primos gêmeos são pares de primos cuja diferença é dois. Encontre os cinco primeiros pares de primos gêmeos.

3) Existem primos trigêmeos, isto é, ternos de primos do tipo p , $p+2$ e $p+4$?

4) Mostre que todos os números pares de 4 a 40 podem ser escritos como soma de primos.

Aula 2 – Algoritmo da Divisão

Nesta aula, você vai conhecer o chamado algoritmo da divisão, que é, na verdade, um teorema, e não propriamente um algoritmo.

Texto 6 – Axioma de Eudoxius

A primeira noção importante a ser reconhecida é que, dados dois inteiros a e b, se a não é múltiplo de b, então situa-se entre dois múltiplos consecutivos de b.

Exemplo: $a=61$ e $b=5$. O inteiro 61 situa-se entre $60=12\times5$ e $65=13\times5$, que são múltiplos consecutivos de 5.

Este princípio, muitas vezes chamado erradamente de Princípio de Arquimedes, aparece nos Elementos de Euclides. Podemos escrevê-lo da seguinte forma:

Dados dois inteiros a e $b\neq0$, existe um inteiro q tal que

para $b>0$, $\quad q\cdot b\leq a<(q+1)b$

para $b<0$, $\quad q\cdot b\leq a<(q-1)b.$

Observe que a possibilidade de a ser múltiplo de b está coberta pelo menor ou igual em $q\cdot b\leq a.$

Exemplos:

- Se $a=35\,e\,b=7$, então $q=5:\ 5\times7=35.$
- Se $a=42\,e\,b=13$, então $q=3:\ 3\times13<42<4\times13.$
- Se $a=42\,e\,b=-13$, então $q=-3:\ (-3)\times(-13)<42<(-4)\times(-13).$

Texto 7 – O Algoritmo da Divisão

O teorema da divisão define precisamente o quociente e o resto de dois inteiros; mostra que eles existem e são únicos.

Teorema: Dados inteiros $a\ e\ b, b>0,$ existe um único par de inteiros $q\ e\ r$ tais que

$a = q \cdot b + r, \quad onde \quad 0 \leq r < b.$

O inteiro q é chamado quociente e r é o resto da divisão de a por b . Observe que se b é divisor de a , então o resto é 0: $a = q \cdot b.$

Demonstração

Pelo teorema de Eudoxius, como $b > 0$, existe q , tal que $q \cdot b \leq a < (q+1)b$.

Subtraindo $q \cdot b$ temos:

$$q \cdot b - q \cdot b \leq a - q \cdot b < (q+1)b - q \cdot b$$
$$0 \leq a - q \cdot b < b$$

Se definirmos $r = a - q \cdot b$, então:

$$0 \leq r < b \quad e \quad r = a - q \cdot b \Rightarrow a = q \cdot b + r .$$

Assim foi demonstrada a existência do quociente e do resto. Veja agora a demonstração da unicidade.

O truque usual para demonstrar a unicidade é supor que há dois e mostrar que são iguais. No caso em questão, vamos supor que há outro par $(q_{1,} \ r_1)$ tal que:

$$a = q_1 \cdot b + r_1 \quad e \quad 0 \leq r_1 < b$$

Subtraindo a equação anterior de $a = q \cdot b + r,$ temos:

$$\begin{array}{r} a = q \cdot b + r \\ a = q_1 \cdot b + r_1 \\ \hline 0 = (q - q_1)b + (r - r_1) \end{array}$$

Portanto, $b(q - q_1) = (r - r_1)$. Logo, $b | (r - r_1)$, isto é, $(r - r_1)$ é múltiplo de b .

Mas, $0 \leq r, r_1 < b \quad e \quad a \leq r, r_1 < b$.

Assim, o maior valor possível de $(r - r_1)$ é $b - 1$ (quando $r = b - 1 \quad e \quad r_1 = 0$) e o menor valor possível de $(r - r_1) \ é \ -(b-1)$ (quando $r = 0 \quad e \quad r_1 = b - 1$). Então, temos que $r - r_1$ é múltiplo de b e

$$-(b-1) \leq r-r_1 \leq b-1 .$$

Mas o único múltiplo de b neste intervalo é o 0, logo $r-r_1=0 \Rightarrow r=r_1$.

Ao substituir em $b\cdot(q_1-q)=0,\ temos\ q_1-q=0\Rightarrow q_1=q$.

No enunciado do teorema, colocamos a restrição $b>0$. No entanto, o teorema continua válido se $b<0$. Neste caso, definimos quociente e resto como $a=q\cdot b+r,\ com\ 0\leq r<|b|$.

Exemplos:

- $a=17\ e\ b=3\Rightarrow q=5\ e\ r=2 \quad (17=5\times 3+2)$
- $a=15\ e\ b=-4\Rightarrow q=-3\ e\ r=3 \quad (15=(-3)\times(-4)+3)$

Alguns argumentos presentes na demonstração do teorema são comuns. Por exemplo, quando queremos provar a unicidade, supomos que existam dois e provamos que são iguais.

Outro ponto chave, que aparece em outras demonstrações, é o argumento de que, se $b|t\ e\ -b<t<b\ ,então\ t=0.$

A demonstração anterior usa o argumento com $t=r-r_1$.

> Estas demonstrações parecem um pouco difíceis no início, porém, caso sinta necessidade, leia com atenção duas ou três vezes para que possa entendê-las. Ao compreender os argumentos, você poderá utilizá-los em outros problemas, com facilidade.

Texto 8 - O máximo divisor comum (mdc)

O conceito de máximo divisor comum de dois inteiros é simples e o algoritmo para calculá-lo tem grande importância em várias aplicações.

A definição de mdc é:

O máximo divisor comum de dois inteiros não-nulos a e b é o maior inteiro que divide a e b . É denotado por $mdc(a,b)$.

Exemplos:

- $mdc(15,25)=5$
- $mdc(300,140)=20$
- $mdc(-20,35)=5$
- $mdc(-8,-28)=4$

Observe que o mdc de dois inteiros é sempre positivo. É fácil ver por que, se d é divisor comum de a e b , $-d$ também é. Assim, os divisores comuns vêm em pares de simétricos $\pm d.$ O maior divisor comum será o maior dos divisores comuns positivos.

Exemplo:

- $mdc(12,18)=mdc(-12,18)=mdc(12,-18)=mdc(-12,-18)=6.$

Outra maneira de definir $mdc(a,b)$ é através dos conjuntos dos divisores $D(a) e D(b).$

$D(a)=divisores\ de\ a$ e $D(b)=divisores\ de\ b.$

Logo, $D(a)\cap D(b)=divisores\ comuns\ de\ a\ e\ b$. Como $mdc(a,b)$ é o maior divisor comum, então:

$$mdc(a,b)=max(D(a)\cap D(b))$$

Dois inteiros a e b são ditos **relativamente primos** se $mdc(a,b)=1.$

Exemplo:

- 20 e 27 são relativamente primos.
- Se p é primo, a é inteiro e $p\nmid a$, então p e a são relativamente primos.

Isso acontece porque os únicos divisores positivos de p são p e 1. Como $p\nmid a$, então p e a não têm divisores comuns além de $\pm 1,$ isto é, $mdc(a,p)=1.$ Ou seja, p e a são relativamente primos.

Uma propriedade muito importante do $mdc(a,b)$ é que ele sempre pode ser escrito como

combinação linear de a e b. Um inteiro n é combinação linear de a e b se existem inteiros $k_1 e k_2$ tais que $n = k_1 \cdot a + k_2 \cdot b$. É exatamente o que acontece com o mdc.

Teorema: Sejam a e b inteiros não-nulos e seja $d = mdc(a,b)$. Então, existem inteiros $k_1 e k_2$ tais que

$$d = k_1 a + k_2 b.$$

Exemplos:

- mdc(60,24)=12. O inteiro 12 pode ser escrito como $12 = 1 \times 60 - 2 \times 24$.
- mdc(50,30) = 10. O inteiro 10 pode ser escrito como $10 = 2 \times 50 - 3 \times 30$.

Observe que até agora não falamos sobre como calcular efetivamente o $mdc(a,b)$, nem como encontrar os inteiros $k_1 e k_2$, tais que $mdc(a,b) = k_1 \cdot a + k_2 \cdot b$. Falaremos sobre isso em breve.

Para terminar esta parte, você vai conhecer agora uma propriedade muito importante do $mdc(a,b)$.

O $mdc(a,b)$ é múltiplo de todos os divisores comuns de a e b.

Exemplos:

$$D(30) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$$

$$D(24) = \{\pm 1, \pm 2, \pm 3, +4, \pm 6, \pm 8, \pm 12, \pm 24\}$$

$$D(30) \cap D(24) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

Observe que $mdc(24,30) = 6$. E 6 é múltiplo de todos os divisores comuns: os elementos de $D(30) \cap D(24)$.

Veja a demonstração deste resultado.

Teorema: Sejam a e b inteiros não-nulos. Então, $d = mdc(a,b)$ se, e somente se,

(i) $d|a \ e \ d|b.$

(ii) Se $d'|a \ e \ d'|b \ então \ d'|d$.

Em outras palavras, o $mdc(a,b)$ se caracteriza por ser um divisor comum e por ser múltiplo de todos os divisores comuns.

Demonstração

Seja $d=mdc(a,b)$, então $d|a \ e \ d|b$, pois d é divisor comum, o que prova o item (i).

Seja d' um inteiro tal que $d'|a \ e \ d'|b$. Sabemos que d é combinação linear de a e b, isto é, existem inteiros $k_1 \ e \ k_2$ tais que $d=k_1 \cdot a+k_2 \cdot b.$

Como $d'|a \ e \ d'|b$, então $d'|(k_1 \cdot a+k_2 \cdot b)$, logo $d'|d$, o que prova o item (ii).

Por outro lado, se um inteiro positivo d atende aos itens (i) e (ii), então é:

- divisor comum pelo item (i);
- o maior divisor comum, pois, pelo item (ii), se d' é outro divisor comum, então $d'|d \Rightarrow d' \leq d$.

Veja a seguir vários resultados referentes ao mdc de dois inteiros. Estes resultados e os exemplos que aparecem em seguida são importantes para que você compreenda como funciona o algoritmo da divisão para encontrar o máximo divisor comum de dois inteiros.

Proposição: Para todo inteiro t, $mdc(t \cdot a, t \cdot b) = t \ mdc(a,b)$.

Esta proposição, por brevidade, vai ficar sem demonstração. Ela pode ser encontrada em Introdução à Teoria dos Números, de José Plínio de Oliveira Santos, 1998.

Exemplo: $mdc(150,35)=mdc(5 \cdot 30, 5 \cdot 7)=5 \cdot mdc(30,7)=5 \cdot 1=5.$

Uma conseqüência da proposição anterior é que, se a e b são divisíveis por um inteiro c, então

$\frac{a}{c} \ e \ \frac{b}{c}$ são inteiros e $mdc(a,b) = mdc(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}) = c \ mdc(\frac{a}{c}, \frac{b}{c})$.

Ao dividir a e b por $d=mdc(a,b)$ temos:

$$d=mdc(a,b)=mdc(d\cdot\frac{a}{d},d\cdot\frac{b}{d})=d\ mdc(\frac{a}{d},\frac{b}{d}),$$

mas $d=d\cdot mdc(\frac{a}{d},\frac{b}{d})\Rightarrow mdc(\frac{a}{d},\frac{b}{d})=1.$

Concluímos que:

Proposição. Se $d=mdc(a,b)$, então os inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.

Exemplo: $a=35$ e $b=75$. Temos que $mdc(35,75)=5.$

Os inteiros $\frac{35}{5}=7$ e $\frac{75}{5}=15$ são primos entre si.

Outra proposição utilizada é

Se $a|bc$ e $mdc(a,b)=1$, então $a|c$.

Demonstração

Como $mdc(a,b)=1$, então 1 é combinação linear de a e b, isto é, existem k_1 e k_2, tais que $1=k_1a+k_2b$. Ao multiplicar esta equação por c, resulta em $c=k_1(ac)+k_2(bc)$.

Mas $a|bc$ (por hipótese) e $a|ac$, logo $a\mid(k_1(ac)+k_2(bc)=c).$

Exemplo. Se t é inteiro qualquer e $7|15\cdot t$, então $7|t$, pois $mdc(7,15)=1.$

Texto 9 – O mínimo múltiplo comum (mmc)

O mínimo múltiplo comum de dois inteiros a e b é o menor inteiro positivo que é múltiplo comum de a e b . É representado por $mmc(a,b)$.

Exemplos:

- $mmc(2,3)=6$
- $mmc(20,25)=100$
- $mmc(1,n)=n,$ para todo inteiro n .
- $mmc(-3,-5)=15.$

Claramente, se $a|b$, então $mdc(a,b)=a$ e $mmc(a,b)=b$.

Exemplo: 15 divide 75, logo $mdc(15,75)=15$ e $mmc(15,75)=75$.

Veremos na próxima aula que o mmc de dois inteiros está diretamente relacionado ao mdc, por meio de uma fórmula simples.

Texto 10 – O mdc e mmc de vários inteiros

Os conceitos de mdc e mmc de dois inteiros podem ser facilmente generalizados para mais de dois inteiros, da seguinte forma:

Para dados inteiros não-nulos $a_1, a_2, \cdots, a_t$, definimos $mdc(a_1, a_2, \cdots, a_t)$ como o maior divisor comum de $a_1, a_2, \cdots, a_t$, e $mmc(a_1, a_2, \cdots, a_t)$ como o menor múltiplo comum de $a_1, a_2, \cdots, a_t$.

Exemplos:

- $mdc(20,30,50)=10$
- $mmc(20,30,50)=300$

Assim, mostramos que:

$mdc(a,b,c)=mdc(mdc(a,b),c)$ e $mmc(a,b,c)=mmc(mmc(a,b),c)$.

Exemplos:

- $mdc(20,30,50)=mdc(mdc(20,30),50)=mdc(10,50)=10.$

- $mmc(20,30,50)=mmc(mmc(20,30),50)=mmc(60,50)=300$.

Texto 11 – Como calcular o máximo divisor comum

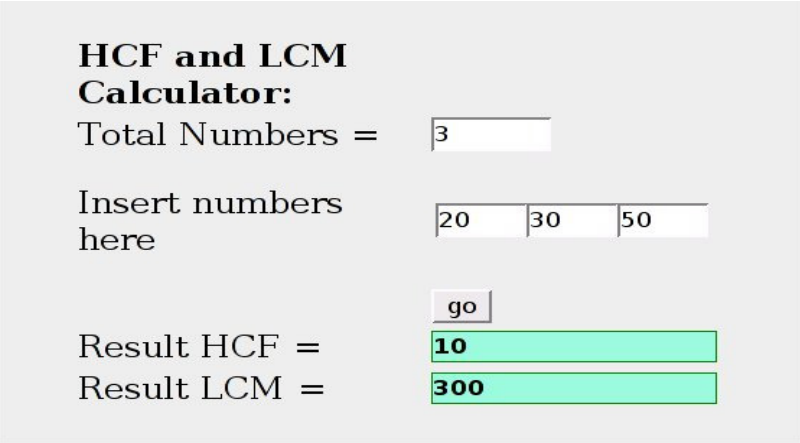
Agora que você conheceu as definições do mdc e do mmc de dois ou mais inteiros positivos, veja como calculá-los.

Uma maneira eficiente de calcular o mdc é utilizar o algoritmo de Euclides. Estudaremos o algoritmo de Euclides na próxima aula. Como o mmc está relacionado ao mdc por uma fórmula simples, podemos calcular o mmc de dois inteiros calculando primeiro o mdc destes inteiros.

No endereço http://www.maths.hscripts.com/hcf.php, há uma calculadora de mdc e mmc online. Em inglês, mdc é chamado GCD (*Greates Commom Divisor*) ou HCF (*Highest Commom Factor*) e mmc é chamado LCD (*Least Commom Multiple*).

Na calculadora online existe um primeiro espaço onde se coloca o número de inteiros para os quais queremos calcular o mdc e o mmc. Em seguida, aparecem os espaços onde devem ser digitados estes números e, após apertar o botão “go”, aparecem os resultados.

A imagem a seguir trata de um exemplo obtido na calculadora online.



Nesta aula, você estudou o teorema da divisão, que define precisamente quociente e resto, e mostra a unicidade destes. Estudou também o máximo divisor comum

(mdc) e mínimo múltiplo comum (mmc) de dois ou mais inteiros e algumas de suas propriedades.

Os próximos passos serão estudar o algoritmo de Euclides para o cálculo do mdc e ver a relação entre o mdc e o mmc de dois inteiros. Faremos esses dois avanços na próxima aula.

Atividades

1) Encontre o quociente e o resto dos seguintes pares de inteiros:
a) a = 35 e b = 12
b) a = -30 e b = 18
c) a = 315 e b = 250

2) Calcule o mdc e o mmc dos pares de inteiros da questão anterior.

3) Na próxima aula, vamos mostrar que, para todo par de inteiros não-nulos, a e b valem $mdc(a,b)\cdot mmc(a,b)=a\cdot b.$ Verifique essa fórmula com os itens da questão 1.

4) Na próxima aula, vamos mostrar também que, para todo par de inteiros não-nulos a e b, se q e r são o quociente e o resto da divisão de a por b, então vale $mdc(a,b)=mdc(q,r)$.
Verifique essa fórmula com os itens da questão 1.

Aula 3 – Algoritmo de Euclides

O algoritmo de Euclides é utilizado para determinar o máximo divisor comum (mdc) de dois inteiros. É, certamente, um dos mais antigos algoritmos matemáticos conhecidos. Surge, por volta de 300 a.C., na coleção de livros Elementos, de Euclides. Há, no entanto, indicações de sua existência muito antes desta data.

Este algoritmo permite determinar o mdc de dois inteiros, sem que seja necessário fatorá-los, sendo este, em geral, um problema mais complexo.

Texto 12 – Dois resultados preliminares

Para demonstrar o algoritmo são necessários dois resultados preliminares. Veja a seguir.

Proposição: Dados dois inteiros não-nulos a e b , para qualquer inteiro k vale que $mdc(a,b)=mdc(a,b+ka)$.

Demonstração

Os pares (a,b) e $(a,b+ka)$ têm os mesmos divisores comuns, pois, por um lado, se $d|a$ e $d|b$, então $d|b+ka;$ por outro lado, se $d|a$ e $d|b+ka$, então $d|b+ka-ka \Rightarrow d|b.$

Como os pares (a,b) e $(a,b+ka)$ têm os mesmos divisores comuns, certamente vão ter o mesmo máximo divisor comum, isto é, $mdc(a,b)=mdc(a,b+ka)$.

Exemplo: $mdc(5,5t+1)=mdc(5,1)=1,$ para todo t inteiro.

Uma conseqüência direta da proposição anterior é que

Proposição: Se a e b são inteiros e $a=qb+r,$ sendo q e r inteiros, então $mdc(a,b)=mdc(b,r)$.

Demonstração

Se $a=qb+r$, então $r=a-qb.$ Portanto

$$mdc(a,b)=mdc(b,a)=mdc(b,a-qb)=mdc(b,r).$$

Essa última proposição é a chave para o algoritmo de Euclides. Perceba que, para calcular o mdc de dois inteiros $a>b,$ basta calcular o mdc dos inteiros b e r , em que $b>r.$ Qual é a vantagem? Simples, os inteiros são menores. Veja um exemplo:

Seja $a=1725 \ e \ b=315.$ A divisão de a por b é $1725=5\cdot 315+150.$
Então,

$$mdc(1725,315)=mdc(315,150).$$

O segundo mdc é facilmente calculado, pois os números são menores. Aliás, podemos aplicar o mesmo processo no segundo mdc.

$$315=2\cdot 150+15 \ \Rightarrow \ mdc(315,150)=mdc(150,15).$$

Como $15|150$, então $mdc(150,15)=15.$

Texto 13 – O Algoritmo de Euclides

Vamos, agora, descrever o algoritmo de um modo mais formal. Sejam a e b dois números inteiros positivos. Podemos assumir que $a\geq b$. Caso contrário, invertemos a ordem dos números.

Se $a=b$, teremos $d=mdc(a,b)=a=b.$

Vamos considerar $a>b$. Pelo Teorema da Divisão de Euclides, existem números $q_1 \ e \ r_1$ tais que:

$$a=q_1\cdot b+r_{1,} \ onde \ 0\leq r_1<b.$$

Se $r_1=0$, então $a=q_1\cdot b$ e b é um dos divisores positivos de a. Nesse caso,

$$d=mdc(a,b)=b.$$

Se $r_1\neq 0,$ temos $0<r_1<b \ \ e \ \ a=q_1\cdot b+r_1$. Nesse caso,

$$d=mdc(a,b)=mdc(b,r_1).$$

Seguimos para um novo passo do algoritmo, agora com os inteiros b e r_1 . Sejam q_2 e r_2 o quociente e o resto da divisão de b por r_1 , respectivamente.

$$b = q_2 \cdot r_1 + r_2, \text{ em que } 0 \leq r_2 < r_1 .$$

Se $r_2 = 0$, temos $b = q_2 \cdot r_1$ e, nesse caso,

$$mdc(b, r_1) = r_1 = mdc(a, b).$$

Paramos o nosso algoritmo nesse estágio.

Se $r_2 \neq 0$, temos $0 < r_2 < r_1$ e $b = q_2 \cdot r_1 + r_2$. Nesse caso,

$$d = mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2).$$

Como a seqüência dos restos satisfaz às condições

$$b > r_1 > r_2 > \cdots > r_k > \cdots \geq 0,$$

partindo de um b fixado, existirá um primeiro índice k tal que $r_k = 0$. Nessa etapa, paramos o algoritmo e temos que:

$$d = mdc(a, b) = mdc(b, r_1) = \cdots = mdc(r_{k-2}, r_{k-1}) = r_{k-1}.$$

Exemplo:

Vamos aplicar o algoritmo de Euclides para determinar $mdc(245,168)$.

$$\begin{aligned} 245 &= 1 \times 168 + 77 \\ 168 &= 2 \times 77 + 14 \\ 77 &= 5 \times 14 + 7 \\ 14 &= 2 \times 7 + 0 \end{aligned}$$

Então,

$$mdc(245,168) = mdc(168,77) = mdc(77,14) = mdc(14,7) = 7, \ pois \ 7 | 14.$$

É comum esse processo ser representado pelo esquema a seguir:

| 1 | 2 | 5 | 2 |

245	168	77	14	7
77	14	7	0	

Texto 14 – Cálculo do mdc e do mmc através da fatoração

Uma outra maneira de calcular o mdc e mmc de dois inteiros a e b é utilizar sua fatoração.

Sejam:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \quad e \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$$

em que escrevemos a e b com todos os primos envolvidos em a e b, usando expoentes nulos, caso seja necessário.

Se um primo p_i divide a, mas não divide b, podemos colocar p_i na fatoração de b, mas com expoente 0, pois $p_i^0 = 1,$ o que não altera a fatoração.

Exemplo: Sejam $a = 12$ e $b = 21$. Temos que $a = 2^2 \cdot 3$ e $b = 3 \cdot 7$. Ao escrever essas fatorações com os mesmos primos, obtemos:

$$a = 2^2 \cdot 3^1 \cdot 7^0 \quad e \quad b = 2^0 \cdot 3^1 \cdot 7^1.$$

Ao colocar os inteiros a e b com os mesmo fatores primos p_i, temos:

$$mdc(a,b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k}, \quad onde \quad \gamma_i = min(\alpha_i, \beta_i).$$

Isto é, o expoente de um primo p_i na fatoração de $mdc(a,b)$ é o <u>mínimo</u> entre os expoentes de p_i nas fatorações de a e b.

Como $\gamma_i = min(\alpha_i, \beta_i)$, então $\gamma_i \leq \alpha_i \quad e \quad \gamma_i \leq \beta_i,$ para todo $i, 1 \leq i \leq k.$

Assim, $p_i^{\gamma_i} \mid p_i^{\alpha_i}$ e $p_i^{\gamma_i} \mid p_i^{\beta_i}$.

Logo,

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k} \mid p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = a \quad \text{e} \quad d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k} \mid p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} = b,$$

ou seja, $d|a$ e $d|b$.

Se d' é outro divisor comum de a e b , e se p_i aparece com expoente ϵ_i na fatoração de d', então,

$$p_i^{\epsilon_i} \mid p_i^{\alpha_i} \ e \ p_i^{\epsilon_i} \mid p_i^{\beta_i} \Rightarrow \epsilon_i \leq \alpha_i \ e \ \epsilon_i \leq \beta_i \Rightarrow \epsilon_i \leq min(\alpha_i, \beta_i) = \gamma_i \Rightarrow p_i^{\epsilon_i} \mid p_i^{\gamma_i}.$$

Lembrando que γ_i é o expoente de p_i na fatoração de d , segue-se que $d' \mid d.$ Portanto d é divisor comum e todo divisor comum d' divide d , o que prova que $d = mdc(a,b)$.

> Pode parecer mais fácil obter o máximo divisor comum de dois inteiros utilizando a fatoração. O grande problema é fatorá-los. Nas aplicações interessantes, lidamos com inteiros muito grandes. Nesse caso, fatorar é um problema mais complexo que usar o algoritmo de Euclides para obter o mdc.

Ao utilizar um raciocínio análogo ao mencionado anteriormente, pode-se deduzir a fatoração do mínimo múltiplo comum de dois inteiros a e b .

Se $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ e $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, então,

$$mmc(a,b) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_k^{\delta_k}, \text{ em que } \delta_i = max(\alpha_i, \beta_i).$$

O expoente de p_i na fatoração de $mmc(a,b)$ é o máximo dos expoentes de p_i na fatoração de a e b .

Exemplo. Seja $a = 84$ e $b = 18.$ Então $a = 2^2 \cdot 3 \cdot 7$ e $b = 2 \cdot 3^2.$

Logo,

$$mmc(84,18) = 2^2 \cdot 3^2 \cdot 7 = 252.$$

No entanto o cálculo do $mmc(a,b)$ não é prático, se os inteiros a e b forem grandes, dada a dificuldade de fatorá-los. Para o cálculo do $mmc(a,b)$, não há um algoritmo de Euclides. O que existe é uma relação direta com o $mdc(a,b)$, permitindo o cálculo de um a partir do outro. É o que você vai estudar no texto a seguir.

Texto 15 – Relação entre $mdc(a,b)$ e $mmc(a,b)$

Para ver a relação entre o $mdc(a,b)$ e o $mmc(a,b)$, perceba inicialmente que, para quaisquer inteiros x e y,

$$max(x,y)+min(x,y)=x+y.$$

Por exemplo, se $x \leq y$ (o caso $x \geq y$ é análogo), então

$$max(x,y)=y \quad e \quad min(x,y)=x \Rightarrow max(x,y)+min(x,y)=x+y.$$

Sejam agora a e b inteiros e $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ e $b=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_k^{\beta_k}$.

Você viu que:

$$mdc(a,b)=p_1^{\gamma_1}\cdot p_2^{\gamma_2}\cdot\ldots\cdot p_k^{\gamma_k}, \text{ onde } \gamma_i=min(\alpha_i,\beta_i) \text{ e}$$
$$mmc(a,b)=p_1^{\delta_1}\cdot p_2^{\delta_2}\cdot\ldots\cdot p_k^{\delta_k}, \text{ onde } \delta_i=max(\alpha_i,\beta_i) .$$

Assim,

$$mdc(a,b)\cdot mmc(a,b)=\left(p_1^{\gamma_1}\cdot p_2^{\gamma_2}\cdot\ldots\cdot p_k^{\gamma_k}\right)\cdot\left(p_1^{\delta_1}\cdot p_2^{\delta_2}\cdot\ldots\cdot p_k^{\delta_k}\right)=p_1^{\gamma_1+\delta_1}\cdot p_2^{\gamma_2+\delta_2}\cdot\ldots\cdot p_k^{\gamma_k+\delta_k},$$

em que são agrupadas as potências de mesma base, somando os expoentes.

Mas, para todo i, $\gamma_i+\delta_i=min(\alpha_i,\beta_i)+max(\alpha_i,\beta_i)=\alpha_i+\beta_i$,

portanto,

$$p_1^{\gamma_1+\delta_1}\cdot p_2^{\gamma_2+\delta_2}\cdot\ldots\cdot p_k^{\gamma_k+\delta_k}=p_1^{\alpha_1+\beta_1}\cdot p_2^{\alpha_2+\beta_2}\cdot\ldots\cdot p_k^{\alpha_k+\beta_k}=\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\right)\cdot\left(p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_k^{\beta_k}\right)=a\cdot b,$$

ou seja,

$$mdc(a,b)\cdot mmc(a,b)=a\cdot b.$$

Exemplo: $a=84=2^2\cdot 3\cdot 7$ e $b=18=2\cdot 3^{2.}$.

Temos $mdc(84,18)=2\cdot 3=6$ e $mmc(84,18)=2^2\cdot 3^2\cdot 7=252.$ Então:

$$mdc(84,18)\cdot mmc(84,18)=6\cdot 252=1512=84\cdot 18=a\cdot b.$$

Texto 16 – Convergência do Algoritmo de Euclides

Veremos agora uma abordagem mais computacional do Algoritmo de Euclides.

Para calcular o mdc de dois inteiros positivos a e b, podem-se listar todos os divisores positivos comuns de a e b e determinar o máximo destes divisores.

Um algoritmo desse tipo pode ser escrito da seguinte forma:

Entrada: inteiros positivos a e b.
Saída: $mdc(a,b)$.

- Para todo inteiro k entre 1 e o mínimo de a e b, teste se $k|a \ e \ k|b$. Em caso afirmativo, inclua k em um conjunto I.
- Retorne o máximo do conjunto I.

Este é um algoritmo que sempre funciona, pois retorna o mdc de dois inteiros a e b. No entanto é extremamente lento. Ainda que possa ser melhorado de diversas maneiras, esse algoritmo não é prático para inteiros grandes, uma vez que são necessárias várias divisões.

> O Algoritmo de Euclides tem duas vantagens: é rápido e fácil de ser implementado computacionalmente.

O Algoritmo de Euclides pode ser escrito do seguinte modo:

Entrada: inteiros positivos a e b.
Saída: $mdc(a,b)$.

- Seja r o resto da divisão de a por b.
- Se $r=0$, então o resultado é b e paramos.
- Se $r\neq 0$, então calculamos $mdc(b,r)$ e retornamos esse valor como resposta.

Este algoritmo é definido por recorrência, isto é, o algoritmo cita ele mesmo várias vezes, a fim de obter o resultado.

Mais quão rápido converge o Algoritmo de Euclides? Por exemplo, ao iniciar com inteiros *a* e *b* de 1000 algarismos, quantos passos, no máximo, seriam necessários para chegarmos ao final do algoritmo?

Essa é uma pergunta muito importante quando consideramos aplicações computacionais práticas que utilizam o Algoritmo de Euclides.

Para respondermos a essa pergunta, precisamos da seguinte proposição:

Proposição. Sejam a e b inteiros positivos, com $a \geq b$, e seja r o resto da divisão de a e b. Então $r \leq a/2$.

Demonstração

Como $0 \leq r < b$, se $b \leq a/2$, então $r \leq a/2$.

Se $b > a/2$, o quociente da divisão de a por b é 1, logo:

$$a = b \cdot 1 + r \Rightarrow r = a - b.$$

Mas $b > a/2 \Rightarrow -b < -a/2 \Rightarrow a - b < a - a/2 = a/2$. Portanto $r < a/2$.

Com essa proposição se determina o número máximo de passos necessários para que o algoritmo de Euclides termine.

No algoritmo de Euclides temos

$$mdc(a,b) = mdc(b,r) = mdc(r,r_1) = mdc(r_1,r_2) = mdc(r_2,r_3) = \cdots$$

Observe que a cada dois passos trocamos os primeiros elementos de um par pelo resto da divisão dos dois elementos do par.

Por exemplo, no 3º passo ($mdc(r,r_1)$), o primeiro elemento do par é r , que é o resto da divisão de a por b (par no 1º passo).

No 4º passo ($mdc(r_1, r_2)$), o primeiro elemento do par é r_1 , que é o resto dos inteiros do 2º passo ($mdc(b, r)$).

Assim, $r \leq a/2 \Rightarrow r_2 \leq r/2 \leq a/4 \Rightarrow r_4 \leq r_2/2 \leq r/4 \leq a/8.$ A cada dois passos, o maior número do par fica reduzido a, no máximo, metade do valor. Você pode observar que os restos r_k, para k inteiro par, satisfazem $r_k \leq \frac{a}{2^{k/2+1}}$.

Na pior hipótese, vale a igualdade na fórmula acima e o algoritmo para quando encontramos resto 1.

Fazendo $r_k = 1$ na fórmula anterior, obtemos:

$$\frac{a}{2^{k/2+1}} = 1 \Rightarrow a = 2^{k/2+1}$$

Ao aplicar logaritmo de base 2 de ambos os lados, temos:

$$\log_2 a = \frac{k}{2} + 1 \Rightarrow \log_2 a - 1 = \frac{k}{2} \Rightarrow k = 2\log_2 a - 2.$$

A conclusão é que o número máximo de passos para terminar o algoritmo de Euclides é $2\log_2 a - 2,$ em que a é o maior dos inteiros que iniciaram o algoritmo.

Exemplo: Se a é um inteiro de mil dígitos, então $a \leq 10^{1000}$.

Assim,

$$k \leq 2\log_2 10^{1000} - 2 = 2000\log_2 10 - 2 \approx 2000 \cdot 3{,}322 - 2 = 6641.$$

O algoritmo chega ao resultado em, no máximo, 6.641 passos.

Nesta aula você teve contato com muitas demonstrações, contas com fatorações em primos e, por isso, pode ter encontrado alguma dificuldade. Algumas vezes é preciso ler mais de uma vez. Há detalhes que só podem ser percebidos depois que os conceitos ficam mais amadurecidos.

Você também estudou o algoritmo de Euclides, a expressão do mdc e do mmc, em

termos da fatoração em primos dos inteiros envolvidos, e a fórmula que relaciona o mdc e o mmc.

Atividade

1) Use o algoritmo de Euclides para calcular o mdc entre os pares de números abaixo. A partir do mdc, calcule o mmc destes números.

   a) $a=847$ e $b=91$.
   b) $a=2475$ e $b=231$.

Aula 4 – Testes de Primalidade

Como afirmar se um inteiro é primo? Trata-se de um problema relevante em várias aplicações de Teoria dos Números, incluindo as aplicações em Criptografia.

Um teste de primalidade é qualquer algoritmo que determina se um inteiro é primo. Não confunda teste de primalidade com um problema relacionado: o de fatoração de inteiros.

> Determinar a fatoração de um dado inteiro é computacionalmente mais difícil do que determinar se esse inteiro é ou não primo.

Nesta aula, você vai estudar um processo clássico para obter todos os primos de 1 a n e a descrição de um teste de primalidade simples.

Texto 17 – Primeiro teste de primalidade

Vamos agora descrever um método simples para determinar se um inteiro n é ou não primo.

Se um inteiro n não é primo, então há algum fator primo menor que ele. A idéia é dividir n por todos os primos menores que ele. Caso não seja divisível por nenhum, então será primo.

Não é necessário testar todos os primos menores que n ; basta avaliar os primos menores ou iguais a $\sqrt{n}$.

Proposição. Se n não é primo, então possui um fator primo menor ou igual a $\sqrt{n}$.

Demonstração

Se n é composto, então existem n_1 e n_2 , tais que $n = n_1 \cdot n_2$, em que $1 < n_1 < n$ e $1 < n_2 < n.$

Suponha que $n_1 \leq n_2$ (o caso $n_2 \leq n_1$ é análogo). Assim:

$$n = n_1 \cdot n_2 \geq n_1 \cdot n_1 = n_1^2 \Rightarrow n_1 \leq \sqrt{n}.$$

Seja p fator primo de n_1 (caso n_1 seja primo, $p = n_1$). Como $n_1 \leq \sqrt{n}$ e $p | n_1$, então $p \leq n_1 \leq \sqrt{n}$ e, como $p | n_1$ e $n_1 | n$, então $p | n$. Logo, p é fator primo de n menor ou igual a $\sqrt{n}$.

Exemplo: Vamos determinar se 127 é primo. Como $\sqrt{127}$ é um pouco maior que 11, basta testar a divisibilidade de 127 pelos primos 2, 3, 5, 7 e 11. Como ele não é divisível por nenhum destes números, então 127 é primo.

Para usar este método, convém ter em mãos uma lista de primos. Uma forma para obtê-la, até um número escolhido, é o conhecido crivo de **Eratóstenes**.

Leia sobre Eratóstenes na seção “Saiba mais” ao final desta aula.

O crivo de Eratóstenes é um método muito antigo para encontrar todos os primos até um certo inteiro específico. A palavra crivo quer dizer peneira. O algoritmo atua, de fato, como uma peneira, separando os múltiplos dos primos em sucessão, deixando passar apenas os que não são divisíveis por estes primos. Ao final do processo, apenas os primos passam pela peneira.

O método consiste em escrever todos os inteiros de 1 a N. Como 1 não é primo, pode ser riscado imediatamente.

O algoritmo prossegue, seqüencialmente, em passos. Em cada etapa, encontramos o primeiro número que não foi riscado, marcamos ele como primo e riscamos todos os seus múltiplos próprios. Enquanto o último número a ser avaliado não excede a raiz quadrada de N, repetimos os passos citados. Quando o algoritmo pára, os inteiros remanescentes são primos.

Por exemplo, vamos escrever o crivo de 1 a 100. Devemos eliminar os múltiplos dos primos menores ou iguais a $\sqrt{100} = 10$.

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

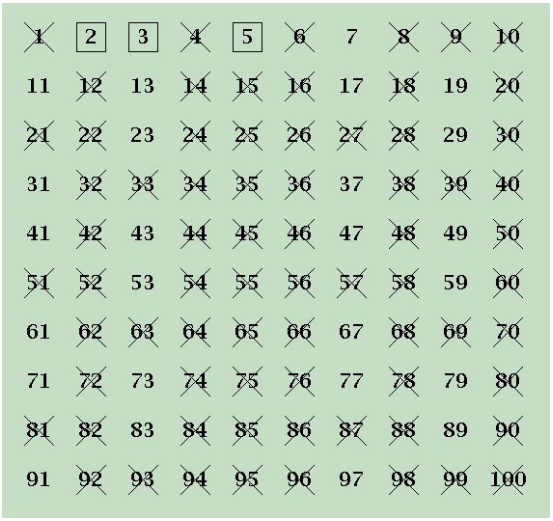
Inicialmente, escrevemos todos os inteiros de 1 a 100. Riscamos o 1, que não é primo.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

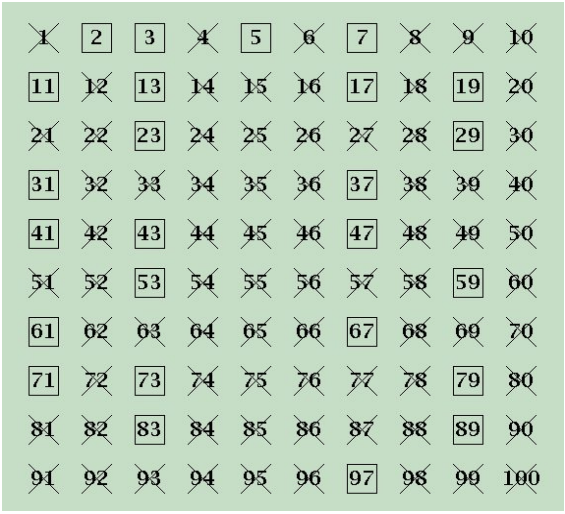
Encontramos e marcamos como primo o número 2. Em seguida, riscamos todos os múltiplos próprios de 2.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

Depois marcamos 3 como primo e riscamos seus múltiplos próprios.



Em seguida, o primeiro inteiro não-riscado é o 5. Marcamos 5 como primo e riscamos seus múltiplos próprios.



O primeiro inteiro não-riscado é o 7. Selecionamos 7 como primo e riscamos seus múltiplos próprios.

Como o próximo número não-riscado é 11, que é maior que a raiz quadrada de 100, o algoritmo pára e os inteiros remanescentes podem ser marcados como primos.

Concluímos que os primos de 1 a 100 são:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97.

Para conhecer mais sobre os crivos de Eratóstenes, visite os dois endereços listados a seguir:

http://www.cut-the-knot.org/Curriculum/Arithmetic/Eratosthenes.shtml

Neste endereço há um aplicativo em que você pode escolher o inteiro N. Então, aparece em um botão o próximo inteiro não-riscado. Ao apertá-lo, são riscados os múltiplos próprios deste inteiro e o próximo não-riscado é exibido.

http://www.faust.fr.bw.schule.de/mhb/eratosiv.htm

Neste outro endereço, você encontra um aplicativo de crivo de Eratóstenes montado de 1 a 400. Ao clicar em um inteiro da tabela, os múltiplos próprios desse inteiro desaparecem.

O teste apresentado inicialmente – dividir um inteiro N pelo primos menores ou iguais a $\sqrt{N}$ – sempre funciona; porém, na prática, não pode ser utilizado para inteiros com fatores primos muito grandes. É comum ser utilizado para testar a primalidade de inteiros pequenos.

Vários testes de primalidade populares são probabilísticos. Esses testes não permitem afirmar com certeza se um inteiro n é primo, mas podem comprovar que n provavelmente é primo.

Se n passa no teste, então apresenta certa probabilidade de ser primo. A chance de erro pode ser reduzida a um valor arbitrariamente baixo, se aplicarmos o teste várias vezes.

O teste probabilístico mais simples é o teste de Fermat, que será estudado na Aula 9.

Texto 18 – Teorema dos Números Primos

Para responder a algumas questões, como, por exemplo,

- existem infinitos primos, mas como eles se distribuem?
- conforme os inteiros ficam maiores, os primos se tornam menos espaçados?
- a densidade dos primos diminui?

é necessário definir a função $\pi(x)$.

Se x é real positivo, então $\pi(x)$ é o número de inteiros primos menores ou iguais a x .

Exemplos:

- $\pi(10)=4$ (os primos 2, 3, 5 e 7 são menores que 10);
- $\pi(100)=25$, há 25 primos menores que 100. Confira na lista que fizemos usando o crivo de Eratóstenes;
- $\pi(1000)=168$;
- $\pi(10^4)=1.229$;
- $\pi(10^5)=9.592$;
- $\pi(10^6)=78.498$.

Um resultado importante, suposto originalmente por Gauss, no século XIX, e provado por Hadamard e Vallé-Poussin, em 1896, é o chamado teorema dos números primos, que afirma que:

$$\lim_{x \to \infty} \frac{\pi(x)}{\left(\frac{x}{\log(x)}\right)} = 1$$

onde $\log x$ é o logaritmo natural de x (logaritmo na base e).

Esse resultado significa que, se x é muito grande, então $\pi(x)$ deve estar próximo de $\frac{x}{\log(x)}$, pelo menos em termos relativos.

Mesmo para valores muito grandes de x , o erro $\pi(x) - \frac{x}{\log(x)}$ é bastante elevado. Por exemplo, para $x = 10^{16}$, o erro é da ordem de 10^{13} .

Há vários problemas não resolvidos na Matemática, relacionados à questão da distribuição dos números primos. Um dos problemas sem solução mais importantes — a chamada hipótese de Riemann — relaciona-se à função $\pi(x)$ e ao teorema dos números primos.

Nesta aula 4, você aprendeu o que são testes de primalidade e estudou o teste mais simples, que é tentar dividir N por todos os primos menores ou iguais a $\sqrt{N}$. Este método nos leva ao crivo de Eratóstenes, que é um algoritmo antigo para elaborar tabelas de primos.

Você também estudou a questão da distribuição dos números primos e o Teorema dos Números Primos.

Vamos voltar à questão dos testes de primalidade ao apresentarmos o pequeno teorema de Fermat, que dá origem a um teste probabilístico, chamado teste de Fermat.

Saiba mais: Eratóstenes

Eratóstenes foi um matemático, geógrafo e astrônomo grego que viveu de 276 a 194 a.C. Nasceu em Cyrene (atual Líbia), mas estudou, trabalhou e morreu em Alexandria, onde atuou como bibliotecário da famosa biblioteca dessa cidade.

Eratóstenes fez contribuições importantes para as áreas de Matemática e Ciências. Foi o primeiro a calcular a circunferência da Terra, usando trigonometria e o conhecimento do ângulo de elevação do Sol ao meio-dia, em duas cidades distantes.

Há controvérsias sobre a unidade de medida usada por Eratóstenes, mas acredita-se que o valor obtido por ele esteja entre 39.690 Km e 46.620 Km, valor próximo ao conhecido hoje, de 40.080 Km. Eratóstenes mediu também a distância da Terra ao Sol, da Terra à Lua e teria compilado um catálogo de 675 estrelas.

Eratóstenes era conhecido na época pelo apelido de beta, a segunda letra do alfabeto grego. A razão do nome é que, segundo seus contemporâneos, ele tinha grande conhecimento em várias áreas, mas em cada uma delas era apenas o segundo melhor.

Atividades

1) Determine se os seguintes inteiros são primos:

a) N = 229
b) N = 1223
c) N = 481

2) Use o crivo de Eratóstenes para determinar todos os primos até N=200. Determine $\pi(200)$.

Aula 5 – Aritmética Modular

Aritmética modular é um sistema em que as operações entre os inteiros são feitas “módulo” um outro inteiro n . O sentido desta frase será melhor compreendido ao longo desta aula.

Para entender o sistema, pense em um relógio. Se ele marca 21 horas neste momento, daqui a 5 horas marcará 2 horas da manhã, certo?

Isso ocorre porque, após as 24 horas, o relógio volta a marcar 0 hora, reiniciando a contagem. Se ele marca 18 horas, após 10 horas marcará 4 horas da manhã. Assim: $18+10=28$ e $28-24=4$.

Esta “aritmética do relógio” acontecerá em qualquer evento cíclico. É semelhante ao **código de César**. Usando um alfabeto de 23 letras, se trocarmos cada letra pela próxima, duas unidades à frente, então temos:

$$\begin{array}{ccc} A(1) & \rightarrow & C(3) \\ B(2) & \rightarrow & D(4) \\ \vdots & & \vdots \\ V(21) & \rightarrow & Z(23) \\ X(22) & \rightarrow & A(1) \\ Z(23) & \rightarrow & B(2) \end{array}$$

Veja que V (letra 21) é substituída por Z (letra 23); X (letra 22) por A (letra 1) e Z (letra 23) por B (letra 2). Em números, esta substituição corresponde à operação $x \rightarrow x+2,$ com o detalhe de, após o 23, voltamos ao início. Isto é uma aritmética modular, no caso módulo 23.

> Como você estudou na primeira disciplina do curso, um código de César é um método em que uma chave, definida por um número, é usada para cifrar e para decifrar a mensagem. Leia mais sobre esse método criptográfico na aula 5 do livro Introdução à Criptografia.

Para definir exatamente essas noções, é importante que você conheça o estudo das relações de equivalência e veja como a aritmética modular se traduz em uma relação de equivalência chamada congruência módulo n .

Assim, nesta aula, você vai estudar a definição de relação e o que é uma relação de equivalência,

e ainda vai aprender que congruência módulo n é uma relação de equivalência.

Texto 19 - Relações

Uma relação em um conjunto S é uma maneira de comparar os elementos de S .

Exemplo:

São relações:

- A relação de igualdade $=$ nos inteiros.
- A relação $\leqslant$ nos inteiros.
- A relação “ter a mesma idade” em um grupo de pessoas.
- A relação “ser da mesma espécie” no conjunto de animais em um zoológico.

Isso lhe dá uma idéia do que seja uma relação. Veja a definição formal de relação no quadro a seguir.

> Podemos definir uma relação em um conjunto S como um subconjunto de $S\times S$ (conjunto dos pares ordenados $\{(x,y);x,y\in S\}$).

Exemplos:

- A relação de igualdade no conjunto $\{1,2,3,4,5\}$ é o subconjunto $R=\{(1,1),(2,2),(3,3),(4,4),(5,5)\}$.

- A relação $\leq$ no conjunto $\{1,2,3,4,5\}$ é o subconjunto

$$R=\{(1,1),(1,2),(1,3),(1,4),(1,5),(2,2),(2,3),(2,4),(2,5),(3,3),(3,4),(3,5),(4,4),(4,5),(5,5)\}.$$

A idéia dessa representação é que, para uma relação em um conjunto S, temos um subconjunto $R\subseteq S\times S$, tal que $(x,y)\in R$, quando x e y se relacionam.

Muitas relações interessantes obedecem às propriedades que serão destacadas a seguir.

Seja S um conjunto e $\sim$ uma relação em S . Dizemos que a relação $\sim$ é

i. **reflexiva**, quando $a \sim a$ para todo $a \in S$.
ii. **simétrica**, quando $a \sim b \Rightarrow b \sim a$ para todo $a, b \in S.$
iii. **transitiva**, quando $a \sim b \ e \ b \sim c \Rightarrow a \sim c$, para todos $a, b, c \in S.$

Confira alguns exemplos.

- A relação de igualdade nos inteiros é reflexiva, simétrica e transitiva (Verifique).

- A relação $\leq$ nos inteiros é reflexiva ($a \leq a$) e transitiva ($a \leq b \ e \ b \leq c \Rightarrow a \leq c$), mas não é simétrica (por exemplo, se $a \neq b$, então não vale $a \leq b \ e \ b \leq a$).

- A relação $<$ no conjunto dos inteiros é transitiva, mas não é reflexiva nem simétrica.

- A relação "ter a mesma idade que" no conjunto dos alunos de uma sala é:
  - reflexiva (aluno A tem a mesma idade que ele mesmo),
  - simétrica (se A tem a mesma idade que B, então B tem a mesma idade que A)
  - transitiva (se A tem a mesma idade que B e B tem a mesma idade que C, então A tem a mesma idade que C).

- A relação de inclusão $\subseteq$ no conjunto $P(X)$ dos subconjuntos de um conjunto X é uma relação reflexiva e transitiva, mas não é simétrica.

Há uma quarta propriedade que surge em várias relações importantes (inclusive $\leq$) :

Uma relação $\sim$ é

iv. **anti-simétrica**, quando $a \sim b \ e \ b \sim a \Rightarrow a = b$.

A relação $\leq$ no conjunto dos inteiros é reflexiva, anti-simétrica e transitiva.

Podemos agora definir a relação de equivalência.

Uma relação em um conjunto S é chamada relação de equivalência, se ela é reflexiva, simétrica e transitiva.

Exemplos.

- A relação de igualdade nos inteiros é relação de equivalência.
- A relação "ter a mesma idade que" no conjunto dos alunos de uma sala é relação de equivalência.

A relação $\leq$ no conjunto dos inteiros não é relação de equivalência, pois não é simétrica, mas é importante.

Muitas relações interessantes são, assim como $\leq$, relações reflexivas, anti-simétricas e transitivas. Elas também recebem um nome especial.

Uma relação reflexiva, anti-simétrica e transitiva é chamada **relação de ordem**.

São relações de ordem:

- A relação $\leq$ no conjunto dos inteiros.
- A relação $\subseteq$ no conjunto dos subconjuntos de um conjunto X .
- A relação "a divide b" no conjunto dos inteiros.

Agora, vamos voltar às congruências módulo n , ponto de partida desta aula.

Texto 20 – Congruência Módulo n

Seja n um inteiro positivo. Dizemos que $a \equiv b \, mod \, n$, se $a-b$ é um múltiplo de n , ou seja, se $a=b+kn$ para algum $k \in \mathbb{N}$.

Exemplos:

- $14 \equiv 6 \, mod \, 4$, pois 4 divide $14-6=8$.
- $-3 \equiv 7 \, mod \, 5$, porque 5 divide $-3-7=-10$.
- $10 \equiv 0 \, mod \, 5$, pois 5 divide $10-0=10$.

Observe que $a \equiv 0 \, mod \, n \Leftrightarrow n|(a-0) \Leftrightarrow n|a$, ou seja, os inteiros que são congruentes a 0 módulo n são exatamente os múltiplos de n.

Sejam a inteiro e n inteiro positivo, q e r o quociente e o resto da divisão de a por n. Temos que:

$$a = q \cdot n + r \Rightarrow a - r = q \cdot n \Rightarrow a \equiv r \, mod \, n.$$

Então, por exemplo, todos os inteiros que têm resto 1 pela divisão por n são congruentes a 1 módulo n.

Encontrar o resto da divisão de a por n é equivalente a achar um inteiro $r, 0 \leq r < n$, tal que $a \equiv r \, mod \, n$. Esta observação é importante porque veremos diversas fórmulas que permitem encontrar facilmente um inteiro pequeno que seja congruente módulo n a uma dada potência.

Agora, vamos estabelecer o fato de que a relação de congruência módulo n é uma relação de equivalência.

Proposição. Para todos a, b e c inteiros e n inteiro positivo, vale que:

1. $a \equiv a \mod n$ (propriedade reflexiva)
2. $a \equiv b \mod n \Rightarrow b \equiv a \mod n$ (propriedade simétrica)
3. $a \equiv b \mod n \; e \; b \equiv c \mod n \Rightarrow a \equiv c \mod n$ (propriedade transitiva)

Como exercício, faça a proposição 1 e 2. Depois, siga e veja a demonstração da proposição 3. Ao final, junto com a resposta dos exercícios, veja as demonstrações feitas.

Demonstração. Quanto à afirmação 3, se

$$a \equiv b \mod n \; e \; b \equiv c \mod n,$$

então,

$$n|(a-b) \; e \; n|(b-c) \Rightarrow n|(a-b)+(b-c)=(a-c) \Rightarrow a \equiv c \mod n.$$

Esta proposição mostra que a relação de congruência módulo n é uma relação de equivalência.

No próximo texto, você vai aprender que uma relação de congruência em um conjunto cria uma partição desse conjunto, que é dada pelas classes de equivalência.

Após você estudar estas classes, vai entender como se aplica a relação de congruência módulo n .

Texto 21 - Classes de Equivalência

Uma relação de congruência em um conjunto S induz naturalmente a uma classificação dos objetos do conjunto.

Por exemplo, a relação de equivalência dada por "ter a mesma idade que" no conjunto dos alunos de uma escola classifica-os em um subconjunto de alunos de mesma idade. Todos os alunos de 15 anos, por exemplo, são equivalentes por esta relação, e ficam dentro da mesma "classe".

Esta classificação é expressa pelo conceito de **classe de equivalência**.

Dada uma relação de equivalência $\sim$ em um conjunto S , a classe de equivalência de um elemento $x \in S$ é formada pelos elementos que são equivalentes a x por $\sim$.

Denotamos a classe de equivalência de x por $\bar{x}$ assim:

$$\bar{x} = \{y \in S \mid y \sim x\}$$

Observe que, se $y \in \bar{x}$, então $x \in \bar{y}$, o que é apenas outra forma de dizer que, se $y \sim x$, *então* $x \sim y$, que é a propriedade de simetria de uma relação de equivalência.

Por outro lado, se $x \in \bar{y}$, então $\bar{x} = \bar{y}$, pois, se $z \in \bar{x}$, então $z \sim x$. Como $x \in \bar{y}$, então $x \sim y$; logo $z \sim x \ e \ x \sim y \Rightarrow z \sim y \Rightarrow z \in \bar{y}$.

Desta forma, $z \in \bar{x} \Rightarrow z \in \bar{y}$, o que mostra que $\bar{x} \subset \bar{y}$.

Podemos mostrar de forma análoga que $\bar{y} \subset \bar{x}$, provando assim que $\bar{x} = \bar{y}$, quando $x \in \bar{y}$.

Isso permite concluir que, se $\bar{x} \cap \bar{y} \neq \emptyset$, então $\bar{x} = \bar{y}$, pois se $z \in \bar{x} \cap \bar{y}$, então $z \in \bar{x} \ e \ z \in \bar{y} \Rightarrow \bar{z} = \bar{x} \ e \ \bar{z} = \bar{y} \Rightarrow \bar{x} = \bar{y}$.
Em outras palavras, duas classes de equivalência ou são iguais, ou são disjuntas.

Observe ainda que, como $x \in \bar{x}$, todo elemento de S está em alguma classe de equivalência.

Essas observações podem ser resumidas em duas propriedades muito importantes das classes de equivalência:

i. Duas classes distintas são disjuntas.
ii. A união de todas as classes de equivalência é todo o conjunto S.

Desse modo, o conjunto das classes de equivalência em um conjunto S é formado por subconjuntos não-vazios disjuntos de S, cuja união é S. Este conjunto é chamado **espaço quociente** da relação de equivalência $\sim$ e é algumas vezes denotado por $S/\sim$.

Uma partição de um conjunto S é uma coleção de subconjuntos não-vazios S_i, disjuntos dois a dois ($S_i \cap S_j = \emptyset$ se $i \neq j$), tal que S é a união dos S_i.

O que foi mostrado anteriormente é que, dada uma relação de equivalência em um conjunto S, o conjunto de suas classes de equivalência forma uma partição de S.

Assim, é fácil mostrar a recíproca.

> Dada uma partição de S, existe uma relação de equivalência tal que suas classes de equivalência são os conjuntos da partição.

Texto 22 – Classes de Congruência

A relação de congruência módulo n é uma relação de equivalência.

> Quais são as classes de equivalência para congruência módulo n ?

Vamos a um exemplo: quais são as classes módulo 5?

Primeiro, vamos obter a classe do 0:

$$x \in \bar{0} \Rightarrow x \equiv 0 \mod 5 \Rightarrow 5 | (x - 0) \Rightarrow 5 | x$$

Portanto, $\bar{0}$ é formado pelos múltiplos de 5:

$$\bar{0}=\{5k \mid k\in\mathbb{Z}\} = \{\ldots,-10,-5,0,5,10,\ldots\}$$

Qual é a classe de 1?

$$x\in\bar{1} \Rightarrow x\equiv 1 \mod 5 \Rightarrow 5\mid(x-1) \Rightarrow x-1=5k \Rightarrow x=5k+1, \text{para algum } k\in\mathbb{Z}.$$

Assim, $\bar{1}$ é formado pelos múltiplos de 5 somados a 1:

$$\bar{1}=\{5k+1 \mid k\in\mathbb{Z}\} = \{\ldots,-9,-4,1,6,11,\ldots\}$$

Continuando, obtemos:

- $\bar{2}=\{5k+2 \mid k\in\mathbb{Z}\} = \{\ldots,-8,-3,2,7,12,\ldots\}$
- $\bar{3}=\{5k+3 \mid k\in\mathbb{Z}\} = \{\ldots,-7,-2,3,8,13,\ldots\}$
- $\bar{4}=\{5k+4 \mid k\in\mathbb{Z}\} = \{\ldots,-6,-1,4,9,14,\ldots\}$

E o $\bar{5}$? Como $5\in\bar{0}$, temos $\bar{5}=\bar{0}$.

As classes $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$ são todas as classes módulo 5. Observe que, para qualquer a inteiro, existem inteiros q e r, tal que $a=5q+r$, onde $0\le r<5$ (divisão de n por 5). Logo $a\equiv r \mod 5 \Rightarrow a\in\bar{r}$.

Assim, $\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$ é o espaço quociente (conjunto das classes de equivalência) da relação de congruência módulo 5. Chamamos este conjunto de $\mathbb{Z}_5$.

Podemos generalizar esta observação. Veja a seguir.

Proposição. Seja n inteiro positivo. O conjunto de todas as classes de congruência módulo n é o conjunto $\{\bar{0},\bar{1},\ldots,\overline{n-1}\}$.

Demonstração

Dado qualquer inteiro a, existem inteiros q e r, tais que:

$$a = q \cdot n + r, \ sendo \ 0 \leq r < n.$$

Portanto $a \equiv r \ mod \ n \Rightarrow a \in \bar{r}$. Desta forma, todos os inteiros estão em alguma das classes $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

Por outro lado, as classes $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ são todas distintas, pois dois inteiros entre 0 e $n-1$ só podem ser congruentes módulo n se forem iguais.

Representamos por $\mathbb{Z}_n$ o conjunto de todas as classes de congruência módulo n.

Então: $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

Cada classe $\bar{a}$ é um conjunto infinito. O inteiro a é um representante da classe $\bar{a}$. Veja que, para uma classe, podemos escolher qualquer elemento dela como representante.

Por exemplo: para módulo 5, qualquer inteiro da forma $5k+1$ é representante da classe $\bar{1}$.

Nesta aula, você estudou as relações de congruência módulo n. Para isso, aprendeu as relações em geral, conheceu algumas propriedades e viu, em particular, que as relações reflexivas, simétricas e transitivas são chamadas relações de equivalência.

> Uma relação de equivalência em um conjunto particiona este conjunto em classes de equivalência.

Outro ponto estudado foi a relação de congruência módulo n, que é uma relação de equivalência. O conjunto das classes de congruência módulo n é denotado por $\mathbb{Z}_n$. Você viu ainda a demonstração de que:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}.$$

A congruência módulo n é uma poderosa ferramenta na Teoria dos Números. E você verá, ao longo da disciplina, que essa é utilizada quase que universalmente.

Atividades

1) Seja $S = \{1,2,3,4\}$. Considere as seguintes relações em S:

$R_1 = \{(1,1), (2,2), (3,3), (4,4)\}$
$R_2 = \{(1,2), (1,3), (2,2), (2,3)\}$
$R_3 = \{(1,1), (1,2), (2,2), (2,3), (3,3), (4,4)\}$
$R_4 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (3,1), (3,3)\}$
$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

Para cada uma das relações anteriores, indique se é reflexiva, simétrica ou transitiva.

2) Determine se as afirmações a seguir são verdadeiras ou falsas:

a) $25 \equiv 1 \; mod \; 12$
b) $-5 \equiv -14 \; mod \; 3$
c) $12 \equiv -2 \; mod \; 3$
d) $5 + 7t \equiv 5 \; mod \; 7, \; para \; todo \; t \in \mathbb{Z}$
e) $x^2 + 17y = 3 \; mod \; 17 \Rightarrow x^2 \equiv 3 \; mod \; 17$

Aula 6 - Operações com Classes de Congruência

A Matemática é a rainha das ciências e a Aritmética é a rainha da Matemática.
Carl Friedrich Gauss

Como você estudou na primeira aula, a aritmética, termo utilizado para se referir à Teoria dos Números, tem como objetivo estudar os números inteiros, suas operações e representações.

Agora você vai estudar as operações com classes de congruência. Neste próximo passo, vai aprender a definição de soma e de produto de classes módulo n .

Você se lembra que a aula anterior, sobre Aritmética Modular, iniciou com a aritmética das horas de um relógio? Vamos ver mais sobre esse exemplo.

Texto 23 – Definição de Soma e de Produto de Classes

A aritmética do relógio é uma aritmética módulo 24. Por exemplo, se o relógio marca 23 horas, após 5 horas vai marcar 4 horas da manhã. Isso acontece porque $23+5-24=4$ (após às 24 horas, o relógio volta a marcar 0 hora). Para uma aritmética módulo 24, temos a soma $23+5=4$. Mais precisamente, em $\mathbb{Z}_{24}$, temos $\overline{23}+\overline{5}=\overline{4}$.

A operação de soma em $\mathbb{Z}_n$ é definida naturalmente por $\bar{a}+\bar{b}=\overline{a+b}$. O problema desta definição é que a e b são representantes das classes $\bar{a}$ e $\bar{b}$, respectivamente.

Nesse caso, se fossem utilizados outros representantes, seria obtido o mesmo resultado? Vamos ver um exemplo.

Em $\mathbb{Z}_8$, $6+5=11\equiv 3 \mod 8$. Logo, $\bar{6}+\bar{5}=\overline{6+5}=\overline{11}=\bar{3}$.

Mas $14\equiv 6 \mod 8$ e $21\equiv 5 \mod 8$, logo $\overline{14}=\bar{6}$ e $\overline{21}\equiv\bar{5} \mod 8$. Se somarmos $\bar{6}+\bar{5}$, usando os representantes 14 e 21, vamos obter o mesmo resultado? Verificamos facilmente que sim, pois

$$\overline{14}+\overline{21}=\overline{14+21}=\overline{35}=\bar{3}.$$

É claro que este é apenas um exemplo. Para que a definição $\bar{a}+\bar{b}=\overline{a+b}$ faça sentido, temos de provar que, para qualquer inteiro positivo n, a soma $\overline{a+b}$ não depende dos representantes escolhidos nas classes $\bar{a}$ e $\bar{b}$.

Na próxima proposição, vamos provar que tanto a soma como o produto de classes não dependem da escolha dos representantes.

Proposição. Em $\mathbb{Z}_n$, se $\bar{a'}=\bar{a}$ e $\bar{b'}=\bar{b}$, então

1. $\overline{a'+b'}=\overline{a+b}$
2. $\overline{a'\cdot b'}=\overline{a\cdot b}$

Demonstração

$\bar{a'}=\bar{a} \Rightarrow a' \equiv a \bmod n \Rightarrow a'=a+k_1 n$, para algum $k_1 \in \mathbb{Z}$.

$\bar{b'}=\bar{b} \Rightarrow b' \equiv b \bmod n \Rightarrow b'=b+k_2 n$, para algum $k_2 \in \mathbb{Z}$.

Logo,

$$a'+b'=(a+k_1 n)+(b+k_2 n)=(a+b)+(k_1+k_2)n \Rightarrow a'+b' \equiv a+b \bmod n,$$

o que mostra que $\overline{a'+b'}=\overline{a+b}$.

$$a'\cdot b'=(a+k_1 n)\cdot(b+k_2 n)=ab+ak_2 n+bk_1 n+k_1 k_2 n^2=ab+n(bk_1+ak_2+k_1 k_2 n)$$

.

Portanto $a'b' \equiv ab \bmod n \Rightarrow \overline{a'\cdot b'}=\overline{ab}$.

Uma forma equivalente de ver a proposição anterior é somar e multiplicar duas congruências módulo n.

Se $a \equiv a' \bmod n$ e $b \equiv b' \bmod n$, então

- $a+b \equiv a'+b' \bmod n$
- $ab \equiv a'b' \bmod n$

Seja k um inteiro positivo. Ao multiplicar uma congruência $a \equiv b \bmod n$ por ela mesma

k vezes, obtemos:

$$a \equiv b \bmod n \Rightarrow a^k \equiv b^k \bmod n$$

Em particular, se $a \equiv 1 \bmod n$, então $a^k \equiv 1 \bmod n$ para todo k inteiro positivo.

Pelo exposto, podemos, com toda a segurança, definir soma e produto de classes por

$$\bar{a} + \bar{b} = \overline{a+b}$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Assim, podemos agora somar e multiplicar classes em $\mathbb{Z}_n$. Este não é só um conjunto, mas um conjunto com operações de soma e multiplicação.

Essas operações herdam diversas propriedades da soma e da multiplicação dos inteiros:

- Propriedades da soma

$$(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$$
$$\bar{a} + \bar{b} = \bar{b} + \bar{a}$$
$$\bar{a} + \bar{0} = \bar{a}$$
$$\bar{a} + \overline{(-a)} = \bar{0}$$

- Propriedades da multiplicação

$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$$
$$\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$$
$$\bar{a} \cdot \bar{1} = \bar{a}$$

- Distributividade

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

Um conjunto com operações de soma e de multiplicação que satisfazem às oito propriedades listadas anteriormente é chamado um anel.

Podemos então falar no Anel $\mathbb{Z}_n$.

Texto 24 – Tabelas de Soma e de Multiplicação

Uma maneira de visualizar as operações de soma e de multiplicação de classes em $\mathbb{Z}_n$ é através de tabelas. Nelas, listamos todas as classes na primeira linha e na primeira coluna. Cada entrada na tabela corresponde à operação dos elementos indicados na primeira linha e na primeira coluna.

Como exemplo, vamos fazer as tabelas de soma e de multiplicação de $\mathbb{Z}_5$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Veja que a última entrada (à direita e abaixo) da tabela soma é $\overline{3}=\overline{4}+\overline{4}$. Na tabela de multiplicação, a última entrada é $\overline{1}=\overline{4}\cdot\overline{4}$.

Analise cuidadosamente todas as entradas dessas tabelas. Confira cada uma delas para ter

certeza de que você entendeu a construção.

Tabelas de soma e de multiplicação de $\mathbb{Z}_4$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Vamos continuar o estudo da estrutura de $\mathbb{Z}_n$ na próxima aula. Agora, vamos trabalhar algumas aplicações da congruência, iniciando pelas regras de divisibilidade.

Texto 25 – Divisibilidade

As regras de divisibilidade por 2, 3, 5, 9 e 11 são bem conhecidas. Como exercício de congruência, vamos entendê-las.

Observe inicialmente que, como usamos um sistema de numeração de base 10, se um inteiro a é escrito como $a = a_k \cdot a_{k-1} \ldots a_1 \cdot a_0$, então:

$$a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 .$$

Por exemplo, se a=257 , então $a = 2 \cdot 10^2 + 5 \cdot 10 + 7 = 200 + 50 + 7$.

A seguir, veja os casos de divisibilidade:

Divisibilidade por 3 e 9

Como $10 \equiv 1 \, mod \, 3$, então $10^i \equiv 1 \, mod \, 3$ para qualquer expoente i . Assim, se $a = a_k \cdot a_{k-1} \ldots a_1 \cdot a_0$, então

$$a \; = \; a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \; \equiv \; a_k + a_{k-1} + \ldots + a_1 + a_0 \, mod \, 3 .$$

O inteiro a é divisível por 3 se, e somente se,

$$3 | a \; \Leftrightarrow \; a \equiv 0 \, mod \, 3 \; \Leftrightarrow \; a_k + a_{k-1} + \ldots + a_1 + a_0 \equiv 0 \, mod \, 3$$

ou seja, a é divisível por 3 se, e somente se, a soma de seus algarismos for divisível por 3.

O mesmo vale para 9. Como $10 \equiv 1 \, mod \, 9$, então $10^i \equiv 1 \, mod \, 9$ para qualquer expoente i . Nesse caso o mesmo raciocínio se aplica. Vale que um inteiro a é divisível por 9 se, e somente se, a soma de seus algarismos for divisível por 9.

Você deve ter percebido, nesse primeiro exemplo, que o artifício para deduzir regras de divisibilidade por n é verificar a classe de congruência de 10 e suas potências módulo n .

Vamos a outro caso.

Divisibilidade por 2 e 4

Como $10 \equiv 0 \, mod \, 2$, então $10^i \equiv 0 \, mod \, 2$, para todo $i > 0$. Assim, se $a = a_k \cdot a_{k-1} \ldots a_1 \cdot a_0$, então

$$a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \; \equiv \; a_0 \, mod \, 2 .$$

Logo, a é divisível por 2 se, e somente se, a_0 for divisível por 2, isto é, quando a é par.

Com relação à divisibilidade por 4, $10 \equiv 2 \, mod \, 4$, mas $10^2 \equiv 0 \, mod \, 4$; logo $10^i \equiv 0 \ \ mod \, 4$ para todo $i \geq 2$.

Portanto, se $a = a_k \cdot a_{k-1} \ldots a_1 \cdot a_0$, então

$$a \ = \ a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \ \equiv \ a_1 \cdot 10 + a_0 \, mod \, 4 \, .$$

Assim, a é divisível por 4 se, e somente se, o número $a_{1 \mathrm{cdot}} a_0$ (número formado por seus dois últimos algarismos) for divisível por 4.

Exemplo: 99.875.320 é divisível por 4, pois o número 20 é.

Divisibilidade por 5 e 10

Como $10 \equiv 0 \, mod \, 5$, então $10^i \equiv 0 \, mod \, 5$, para todo $i \geq 1$.

Assim, se $a = a_k \cdot a_{k-1} \ldots a_1 \cdot a_0$, então:

$$a \ = \ a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \ \equiv \ a_0 \, mod \, 10 \, .$$

Portanto, a é divisível por 5 se, e somente se, $a_0 = 0$ ou $a_0 = 5$.

Como $10 \equiv 0 \, mod \, 10$, vale o mesmo raciocínio, e um inteiro a é divisível por 10 se, e somente se, a_0 for divisível por 10, isto é, quando $a_0 = 0$.

Divisibilidade por 11

Observe as classes módulo 11 das potências de 10.

- $10 \equiv -1 \, mod \, 11$.
- $10^2 \equiv (-1)^2 \, mod \, 11 \ \Rightarrow \ 10^2 \equiv 1 \, mod \, 11$
- $10^3 \equiv (-1)^3 \, mod \, 11 \ \Rightarrow \ 10^3 \equiv -1 \, mod \, 11$

Em geral, ao elevar $10 \equiv -1 \, mod \, 11$ à potência i, temos: $10^i \equiv (-1)^i \, mod \, 11$.

Mas $(-1)^i = \begin{cases} 1 & se \ i \ é \ par \\ -1 & se \ i \ é \ ímpar \end{cases}$, logo $10^i \equiv \begin{cases} 1 \, mod \, 11 & se \ i \ é \ par \\ -1 \, mod \, 11 & se \ i \ é \ ímpar \end{cases}$.

Assim,

$$a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} \ldots a_1 \cdot 10 + a_0 \equiv a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \ldots + a_2 - a_1 + a_0 \, mod \, 11$$

Temos aqui uma soma alternada dos algarismos de a. O inteiro a é divisível por 11 se, e somente se,

$$a \equiv 0 \, mod \, 11 \ \Leftrightarrow \ a_0 - a_1 + a_2 - a_3 + \ldots + (-1) a_k \equiv 0 \, mod \, 11 .$$

Ou seja, a é divisível por 11 se, e somente se, $a_0 - a_1 + a_2 - a_3 + \ldots + (-1) a_k$ for divisível por 11.

Exemplo: a=28.435 é divisível por 11, pois $5 - 3 + 4 - 8 + 2 = 0$, que é divisível por 11.

No próximo texto, vamos mostrar outra aplicação das congruências: o cálculo de potências módulo n.

Texto 26 – Potências

Outra aplicação muito útil da congruência é determinar o resto da divisão de uma potência a^k por um inteiro n. A idéia é encontrar algum s, tal que a^s seja um inteiro pequeno, e fazer a divisão do expoente k pelo inteiro s.

Se $k = q \cdot s + r$, com $0 \leq r < s$, então $a^k = a^{q \cdot s + r} = (a^s)^q \cdot a^r$.

Se a^s é congruente módulo n a um inteiro pequeno, então podemos reduzir a^k a uma potência menor. Se, por exemplo, $a^s \equiv 1 \, mod \, n$, então:

$$a^k = (a^s)^q \cdot a^r \ \equiv \ (1)^1 \cdot a^r \ \equiv \ a^r \, mod \, n, com \, 0 \leq r < s.$$

Veja a seguir alguns exemplos que vão facilitar a compreensão destas técnicas.

Exemplos:

1) Calcule o resto da divisão de 10^{33} por 99.

Vamos usar o fato de que $10^2 \equiv 1 \, mod \, 99$. Como $33 = 2 \cdot 16 + 1$, então:

$$10^{33} = 10^{2 \cdot 16 + 1} = (10^2)^{16} \cdot 10^1 \equiv 1 \cdot 10 \, mod \, 99 \equiv 10 \, mod \, 99$$

Portanto, 10 é o resto da divisão de 10^{33} por 99.

2) Calcule o resto da divisão de 2^{34} por 15.

Inicialmente, vamos determinar se alguma potência de 2 pode facilitar a solução.

Veja:

$$2^1 = 2, \; 2^2 = 4, \; 2^3 = 8, \; 2^4 = 16 \equiv 1 \, mod \, 15 .$$

Agora, utilizamos a potência 2^4. Sendo $343 = 4 \times 85 + 3$, temos:

$$2^{343} = 2^{4 \text{times} 85 + 3} = (2^4)^{85} \cdot 2^3 \equiv (1)^{85} \cdot 2^3 \, mod \, 15 \equiv 8 \, mod \, 15 .$$

Portanto, o resto da divisão de 2^{343} por 15 é 8.

3) Calcule o resto de 3^{125} por 7.

Vamos tentar as potências de 3:

$$3^1 = 3, \; 3^2 = 9 \equiv 2 \, mod \, 7, \; 3^3 = 27 \equiv (-1) \, mod \, 7$$

Podemos usar tanto 3^2 como 3^3 para resolver o problema. Para ilustrar, vamos fazer das duas maneiras.

- Usando $3^2 \equiv 2 \, mod \, 7$ e sendo $125 = 2 \times 62 + 1$, temos

$$3^{125} = 3^{2 \times 62 + 1} = (3^2)^{62} \cdot 3 \equiv 2^{62} \cdot 3 \, mod \, 7 .$$

Agora, vamos tentar uma potência de 2 adequada. Como $2^3 = 8 \equiv 1 \ mod\ 7$, a divisão de 62 por 3 resolve o problema. Sendo $62 = 20 \times 3 + 2$, temos:

$$3^{125} \equiv 2^{62} \cdot 3 \ mod\ 7 \equiv 2^{3 \times 20 + 2} \cdot 3 \ mod\ 7 \equiv (2^3)^{20} \cdot 2^2 \cdot 3 \ mod\ 7 \equiv 1 \cdot 2^2 \cdot 3 \ mod\ 7$$

ou seja, $3^{125} \equiv 12 \ mod\ 7 \equiv 5 \ mod\ 7$. Portanto, o resto de 3^{125} por 7 é 5.

- A outra solução usa $3^3 \equiv (-1) \ mod\ 7$. Temos que $125 = 41 \times 3 + 2$, logo

$$3^{125} = (3^3)^{41} \cdot 3^2 \ \equiv \ (-1)^{41} \cdot 3^2 \ \equiv \ (-9) \ mod\ 7 \ \equiv \ 5 \ mod\ 7,$$

o que confirma que o resto da divisão de 3^{125} por 7 é 5.

Esses três exemplos demonstram o uso de congruência para encontrar restos de potências. Vale destacar que a potência exata a ser usada em cada caso depende do problema. Como vimos no último exemplo, nem sempre uma potência é a única ou a melhor escolha.

Outra questão é que, dados inteiros positivos a e n, nem sempre há uma potência de a que seja congruente a 1 módulo n. Vamos voltar a esse assunto nas próximas aulas.

No endereço http://britton.disted.camosun.bc.ca/modart/jbmodart.htm há uma discussão interessante sobre aritmética modular e arte. Você também encontra um aplicativo que constrói dinamicamente tabelas de soma e de multiplicação modulares.

Nesta aula, definimos soma e produto de classes em $\mathbb{Z}_n$. Com estas operações, $\mathbb{Z}_n$ deixa de ser só um conjunto e passa a ser um anel, isto é, um conjunto com operações de soma e de produto que satisfazem às oito propriedades listadas

nesta aula.

Nas próximas aulas vamos aplicar as técnicas de congruência a dois problemas: o dos testes de divisibilidade e o de determinação do resto pela divisão de potências grandes de um inteiro por n .

Saiba mais: Módulo

A palavra **módulo** foi introduzida na Matemática pelo alemão Carl Friedrich Gauss, em 1801, no seu famoso livro Disquisitiones Arithmeticae. Este é um livro-texto de Teoria de Números; nele o matemático Gauss reúne os resultados obtidos anteriormente por Fermat, Euler, Lagrange, Legendre e pelo próprio autor.

Antes do livro, a Teoria dos Números era considerada uma coleção de resultados isolados e de conjecturas. Gauss, então com 24 anos, deu uma estrutura lógica aos resultados conhecidos, corrigiu demonstrações falhas, preencheu as lacunas e ampliou vários resultados.

Atividades

1) Elabore as tabelas de soma e de multiplicação de $\mathbb{Z}_6$.

2) Determine um teste de divisibilidade para 8.

3) Calcule o resto da divisão de:

a) 2^{303} por 15.

b) $7^{250}\ por\ 48$.

c) $5^{61}\ por\ 7$.

Aula 7 – Divisão Modular

Na última aula, você estudou as definições de operações de soma, diferença e multiplicação em $\mathbb{Z}_n$. Agora, vamos apresentar a divisão módulo n .

Nesta parte, você vai aprender também como escrever o mdc de dois inteiros como combinação linear deles, utilizando o algoritmo de Euclides.

Texto 27 – A inversa de uma classe de congruência módulo n

Para iniciar o estudo, vamos a uma questão:

> O que significa dividir a por b ?

Se $c = a/b$, então $a = b \cdot c$. Podemos assim entender que dividir a por b é como encontrar um x tal que $b \cdot x = a.$ Em $\mathbb{Z}_n$, seria a operação de encontrar uma classe $\bar{x}$ tal que $\bar{b} \cdot \bar{x} = \bar{a}$, ou seja, encontrar x de modo que

$$bx \equiv a \bmod n.$$

Assim, dividir a por b é equivalente a resolver a equação de congruência anterior.

Uma outra forma de entender a divisão é ver a/b como $a \cdot (1/b) = a \cdot b^{-1}$, isto é, a divisão de a e b é o produto de a pela inversa de b . Já a inversa de b é o número que multiplicado por b resulta em 1, isto é, $b \cdot b^{-1} = 1.$

Em $\mathbb{Z}_n$, a inversa de $\bar{b}$ é uma classe $\bar{b'}$, tal que $\bar{b} \cdot \bar{b'} = 1$. Assim, o problema de encontrar a inversa de b é equivalente a encontrar um inteiro b' tal que:

$$b \cdot b' \equiv 1 \bmod n.$$

Perceba que neste ponto temos duas dificuldades: nem sempre uma classe em $\mathbb{Z}_n$ tem inversa, assim como nem sempre a equação $bx \equiv a \bmod n$ tem solução. Em conseqüência, nem

sempre é possível dividir duas classes em $\mathbb{Z}_n$.

Exemplos:

- Em $\mathbb{Z}_{10}$, a classe $\bar{3}$ tem inversa, que é a classe $\bar{7}$, pois $\bar{3}\cdot\bar{7}=\overline{21}=\bar{1}$. Por outro lado, a classe $\bar{2}$ não tem inversa em $\mathbb{Z}_{10}$. Note que, se você tentar encontrar uma classe $\bar{x}$ tal que $\bar{2}\cdot\bar{x}=\bar{1}$, não vai obter a solução.

- Em $\mathbb{Z}_5$, todas as classes não-nulas têm inversa: $\bar{1}\cdot\bar{1}=\bar{1}$, $\bar{2}\cdot\bar{3}=\bar{1}$ e $\bar{4}\cdot\bar{4}=\bar{1}$.

De acordo com o que foi apresentado anteriormente, somos levados à seguinte questão: quais as classes que possuem inversa em $\mathbb{Z}_n$?

Texto 28 – Quando uma classe em $\mathbb{Z}_n$ tem inversa?

Seja $\bar{a}\in\mathbb{Z}_n$. Se $\bar{a}$ tem inversa $\bar{a'}$, então:

$$\bar{a}\cdot\bar{a'}=\bar{1} \Rightarrow a\cdot a'\equiv 1 \bmod n \Rightarrow n \mid a\cdot a'-1 .$$

Logo, existe $k\in\mathbb{Z}$, tal que:

$$aa'+kn=1.$$

Seja agora $d=mdc(a,n)$. Como $d|a$ e $d|n$, então:

$$d|(aa'+kn) \Rightarrow d|1 \Rightarrow d=1.$$

Provamos, assim, que, se uma classe $\bar{a}\in\mathbb{Z}_n$ tem inversa, então $mdc(a,n)=1$. Portanto, $mdc(a,n)=1$ é uma condição necessária para que a classe $\bar{a}$ possua inversa.

Mas será essa uma condição suficiente?

De fato, se $mdc(a,n)=1$, então existem k_1 e k_2 , tais que $ak_1+nk_2=1$. Logo $ak_1-1=nk_2$ é múltiplo de n , ou seja,

$$ak_1 \equiv 1 \bmod n \;\Rightarrow\; \bar{a}\cdot\bar{k}_1 = \bar{1}$$

o que mostra que $\bar{a}$ tem inversa em $\mathbb{Z}_n$.

Provamos desta forma a

Proposição: A classe $\bar{a}$ em $\mathbb{Z}_n$ tem inversa se, e somente se, $mdc(a,n)=1$.

Exemplos:

- As classes que têm inversa em $\mathbb{Z}_{12}$ são $\{\bar{1},\bar{5},\bar{7},\bar{11}\}$.
- As classes que possuem inversa em $\mathbb{Z}_{10}$ são $\{\bar{1},\bar{3},\bar{7},\bar{9}\}$.
- As classes que têm inversa em $\mathbb{Z}_5$ são $\{\bar{1},\bar{2},\bar{3},\bar{4}\}$.

Uma conseqüência da proposição é que se p é primo, então todas as classes não-nulas em $\mathbb{Z}_p$ possuem inversa. Isto acontece porque, sendo p primo e $1 \le a \le p-1$, então $mdc(a,p)=1$. É o caso de $\mathbb{Z}_5$, no exemplo anterior.

Chamamos de $\mathbb{Z}_n^*$ o subconjunto de $\mathbb{Z}_n$ formado pelas classes que têm inversa. Assim:

- $\mathbb{Z}_{12}{}^* = \{\bar{1},\bar{5},\bar{7},\bar{11}\}$.
- $\mathbb{Z}_{10}{}^* = \{\bar{1},\bar{3},\bar{7},\bar{9}\}$.
- $\mathbb{Z}_p{}^* = \{\bar{1},\cdots,\overline{p-1}\} = \mathbb{Z}_p{}^* - \{\bar{0}\}$.

O conjunto $\mathbb{Z}_n{}^*$ não é fechado para a soma, isto é, a soma de dois elementos que têm inversa módulo n pode não ter inversa módulo n. Por exemplo, em $\mathbb{Z}_{12}^*$, as classes $\bar{1}$ e $\bar{5}$ têm inversa, mas $\bar{1}+\bar{5}=\bar{6}$ não possui inversa.

No entanto, vale que:

Lema: o conjunto $\mathbb{Z}_n{}^*$ é fechado para a multiplicação. Assim, o produto de duas classes que possuem inversa sempre tem inversa.

Demonstração

Sejam $\bar{a}$ e $\bar{b}$ duas classes em $\mathbb{Z}_n^*$ que têm inversa. Sejam suas inversas $\bar{\alpha}$ e $\bar{\beta}$, respectivamente. A inversa de $\bar{a}\cdot\bar{b}$ é classe $\bar{\alpha}\cdot\bar{\beta}$, pois:

$$(\bar{a}\cdot\bar{b})\cdot(\bar{\alpha}\cdot\bar{\beta}) = (\bar{a}\cdot\bar{\alpha})\cdot(\bar{b}\cdot\bar{\beta}) = \bar{1}\cdot\bar{1} = \bar{1}.$$

Texto 29 – A congruência linear $ax \equiv b \bmod n$

Vamos voltar à seguinte questão: a congruência linear $ax \equiv b \bmod n$ tem solução? Com o que vimos anteriormente, podemos indicar uma situação em que a congruência tenha solução: quando $mdc(a,n)=1$.

Se $mdc(a,n)=1$, então o inteiro a tem inversa α módulo n. Logo

$$ax \equiv b \bmod n \Rightarrow (\alpha a)x \equiv \alpha b \bmod n \Rightarrow 1\cdot x \equiv \alpha b \bmod n \Rightarrow x \equiv \alpha b \bmod n,$$

o que mostra que $ax \equiv b \bmod n$ tem uma solução quando $mdc(a,n)=1$.

E o que acontece quando $mdc(a,n)>1$? Neste caso, a equação $ax \equiv b \bmod n$ pode ter várias soluções ou nenhuma. Veja os exemplos:

- $2x \equiv 6 \bmod 8$ tem duas soluções: $x \equiv 3 \bmod 8$ e $x \equiv 7 \bmod 8$, pois $2\cdot 3 \equiv 6 \bmod 8$ e $2\cdot 7 \equiv 6 \bmod 8$, respectivamente. Observe que não há outra solução módulo 8 testando todos os inteiros entre 0 e 7.

- A congruência $2x \equiv 7 \bmod 8$ não tem solução, pois $mdc(2,8)=2 \nmid 7$. Você pode comprovar que isto é verdade, testando os inteiros de 0 a 7.

A solução completa para o problema sobre o número de soluções da equação de congruência linear $ax \equiv b \bmod n$ é o seguinte

Teorema: A equação de congruência $ax \equiv b \bmod n$ tem solução se, e somente se, b for múltiplo de $d = mdc(a,n)$.

Além disso, se $d \mid b$, a equação possui exatamente d soluções módulo n. Se x_0 é uma solução qualquer, então as d soluções módulo n são dadas por:

$$x_k = x_0 + \frac{n}{d}k, \quad k = 0 \cdots (d-1).$$

Uma demonstração do teorema pode ser encontrada em Introdução à Teoria dos Números, de José Plínio de Oliveira Santos, 1998.

Retornando aos dois exemplos anteriores:

- $2x \equiv 6 \, mod \, 8$ tem duas soluções, pois $mdc(2,8) = 2$ e $2 divides 6$
- O valor $x \equiv 3 \, mod \, 8$ é uma solução óbvia, pois $2 \cdot 3 = 6$. A outra solução é

  $$x \equiv 3 + \frac{8}{2} \equiv 7 \, mod \, 8.$$

- $2x \equiv 7 \, mod \, 8$ não tem solução, porque $mdc(2,8) = 2$ e $2 \nmid 7$.

Observe que, quando dizemos que há d soluções módulo n , queremos mostrar que há d classes módulo n distintas que são soluções da equação. Há infinitos inteiros que são solução de $ax \equiv b \, mod \, n$. No entanto, estes inteiros representam exatamente d classes de congruência módulo n .

Por exemplo, a equação $2x \equiv 6 \, mod \, 8$ tem soluções $x \equiv 3 \, mod \, 8$ e $x \equiv 7 \, mod \, 8$, que são as classes $\bar{3}$ e $\bar{7}$ em $\mathbb{Z}_8$. O inteiro $x = 11$ também é solução, mas $11 \in \bar{3}$. Observe que $x = 15$ também é solução, mas $15 \in \bar{7}$.

Confira outro exemplo a seguir.

Determine todas as soluções para a equação $6x \equiv 9 \, mod \, 21$.

Inicialmente, observamos que $d = mdc(6,21) = 3$ e 3 divide 9; logo a equação tem três soluções módulo 21. Tentando valores de x a partir de 0, encontramos a solução $x_0 = 5$.
($6 \cdot 5 = 30 \equiv 9 \, mod \, 21$).

A partir desta, encontramos todas as soluções:

$$x_k = x_0 + \frac{n}{d}k,\ k = 0 \cdots (d-1) \Rightarrow x_k = 5 + 7\mathrm{k},\ k = 0,1\ e\ 2.$$

Portanto, as soluções são $x \equiv 5 \bmod 21$, $x \equiv 12 \bmod 21$ e $x \equiv 19 \bmod 21$.

Neste exemplo, a primeira solução não era totalmente óbvia, mas conseguimos encontrá-la com poucas tentativas. É claro que para números maiores vamos precisar de outras técnicas.

Uma técnica que sempre funciona é escrever $d = mdc(a,n)$ em termos de a e n. Sabemos que existem inteiros x_0 e y_0, tais que $d = x_0 a + y_0 n$. Como $d|b$, então b/d é um inteiro.

Ao multiplicar a equação anterior por este inteiro, o resultado é:

$$\frac{b}{d}d = \frac{b}{d}x_0 a + \frac{b}{d}y_0 n \Rightarrow b = \left(\frac{bx_0}{d}\right)a + \left(b\frac{y_0}{d}\right)n \Rightarrow \left(\frac{bx_0}{d}\right)a \equiv b \bmod n.$$

Vale destacar que a aplicação dessa técnica depende de saber escrever o mdc de dois inteiros como combinação linear desses inteiros. Será o assunto do próximo texto.

Texto 30 - Como escrever o MDC de dois inteiros em combinação linear

A solução para o problema está no algoritmo de Euclides, o mesmo utilizado para determinar o máximo divisor comum de dois inteiros. Uma pequena modificação no algoritmo permite que ele não apenas forneça o $mdc(a,b)$, mas também escreva d como combinação linear de a e b.

Vamos iniciar com um exemplo para ilustrar o processo.

Exemplo:

Calcule $mdc(4723,2350)$ e expresse esse mdc em termos de 4723 e 2350.

Para o cálculo do mdc, fazemos as divisões sucessivas:

$$\begin{aligned} 4723 &= 2\times 2350+23 \\ 2350 &= 102\times 23+4 \\ 23 &= 5\times 4+3 \\ 4 &= 1\times 3+1 \end{aligned}$$

O que mostra que $mdc(4723,2350)=1.$

Agora, vamos escrever 1 como combinação linear de 4723 e 2350 . O processo é obter o valor do resto na última equação e ir substituindo os valores dos restos, usando as outras equações, até chegarmos à primeira. Veja:

- Isolamos o 1 na última equação, obtendo: $1=4-1\times 3.$
- Obtemos o valor de 3 na penúltima equação e substituímos:
  $3=23-5\times 4 \Rightarrow 1=4-1\text{times}3=4-1\times(23-5\times 4)=6\times 4-1\times 23.$
- Obtemos o valor de 4 (2ª equação) e substituímos:
  $$4=2350-102\times 23 \Rightarrow 1=6\times 4-1\times 23=6\times(2350-102\times 23)-1\times 23$$
  $$=6\times 2350-613\times 23.$$
- Obtemos o valor de 23 (1ª equação) e substituímos:
  $$23=4723-2\text{times}2350 \Rightarrow 1=6\times 2350-613\times 23=6\times 2350-613\times(4723-2\text{times}2350)$$
  $$=1232\times 2350-613\times 4723.$$

Concluímos que $1=1232\times 2350-613\times 4723.$ Esta expressão também permite calcular a inversa de 2350 módulo 4723 . Reduzindo o módulo 4723 a expressão, obtemos $1232\times 2350\equiv 1\ mod\ 4723,$ ou seja, 1232 é a inversa de 2350 módulo 4723 .

O método apresentado é simples e sempre funciona, embora seja trabalhoso. Do ponto de vista computacional, apresenta o sério inconveniente de que precisamos armazenar todos os quocientes e restos intermediários até o final. Em uma conta com muitos passos, armazenar estes inteiros pode ser um problema.

Há, no entanto, uma pequena mudança no algoritmo de Euclides que permite expressar o $mdc(a,b)$ como combinação linear de a e b , sem armazenar os quocientes e restos intermediários. A idéia é expressar cada resto intermediário em termos de a e b , ou seja, para todo resto intermediário r_k obter os inteiros x_k e y_k , tais que $r_k=a\cdot x_k+b\cdot y_k.$

Os passos do algoritmo de Euclides são:

$$\begin{aligned} a &= b\,q_1 + r_1 \\ b &= r_1\,q_2 + r_2 \\ r_1 &= r_2\,q_3 + r_3 \\ &\vdots \\ r_{k-2} &= r_{k-1}\,q_k + r_k \end{aligned}$$

O termo geral $r_{k-2} = r_{k-1}\,q_k + r_k$ implica em $r_k = r_{k-2} - r_{k-1}\,q_k$. Substituindo $r_{k-1} = a \cdot x_{k-1} + b \cdot y_{k-1}$ e $r_{k-2} = a \cdot x_{k-2} + b \cdot y_{k-2}$, que são as fórmulas que expressam r_{k-1} e r_{k-2} em termos de a e b, obtemos:

$$\begin{aligned} r_k = r_{k-2} - r_{k-1}\,q_k &= \left(a \cdot x_{k-2} + b \cdot y_{k-2}\right) - q_k\left(a \cdot x_{k-1} + b \cdot y_{k-1}\right) \\ &= a(x_{k-2} - q_k \cdot x_{k-1}) + b(y_{k-2} - q_k \cdot y_{k-1}) \end{aligned}$$

Ao compararmos esta fórmula com $r_k = a \cdot x_k + b \cdot y_k$, temos que:

$$\begin{cases} x_k = x_{k-2} - q_k \cdot x_{k-1} \\ y_k = y_{k-2} - q_k \cdot y_{k-1} \end{cases} \qquad (1)$$

Assim, você pode observar que o valor de um par (x_k, y_k) depende apenas dos valores (x_{k-1}, y_{k-1}) e (x_{k-2}, y_{k-2}) correspondentes aos dois passos anteriores.

Para começarmos a aplicar a fórmula, falta ainda um detalhe: o primeiro passo.

O primeiro passo do algoritmo é a linha $a = b \cdot q_1 + r_1 \Rightarrow r_1 = 1 \cdot a - q_1 \cdot b$. Assim, temos $x_1 = 1$ e $y_1 = -q_1$ na fórmula $r_1 = a \cdot x_1 + b \cdot y_1$. Para que a fórmula (1) seja válida também para $k = 1$, temos que definir os valores de (x_0, y_0) e de (x_{-1}, y_{-1}).

É fácil ver que, ao definir $(x_0, y_0) = (0,1)$ e $(x_{-1}, y_{-1}) = (1,0)$, então $x_1 = x_{-1} - q_1 \cdot x_0$ e $y_1 = y_{-1} - q_1 \cdot y_0$, ou seja, a fórmula (1) permanece válida para $k = 1$.

Parece complicado, não? Na verdade não é. Acompanhe a seguir dois exemplos que vão facilitar a compreensão.

Exemplo: Vamos refazer o exercício de expressar $1 = mdc(4723, 2350)$ em termos de 4723 e 2350.

À direta das divisões do algoritmo, escrevemos duas colunas para os valores de x_k e de y_k. A cada passo fazemos $x_k = x_{k-2} - q_k \cdot x_{k-1}$ e $y_k = y_{k-2} - q_k \cdot y_{k-1}$. Começamos com as duas linhas "especiais" com os valores de $(x_{-1}, y_{-1}) = (1,0)$ e $(x_0, y_0) = (0,1)$. O algoritmo está representado a seguir. Em cada linha está escrito o quociente em negrito para facilitar a visualização.

	x_k	y_k
	1	0
	0	1
$4723 = \mathbf{2} \cdot 2350 + 23$	$1 - 2 \cdot 0 = 1$	$0 - 2 \cdot 1 = -2$
$2350 = \mathbf{102} \cdot 23 + 4$	$0 - 102 \cdot 1 = -102$	$1 - 102 \cdot (-2) = 205$
$23 = \mathbf{5} \cdot 4 + 3$	$1 - 5(-102) = 511$	$-2 - 5 \cdot 205 = -1027$
$4 = \mathbf{1} \cdot 3 + 1$	$-102 - 1(511) = -613$	$205 - 1(-1027) = 1232$

Obtivemos o resultado $1 = (-613) \cdot 4723 + 1232 \cdot 2350.$

Para reforçar, veja mais um exemplo. Desta vez vamos utilizar números menores.

Exemplo: Calcule a inversa de 23 módulo 41.

Temos que $mdc(23,41) = 1$. Vamos usar o algoritmo de Euclides para escrever 1 em termos de 23 e 41.

	x_k	y_k
	1	0
	0	1
$41 = \mathbf{1} \cdot 23 + 18$	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$
$23 = \mathbf{1} \cdot 18 + 5$	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-1) = 2$
$18 = \mathbf{3} \cdot 5 + 3$	$1 - 3(-1) = 4$	$-1 - 3 \cdot 2 = -7$
$5 = \mathbf{1} \cdot 3 + 2$	$-1 - 1 \cdot 4 = -5$	$2 - 1(-7) = 9$
$3 = \mathbf{1} \cdot 2 + 1$	$4 - 1(-5) = 9$	$-7 - 1 \cdot 9 = -16$

A conclusão é que $1 = 9 \cdot 41 - 16 \cdot 23$. Obtemos, então, a congruência: $-16 \cdot 23 \equiv 1 \; mod \; 41.$

Portanto a inversa de 23 módulo 41 é -16. Como $23 - 16 = 7$, podemos dizer que 7 é a inversa de 23 módulo 41. Em outras palavras, $x \equiv 7 \; mod \; 41$ é a única solução da equação $23x \equiv 1 \; mod \; 41$.

A aula 7 iniciou-se com a questão da divisão modular, o que nos levou a duas

perguntas:

1. Quando uma classe $\bar{a}$ em $\mathbb{Z}_n$ tem inversa?
2. Quando a equação de congruência linear $ax \equiv b \bmod n$ tem solução?

A resposta à primeira pergunta é que uma classe $\bar{a}$ em $\mathbb{Z}_n$ tem inversa se, e somente se, $mdc(a,n)=1$.

No caso da segunda questão, a resposta é que a equação $ax \equiv b \bmod n$ tem solução se, e somente se, $d=mdc(a,n)$ divide b . Neste caso, a equação tem exatamente d soluções módulo n .

Outra questão apresentada foi: sendo $mdc(a,n)=1$, como é possível efetivamente calcular a inversa de a módulo n ? A resposta está em usar a versão estendida do algoritmo de Euclides, apresentada durante a aula.

Atividades

1) Determine as classes que têm inversa em $\mathbb{Z}_9$ e em $\mathbb{Z}_{20}$

2) Para cada uma das seguintes equações de congruência, determine se ela tem solução. Caso tenha, determine todas as soluções.

a) $3x \equiv 8 \bmod 15$
b) $2x \equiv 20 \bmod 32$
c) $5x \equiv 7 \bmod 11$

3) Usando o algoritmo de Euclides estendido, escreva $mdc(a,b)$ em termos de a e b para cada um dos pares de inteiros a seguir.

a) $a=35 \ \ e \ \ b=65$
b) $a=15 \ \ e \ \ b=23$

4) Calcule a inversa de 45 módulo 91 .

Aula 8 - Teorema de Fermat

Nesta aula, você vai estudar o teorema de Fermat e sua aplicação ao cálculo de algumas potências.

Vamos iniciar o estudo apresentando quem foi Fermat, personagem importante na história da Matemática.

Texto 31 - Fermat

O francês Pierre de Fermat (1601-1665) estudou direito e trabalhou como juiz em Toulouse. Era, de certa forma, um matemático amador, mas que fez enormes contribuições a várias áreas da Matemática.

É considerado um dos precursores do cálculo diferencial, sendo responsável por avanços notáveis nas áreas de geometria analítica e de probabilidade. Fez contribuições importantes para a Teoria dos Números.

Fermat trabalhou a Teoria dos Números, enquanto lia uma tradução, para o latim, do livro Aritmética, do matemático grego Diofante, que viveu de 200/214 a 284/298 d.C. Esse livro apresentava todos o conhecimento dos gregos em Teoria dos Números, organizado na forma de perguntas e respostas. Continha mais de 100 problemas, cada qual com uma solução detalhada.

Durante a leitura da publicação, Fermat escrevia notas nas margens largas do livro, detalhando novas soluções para os problemas, resultados que ele descobria. O matemático morreu em janeiro de 1665. Sua notável contribuição à Matemática não foi registrada em livros, pois Fermat não teve interesse em publicar. Ela consta apenas em trocas de cartas com matemáticos contemporâneos e em anotações soltas.

As contribuições teriam se perdido, se o filho mais velho de Fermat, chamado Clément-Samuel, não tivesse a preocupação de reunir e divulgar as soluções do pai. Cinco anos após a morte do matemático, Clément-Samuel publicou uma edição especial de Aritmética, com as observações de Fermat. A edição foi intitulada Aritmética de Diofante contendo observações de P. de Fermat.

Uma dessas observações é um teorema famoso conhecido como Último Teorema de Fermat.

No próximo texto, vamos estudar o “pequeno teorema de Fermat” ou, simplesmente, “teorema de Fermat”. Fique atento para não confundir com o “último teorema de Fermat”, que vamos apresentar ao final da aula 8.

Texto 32 – O Teorema de Fermat

Para ter uma idéia do que diz o teorema de Fermat, vamos iniciar com um caso particular: o inteiro 2^p-2. Veja o valor de $N=2^p-2$ para alguns primos.

$$p=2 \rightarrow N=2^2-2 = 2 = 2\cdot 1$$
$$p=3 \rightarrow N=2^3-2 = 8-2 = 6 = 3\cdot 2$$
$$p=5 \rightarrow N=2^5-2 = 32-2 = 30 = 5\cdot 6$$
$$p=7 \rightarrow N=2^7-2 = 128-2 = 126 = 7\cdot 18$$
$$p=11 \rightarrow N=2^{11}-2 = 2.048-2 = 2.046 = 11\cdot 186$$

Você deve ter percebido que, para estes valores de p primo, vale que p divide 2^p-2. Esse fato já era conhecido pelos chineses desde a Antiguidade. O teorema de Fermat mostra que o fato observado anteriormente é sempre verdadeiro, sendo válido para todo primo p e base inteira a.

Teorema de Fermat: Seja p um número primo e a um inteiro. Então,

$$a^p \equiv a \bmod p.$$

Perceba que $a^p \equiv a \bmod p$ é o mesmo que $p \mid (a^p-a)$.

Acompanhe mais alguns exemplos:

$$p=3 \ e \ a=5 \rightarrow 3 \ divide \ a^p-a = 5^3-5 = 120$$
$$p=5 \ e \ a=4 \rightarrow 5 \ divide \ a^p-a = 4^5-4 = 1.020$$

Vamos demonstrar o teorema de Fermat em breve, mas antes precisamos de um resultado auxiliar.

Vimos que as classes $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ são todas as classes de congruência módulo n.

Qualquer conjunto formado por n elementos, em que cada um representa uma das classes $\bar{0},\bar{1},\ldots,\overline{n-1}$, é um sistema completo de representantes módulo n, também chamado sistema completo de resíduos módulo n.

Assim:

- $\{0,1,2,3,4\}$ é um sistema completo de resíduos módulo 5.
- $\{0,6,2,13,24\}$ também é um sistema completo de resíduos módulo 5, pois $0\in\bar{0},\ 6\in\bar{1},\ 2\in\bar{2},\ 13\in\bar{3}\ e\ 24\in\bar{4}$.

Observe que, em um sistema completo de resíduos, toda classe está representada e cada uma é representada uma única vez.

Considere o conjunto $\{0,1,2,\ldots,p-1\}$. Seja *a* inteiro, onde $p\nmid a$. Quais são as classes que aparecem no conjunto $\{0\cdot a,1\cdot a,2\cdot a,\ldots,(p-1)\cdot a\}$?

Veja o exemplo a seguir.

Seja $p=7$ e $a=4$. Vamos multiplicar os elementos do conjunto $\{0,1,2,3,4,5,6\}$ por 4:

$$\begin{aligned}
0\cdot 4 &\equiv 0 \bmod 7\\
1\cdot 4 &\equiv 4 \bmod 7\\
2\cdot 4 &\equiv 1 \bmod 7\\
3\cdot 4 &\equiv 5 \bmod 7\\
4\cdot 4 &\equiv 2 \bmod 7\\
5\cdot 4 &\equiv 6 \bmod 7\\
6\cdot 4 &\equiv 3 \bmod 7
\end{aligned}$$

Observe que, na coluna da direita, aparecem todas as classes $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\ e\ \bar{6}$. Portanto o conjunto $\{0\cdot 4,\ 1\cdot 4,\ 2\cdot 4,\ 3\cdot 4,\ 5\cdot 4,\ 6\cdot 4\}$ forma um sistema completo de resíduos módulo 7.

Viu que interessante? Elabore você mesmo um exemplo. Tente com qualquer p primo e a inteiro, em que p não divide a, e verifique que o conjunto $\{0\cdot a,1\cdot a,\ldots,(p-1)\cdot a\}$ é um

sistema completo de resíduos módulo p .

A demonstração é simples. Lembre-se que $0 \cdot a = 0 \equiv 0 \, mod \, p$. Para $1 \leq i \leq p-1$, como $mdc(a, p) = 1$, $p \nmid i$, então $p \nmid i \cdot a$. Assim nenhum $i \cdot a$, com $1 \leq i \leq p-1$ está em $\bar{0}$.

Agora, basta mostrar que os $p-1$ inteiros $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ estão todos em classes de congruência diferentes, o que implica que representam as $p-1$ classes $\bar{1}, \bar{2}, \ldots, \overline{p-1}$.

Se $j \cdot a \equiv k \cdot a \, mod \, p$, com $1 \leq j, k \leq p-1$, então:

$$p \mid (j \cdot a - k \cdot a) \Rightarrow p \mid (j-k)a \Rightarrow p \mid (j-k),$$

pois $mdc(p, a) = 1$. Mas $-(p-1) < j-k < p-1$, porque $1 \leq j, k \leq p-1$. Logo, se $j-k$ é múltiplo de p , então $j-k = 0 \Rightarrow j = k$.

Assim, dois inteiros distintos $j \cdot a \;\; e \;\; k \cdot a$, $1 \leq j, k \leq p-1$ são não-congruentes módulo p .

Desta forma, demonstra-se a

Proposição: Seja p primo e a inteiro, onde $p \nmid a$, o conjunto $\{0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a\}$ forma um sistema completo de resíduos módulo p .

Uma conseqüência é que, ao multiplicar todos os elementos do conjunto $\{0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a\}$, vamos obter um resultado congruente módulo p ao produto $1 \cdot 2 \cdot \ldots \cdot (p-1)$, pois as classes são as mesmas. Assim:

$$(1 \cdot a) \cdot (2 \cdot a) \cdot (3 \cdot a) \cdot \ldots \cdot ((p-1) \cdot a) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \;\; mod \, p$$

Veja que nesse ponto estamos prontos para demonstrar o teorema de Fermat.

Demonstração do Teorema de Fermat

Sejam p primo e a inteiro. Se p divide a , então $a \equiv 0 \, mod \, p \;\; e \;\; a^p \equiv 0 \, mod \, p$, logo $a^p \equiv a \, mod \, p$ e nada temos a fazer.

Suponha que p não divide a . O artifício é usar o conjunto $\{1\cdot a, 2\cdot a, \ldots, (p-1)\cdot a\}$.

Vimos anteriormente que

$$(1\cdot a)\cdot(2\cdot a)\cdot(3\cdot a)\cdot\ldots\cdot((p-1)\cdot a) \equiv 1\cdot 2\cdot 3\cdot\ldots\cdot(p-1) \mod p$$

Lembre-se que $(p-1)!=1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)$. Ao colocar os $(p-1)$ inteiros que aparecem no lado esquerdo da equação anterior como potência, temos:

$$a^{p-1}\cdot(p-1)! \equiv (p-1)! \mod p$$
$$a^{p-1}\cdot(p-1)!-(p-1)! \equiv 0 \mod p$$
$$\left(a^{p-1}-1\right)(p-1)! \equiv 0 \mod p$$
$$p \text{ divide } (a^{p-1}-1)(p-1)!$$

É fácil ver que $mdc(p,(p-1)!)=1$, porque o primo p não aparece em $(p-1)!=1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)$. Como $p|(a^{p-1}-1)\cdot(p-1)!$ e $mdc(p,(p-1)!)=1$.

Assim, p divide $a^{p-1}-1$, isto é, $a^{p-1}\equiv 1 \mod p$. Ao multiplicar os dois lados por a , obtemos:

$$a^p \equiv a \mod p,$$

o que conclui a demonstração do teorema de Fermat.

Uma forma equivalente de enunciar este teorema é:

> **Teorema:** Sejam a e p inteiros e p primo. Se $p\nmid a$, então:
>
> $$a^{p-1}\equiv 1 \mod p$$

Esta formulação é equivalente à primeira, porque:

- Se $p|a$, então $a^p\equiv a \mod p$ é sempre verdade.
- Se $p\nmid a$, então $a^p\equiv a \mod p \Leftrightarrow a^{p-1}\equiv 1 \mod p$.

Texto 33 – Aplicação do Teorema de Fermat à solução de potências

O teorema de Fermat pode ser aplicado à solução de potências módulo n . Veja algumas aplicações.

Exemplos:

- Determine o resto de 2^{182} por 19 .

Como $p=19$ é primo e $19\nmid 2$, temos que $2^{19-1}=2^{18}\equiv 1\ mod\ 19$.

Sendo $182=18\cdot 10+2$, obtemos:

$$2^{182}=(2^{18})^{10}\cdot 2^2 \equiv 1^{10}\cdot 4 \ mod 19 \Rightarrow 2^{182} \equiv 4 \ mod 19$$

Portanto o resto da divisão de 2^{182} por 19 é 4 .

- Encontre o resto da divisão de 3^{100} por 7 .

Como $p=7$ é primo e $7\nmid 3$, então $3^{7-1}=3^6 \equiv 1\ mod\ 7$.

Sendo $100=6\cdot 16+4$, temos:

$$3^{100}=(3^6)^{16}\cdot 3^4 \equiv 3^4\ mod\ 7$$

Como $3^4=81 \equiv 4\ mod\ 7$, então o resto de 3^{100} por 7 é 4 .

- Mostre que $n=2^{70}+3^{70}$ é um múltiplo de 13 .

Para provar que $13|n$, vamos calcular separadamente as classes de 2^{70} e 3^{70} .

Como $p=13$ é primo e $13\nmid 2$, então $2^{12}\equiv 1 \mathrm{mod} 13$.

Sendo $70=5\cdot 12+10$, obtemos:

$2^{70}=(2^{12})^5\cdot 2^{10}\equiv 2^{10}\ mod\ 13$

Para reduzir ainda mais esta potência, podemos usar o fato de que $2^5=32\equiv 6\ mod\ 13$, logo $2^{10}=(2^5)^2 \equiv 6^2\ mod\ 13 \Rightarrow 2^{10} \equiv 36\ mod\ 13 \Rightarrow 2^{10} \equiv 10\ mod\ 13$.

Assim, $2^{70}\equiv 10\ mod\ 13$.

Agora vamos ao 3^{70} . Em vez de usar o teorema de Fermat, é mais simples considerar que $3^3=27\equiv 1\ mod\ 13$. Sendo $70=3\cdot 23+1$, temos $3^{70}=(3^3)^{23}\cdot 3^1\equiv 3\ mod\ 13$.

Concluindo,
$2^{70}+3^{70}\equiv 10+3\ mod\ 13 \Rightarrow 2^{70}+3^{70}\equiv 0\ mod\ 13$.

Portanto 13 divide $2^{70}+3^{70}$.

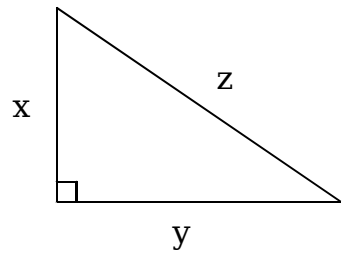
Texto 34 – Equações diofantinas

Uma aula que trata de Fermat não pode terminar sem menção ao último teorema de Fermat. Neste texto, vamos apresentar as equações diofantinas, de forma geral, e mostrar como as congruências módulo n podem ser usadas para resolver algumas destas equações .

> Uma equação diofantina é uma equação polinomial para a qual buscamos apenas soluções inteiras.

Veja alguns exemplos:

- $ax+by=1$. Esta é uma equação diofantina linear: todos os termos têm grau 1 .
- $x^2+y^2=z^2$. Esta equação está relacionada ao teorema de Pitágoras. Um trio de inteiros não-nulos que satisfaz esta equação é chamado de terno pitagórico e são lados de um triângulo retângulo, tendo o inteiro z como hipotenusa.



- $x^2 - n y^2 = 1$. É a chamada equação de Pell. Foi uma das equações diofantinas estudadas por Fermat.

A equação $x^2 + y^2 = z^2$ tem infinitas soluções. Fermat estudou o caso de equações $x^n + y^n = z^n$ para $n \geq 3$ e afirmou que nenhuma equação deste tipo tem solução formada por inteiros não-nulos.

Fermat escreveu este teorema em uma das margens da Aritmética de Diofanto e assinalou que tinha uma demonstração maravilhosa para o teorema, mas a margem era muito pequena para contê-la. O matemático nunca escreveu a ninguém sobre sua prova "maravilhosa". O fato é que esse teorema se tornou o famoso último teorema de Fermat e desafiou os maiores matemáticos do mundo pelos 357 anos seguintes.

Em junho de 1993, o matemático inglês Andrew Wiles anunciou uma demonstração do teorema. Após a divulgação, vários problemas foram encontrados. Em setembro de 1994, Wiles, com a ajuda do matemático inglês Richard Taylor, seu antigo aluno, conseguiu demonstrar definitivamente o teorema.

A história do último teorema de Fermat é muito curiosa e rica, repleta de episódios fascinantes. Uma ótima descrição pode ser encontrada no livro O último teorema de Fermat, de Simon Singh, Editora Record, 1999.

Há outras questões importantes em Teoria dos Números que podem ser facilmente resolvidas com o uso de congruências. Vamos examinar alguns problemas.

Texto 35 - Uso das congruências para resolver equações diofantinas

Em alguns casos, congruências podem ser usadas para mostrar que uma certa equação não tem solução, ou para fornecer indicações sobre estas soluções. Vamos explicar essa questão com um exemplo.

1. Existem inteiros x , y e k tais que

$$x^2+y^2=4\mathrm{k}+3 \text{ ?}$$

Uma outra maneira de formular essa questão é a seguinte: algum inteiro da forma $n=4\mathrm{k}+3$ pode ser escrito como soma de dois quadrados?

A resposta é não. Uma maneira simples de provar isso é usar congruência módulo 4 . Observe que:

$x^2+y^2=4\mathrm{k}+3 \Rightarrow x^2+y^2\equiv 3\, mod\, 4$

Vamos provar que essa última equação não tem solução. Para tal, verificamos os valores possíveis para x^2+y^2 módulo 4 .

Há quatro classes de congruência módulo 4 . Seus quadrados são:

$\overline{\mathrm{x}}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{\mathrm{x}}^2$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{1}$

Observe que $\overline{2}^2=\overline{4}=\overline{0}$ e $\overline{3}^2=\overline{9}=\overline{1}$.

Assim, $x^2+y^2 mod\, 4$ pode ser $\overline{0}+\overline{0}=\overline{0}$, $\overline{0}+\overline{1}=\overline{1}$ ou $\overline{1}+\overline{1}=\overline{2}$. Não há classes $\overline{x}$ e $\overline{y}$, tais que $\overline{x}^2+\overline{y}^2=\overline{3}$, ou seja, não há valores de x e y tais que $x^2+y^2\equiv 3\, mod\, 4$.

Portanto, a equação diofantina $x^2+y^2=4\mathrm{k}+3$ não apresenta soluções.

Esta aula teve como tema central a figura de Pierre de Fermat. Falamos um pouco deste grande matemático. Em seguida, enunciamos e provamos o teorema de Fermat.

Você também estudou algumas aplicações do teorema de Fermat, a solução de potências e as equações diofantinas.

Trecho escrito por Fermat na margem do livro Aritmética de Diofanto.

Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exigitas non caperet.

Pierre de Fermat

A tradução é:

"É impossível separar um cubo em dois cubos, uma quarta potência em duas quartas potências, e, em geral, qualquer potência mais alta que a segunda em duas potências iguais. Eu descobri uma prova verdadeiramente maravilhosa para isso, que essa margem é pequena demais para conter."

Atividades

1) Calcule o resto da divisão:

a) de 2^{172} por 17 ;
b) de 3^{334} por 23 ;
c) de 5^{1266} por 127 .

2) Usando congruência módulo 8, mostre que a equação diofantina $x^2+y^2-8z=6$ não tem soluções.

Unidade 2

Criptografia de Chave Pública

Caro aluno, na unidade 2 você vai estudar as aplicações em criptografia de chave pública dos conceitos e resultados matemáticos vistos na unidade 1.

Bom estudo!

Aula 9 – Teste de Primalidade de Fermat

Uma questão importante em Teoria dos Números e que tem interessantes aplicações em criptografia é a questão de decidir se um dado inteiro é ou não primo. Testes que permitem tal decisão são chamados testes de primalidade. O pequeno teorema de Fermat, estudado na aula passada, dá origem a um teste de primalidade bastante útil.

Texto 36 - Testes de Primalidade

O teste de primalidade é um algoritmo que determina se um dado número inteiro é um primo. É importante notar que este é um problema diferente e mais simples que o de fatorar um inteiro.

Na aula anterior, vimos o método simples que consiste em dividir um inteiro n por todos os primos menores ou iguais a $\sqrt{n}$. Caso nenhum destes primos seja divisor de n , então n é primo.

Este é um teste determinístico, ou seja, que determina com certeza se o inteiro dado é primo ou não. No entanto, é prático apenas para inteiros pequenos ou inteiros que sejam divisíveis por um primo pequeno. Em criptografia, por exemplo, onde lidamos com inteiros bastante grandes, este teste simples é de pouca utilidade.

Além dos testes determinísticos, existem os probabilísticos, que são os testes que podem provar que um número é composto, mas podem indicar, apenas com certa probabilidade, que um inteiro é primo.

Os testes probabilísticos são muito utilizados por serem mais rápidos que os testes determinísticos. Além disso, testes probabilísticos modernos, como o de Rabin-Miller, são extremamente eficientes, no sentido de que, se um inteiro passar em várias execuções do teste, há grande probabilidade de ele ser primo.

Vamos iniciar a aula apresentando um teste probabilístico simples, derivado do teorema de Fermat.

Texto 37 – Teste de Fermat

O teorema de Fermat dá origem a um teste de primalidade probabilístico muito interessante, chamado teste de Fermat.

Demonstração.

Seja n um inteiro cuja primalidade queremos determinar. Pelo teorema de Fermat, se n é primo, então $a^{n-1}-1\equiv 0\ mod\ n$ para todo a, tal que $mdc(a,n)=1$.

1. Escolhemos uma base a (geralmente um número primo pequeno), tal que $mdc(a,n)=1$.

2. Testamos se $a^{n-1}-1\equiv 0\ mod\ n$.

3. Se não vale $a^{n-1}-1\equiv 0\ mod\ n$, então n não é primo e dizemos que a base a é testemunha de que n é composto.

4. Se $a^{n-1}-1\equiv 0\ mod\ n$, então n passou no teste para a base a.

Se um inteiro n é composto, mas passa no teste de Fermat para a base a, dizemos que n é pseudoprimo de Fermat para base a. Por exemplo, o número 341 é pseudoprimo para a base 2, pois $2^{340}\equiv 1\ mod\ 341$, mas $341=11\cdot 31$ é composto. Na verdade, 341 é o menor pseudoprimo para a base 2.

A existência de pseudoprimos atesta que o teste de Fermat não é determinístico. Mas pseudoprimos são raros. Por exemplo, há apenas três pseudoprimos para a base 2 menores que mil: os inteiros 341, 561 e 645. Há apenas 245 pseudoprimos para a base 2 entre 1 e um milhão.

Podemos aumentar ainda mais a eficácia do teste de Fermat, aplicando-o repetidamente e usando várias bases. O número 341, por exemplo, não passa no teste para a base 3, porque $3^{340}\equiv 56\ mod\ 341$. Portanto 3 é testemunha de que 341 é composto.

O uso de duas bases aumenta a eficácia do teste de Fermat. Veja:

- Entre 1 e 10^5, por exemplo, há apenas 23 pseudoprimos para as bases 2 e 3.

- Entre 1 e $2{,}5\times10^9$ existem 4.709 pseudoprimos para as bases 2 e 3.

Ao adicionar a base 5, restam apenas 2.552 pseudoprimos no mesmo intervalo. Já, ao acrescentar a base 7, sobram apenas 1.770 pseudoprimos até $2{,}5\times10^9$.

> A expressão pseudoprimo é utilizada com significados diferentes nas referências. Alguns autores chamam de pseudoprimo qualquer inteiro (primo ou não) que passe no teste de Fermat. Aqui estamos definindo pseudoprimo como um inteiro composto ímpar que passe nesse teste. Pseudoprimos para a base 2 recebem também o nome de números de Poulet.

A expressão “pseudoprimo” também é utilizada para designar um inteiro composto que passa em um teste probabilístico. Por exemplo, um pseudoprimo de Euler é um composto que passa no teste de Euler. Há também pseudoprimos de Lucas, pseudoprimos fortes etc.

A raridade dos pseudoprimos tem aplicações práticas importantes na criptografia RSA, em que, como vamos estudar, deve-se escolher um inteiro que seja produto de dois primos grandes.

> O algoritmo usual para gerar primos grandes é escolher um inteiro ímpar grande e testar se é primo. Caso não seja, escolhemos arbitrariamente outro ímpar, ou somamos 2 ao ímpar anterior, e testamos novamente.

Para que seja eficiente, este algoritmo de geração de primos depende de testes de primalidade rápidos, pois os algoritmos determinísticos são lentos. Muitas vezes é preferível tolerar uma possibilidade muito pequena de usar um pseudoprimo e utilizar testes muito mais rápidos e simples.

A tabela a seguir mostra o menor pseudoprimo para as bases entre 2 e 20. Uma tabela semelhante, mas para bases até 200, pode ser encontrada no website da Wikipedia (disponível em http://en.wikipedia.org/wiki/Pseudoprime).

Inteiro a	*Menor pseudoprimo para a base a*	*Inteiro a*	*Menor pseudoprimo para a base a*
		11	$15=3\cdot5$
2	$341=11\cdot13$	12	$65=5\cdot13$
3	$91=7\cdot13$	13	$21=3\cdot7$
4	$15=3\cdot5$	14	$15=3\cdot5$
5	$124=2^2\cdot31$	15	$341=11\cdot13$
6	$35=5\cdot7$	16	$51=3\cdot17$
7	$25=5^2$	17	$45=3^2\cdot5$
8	$9=3^2$	18	$25=5^2$
9	$28=2^2\cdot7$	19	$45=3^2\cdot5$
10	$33=3\cdot11$	20	$21=3\cdot7$

Texto 38 - Números de Carmichael

Neste ponto, pode parecer que a solução para evitar os pseudoprimos seria utilizar muitas bases diferentes. Como vimos anteriomente, ao usar apenas as bases $2,3,5\,e\,7,$ restam apenas 1.770 pseudoprimos entre 1 e $2{,}5\times10^9$. Usando mais bases, teremos ainda menos pseudoprimos.

Testar para diversas bases é um procedimento utilizado, mas não é suficiente para garantir primalidade. O fato é que há inteiros que enganam o teste de Fermat para todas as bases.

Um "número de Carmichael" é um inteiro positivo composto n que satisfaz a congruência $b^{n-1}\equiv1\,(mod\,n)$ para todos os inteiros b co-primos com n. Ele recebe esse nome em homenagem ao matemático americano Robert Carmichael (1879-1967).

Portanto números de Carmichael são pseudoprimos de Fermat para todas as bases. Por isso, são algumas vezes chamados de pseudoprimos absolutos.

Uma caracterização para os números de Carmichael é dada pelo teorema de Korselt, de 1899.

Teorema (Korselt): Um inteiro positivo composto n é um número de Carmichael se, e somente se, todo fator primo p de n satisfaz as duas condições a seguir:

1. p^2 não divide n.

2. $p-1$ divide $n-1$.

Korselt observou essas propriedades, mas não conseguiu encontrar um exemplo de tal número. O primeiro exemplo foi descoberto em 1910 por Robert Carmichael, que observou que o número 510 atende às condições do teorema, pois $561=3\cdot 11\cdot 17$ é livre de quadrados. E vale que:

$$2|560,\ 10|560\ e\ 16|560.$$

O número 561 é o menor número de Carmichael. Os próximos seis números de Carmichael são:

$$1105=5\cdot 13\cdot 17 \quad (4 \mid 1104, 12 \mid 1104, 16 \mid 1104)$$
$$1729=7\cdot 13\cdot 19 \quad (6 \mid 1728, 12 \mid 1728, 18 \mid 1728)$$
$$2465=5\cdot 17\cdot 29 \quad (4 \mid 2464, 16 \mid 2464, 28 \mid 2464)$$
$$2821=7\cdot 13\cdot 31 \quad (6 \mid 2820, 12 \mid 2820, 30 \mid 2820)$$
$$6601=7\cdot 23\cdot 41 \quad (6 \mid 6600, 22 \mid 6600, 40 \mid 6600)$$
$$8911=7\cdot 19\cdot 67 \quad (6 \mid 8910, 18 \mid 8910, 66 \mid 8910)$$

Os números de Carmichael não seriam um problema tão grande para o teste de Fermat, se houvesse apenas um número finito deles. O problema de existirem infinitos números de Carmichael permaneceu em aberto por bastante tempo até que, em 1994, os matemáticos William Alford, Andrew Granville e Carl Pomerance provaram que há infinitos números de Carmichael.

Todos os números de Carmichael listados anteriormente têm três fatores primos. O número desse tipo com quatro fatores primos é $41041=7\cdot 11\cdot 13\cdot 41$.

Demonstração do teorema de Korselt

A prova completa do teorema de Korselt depende de alguns resultados que não serão estudados nesta demonstração. Você pode encontrá-los em Coutinho (1997).

Vamos provar aqui metade do teorema e comprovar que um inteiro que satisfaz as duas

condições do teorema é um número de Carmichael.

Seja n um inteiro que satisfaz as condições 1 e 2. Seja b inteiro co-primo com n. Se p é um fator primo de n, então $p \nmid b$. Pelo teorema de Fermat, $b^{p-1} \equiv 1 \pmod{p}$. Como, por hipótese, $(p-1) \mid (n-1)$, temos que $n-1=(p-1)q$ para algum inteiro positivo q. Portanto

$$b^{p-1} \equiv 1 \pmod{p} \Rightarrow \left(b^{p-1}\right)^q \equiv 1 \pmod{p} \Rightarrow b^{n-1} \equiv 1 \pmod{p}.$$

Assim, para todo primo p divisor de n, temos $b^{n-1} \equiv 1 \pmod{p}$.

Observe agora que a fatoração de n é da forma $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, em que todos os primos distintos $p_1, p_2, \ldots, p_k$ têm expoente 1, pela condição 1 do teorema ($p_i^2 \nmid n$).

Como provamos que $b^{n-1} \equiv 1 \pmod{p_i}$ para todo primo p_i que divide n, segue-se que $b^{n-1}-1$ é múltiplo de todos os p_i, logo é múltiplo de $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, ou seja, $b^{n-1}-1 \equiv 0 \pmod{n} \Rightarrow b^{n-1} \equiv 1 \pmod{n}$.

O inteiro n é, portanto, um número de Carmichael.

Texto 39 – Teste de Miller-Rabin

O teste de primalidade de Miller-Rabin é um teste probabilístico criado em 1976 por G.L. Miller e modificado por M.O. Rabin. O teste é uma pequena modificação do teste de Fermat, sendo bem mais eficiente que este, ainda que permaneça uma pequena chance de erro.

Seja n um inteiro positivo ímpar cuja primalidade queremos testar. O inteiro $n-1$ é par. Seja s a maior potência de 2 que divide $n-1$, isto é,

$$n-1 = 2^s \cdot d, \text{ onde } d \text{ é ímpar.}$$

Seja $1 < b < n-1$ um inteiro que servirá de base para o teste. Considere as seguintes potências de b :

$$b^d,\ b^{2d},\ b^{2^2 d},\ \ldots,\ b^{2^{s-1} d},\ b^{2^s d}.$$

Se n for um número primo, então a última desta potência é congruente a 1 módulo n , pois, pelo teorema de Fermat,

$$b^{2^s d} = b^{n-1} \equiv 1 \pmod{n}.$$

Talvez alguma potência anterior a essa seja congruente a 1 módulo n . Seja k o menor expoente tal que $b^{2^k d} \equiv 1 \pmod{n}$, isto é, tal que n divide $b^{2^k d} - 1$.

Se $k = 0$, então $b^{2^0 d} \equiv 1 \pmod{n} \Rightarrow b^d \equiv 1 \pmod{n}$. Caso contrário, se $k > 0$, então podemos fatorar $b^{2^k d} - 1$ como

$$b^{2^k d} - 1 = \left(b^{2^{k-1} d} - 1\right)\left(b^{2^{k-1} d} + 1\right).$$

Como n é primo e divide $b^{2^k d} - 1$, então divide um dos dois fatores à direita na equação anterior. Mas n não pode dividir $b^{2^{k-1} d} - 1$ pela escolha de k como o <u>menor</u> inteiro, tal que n divide $b^{2^k d} - 1$. Portanto n divide $b^{2^{k-1} d} + 1$, isto é, $b^{2^{k-1} d} \equiv -1 \pmod{n}$.

Nossa análise revelou o seguinte: se n é primo, então para toda base b , $1 < b < n-1$, escrevendo as <u>d</u> potências b^d , b^{2d} , $b^{2^2 d}$, … , $b^{2^{s-1} d}$, ou a primeira é congruente a 1 módulo n (caso $k = 0$ como dito anteriormente), ou alguma delas será congruente a -1 módulo n . Se nada disso acontecer, então o inteiro n é composto e dizemos que b é <u>testemunha</u> de que n é composto.

Se um inteiro positivo composto n passa no teste de Miller-Rabin para a base b , então afirmamos que n é **pseudoprimo forte** para a base b .

Exemplos

Vamos ver agora algumas aplicações.

1) Vimos que 341 é pseudoprimo de Fermat para a base 2 . Vamos testá-lo com o teste de Miller-Rabin.

Se $n = 341$, temos que $n - 1 = 340 = 2^2 \cdot 85$. Precisamos calcular duas potências: 2^{85} e

$2^{2\cdot 85}$. Calculando as potências obtemos:

$$2^{85} \equiv 32 \pmod{341}$$
$$2^{170} = \left(2^{85}\right)^2 \equiv (32)^2 \equiv 1 \pmod{341}$$

Como nem a primeira potência é congruente a 1 módulo 341, nem alguma delas é congruente a -1 módulo 341, então 2 é testemunha de que 341 é composto.

O segundo pseudoprimo de Fermat para a base 2 é o número de Carmichael 561. Vamos ver se passa no teste de Miller-Rabin com a base 2?

Se $n = 561$, então $n - 1 = 560 = 2^4 \cdot 35$. Temos, então, que calcular as potências módulo 561 a seguir: 2^{35}, $2^{2\times 35}$, $2^{2^2\times 35}$, $2^{2^3\times 35}$. Calculando essas potências, obtemos:

$$2^{35} \equiv 263 \pmod{561}$$
$$2^{2\times 35} = \left(2^{35}\right)^2 \equiv (263)^2 \equiv 166 \pmod{561}$$
$$2^{4\times 35} = \left(2^{70}\right)^2 \equiv (166)^2 \equiv 67 \pmod{561}$$
$$2^{8\times 35} = \left(2^{140}\right)^2 \equiv (67)^2 \equiv 1 \pmod{561}$$

Como nem a primeira potência é congruente a 1 módulo 561, nem alguma delas é congruente a -1 módulo 561, então 2 é testemunha de que 561 é composto.

Mas mesmo esse teste tem os seus algozes. Os primeiros pseudoprimos fortes para a base 2 são 2.047, 3.277, 4.033, 4.681, 8.321, 15.841, 2.934, ...

Os primeiros pseudoprimos fortes para a base 3 são 121, 703, 1.891, 3.281, 8.401, 8.911, 10.585, ...

Há mesmo alguns pseudoprimos fortes bem pequenos. É fácil verificar que 25 é pseudoprimo forte para a base 7.

Apesar da existência de pseudoprimos fortes, a aplicação do teste de Miller-Rabin com o uso de várias bases é extremamente eficiente. Usando as bases 2, 3 e 5, o teste falha apenas para 13 inteiros entre 1 e $2{,}5\times 10^{10}$.
Se adicionamos a base 7, então existe um único inteiro composto neste intervalo que passa no

teste de Miller, a saber, o inteiro $3.215.031.751$. Adicionando a base 11 , não há pseudoprimos fortes para as bases 2 , 3 , 5 , 7 e 11 entre 1 e 10^{12} . Veja no endereço http://mathworld.wolfram.com/StrongPseudoprime.html.

Não há um inteiro composto que passe no teste de Miller-Rabin para todas as bases. De fato, pode-se provar que, se um inteiro n passa nesse teste para $n/4$ bases, então n é certamente primo. Embora esta afirmação forneça um critério determinístico de primalidade, este não é prático, uma vez que testar $n/4$ bases para inteiros n grandes é totalmente inviável.

Nesta aula, estudamos dois testes de primalidade: os testes de Fermat e o de Miller-Rabin. São dois testes probabilísticos: um número que não passa em um destes testes é certamente composto e, se passar no teste, então, muito provavelmente, será primo. Porém há inteiros que enganam o teste; são os chamados pseudoprimos.

Pseudoprimos para uma base b são inteiros compostos que passam no teste de Fermat para a base b , enquanto que pseudoprimos fortes para uma base b são inteiros compostos que passam no teste de Miller-Rabin para a base b .

Há inteiros, aliás um número infinito deles, que são compostos, mas passam no teste de Fermat para todas as bases. São os chamados números de Carmichael. Não há inteiros compostos que passam no teste de Miller-Rabin para todas as bases.

Atividades

1) Mostre que 15 é pseudoprimo para a base 4.

2) Mostre que 25 é pseudoprimo para a base 7.

3) Mostre que 91 é pseudoprimo para a base 3.

4) Mostre que 25 é pseudoprimo forte para a base 7.

Aula 10 – Teorema de Euler

Nesta aula, você vai estudar a função ϕ (letra grega – pronuncia-se fi) de Euler e conhecer o teorema de Euler, que tem grande importância na criptografia RSA.

Texto 40 – Euler

Leonhard Euler nasceu na Basiléia, Suíça, em 1707, e morreu aos 74 anos. Foi, sem dúvida, um dos grandes matemáticos do século XVIII. As obras completas de Euler ocupam 75 volumes. Foi estimado que, só para copiar à mão as obras do matemático, uma pessoa levaria 50 anos, trabalhando oito horas por dia.

Euler ficou completamente cego durante os últimos 17 anos de sua vida. Sua produção matemática neste período, no entanto, aumentou graças à sua incrível memória e capacidade de realizar cálculos complexos, sem auxílio de lápis e papel. Cerca de metade de sua produção matemática foi feita neste período.

Texto 41 – A função ϕ de Euler

Vimos que um inteiro a tem inversa módulo n se, e somente se, $mdc(a,n)=1$. Assim, as classes que têm inversa em $\mathbb{Z}_n$ são:

$$\mathbb{Z}_n^*=\{\bar{a} \mid 1\leq a\leq n-1 \ \ e \ \ mdc(a,n)=1\}$$

Quantos elementos tem $\mathbb{Z}_n^*$? Observe que o número de elementos de $\mathbb{Z}_n^*$ é o número de inteiros entre 1 e $n-1$ que são co-primos com n. Este número é, por definição, $\phi(n)$.

Portanto, para $n\geq 1$,

$\phi(n)=$ número de inteiros entre 1 e $n-1$ co-primos com n.

Exemplos:

- $\phi(10)=4$
- $\phi(12)=4$
- $\phi(15)=8$
- $\phi(20)=48$

Antes de prosseguir, certifique-se de que entendeu a definição de $\phi(n)$, verificando os valores do exemplo anterior.

A função $\phi(n)$ desempenha um papel importante na criptografia RSA, como você verá nas próximas aulas.

Se o valor de n é pequeno, podemos calcular o valor de $\phi(n)$ simplesmente contando os inteiros entre 1 e $n-1$ co-primos com n. Porém, para valores maiores de n, precisamos utilizar algumas propriedades dessa função. Vamos enunciar estas propriedades como proposições.

A primeira proposição diz respeito à situação em que n é primo. Nesse caso, todo inteiro a entre 1 e $p-1$ é co-primo com p. Provamos assim que:

Proposição 1 - Se p é primo, então $\phi(p)=p-1$.

Exemplos:

- $\phi(5)=4$
- $\phi(17)=16$

O próximo caso a tratar é o da potência de um primo.

Se $n=p^{\alpha}$, então quantos inteiros entre 1 e $n-1$ são co-primos com n ? Observe que $mdc(a,p^{\alpha})=1$ se, e somente se, $mdc(a,p)=1$. Então, a pergunta é: quantos inteiros entre 1 e $n-1$ não são divisíveis por p ?

Uma maneira de responder esta pergunta é determinar quantos inteiros entre 1 e $n-1=p^{\alpha}-1$ são múltiplos de p. A questão é complexa. Os múltiplos de p entre 1 e $n-1=p^{\alpha}-1$ são:

$$1\cdot p,\ 2\cdot p,\ 3\cdot p,\ \cdots,\ (p^{\alpha-1}-1)\cdot p$$

Observe que o último número da lista é exatamente $p^{\alpha}-p$, ou seja, o último múltiplo de p antes de $p^{\alpha}-1$, e que a lista tem exatamente $p^{\alpha-1}-1$ inteiros.
Como há $p^{\alpha-1}-1$ múltiplos de p entre 1 e $p^{\alpha}-1$, então existem:

$$\underbrace{(p^{\alpha}-1)}_{\text{total de inteiros}} - \underbrace{(p^{\alpha-1}-1)}_{\text{múltiplos de } p} = \underbrace{p^{\alpha}-p^{\alpha-1}}_{\text{inteiros coprimos com } p^{\alpha}}$$

inteiros que não são múltiplos de p entre 1 e $p^{\alpha}-1$. Esse é o total de inteiros co-primos com p^{α}, logo:

$$\phi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$$

Provamos então a

Proposição 2 - Se p é primo, então $\phi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$.

Exemplos:

- $\phi(27)=\phi(3^3)=3^3-3^2=27-9=18.$
- $\phi(25)=\phi(5^2)=5^2-5^1=25-5=20.$
- $\phi(64)=\phi(2^6)=2^6-2^5=64-32=32.$

Observe que a proposição 1 é um caso particular da proposição 2. Se fizermos $\alpha=1$ na proposição 2 , obtemos:

$$\phi(p^1)=p^1-p^{1-1}=p-p^0=p-1.$$

A próxima proposição diz respeito às situações em que desejamos calcular $\phi(n)$, e n é produto de primos distintos. Com ela e a proposição anterior, somos capazes de calcular $\phi(n)$ para qualquer inteiro n que consigamos fatorar em produto de potências de primos.

Proposição 3 - Se a e b são inteiros positivos e $mdc(a,b)=1$, então $\phi(a\cdot b)=\phi(a)\phi(b)$.

A demonstração do teorema pode ser encontrada em José Plínio de Oliveira Santos, *op. cit*.

Alguns exemplos bastam para tornar bem claro como as proposições 2 e 3 são suficientes para calcularmos $\phi(n)$, para qualquer n a partir de sua fatoração em produtos de primos.

Exemplos:

- $\phi(15)=\phi(3\cdot 5)=\phi(3)\cdot\phi(5)=2\cdot 4=8.$ Observe que $mdc(3,5)=1$.
- $\phi(375)=\phi(3\cdot 5^3)=\phi(3)\phi(5^3)=2(5^3-5^2)=2\cdot 120=240.$

Preste atenção à fórmula $\phi(ab)=\phi(a)\phi(b)$ que, em geral, não se verifica quando a e b não são co-primos.

Exemplos:

- $\phi(10)=\phi(2\cdot 5)=\phi(2)\cdot\phi(5)=1\cdot 4=4.$ (2 e 5 são co-primos)
- $\phi(4)=2.$
- $\phi(40)=\phi(2^3\cdot 5)=\phi(2^3)\phi(5)=(2^3-2^2)4=16.$
- Veja que $\phi(40)\neq\phi(4)\phi(10).$ (4 e 10 não são co-primos)

É fácil provar, por indução, que a fórmula vale para o produto de vários fatores, desde que eles sejam todos primos entre si, ou seja, se $a_1, a_2, \cdots, a_k$ são inteiros positivos, tais que $mdc(a_i, a_j)=1$ para $i\neq j$. Então

$$\phi(a_1 a_2\cdots a_k)=\phi(a_1)\phi(a_2)\cdots\phi(a_k).$$

Exemplos:

- $\phi(120)=\phi(8\cdot 3\cdot 5)=\phi(8)\phi(3)\phi(5)=4\cdot 2\cdot 4=32.$
- $\phi(300)=\phi(2^2\cdot 3\cdot 5^2)=(2^2)\phi(3)\phi(5^2)=2\cdot 2\cdot 20=80.$

Podemos concluir esta parte reunindo as propriedades 2 e 3 em uma única fórmula. Se n é inteiro positivo e fatora-se como

$$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

então:

$$\begin{aligned}
&\phi(n)=\phi\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_k^{\alpha_k}\right)\\
&=\phi(p_1^{\alpha_1})\cdot\phi(p_2^{\alpha_2})\cdot\ldots\cdot\phi(p_k^{\alpha_k})=(p_1^{\alpha_1}-p_1^{\alpha_1-1})\cdot(p_2^{\alpha_2}-p_2^{\alpha_2-1})\cdot\ldots\cdot(p_k^{\alpha_k}-p_k^{\alpha_k-1})\\
&=p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\cdot p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)
\end{aligned}$$

Na última igualdade, fatoramos cada expressão $(p_k^{\alpha_k} - p_k^{\alpha_k - 1})$ por $p_k^{\alpha_k}$, resultando em

$p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)$. Podemos agora reunir todos os termos $p_k^{\alpha_k}$ da expressão.

Como $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, resulta que:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

onde p_i são os primos que dividem n. Pode-se ainda tornar esta fórmula um pouco mais compacta, usando uma notação comum para produtos, que é o símbolo $\prod$.

Podemos escrever, então, que:

$$\phi(n) = n \prod_{\substack{p_i \text{ primo} \\ p_i \text{ divide } n}} \left(1 - \frac{1}{p_i}\right)$$

Antes de passar ao próximo tópico, acompanhe um último comentário que é de extrema importância para a criptografia RSA.

Vimos anteriormente que é fácil calcular $\phi(n)$, caso conheçamos a fatoração de n. Porém o que acontece quando não conhecemos essa fatoração? Se n for muito grande, pode ser computacionalmente impraticável checar diretamente quais inteiros entre 1 e $n-1$ são co-primos com n.

De forma geral, a maneira mais rápida de calcular $\phi(n)$ é fatorar n. Se não for possível fatorar n, não há como calcular $\phi(n)$. Este simples fato está na base da segurança do RSA. Veremos que a chave pública do RSA é um par (n, e), em que n é um produto de dois primos distintos $n = p \cdot q$ e o inteiro e tem inversa módulo $\phi(n)$.

A chave privada é o par (n, d), em que d é a inversa de e módulo $\phi(n)$. Quem conhece $\phi(n)$ pode facilmente calcular a inversa de e módulo $\phi(n)$, usando o algoritmo de Euclides estendido.

Quem gerou as chaves sabe a fatoração $n = p \cdot q$ e pode calcular facilmente:

$$\phi(n)=\phi(p\cdot q)=\phi(p)\phi(q)=(p-1)(q-1).$$

Quem conhece n **,** mas não conhece a fatoração $n=p\cdot q$, deve fatorar n antes de poder calcular $\phi(n)$.

A segurança do RSA baseia-se no fato de que calcular $\phi(n)$ é essencialmente equivalente a fatorar n , e que fatorar um inteiro grande n é um problema difícil.

Mas ainda é cedo para explicarmos exatamente como funciona o RSA. Antes disso, deve-se entender o Teorema de Euler, que é o assunto da próxima parte.

Texto 42 – Teorema de Euler

Vamos iniciar recordando o teorema de Fermat.

Se p é primo e $p\nmid a$, então $a^{p-1}\equiv 1 \bmod p$. O teorema de Euler é uma generalização deste resultado, apresentando uma fórmula para o caso de um inteiro n qualquer. Veja a seguir.

Teorema. Sejam n e a inteiros. Se $mdc(a,n)=1$, então

$$a^{\phi(n)}\equiv 1 \bmod n.$$

Exemplos:

- Sejam $a=3$ e $n=10$. Temos que $mdc(3,10)=1$. Pelo teorema, $3^{\phi(10)}\equiv 1 \bmod 10$, ou seja, $3^4\equiv 1 \bmod 10$. De fato, $3^4=81\equiv 1 \bmod 10$.

- Sejam $a=5$ e $n=12$. Como $mdc(5,12)=1$, então $5^{\phi(12)}\equiv 1 \bmod 12$, ou seja, $5^4\equiv 1 \bmod 12$. De fato, $5^2=25\equiv 1 \bmod 12 \Rightarrow 5^4=(5^2)^2\equiv 1 \bmod 12$.

Para demonstrar o teorema, precisamos primeiro provar o lema que vamos enunciar a seguir.

Lembre-se que há $\phi(n)$ classes que têm inversa módulo n . Portanto, qualquer conjunto formado por inteiros que pertencem a classes módulo n distintas e que representam todas as classes que têm inversa módulo n , tem $\phi(n)$ elementos.

Lema: Se $\{a_{1,}a_{2,}\cdots,a_{\phi(n)}\}$ é um conjunto de representantes de todas as classes que tem inversa módulo n , e se α é inteiro que tem inversa módulo n (isto é, $mdc(\alpha,n)=1$), então $\{\alpha a_{1,}\alpha a_{2,}\cdots,\alpha a_{\phi(n)}\}$ também é um conjunto de representantes de todas as classes que tem inversa módulo n .

Demonstração

Inicialmente, observe que $\alpha a_{1,}\alpha a_{2,}\cdots,\alpha a_{\phi(n)}$ são todos inversíveis módulo n , pois o produto de elementos inversível módulo n é inversível módulo n .

Os inteiros $\alpha a_{1,}\alpha a_{2,}\cdots,\alpha a_{\phi(n)}$ representam classes distintas módulo n , porque:

$$\alpha a_i\equiv\alpha a_j mod\, n \;\Rightarrow\; \alpha^{-1}\alpha a_i\equiv\alpha^{-1}\alpha a_j mod\, n \;\Rightarrow\; a_i\equiv a_j mod\, n \;\Rightarrow\; i=j$$

(lembre que os $a_i's$ estão em classes distintas módulo n , logo $a_i\equiv a_j mod\, n \;\Rightarrow\; i=j$.)

Portanto, o conjunto $\{a_{1,}a_{2,}\cdots,a_{\phi(n)}\}$ é formado por $\phi(n)$ elementos, todos inversíveis módulo n , e que estão em classes distintas módulo n , o que prova que formam um conjunto de representantes das classes inversíveis módulo n .

Veja que provamos, em outras palavras, que:

$$\{\overline{a_1},\overline{a_2},\cdots,\overline{a_{\phi(n)}}\}=\{\overline{\alpha a_1},\overline{\alpha a_2},\cdots,\overline{\alpha a_{\phi(n)}}\}.$$

Agora, estamos em posição de provar o teorema de Euler.

Demonstração do Teorema de Euler

Seja a inteiro, em que $mdc(a,n)=1$. Escolha um conjunto $\{a_{1,}a_{2,}\cdots,a_{\phi(n)}\}$ de representantes das classes que possua inversa módulo n . Pelo lema anterior, o conjunto $\{a\cdot a_{1,}a\cdot a_{2,}\cdots,a\cdot a_{\phi(n)}\}$ também é um conjunto de representantes das classes que tem inversa

módulo n . Ao multiplicar os elementos desses conjuntos obtemos:

$$\overline{a_1}\cdot\overline{a_2}\cdot\ldots\cdot\overline{a_{\phi(n)}}=\overline{a\cdot a_1}\cdot\overline{a\cdot a_2}\cdot\ldots\cdot\overline{a\cdot a_{\phi(n)}}$$

ou seja,

$$a_1\cdot a_2\cdot\ldots\cdot a_{\phi(n)}\equiv a\cdot a_1\cdot a\cdot a_2\cdot\ldots\cdot a\cdot a_{\phi(n)}\,mod\,n$$

Ao fatorar o termo a do lado direito da congruência, obtemos:

$$a_1\cdot a_2\cdot\ldots\cdot a_{\phi(n)}\equiv a^{\phi(n)}\left(a_1\cdot a_2\cdot\ldots\cdot a_{\phi(n)}\right)mod\,n$$

Por fim, observe que o termo $a_1\cdot a_2\cdot\ldots\cdot a_{\phi(n)}$ é um produto de elementos inversíveis módulo n , logo é inversível módulo n e pode ser cancelado dos dois lados da congruência (o que é equivalente a multiplicar os dois lados da congruência pela inversa dele). Daí resulta que

$$a^{\phi(n)}=1\,mod\,n\,.$$

Exemplo:

Calcule o resto da divisão de 9^{122} por 28 .

Como $\phi(28)=\phi(4\cdot7)=2\cdot6=12$ e $mdc(9,28)=1$, pelo teorema de Euler $9^{12}\equiv1\,mod\,28$.

Sendo $120=12\cdot10=2$, obtemos:

$$9^{122}=9^{12\cdot10+2}=\left(9^{12}\right)^{10}\cdot9^2\equiv9^2\,mod\,28\,.$$

Como $9^2=81\equiv25\,mod\,28$, temos que o resto de 9^{122} por 28 é 25 .

Para terminar, observe que o teorema de Fermat é um caso especial do teorema de Euler, pois, se p é primo, vale que $\phi(p)=p-1$. Logo, para $p\nmid a$, o teorema de Euler assegura que:

$$a^{\phi(p)}=a^{p-1}\equiv1\,mod\,p\,,$$

sendo exatamente o teorema de Fermat.

Chegamos ao fim desta aula. Nela, estudamos a função ϕ de Euler, definida por $\phi(n)$, que é o número de inteiros entre 1 e $n-1$ que são co-primos com n.

Você também estudou as principais propriedades da função ϕ. São elas:

- $\phi(p)=p-1$ para todo p primo.
- $\phi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}=p^{\alpha}\left(1-\frac{1}{p}\right)$
- Se $mdc(a,b)=1$, então $\phi(a\cdot b)=\phi(a)\phi(b)$.

Como um inteiro a possui inversa módulo n se, e somente se, $mdc(a,n)=1$, então $\phi(n)$ é exatamente o número de classes módulo n que têm inversa.

Vimos o teorema de Euler, que diz que $a^{\phi(n)}\equiv 1 \bmod n$ se $mdc(a,n)=1$, generalizando o teorema de Fermat, visto na aula passada.

O teorema de Euler é o que faz o método empregado na criptografia RSA funcionar, como veremos na aula sobre o RSA, ainda nesta disciplina.

Atividades

1) Encontre o valor de $\phi(n)$ para os seguintes valores de n:

a) $n=90$.

b) $n=250$

c) $n=1620$

2) Mostre que:

a) $\{1,5,711\}$ é um conjunto de representantes das classes que têm inversa módulo 12 .

b) Multiplique todos os elementos deste conjunto por 7 e mostre que o conjunto resultante também é formado por representantes de todas as classes inversíveis módulo 12 .

3) Usando o teorema de Euler, calcule os restos de:

a) 17^{81} por 24.

b) 2^{4208} por 49.

Aula 11 - Teorema Chinês dos Restos

O chinês Qin Jiushao, que viveu de 1202 a 1261, é considerado um dos grandes matemáticos do século XIII. Jiushao não se dedicava exclusivamente à Matemática. Possuía conhecimentos em várias áreas e ocupou cargos burocráticos em diversas províncias chinesas.

O matemático chinês publicou, em 1247, o livro chamado Shu-shu chiu-chang, tratado matemático dividido em nove seções. Nele aparece, pela primeira vez, o que hoje é chamado **Teorema Chinês dos Restos**, assunto desta aula.

Jiushao contribuiu também para a solução de sistemas lineares, cálculo de somas de séries aritméticas e técnicas de solução de equações. Foi o responsável pela adoção do símbolo zero na matemática chinesa.

Para iniciar o estudo sobre o Teorema Chinês dos Restos e a aplicação deste à criptografia, vamos começar com um exemplo.

Texto 43 – Exemplo com duas equações

Em nosso exemplo, encontramos uma solução para o sistema de congruências:

$$\begin{cases} x \equiv 4 \, mod \, 3 \\ x \equiv 2 \, mod \, 5 \end{cases}$$

Uma forma de resolver o sistema é encontrar a solução geral da primeira congruência e fazer a substituição na segunda.

Como $x \equiv 4 \, mod \, 3$, então $x = 4 + 3t$, para algum $t \in \mathbb{Z}$. Substituindo este valor na segunda, obtemos:

$$x \equiv 2 \, mod \, 5 \;\Rightarrow\; 4 + 3t \equiv 2 \, mod \, 5 \;\Rightarrow\; 3t \equiv -2 \, mod \, 5$$

Ao multiplicar pela inversa de 3 módulo 5, que é 2 $(2 \cdot 3 = 6 \equiv 1 \, mod \, 5)$, temos:

$$2 \cdot (3t) \equiv 2 \cdot (-2) \, mod \, 5 \;\Rightarrow\; 6t \equiv -4 \, mod \, 5 \;\Rightarrow\; t \equiv 1 \, mod \, 5 \, .$$

Assim, $t = 1 + 5k$, para algum $k \in \mathbb{Z}$.

Finalmente, substituindo este valor de t em $x=4+3\mathrm{t}$, obtemos:

$$x=4+3\cdot(1+5\mathrm{k})=4+3+15\mathrm{k}=7+15\mathrm{k}$$

O cálculo anterior mostra que todo inteiro da forma $x=7+15\mathrm{k}$ é solução para o sistema e, reciprocamente, toda solução é da forma $x=7+15\mathrm{k}$. Isso mostra que, se por um lado o sistema tem infinitas soluções inteiras, por outro, todos são congruentes a 7 módulo 15.

Dizemos então que a solução é única módulo 15.

Assim, o sistema $\begin{cases} x \equiv 4 \, mod \, 3 \\ x \equiv 2 \, mod \, 5 \end{cases}$ tem solução única módulo 15, dada por $x \equiv 7 \, mod \, 15$.

Antigos chineses e gregos estudavam este tipo de problema relacionando-o com a astronomia. O sistema de congruência anterior resolve um problema do tipo: se um astro A foi visível no mês 4 e é visível a cada três meses, e o astro B foi visto no mês 2 e é visível a cada cinco meses, de quantos em quantos meses serão visíveis juntos?

A resposta, que calculamos resolvendo o sistema, é que serão visíveis no mês 7 e, depois, a cada 15 meses.

Texto 44 – Exemplo com três equações

Vamos agora usar a mesma técnica para resolver um sistema de três equações.

Apresentamos o exemplo como problema de astronomia, traduzimos em forma de sistema e resolvemos a questão com a mesma técnica empregada para o sistema de duas equações, conforme resolução anterior.

Problema:
Um certo corpo celeste foi visível no mês 1 e observações anteriores revelam que é visível a cada 11 meses. Outro astro foi visível no mês 3 e sabe-se que é visível a cada 13 meses. Um terceiro astro foi visível no mês 4 e é visível a cada 15 meses. Quando os três corpos celestes serão visíveis no mesmo mês?

Chamando de x o mês:

- o primeiro astro é visível nos meses $x=1+11\mathrm{t}$,

- o segundo em $x = 3 + 13k$,
- e o terceiro em $x = 4 + 15l$.

Escrevendo em forma de congruência, temos que encontrar uma solução para o sistema:

$$\begin{cases} x \equiv 1 \, mod \, 11 \\ x \equiv 3 \, mod \, 13 \\ x \equiv 4 \, mod \, 15 \end{cases}$$

Vamos empregar a mesma técnica utilizada para o sistema anterior, com duas equações. A primeira congruência nos diz que $x = 1 + 11t$ para algum $t \in \mathbb{Z}$.

Substituindo este valor na segunda congruência, obtemos:

$$x \equiv 3 \, mod \, 13 \Rightarrow 1 + 11t \equiv 3 \, mod \, 13 \Rightarrow 11t \equiv 2 \, mod \, 13$$

A inversa de 11 módulo 13 é 6, pois $11 \cdot 6 = 66 \equiv 1 \, mod \, 13$. Ao multiplicar os dois lados da congruência por 6, temos:

$$6(11t) \equiv 6 \cdot 2 \, mod \, 13 \Rightarrow 66t \equiv 12 \, mod \, 13 \Rightarrow t \equiv 12 \, mod \, 13 .$$

Assim, $t = 12 + 13k$, para $k \in \mathbb{Z}$. Substituindo esse valor de t no valor de x ,

$$x = 1 + 11t = 1 + 11(12 + 13k) = 133 + 143k .$$

Para todo $k \in \mathbb{Z}$, o valor de $x = 133 + 143k$ satisfaz às duas primeiras congruências.

Substituindo-o na terceira, temos:

$$x \equiv 4 \, mod \, 15 \Rightarrow 133 + 143k \equiv 4 \, mod \, 15 .$$

Mas $143 \equiv 8 \, mod \, 15$ e $133 \equiv 13 \, mod \, 15$, logo

$$13 + 8k \equiv 4 \, mod \, 15 \Rightarrow 8k \equiv -9 \, mod \, 15 \Rightarrow 8k \equiv 6 \, mod \, 15$$

A inversa de 8 módulo 15 é 2 , pois $8 \cdot 2 = 16 \equiv 1 \, mod \, 15$. Assim,

$$2\cdot(8\mathrm{k})\equiv 2\cdot 6\ mod\ 15\ \Rightarrow\ 16k\equiv 12\ mod\ 15\ \Rightarrow\ k\equiv 12\ mod\ 15\ .$$

Temos então $k=12+15\mathrm{w}$ para $w\in\mathbb{Z}$. Substituindo no valor de x, obtemos:

$$x=133+143\mathrm{k}=133+143(12+15\mathrm{w})=1.849+2145\mathrm{w}\ .$$

Assim, os astros serão simultaneamente visíveis no mês 1.849, e daí a cada 2.145 meses.

Observe que $2.145=11\cdot 13\cdot 15$ é o produto dos módulos. Novamente, a solução é única módulo o produto entre os módulos.

Este método de resolver os sistemas lidando com as equações, duas a duas, pode ser empregado com um número qualquer de equações. Contudo, nem sempre há soluções, como mostra o próximo exemplo.

Exemplo.

Resolva o sistema:

$$\begin{cases} x\ \equiv\ 3\ mod\ 5 \\ x\ \equiv\ 6\ mod\ 15 \end{cases}$$

Da primeira equação obtemos $x=3+5\mathrm{t}$. Substituindo na segunda, temos:

$$x\equiv 6\ mod\ 15\ \Rightarrow\ 3+5\mathrm{t}\equiv 6\ mod\ 15\ \Rightarrow\ 5\mathrm{t}\equiv 3\ mod\ 15\ .$$

Mas $mdc(5,15)=5\nmid 3$; logo a equação anterior não tem solução, o que mostra que o sistema também não possui.

Texto 45 – Teorema Chinês dos Restos

Vamos agora enunciar e demonstrar o teorema para um sistema com duas equações, utilizando a mesma técnica anterior.

Teorema Chinês dos Restos

Sejam m_1 e m_2 inteiros positivos e primos entre si. Então o sistema

$$\begin{cases} x \equiv b_1 \, mod \, m_1 \\ x \equiv b_2 \, mod \, m_2 \end{cases}$$

tem solução, e essa solução é única módulo $m_1 \cdot m_2$.

Demonstração

A primeira equação pode ser escrita na forma $x = b_1 + k \cdot m_1$. Substituindo na segunda, obtemos:

$$x \equiv b_2 (mod \, m_2) \Rightarrow b_1 + k \cdot m_1 \equiv b_2 (mod \, m_2) \Rightarrow m_1 \cdot k \equiv b_2 - b_1 (mod \, m_2)$$

Para que essa congruência tenha solução, é necessário (e suficiente) que $mdc(m_1, m_2)$ divida $b_2 - b_1$.

Como, por hipótese, $mdc(m_1, m_2) = 1$, então a congruência sempre tem solução.

Seja α o inverso de $m_1 \, módulo \, m_2$.

$$\alpha \cdot (m_1 \cdot k) \equiv \alpha \cdot (b_2 - b_1) \, mod \, m_2 \Rightarrow (\alpha \cdot m_1) \cdot k \equiv \alpha (b_2 - b_1) \, mod \, m_2 \Rightarrow$$
$$\Rightarrow k \equiv \alpha (b_2 - b_1) \, mod \, m_2$$

Logo, existe $t \in \mathbb{Z}$, tal que $k = \alpha (b_2 - b_1) + t \cdot m_2$.

Substituindo esse valor de k em $x = b_1 + m_1 \cdot k$, temos:

$$x = b_1 + m_1 (\alpha (b_2 - b_1) + t \cdot m_2)$$
$$x = b_1 + \alpha \cdot m_1 (b_2 - b_1) + t \cdot m_1 \cdot m_2$$
$$x = (1 - \alpha \cdot m_1) b_1 + \alpha \cdot b_2 \cdot m_1 + t \cdot m_1 \cdot m_2 .$$

Como α é inversa de $m_1 \, módulo \, m_2$, então:

$$\alpha \cdot m_1 \equiv 1 (mod\ m_2) \ \Rightarrow \ \alpha \cdot m_1 + \beta \cdot m_2 = 1 \ \Rightarrow \ \beta \cdot m_2 = 1 - \alpha \cdot m_1$$

para algum $\beta \in \mathbb{Z}$.

Substituindo este valor, obtemos:

$x = \alpha \cdot b_2 \cdot m_1 + \beta \cdot b_1 \cdot m_2 + t \cdot m_1 \cdot m_2$, em que $\alpha \ \ e \ \ \beta$ são inteiros tais que $\alpha m_1 + \beta m_2 = 1$ e podem ser facilmente calculados usando o algoritmo de Euclides estendido.

Provamos então que há solução e, no processo, encontramos uma fórmula que fornece as soluções.

Vejamos agora a questão da unicidade. A maneira usual de provar unicidade módulo $m_1 \cdot m_2$ é supor que haja outra solução y e mostrar que $x \equiv y \ mod \ m_1 \cdot m_2$.

Sejam, portanto, x e y duas soluções do sistema.

Então:

$$\begin{cases} x \ \equiv \ b_1 mod\ m_1 \\ x \ \equiv \ b_2 mod\ m_2 \end{cases} \quad \text{e} \quad \begin{cases} y \ \equiv \ b_1 mod\ m_1 \\ y \ \equiv \ b_2 mod\ m_2 \end{cases}$$

Subtraindo as equações com o mesmo módulo, resulta em $x - y \equiv 0 \ mod \ m_1 \ \Rightarrow \ m_1 | (x - y)$ e $(x - y) \equiv 0 \ mod \ m_2 \ \Rightarrow \ m_2 | (x - y)$.

Mas $mdc(m_1, m_2) = 1$. Como $(x - y)$ é múltiplo comum de m_1 e m_2 , então é múltiplo de $mmc(m_1, m_2) = m_1 \cdot m_2$, ou seja, $x - y \equiv 0 (mod\ m_1 \cdot m_2) \ \Rightarrow \ x \equiv y \ mod \ (m_1 \cdot m_2)$.

Observe que a condição $mdc(m_1, m_2) = 1$ garante a existência de solução, porém, segundo a a demonstração anterior, haverá também solução de $mdc(m_1, m_2) > 1$ desde que $mdc(m_1, m_2)$ divida $b_2 - b_1$.

E se tivermos mais de duas equações?

Nesse caso, a condição para garantir a existência da solução é que os módulos sejam dois a dois primos entre si. Por exemplo, se forem três equações:

$$\begin{cases} x \equiv b_1 \, mod \, m_1 \\ x \equiv b_2 \, mod \, m_2 \\ x \equiv b_3 \, mod \, m_3 \end{cases}$$

então, a condição é $mdc(m_1, m_2) = mdc(m_1, m_3) = mdc(m_2, m_3) = 1$.

Como $mdc(m_1, m_2) = 1$, o teorema para um sistema de duas equações mostra que há solução $x \equiv f_1 \, mod \, m_1 \cdot m_2$.

As duas equações $x \equiv b_1 (mod \, m_1)$ e $x \equiv b_2 (mod \, m_2)$ podem ser substituídas pela equação $x \equiv f_1 (mod \, m_1 \cdot m_2)$, pois x é solução das duas equações se, e somente se, a solução de $x \equiv f_1 (mod \, m_1 \cdot m_2)$.

Assim, o sistema com três equações é equivalente (tem as mesmas soluções) que o sistema com duas equações:

$$\begin{cases} x \equiv f_1 (mod \, m_1 \cdot m_2) \\ x \equiv b_3 (mod \, m_3) \end{cases} .$$

É claro que $mdc(m_3, m_1 \cdot m_2) = 1$, pois $mdc(m_3, m_2) = 1$ e $mdc(m_3, m_1) = 1$.

Ao aplicar novamente o teorema para duas equações, resulta que existe, e é única módulo $m_1 \cdot m_2 \cdot m_3$, uma solução para:

$$\begin{cases} x \equiv f_1 (mod \, m_1 \cdot m_2) \\ x \equiv b_3 (mod \, m_3) \end{cases}$$

o que prova o teorema para três equações.

O processo descrito anteriormente permite demonstrar o teorema para um sistema com um número qualquer de equações. Usando o teorema já demonstrado para duas equações, reduzimos de n equações para $n-1$ equações, daí para $n-2$ etc., sucessivamente até chegarmos a duas equações.

Dessa forma, concluímos o

Teorema chinês dos restos: Se $m_1, m_2, \ldots, m_k$ são inteiros positivos dois a dois primos entre si, então o sistema

$$\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \\ \quad \vdots \\ x \equiv b_k \bmod m_k \end{cases}$$

tem uma única solução módulo $m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

Texto 46 – Aplicações à criptografia: partilha de um segredo

Há uma aplicação muito interessante do Teorema Chinês dos Restos à criptografia, no que diz respeito ao problema da partilha de um segredo.

Em criptografia, um esquema de partilha de um segredo é um método para distribuição deste entre vários participantes de um grupo. Assim, cada um recebe uma parte do segredo, que só pode ser reconstruído quando todas as partes forem reunidas. Partes individuais não permitem por si só descobri-lo.

Contudo, há aplicações em que não é necessária a junção de todas as partes para que o segredo seja revelado, mas sim um número suficiente de pessoas. Por exemplo, um segredo industrial pode ser partilhado entre dez funcionários de uma indústria, de tal forma que, se seis deles se reunirem, suas partes poderão reconstruir o segredo. A idéia aqui pode ser que talvez alguns funcionários possam ser subornados, descuidados com sua parte do segredo etc., mas não seis deles ao mesmo tempo.

Sejam n e k inteiros positivos, $k < n$. Um esquema de divisão de um segredo, em que este é partilhado em um grupo de n pessoas, é chamado (k, n) -crítico se:

1. Ao reunirem-se k ou mais partes, é possível descobrir o segredo.
2. A reunião de um número menor que k de partes não permite descobrir o segredo.

Há vários esquemas simples que são (n, k) -críticos. Veja alguns exemplos:

- Suponha que o segredo seja a palavra criptografia e desejamos partilhá-lo entre quatro pessoas em um esquema $(4,4)$ -crítico. Um esquema simples seria usar as quatro partes:

"CRIP _ _ _ _ _ _ _ _ _",
"_ _ _ _ TO _ _ _ _ _ _",
"_ _ _ _ _ _ GRA _ _ _ " e
"_ _ _ _ _ _ _ _ _ FIA".

Apenas as quatro partes juntas poderiam recuperar a palavra toda. Uma pessoa que tivesse apenas uma das partes teria que tentar todas as possibilidades nas outras posições de letras, o que seria um número muito grande de combinações possíveis.

Note que esse esquema não será bem sucedido, uma vez que o conhecimento de um número menor que quatro partes provê informação valiosa sobre o segredo. Uma pessoa que tivesse a primeira parte saberia que se trata de uma palavra com 12 letras começando por "CRIP". Não seria difícil adivinhar o resto.

- Outro esquema (n,n) -crítico é o seguinte:

Codifique o segredo como um inteiro s . Gere $n-1$ inteiros aleatórios $r_{1,}r_{2,}\ldots,r_{n-1}$. Distribua esses inteiros para $n-1$ pessoas e dê à última pessoa o inteiro $s-r_1-r_2-\ldots-r_{n-1}$. Se as n pessoas revelarem juntas suas partes, então podem somá-la:

$$r_1+r_2+\ldots+r_{n-1}+(s-r_1-r_2-\ldots-r_{n-1})=s$$

No entanto cada parte é totalmente aleatória, não revelando nenhuma informação sobre o inteiro s .

No próximo texto, vamos usar o Teorema Chinês dos Restos para construir um esquema (n,k) -crítico de partilha de um segredo.

Texto 47 – Partilha de um segredo com o Teorema Chinês dos Restos

Sejam n e k inteiros, $k<n$. Vamos usar o Teorema Chinês dos Restos para desenvolver um sistema de partilha de um segredo que seja (n,k) -crítico. Suponha que o segredo que desejamos dividir seja codificado como um inteiro s .
Temos que escolher um conjunto S de n inteiros com uma propriedade muito especial.

Seja A o produto dos k menores elementos de S. Então, o produto s de quaisquer k ou mais elementos é sempre maior ou igual a A.

Seja B o produto dos $k-1$ maiores elementos do conjunto. Então, o produto de menos de k elementos do conjunto é sempre menor ou igual a B. Suponha que o conjunto S seja escolhido de tal forma que:

$$B < s < A.$$

Sejam $m_1, m_2, \ldots, m_n$ os n elementos do conjunto S. Distribui-se entre os participantes os pares (m_i, s_i), onde $s_i \equiv s \pmod{m_i}$. Se t participantes se reúnem para tentar descobrir o segredo, devem resolver o sistema:

$$\begin{aligned} x &\equiv s_1 \pmod{m_1} \\ x &\equiv s_2 \pmod{m_2} \\ &\vdots \\ x &\equiv s_t \pmod{m_t} \end{aligned}$$

Como os módulos $m_i, 1 \le i \le t$ são primos dois a dois, então, pelo Teorema do Resto Chinês, o sistema sempre tem solução, que é única módulo $m_1 \cdot m_2 \cdot \ldots \cdot m_t$.

Mas será esta solução igual ao segredo inicial s ?

Seja s_0 a solução encontrada para o sistema anterior. Como s também é solução — já que $s \equiv s_i \pmod{m_i}$ — e a solução é única módulo $m_1 \cdot m_2 \cdot \ldots \cdot m_t$, então:

$$s_0 \equiv s \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_t}.$$

Se $t < k$, então $m_1 \cdot m_2 \cdot \ldots \cdot m_t$ é o produto de menos de k elementos no conjunto S; portanto é menor ou igual a B. Assim, podemos apenas garantir que $s - s_0$ é múltiplo de $m_1 \cdot m_2 \cdot \ldots \cdot m_t$. Como $s > B$ e $s_0 < m_1 \cdot m_2 \cdot \ldots \cdot m_t < B$, então $s \neq s_0$.

Se $t \ge k$, então $m_1 \cdot m_2 \cdot \ldots \cdot m_t$ é o produto de k ou mais elementos de S, logo será maior ou igual a A. Como $s < A$, $s_0 \equiv s \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_t}$ e $A < m_1 \cdot m_2 \cdot \ldots \cdot m_t$, então devemos ter $s = s_0$ e o segredo estará recuperado.

No caso de $t<k$, a segurança do sistema está na existência de muitos múltiplos de $m_1 \cdot m_2 \cdot \ldots \cdot m_t$ entre A e B, uma vez que $A<s<B$ e que $s_0 \equiv s \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_t}$.

Isto é, queremos que $A-B$ seja grande se comparado com todos os produtos $m_1 \cdot m_2 \cdot \ldots \cdot m_t$ possíveis ($t<k$).

Exemplo.

Queremos desenvolver um sistema de partilha de um segredo que seja $(5,4)$ -crítico, ou seja, são cinco participantes, mas o segredo será descoberto se quatro deles revelarem suas partes ao mesmo tempo.

Seja $S=\{11,13,15,16,17\}$. O produto dos três maiores elementos é $15 \cdot 16 \cdot 17 = 4080$. Por outro lado, o produto dos quatro menores elementos é $11 \cdot 13 \cdot 15 \cdot 16 = 34320$. Suponha que o segredo seja codificado como o número $s=32000$. Os participantes receberão o seguinte:

- $s \equiv 1 \pmod{11}$ - participante 1 recebe o par $(1,11)$.
- $s \equiv 7 \pmod{13}$ - participante 2 recebe o par $(7,13)$.
- $s \equiv 5 \pmod{15}$ - participante 3 recebe o par $(5,15)$.
- $s \equiv 0 \pmod{16}$ - participante 4 recebe o par $(0,16)$.
- $s \equiv 6 \pmod{17}$ - participante 5 recebe o par $(6,17)$.

A reunião de apenas três desses sistemas resulta em um que terá solução s_0 que é única módulo M, onde M é o produto dos três módulos envolvidos.

Temos que $M \leq 15 \cdot 16 \cdot 17 = 4080$. Como s é solução, então $s \equiv s_0 \pmod{M}$. Portanto fica revelada a classe de s módulo M, o que dá informação relevante sobre s , mas não seu valor exato.

Nesta aula, você estudou o famoso Teorema Chinês dos Restos. Apresentamos

alguns exemplos e provamos o teorema para módulos primos entre si.

Você aprendeu também uma aplicação prática deste teorema em criptografia, o que permite construir um sistema de partilha de um segredo que seja (n,k) - crítico.

Atividades

1. Resolva o sistema

$$\begin{cases} x \equiv 1 \, mod \, 11 \\ x \equiv 7 \, mod \, 15 \end{cases}$$

2. Resolva o sistema

$$\begin{cases} x \equiv 1 \, mod \, 7 \\ x \equiv 4 \, mod \, 9 \\ x \equiv 5 \, mod \, 10 \end{cases}$$

3. Resolva o sistema

$$\begin{cases} 2\mathrm{x} \equiv 1 \, mod \, 3 \\ 3\mathrm{x} \equiv 4 \, mod \, 7 \\ x \equiv 1 \, mod \, 8 \end{cases}$$

Sugestão: multiplique a primeira equação pelo inverso de 2 módulo 3 e a segunda pelo inverso de 3 módulo 7. Depois, resolva de maneira usual.

4. Crie um sistema de partilha de um segredo que seja $(6,3)$ -crítico.

Aula 12 – RSA

Na disciplina “Criptografia Geral”, conhecemos a criptografia de chave pública. Naquele momento, descrevemos os princípios gerais dos sistemas de chave pública e mostramos que eles funcionam com base em funções matemáticas que envolvem conhecimentos na área de Teoria dos Números.

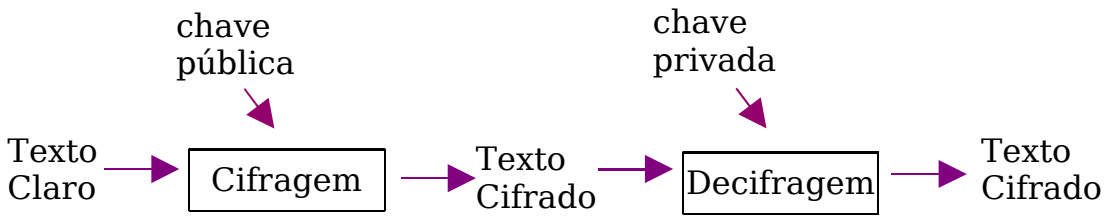
Bem, chegou a hora de descrevermos o funcionamento exato do RSA.

Texto 48 – A criptografia de chave pública

Vamos iniciar com uma revisão do conceito de criptografia de chave pública.

Um sistema desse tipo permite ao usuário enviar uma mensagem de forma segura sem conhecer qualquer chave secreta. O sistema opera com um par de chaves criptográficas, geralmente denominadas chave privada e chave pública. Essas chaves são relacionadas matematicamente, mas o conhecimento de uma delas não permite descobrir o valor da outra.

A chave privada é utilizada para cifrar uma mensagem, enquanto a chave pública será utilizada para decifrá-la. A figura a seguir ilustra o esquema usual de criptografia de chave pública.



Neste esquema, cada um gera seu par de chaves. Se duas pessoas, Alice e Bob, querem se comunicar, cada qual gera seu par de chaves (D_A, E_A) e (D_B, E_B), onde D_A é a chave privada de Alice e E_A é sua chave pública. D_B e E_B são as chaves privada e pública de Bob.

As chaves públicas podem ser divulgadas e as chaves privadas devem ser mantidas em sigilo.

Para mandar a mensagem P para Bob, Alice a criptografa usando E_B, o que resulta no texto criptografado $E_B(P)$, que é enviado. Para decifrar a mensagem, Bob usa sua chave privada D_B e recupera o texto inicial: $D_B\big(E_B(P)\big)=P$.

Na criptografia moderna, toda mensagem ou, de maneira geral, qualquer informação, é representada por um número inteiro. Os processos de cifrar e decifrar são, na verdade, funções que atuam em inteiros. Assim, D_B e E_B são funções matemáticas inversas uma da outra:

$$D_B\left(E_B(P)\right)=P \quad e \quad E_B\left(D_B(C)\right)=C$$

tais que o conhecimento de uma delas não permite a dedução da outra. Isto é, são funções que têm inversa, porém não é computacionalmente viável calcular essa inversa.

Descrevemos assim um sistema de chave pública em linhas gerais. A questão que surge agora é: como isto é implementado na prática? Que funções matemáticas são utilizadas?

Há várias implementações para o esquema de chave pública: uma das primeiras e mais conhecidas é o RSA, que vamos estudar em detalhe nesta aula. Mas existem outras implementações. Algumas destas serão apresentadas ao longo do curso, como o esquema chamado ElGamal, as técnicas baseadas em curvas elípticas, entre outras.

A criptografia de chave pública foi inventada, no início da década de 70, pelo matemático Clifford Cocks, que trabalhava para o serviço secreto inglês, o GCHQ. A descoberta foi mantida em sigilo até 1997. Em 1976, um esquema geral de criptografia de chave pública foi proposto por Diffie e Hellman, que trabalhavam no problema de combinação de chaves na criptografia tradicional.

Em 1977, os matemáticos Rivest, Shamir e Adleman criaram um algoritmo de chave pública chamado RSA, as iniciais de seus nomes. O RSA usa exponenciação módulo o produto de dois primos grandes para cifrar e decifrar uma mensagem. Sua segurança está baseada na dificuldade matemática de fatorar um inteiro grande.

No próximo texto, vamos detalhar o funcionamento do RSA.

Texto 49 – RSA

O primeiro passo no algoritmo é a geração das chaves. Cada participante deve gerar seu par de chaves.

Geração de chaves

Os passos envolvidos na geração das chaves são:

Passo 1 – Escolha, de modo aleatório, dois primos grandes distintos $p \neq q$.

Passo 2 – Calcule $n = p \cdot q$.

Passo 3 – Calcule o valor da função de Euler $\phi(n)$:

$$\phi(n) = \phi(p \cdot q) = \phi(p)\phi(q) = (p-1)(q-1).$$

Passo 4 – Escolha um inteiro e, em que $1 < e < \phi(n)$ e $MDC(e, \phi(n)) = 1$.

Passo 5 – Calcule o inteiro d, tal que $1 < d < \phi(n)$ e $d \cdot e \equiv 1 \pmod{\phi(n)}$.

As chaves são:

- a chave pública é o par (e, n).
- a chave privada é o par (d, n).

Algumas observações sobre os passos do processo de geração de chaves:

- No passo 1 – no procedimento da escolha de dois primos aleatórios distintos, pode-se escolher um inteiro ímpar aleatório. Depois, faz-se o teste nesse inteiro, para determinar se é primo. Caso não seja, testa-se o inteiro ímpar consecutivo a ele e assim por diante. Esse método requer testes de primalidade rápidos que tenham uma margem de erro muito pequena.

  O teste de Fermat, utilizando várias bases, é uma boa opção: é rápido e seguro. Embora os números de Carmichael enganem o teste, eles são extremamente raros.

- Os passos 4 e 5 podem ser realizados por meio do algoritmo de Euclides estendido. Como $mdc(e, \phi(n)) = 1$, então o inteiro e tem inversa módulo $\phi(n)$, isto é, existe inteiro d, $1 < d < \phi(n)$, tal que $e \cdot d \equiv 1 \mod \phi(n)$.

Processo de criptografia

Suponha que a mensagem a ser cifrada seja o inteiro P . Em sistemas criptográficos, as mensagens são transformadas em números e quebradas em blocos de bits de tamanho especificado. Assim, P é na verdade um certo inteiro de tamanho máximo conhecido. O inteiro n , que faz parte da chave pública (n,e) , deve ser maior que P .

Se um outro participante, Bob, por exemplo, deseja enviar mensagem para alguém, digamos Alice, deve obter a chave pública de Alice (n,e) .

O processo de cifragem é muito simples. A mensagem cifrada é o inteiro C, $1 \leq C \leq n$, tal que $C \equiv P^e \pmod{n}$.

O cálculo de $P^e \pmod{n}$, uma exponenciação módulo n , pode ser feito de forma rápida.

Processo de decifragem

Decifrar uma mensagem consiste em realizar uma nova exponenciação, desta vez usando a chave privada d , que só Alice conhece. Para decifrar a mensagem C , Alice calcula $C^d \pmod{n}$. Com isso, Alice recupera a mensagem original.

Como $e \cdot d \equiv 1 \mod \phi(n)$, então $ed = 1 + k\phi(n)$ para algum $k \in \mathbb{Z}$. Logo:

$$C^d = \left(P^e\right)^d = P^{ed} = P^{1+k\phi(n)} = P \cdot \left(P^{\phi(n)}\right)^k .$$

Aqui entra o teorema de Euler. Se $mdc(P,n) = 1$, então $P^{\phi(n)} \equiv 1 \pmod{n}$.

Portanto:

$$C^d = P\left(P^{\phi(n)}\right)^k \equiv P \pmod{n} .$$

Assim, a mensagem original P é recuperada.

Exemplo:

Faremos um exemplo completo, mas com números pequenos. O exemplo é apenas didático, uma vez que uma escolha de números tão pequenos não oferece qualquer segurança.

Vamos escolher o módulo e gerar as chaves:

Passo 1 - Escolhemos $p=61$ e $q=71$, dois primos distintos.

Passo 2 - $n=61\cdot 71=4331$ será o módulo utilizado.

Passo 3 - Calculamos $\phi(n)=60\cdot 70=4200$.

Passo 4 - Escolhemos $e=23$ como parte da chave pública.

Passo 5 - Calculamos $d\equiv e^{-1}\ (mod\,4200)$. Usando o algoritmo estendido de Euclides, verificamos que $d=3287$ é a inversa de 23 módulo 4200 .

A chave pública é o par $(23,4331)$.

A chave privada é o par $(3287,4331)$.

A função de cifragem é a função $E(P)=P^{23}\ (mod\,4331)$.

A função de decifragem é a função $D(C)=C^{3287}\ (mod\,4331)$.

Por exemplo, a mensagem $P=20$ cifrada por:

$$E(20)=20^{23}\ (mod\,4331)=2388\ (mod\,4331).$$

Para decifrar esta mensagem, usamos a função

$$D(2388)=2388^{3287}\ (mod\,4331)=20\ (mod\,4331)$$

que recupera a mensagem original.

Evidentemente, o módulo escolhido anteriormente $n=4331$ é muito pequeno para oferecer qualquer segurança real. Por outro lado, mesmo para esse valor pequeno, as contas de exponenciação são grandes para serem feitas à mão.

No próximo texto, mostraremos como as contas anteriores foram feitas utilizando um pacote de computação algébrica.

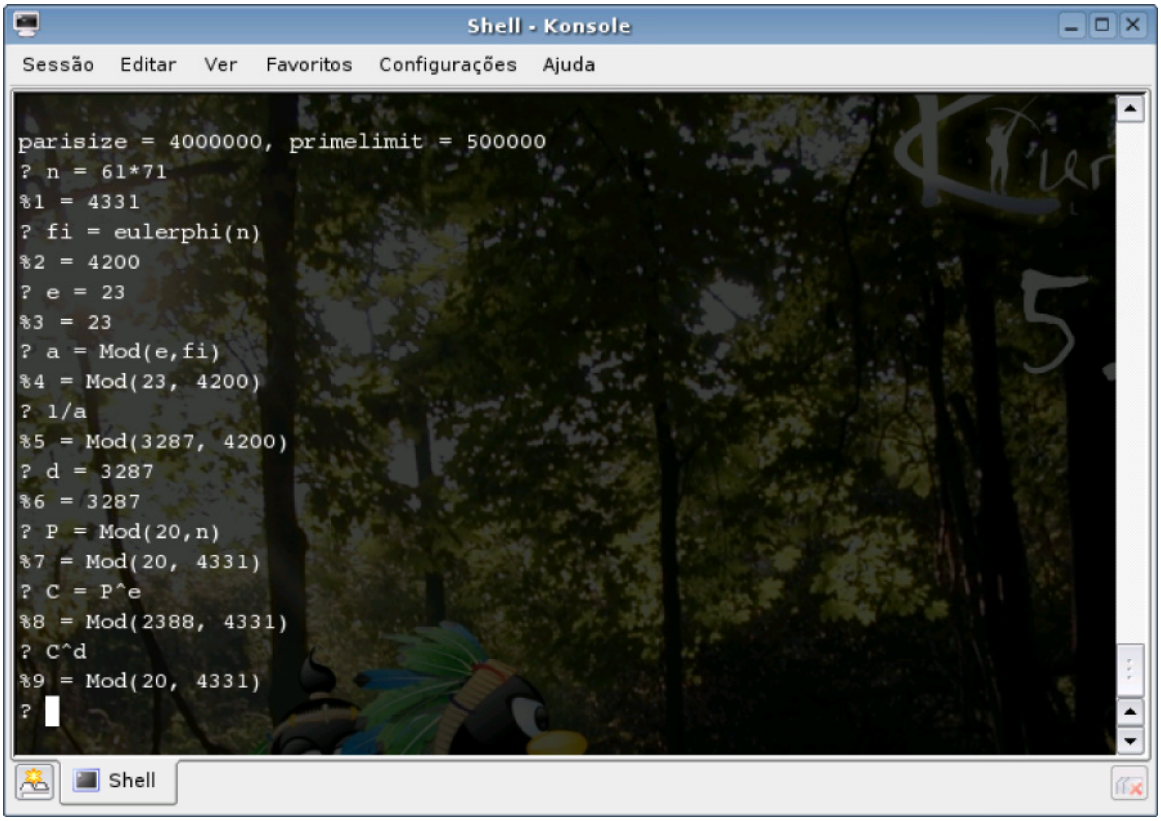
Texto 50 – O GP/Pari

Há muitos programas matemáticos de uso geral que lidam bem com aritmética modular. Há vários deles comerciais, com o Maple e o Mathematica, alguns gratuitos e outros ainda de código livre.

Um programa de código livre bastante popular entre os matemáticos que trabalham com Teoria

dos Números é o programa PARI/GP. Há versões para diversos sistemas operacionais e pode ser obtido (código fonte inclusive) no endereço http://pari.math.u-bordeaux.fr/. Há um manual detalhado e um tutorial para os que quiserem utilizar o programa.

Pari/GP possui amplo suporte para aritmética modular, testes de primalidade, fatoração de inteiros etc. As contas do exemplo anterior foram feitas usando o Pari/GP. Segue, na figura, a captura de tela das operações realizadas, utilizando o GP/Pari em sistema Linux.



Vamos acompanhar, passo a passo, as operações realizadas:

Linha 1 – Definimos $n=61\cdot 71=4331$. A multiplicação é dada pelo símbolo $*$. Observe que o sistema numera os resultados obtidos. O prompt $?$ é o sinal que o sistema aguarda nova entrada. O valor 4331 está agora armazenado na variável n .

Linha 2 – Armazenamos na variável fi o valor $eulerphi(n)$. Esta é a função $\phi(n)$. Assim, $fi=4200=\phi(4331)$.

Linha 3 – Definimos $e=23$.

Linha 4 – Definimos $a = Mod(e, fi) = Mod(23, 4200)$. A função Mod é utilizada para aritmética modular. Assim, o que fizemos foi definir $a = 23 \ mod \ 4200$.

Linha 5 – Para calcular a inversa de 23 módulo 4200, pedimos o valor de $1/a$, que o sistema entende como a inversa de $23 \ mod \ 4200$. O resultado é $3287 \ mod \ 4200$.

Linha 6 – Definimos $d = 3287$.

Agora que calculamos as chaves, vamos criptografar a mensagem.

Linha 7 – Definimos $P = 20 \ mod \ 4331$.

Linha 8 – A mensagem criptografada é $C = P^e$. A exponenciação em GP/Pari é dada pelo símbolo `^`. Obtivemos $C = 2388 \ mod \ 4331$.

Linha 9 – Para decifrar a mensagem, fazemos C^d, o que resulta em $20 \ mod \ 4331$, que é a mensagem original P.

Embora o GP/Pari não seja um sistema específico para criptografia, é uma ferramenta bastante útil para todos aqueles interessados em Teoria dos Números.

Texto 51 – Considerações práticas: escolha dos primos e preenchimento de bits

Várias questões práticas devem ser consideradas em uma implementação real do RSA.

A primeira está relacionada com a escolha dos primos. Os primos p e q devem ser grandes, uma vez que é fácil fatorar um inteiro que tenha um fator primo pequeno.

Outra consideração é que p e q não devem ser muito próximos. Pois, nesse caso, o inteiro $n = p \cdot q$ pode ser facilmente fatorado com o método de fatoração de Fermat.

Outro fator que deve ser considerado é que as mensagens $m = 0$ e $m = 1$ resultam em $c = 0^e = 0$ e $c = 1^e = 1$, o que fornece a um atacante informação sobre o texto claro.

Além disso, caso a mensagem m e a chave pública e forem tão pequenas que $m^e < n$,

então a mensagem transmitida é m^e. Um atacante pode recuperar a mensagem m simplesmente extraindo a raiz e-ésima de m^e (como número real).

Os problemas expostos anteriormente exigem que se faça alguma forma de pré-tratamento da mensagem, um sistema de preenchimento de bits, conhecido por ambos os participantes, e que evite que mensagens pequenas sejam criptografadas.

Outro problema é que o sistema descrito é totalmente determinístico, devido à ausência de qualquer componente aleatória. Assim, uma vez escolhido um par de chaves, uma mesma mensagem clara M resultará sempre na mesma mensagem criptografada C.

Nesse caso, um atacante pode cifrar uma série de palavras escolhidas, criando seu próprio dicionário de textos criptografados. Ao tentar decifrar uma mensagem criptografada, ele pode comparar a mensagem com seu dicionário, procurando por textos cifrados para os quais ele conhece o texto claro, e assim ganhar informação sobre a mensagem.

> A solução é algum tipo de pré-tratamento que faça com que a mesma mensagem clara na entrada resulte em diferentes textos cifrados na saída do algoritmo, tornando impraticável a construção de um dicionário de textos cifrados.

Observe que o uso de preenchimento da mensagem é uma técnica antiga, utilizada há séculos. Uma forma comum é adicionar no início e/ou no final da mensagem expressões escolhidas em uma lista combinada. O recipiente da mensagem pode facilmente reconhecer as expressões e retirá-las, mas o uso destas expressões torna o número de textos cifrados possíveis, correspondendo a um certo texto claro, bem extenso.

Existem diversos esquemas de preenchimento padronizados que são usados em implementações reais do RSA, tais como o **PCKS**.

> Saiba mais informações sobre o PCKS no endereço http://www.rsasecurity.com/rsalabs/node.asp?id=2124.

Texto 52 – Assinatura digital

A criptografia de chave pública também é utilizada como um meio de assinatura digital. Esta, tal como uma assinatura em papel, consiste em um bloco de informação adicionado à mensagem que comprova a identidade do emissor, confirmando quem ele diz ser.

Há três usos básicos para assinaturas digitais:

1. Garantir autenticidade – como a chave pública é conhecida, qualquer pessoa pode usar a chave pública de Alice e enviar uma mensagem para ela fazendo-se passar por Bob.

Outro exemplo: uma pessoa deposita R$ 100,00 em uma agência bancária, intercepta a mensagem da agência para a central, informando o depósito, e passa a repetir a mensagem várias vezes.

2. Garantir integridade – uma pessoa pode interceptar uma mensagem que foi enviada por Bob para Alice (usando a chave pública de Alice), alterar a mensagem, recriptografar a mensagem com a chave pública de Alice e enviá-la novamente a Bob.

3. Garantir não-repudiação – Bob pode enviar uma mensagem para Alice e depois negar tê-la enviado. Uma assinatura digital garante que só Bob poderia ter enviado a mensagem.

Todos esses três serviços são garantidos por um esquema de assinatura. Mas como implementar um esquema de assinatura digital usando a criptografia de chave pública?

Existem vários esquemas de assinatura digital. Veja um exemplo a seguir.

Esquema

Bob usa sua chave privada para criptografar algum texto que ele e Alice conhecem. Alice usa a chave pública de Bob para decifrar a mensagem e comparar com o texto combinado. Se são iguais, então foi de fato Bob quem enviou a mensagem, uma vez que só ele conhece sua chave privada.

O texto combinado deve ser algo que não possa ser reutilizado; caso contrário, um atacante poderia usar posteriormente a mesma assinatura.

Usualmente, utilizam-se as chamadas funções de hash, que têm como entrada a mensagem e resultam em um inteiro. Uma função de hash deve possuir características que tornem improvável que dois textos distintos tenham o mesmo hash e seja impossível inverter a função (a partir do

hash obter o texto).

Assim, Bob envia uma mensagem para Alice, criptografando a mensagem com a chave pública de Alice, e assina, criptografando o hash da mensagem com sua chave privada. Ou seja, Bob envia:

$$\left(E_A(P), D_B(H(P))\right)$$

onde:

- E_A é a chave pública de A;
- D_B é a chave privada de B;
- P é o texto claro;
- H é a função de hash utilizada.

Alice recebe este par e usa sua chave privada para recuperar a mensagem $P = D_A(E_A(P))$.

Ao obter a mensagem, calcula seu hash $H(P)$. Então, ela aplica E_B na segunda parte do par, obtendo $E_B(D_B(H(P)))$, e compara com $H(P)$. Se forem idênticos, então a assinatura confere.

Texto 53 – A segurança do RSA

A segurança do RSA está baseada na dificuldade de dois problemas matemáticos:

- a fatoração de inteiros grandes;
- o problema RSA.

Este último pode ser definido como o problema de extrair a e-ésima raiz módulo de um inteiro composto n. Em outras palavras, dados inteiros n, e e $m^e \bmod n$, como se faz para deduzir o valor de m.

Atualmente, a melhor forma de resolver o problema RSA é fatorar o inteiro n. Se um atacante conseguir fatorar $n = p \cdot q$, então poderá calcular facilmente o valor de $\phi(n)$ e, assim, o valor de $d \equiv e^{-1} \bmod n$, descobrindo a chave privada.
Até o momento, não se conhece um algoritmo para fatoração de inteiros grandes, em um computador clássico, que funcione em tempo polinomial. Nem foi provado que um algoritmo deste

tipo possa existir.

Portanto, para chaves suficientemente grandes, o RSA é seguro, levando-se em conta o conhecimento matemático atual do problema da fatoração de inteiros grandes.

Em 1993, Peter Schor mostrou que uma nova forma de computadores, o computador quântico, pode, em princípio, fatorar inteiros grandes em tempo polinomial, usando o algoritmo de Schor. No entanto não se espera que haja computadores quânticos em funcionamento antes de 2015.

Até meados de 2005, o maior inteiro fatorado usando métodos gerais é um inteiro de 663 bits, isto é, escrevendo estes inteiros em base 2, usamos 663 bits. Quando falamos em métodos gerais, aludimos ao fato de que há inteiros muito maiores já fatorados, mas inteiros de um tipo específico, o que permite métodos especiais de fatoração.

O inteiro de 663 bits foi fatorado como parte do esforço de quebrar o RSA-200, um dos desafios RSA (falaremos sobre isto a seguir). Este feito foi alcançado com um grande número de computadores, trabalhando de forma distribuída. Estima-se que um computador com processador de 2.2 Ghz levaria algo em torno de 75 anos para fatorar esse inteiro. Normalmente, são usadas chaves RSA de 1024 a 2048 bits, o que dá uma idéia da segurança que estes algoritmos oferecem.

Texto 54 – Os desafios RSA

Os desafios RSA são colocados pela empresa RSA Laboratories. Trata-se de inteiros semiprimos (produto de dois primos distintos) e o desafio é fatorá-los. Os inteiros são numerados de acordo com seu tamanho. No início, eram numerados conforme o número de dígitos decimais. O primeiro desafio foi o RSA-100 (um semiprimo com 100 dígitos decimais), que foi fatorado em poucos dias.

O último inteiro a ser fatorado foi o RSA-200 (200 dígitos decimais), fatorado em maio de 2005. O maior inteiro na lista de desafios RSA é um inteiro de 2048 bits (RSA-2048), com 617 dígitos decimais. Atualmente, é oferecido um prêmio de US$ 200 mil para quem conseguir fatorar este número. Isso mostra a confiança existente de que números desta ordem ainda estão muito além dos que podem ser fatorados hoje em dia.

Nesta aula, detalhamos o funcionamento do algoritmo de chave pública RSA,

discutimos alguns detalhes de sua implementação e aspectos de sua segurança.

Vimos também um software de computação algébrica de uso geral bastante útil para aqueles interessados em Teoria dos Números, o GP/Pari. Exploramos uma das aplicações importantes da criptografia de chave pública, que é a de possibilitar as assinaturas digitais.

Atividade

1) A chave pública de Alice é (143,23). Bob utiliza essa chave para criptografar uma mensagem para Alice. Bob envia a mensagem $C=2$. Quebre o código, descubra a chave privada de Alice e revele a mensagem original.

Aula 13 – Logaritmo Discreto

Nesta aula, você vai estudar os logaritmos discretos, que têm aplicação importante em criptografia, em especial no esquema de troca de chaves de Diffie-Hellman, no algoritmo de assinatura digitas (*digital signature algorithm* – DSA) e no sistema criptográfico ElGamal.

Texto 55 – Raízes primitivas Módulo n

Pelo teorema de Euler, que você estudou na aula 10, se a e n são inteiros primos entre si, então:

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

o que mostra que a equação

$$a^x \equiv 1 \pmod{n}$$

sempre tem pelo menos uma solução.

De fato, em geral, esta equação tem várias soluções, inclusive, em alguns casos, inteiros positivos menores que $\phi(n)$. Chamaremos de ordem de a módulo n **,** denotado $ord_n(a)$, ao menor inteiro positivo m , tal que $a^m \equiv 1 \pmod{n}$.

Exemplos:

- A ordem de 7 módulo 15 é 4 , pois:

- $7^1 \equiv 7 \pmod{15}$.
- $7^2 = 49 \equiv -1 \pmod{15}$.
- $7^3 = 7 \cdot 49 \equiv -7 \equiv 8 \pmod{15}$.
- $7^4 = \left(7^2\right)^2 \equiv (-1)^2 \equiv 1 \pmod{15}$.

Dessa forma, percebemos que $7^4 \equiv 1 \pmod{15}$ e que nenhuma potência de 7 menor que 4 é congruente a 1 módulo 15 . Logo, $ord_{15}(7) = 4$. Observe que $\phi(15) = 8$.
Como atividade, desenvolva os dois exemplos a seguir.

- A ordem de 4 módulo 9 é 3 . Observe que $\phi(9)=6$.

- A ordem de 2 módulo 9 é 6 .

Dos três exemplos anteriores, apenas no último temos que a ordem de a módulo n é $\phi(n)$. No entanto, nos três casos, $ord_n(a)$ é um divisor de $\phi(n)$. Esse fato é conseqüência do teorema a seguir.

Teorema: Sejam a e n inteiros positivos primos entre si e seja $ord_n(a)$ a ordem de a módulo n . Então, $a^x \equiv 1 \pmod n$ se, e somente se, x é múltiplo de $ord_n(a)$.

Demonstração

Seja $m = ord_n(a)$. Por um lado, se x é múltiplo de m , então $x = m \cdot k$ para algum k inteiro. Logo

$$a^x = a^{m \cdot k} = \left(a^m\right)^k \equiv 1^k = 1 \pmod n.$$

Por outro lado, se x não é múltiplo de m e $a^x \equiv 1 \pmod n$, então sejam q e r , respectivamente, o quociente e o resto da divisão de x por m :

$$x = m \cdot q + r, \quad 0 < r < m.$$

Observe que $r \neq 0$, pois $m \nmid x$. Portanto

$$a^x = a^{m \cdot q + r} \Rightarrow a^x = a^r \cdot \left(a^m\right)^q \Rightarrow 1 \equiv a^r \cdot 1^q \pmod n \Rightarrow a^r \equiv 1 \pmod n,$$

em que usamos $a^x \equiv 1 \pmod n$ e $a^m \equiv 1 \pmod n$.

Porém $a^r \equiv 1 \pmod n$ e $0 < r < m$ contrariam a escolha de m como o menor inteiro positivo, tal que $a^m \equiv 1 \pmod n$.

Assim, se x não é múltiplo de m , então não pode ocorrer $a^x \equiv 1 \pmod n$, o que conclui a demonstração do teorema.

Pelo teorema de Euler, $a^{\phi(n)} \equiv 1 \pmod n$. Dessa forma, pelo teorema anterior, $\phi(n)$ é

necessariamente um múltiplo da ordem de a módulo n , o que confirma a observação feita após os exemplos.

Quando $\phi(n)$ é a ordem de a módulo n , então dizemos que a é uma raiz primitiva módulo n .

Exemplo: O inteiro 2 é uma raiz primitiva módulo 9 , porque a ordem de 2 módulo 9 é $\phi(9)=6.$

Raízes primitivas têm importantes aplicações em criptografia.
Você estudará algumas delas ainda nesta aula.

Texto 56 – Grupos e Subgrupos

Quando estudamos aritmética modular, definimos $\mathbb{Z}_n$ como o conjunto das classes de congruência módulo n e definimos soma e produto de classes.

Você também estudou que estas operações atendem a certas propriedades, caracterizando assim uma estrutura chamada anel.

O conjunto dos elementos inversíveis módulo n , denotado $\mathbb{Z}_n^*$, é fechado para a operação de multiplicação. Isso significa que o produto de dois elementos em $\mathbb{Z}_n^*$ é um elemento em $\mathbb{Z}_n^*$, ou seja, o produto de duas classes inversíveis é uma classe inversível.

Acontece que $\mathbb{Z}_n^*$, com a operação de multiplicação de classes, atende as seguintes propriedades que caracterizam uma estrutura denominada grupo:

- associatividade: $(\bar{a}\cdot\bar{b})\cdot\bar{c}=\bar{a}\cdot(\bar{b}\cdot\bar{c})$.
- comutatividade: $\bar{a}\cdot\bar{b}=\bar{b}\cdot\bar{a}$.
- existência do elemento neutro: $\bar{a}\cdot\bar{1}=\bar{a}$.
- existência do elemento inverso: para toda classe $\bar{a}$ existe classe $\bar{\alpha}$, tal que $\bar{a}\cdot\bar{\alpha}=1$.

Podemos dizer, então, que $\mathbb{Z}_n^*$ é um grupo.

Estudo de grupos

O estudo de grupos é muito interessante. Os grupos podem subdividirem-se em subgrupos.

Se G é um subconjunto de $\mathbb{Z}_n^*$, então este herda automaticamente a associatividade e comutatividade de $\mathbb{Z}_n^*$.

Caso G seja fechado para o produto de classes, possua a classe $\bar{1}$ e todo elemento em G contenha uma inversa em G, então G é um subgrupo dentro do grupo $\mathbb{Z}_n^*$.

Todo elemento $a \in \mathbb{Z}_n^*$ gera um subgrupo de $\mathbb{Z}_n^*$ da seguinte forma: se m é a ordem de a módulo n, então o conjunto

$$\langle \bar{a} \rangle = \{1, \bar{a}, \bar{a}^2, \bar{a}^3, \ldots, \bar{a}^{m-1}\}$$

forma um subgrupo de $\mathbb{Z}_n^*$.

Para compreender que $\langle \bar{a} \rangle$ é subgrupo, observe que

- $\langle \bar{a} \rangle$ é fechado para o produto.
  De fato, qualquer potência de $\bar{a}$ está no conjunto, pois dado z inteiro positivo, existem q e r, tais que $z = q \cdot m + r$, $0 \leq r < m$.
  Logo, $\bar{a}^z = \bar{a}^{q \cdot m + r} = \left(\bar{a}^m\right)^q \cdot \bar{a}^r = \bar{1}^q \cdot \bar{a}^r = \bar{a}^r$. Como $0 \leq r < m$, então $\bar{a}^z = \bar{a}^r \in \langle \bar{a} \rangle$.

- $\bar{1} \in \langle \bar{a} \rangle$.

- Dados $\bar{a}^j$ em $\langle \bar{a} \rangle$, com $1 \leq j \leq m-1$, sua inversa é $\bar{a}^{m-j}$, que também está em $\langle \bar{a} \rangle$, pois $\bar{a}^j \cdot \bar{a}^{m-j} = \bar{a}^m = \bar{1}$.

Observe que, se m é a ordem de a módulo n, então os inteiros $1, a, a^{2,}, \ldots, a^{m-1}$ são todos não-congruentes módulo n.

Para provar isso, note que, se $a^i \equiv a^j \pmod{n}$, com $0 \leq i \leq j \leq m-1$, então, ao dividir ambos os lados da congruência por a^i — o que é possível, pois $mdc(a, n) = 1$ —, temos

$a^{j-i} \equiv 1 \pmod{n}$. Se $i \neq j$, então a congruência anterior contraria a minimalidade de m, porque $0 \leq j-i < m$.

O subgrupo $\langle \bar{a} \rangle$ é chamado subgrupo cíclico de $\mathbb{Z}_n^*$ gerado por $\bar{a}$. Quando a for uma raiz primitiva módulo n, acontece algo muito interessante: como as $\phi(n)$ classes $\{1, \bar{a}, \bar{a}^2, \bar{a}^3, \ldots, \bar{a}^{\phi(n)-1}\}$ são todas não-congruentes módulo n e $\mathbb{Z}_n^*$ tem exatamente $\phi(n)$ elementos, então

$$\mathbb{Z}_n^* = \{1, \bar{a}, \bar{a}^2, \bar{a}^3, \ldots, \bar{a}^{\phi(n)-1}\},$$

isto é, o próprio grupo $\mathbb{Z}_n^*$ é cíclico e gerado por $\langle \bar{a} \rangle$.

Observe que nem todo inteiro positivo n tem uma raiz primitiva. Pode-se mostrar que n tem raiz primitiva se, e somente se, n for da forma 2, 4, p^α e $2 \cdot p^\alpha$, em que p é um primo ímpar.

Exemplos:

- Vimos anteriormente que 2 é raiz primitiva módulo 9. O inteiro 9 é da forma 3^2.

- Não há raiz primitiva módulo 8. De fato, $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.
  A classe $\bar{1}$ tem ordem 1 e as classes $\bar{3}, \bar{5}$ e $\bar{7}$ possuem ordem 2, enquanto que $\phi(8) = 4$.

Texto 57 – Logaritmos discretos

Os logaritmos discretos na aritmética modular têm propriedades semelhantes ao logaritmos de números reais positivos. Por isso, antes de definir logaritmos discretos, vamos fazer uma breve revisão da função logaritmo.

Sejam b e y números reais positivos, com b ≠ 1. O **logaritmo de** y **na base** b é um número real x, tal que $y = b^x$, o que se denota por

$$x = \log_b y$$

Exemplos:

- $\log_2 8 = 3$, pois $2^3 = 8$.

- $\log_{\frac{1}{2}} 16 = -4$, porque $\left(\frac{1}{2}\right)^{-4} = 16$.
- $\log_{10} 0{,}01 = -2$, pois $10^{-2} = 0{,}01$.
- $\log_{10} 1 = 0$, porque $10^{0} = 1$.

São conseqüências diretas da definição que, para todo b real positivo, b ≠ 1.

- $\log_b 1 = 0$
- $\log_b b = 1$

São válidas também as seguintes propriedades, em que b, y e z são reais positivos e b ≠ 1.

- $\log_b(yz) = \log_b(y) + \log_b(z)$
- $\log_b(y/z) = \log_b(y) - \log_b(z)$
- $\log_b\left(y^r\right) = r \cdot \log_b y$
- $y = b^{\log_b(y)}$

Todas essas propriedades podem ser demonstradas facilmente a partir da definição de logaritmo.

Vamos agora voltar à aritmética modular.

Seja p um primo e a uma raiz primitiva módulo p (lembre-se que sempre há raízes primitivas módulo um primo p). A ordem de a módulo p é $\phi(p) = p - 1$, isto é, $p - 1$ é a menor potência de a congruente a 1 módulo p .

Assim, os inteiros $a^1, a^{2,} \ldots, a^{p-1}$ são todos não-congruentes módulo p . Como $\mathbb{Z}_p^*$ tem $p - 1$ elementos, então

$$\mathbb{Z}_p^* = \{a^1, a^{2,} \ldots, a^{p-1}\}.$$

Para todo inteiro b , se $p \nmid b$, então $\bar{b} \in \mathbb{Z}_p^*$. Logo existe um único inteiro j , $0 \leq j \leq p-1$, tal que:

$$b \equiv a^j \pmod{p}.$$

Vamos denotar este inteiro j por $ind_{a,p}(b)$ e chamá-lo índice do inteiro b na base a módulo p .

Portanto, por definição, $ind_{a,p}(b)$ é o menor inteiro maior ou igual a zero, tal que:

$$a^{ind_{a,p}(b)} \equiv b \pmod{p}.$$

Exemplo:

As potências de 2 módulo 11 são as seguintes:

$$\begin{array}{lll} 2^0=1 & 2^4=16\equiv 5 & 2^8=256\equiv 3 \\ 2^1=2 & 2^5=32\equiv 10 & 2^9=512\equiv 6 \\ 2^2=4 & 2^6=64\equiv 9 & 2^{10}=1024\equiv 1 \\ 2^3=8 & 2^7=128\equiv 7 & \end{array} \pmod{11},$$

o que mostra que 2 é raiz primitiva módulo 11.

A tabela anterior indica também os valores de $ind_{2,11}(x)$. Por exemplo, $ind_{2,11}(1)=0$, pois $2^0=1$ e $ind_{2,11}(6)=9$. E $2^9 \equiv 6 \pmod{11}$.

A próxima tabela mostra os valores de $ind_{2,11}(x)$ para todos os valores de x entre 1 e 10. Compare com os valores da tabela anterior para ter certeza de que entendeu a definição de índice.

x	1	2	4	8	5	10	9	7	3	6
$ind_{2,11}(x)$	0	1	2	3	4	5	6	7	8	9

Agora, podemos verificar que esta função $ind_{a,p}(x)$ satisfaz propriedades semelhantes às propriedades do logaritmo listadas anteriormente.

Vale que:

1) $ind_{a,p}(1)=0$

2) $ind_{a,p}(a)=1$

3) $ind_{a,p}(xy) \equiv ind_{a,p}(x)+ind_{a,p}(y) \ (mod(p-1))$

4) $ind_{a,p}(x^r) \equiv r \cdot ind_{a,p}(x) \ (mod(p-1))$

As duas primeiras afirmações são conseqüências diretas da definição. Em relação à terceira, temos que

$$a^{ind_{a,p}(x)} \equiv x \ (mod\ p) \quad e \quad a^{ind_{a,p}(y)} \equiv y \ (mod\ p).$$

Ao multiplicar as duas congruências obtemos:

$$a^{ind_{a,p}(x)+ind_{a,p}(y)} \equiv xy \equiv a^{ind_{a,p}(xy)} \ (mod\ p),$$

Mas, como a é raiz primitiva módulo p , então $a^u \equiv a^v \ mod\ p \Rightarrow u \equiv v \ (mod\ p-1)$.

Portanto, a congruência anterior mostra que:

$ind_{a,p}(xy) \equiv ind_{a,p}(x)+ind_{a,p}(y) \ (mod(p-1))$.

Em relação à quarta afirmação, $ind_{a,p}(x^r) \equiv r \cdot ind_{a,p}(x) \ (mod(p-1))$, basta fazer $x=y$ na terceira afirmação e aplicá-la novamente.

Exemplo:

Na tabela anterior, para $x=9$ e $y=7$ temos:

$$ind_{2,11}(9)=6 \quad \text{e} \quad ind_{2,11}(7)=7$$
$$ind_{2,11}(9 \cdot 7)=ind_{2,11}(63)=ind_{2,11}(8)=3$$

Por outro lado, $ind_{2,11}(9)+ind_{2,11}(7)=6+7=13 \equiv 3 \ (mod\ 10)$, de acordo com a terceira afirmação.

As quatro afirmações listadas anteriormente, válidas para a função $ind_{a,p}(x)$, mostram que, se definirmos esta função como

$$ind_{a,p}(x): \mathbb{Z}_n^* \rightarrow \mathbb{Z}_{n-1}$$

então a função possui as mesmas propriedades do logaritmo usual.

> Esta função é chamada logaritmo discreto de base a módulo p e tem várias aplicações interessantes em criptografia. Você vai estudá-las na próxima aula.

Devido à complexidade dos temas levantados durante a aula 13, segue uma dica: leia algumas vezes os pontos abordados até compreendê-los totalmente. São conhecimentos importantes, em virtude da variedade de aplicações em criptografia que usam os conceitos de raiz primitiva módulo n, os grupos e grupos cíclicos, e o logaritmo discreto de base a módulo p.

Atividades

1) Encontre todas as raízes primitivas módulo 18.

2) Calcule:
   a) a ordem de 3 módulo 8.
   b) a ordem de 5 módulo 16.
   c) a ordem de 7 módulo 20.

3) Elabore uma tabela com todos os valores da função $ind_{a,p}(x)$ com $a=2$ e $p=13$.

Aula 14 – Aplicações à Criptografia

Nesta aula, você vai estudar as aplicações à criptografia dos conceitos vistos nas aulas anteriores, sobre ordem módulo n , raiz primitiva módulo n e sobre o problema do logaritmo discreto.

Texto 58 – Teste de Lucas

Na última aula, observamos que existe uma raiz primitiva módulo n se, e somente se, n for da forma 2 , 4 , p^{α} e $2\mathrm{p}^{\alpha}$, em que p é um primo ímpar.

Em particular, se p é primo, então existe uma raiz primitiva b módulo p . Como b tem ordem $\phi(p)=p-1$, então os $p-1$ elementos

$$b, b^{2,} b^{3,} \ldots, b^{p-1}$$

são todos não-congruentes módulo p , o que mostra que

$$\mathbb{Z}_p^*=\{b, b^{2,} b^{3,} \ldots, b^{p-1}\} .$$

Isso demonstra, portanto, que $\mathbb{Z}_p^*$ é cíclico.

Esse fato pode ser usado como teste de primalidade. Dado um inteiro n , caso possamos testar facilmente se o grupo $\mathbb{Z}_n^*$ dos inteiros inversíveis módulo n é cíclico de ordem $n-1$, então podemos testar a primalidade de n .

A questão é como provar que $\mathbb{Z}_n^*$ é cíclico de ordem $n-1$. Isso é o mesmo que perguntar se existe algum inteiro b inversível módulo n , tal que b tenha ordem $n-1$.

Dado um inteiro b inversível módulo n , caso b possua ordem $n-1$, então $b^{n-1}\equiv 1 \pmod{n}$ e $n-1$ é o menor expoente.

Se $b^{n-1}\equiv 1 \pmod{n}$ e $n-1$ não é ordem de b , então $n-1$ é um múltiplo da ordem de b , ou seja, existe $k\in\mathbb{Z}$ tal que $n-1=k\cdot ord_n(b)$.

Seja p um divisor primo de k . Como k divide $n-1$, então p também é divisor de $n-1$. Assim, temos que:

$$\frac{n-1}{p}=\frac{k}{p}ord_n(b) \Rightarrow b^{\frac{n-1}{p}}=\left(b^{ord_n(b)}\right)^{\frac{k}{p}}\equiv 1 \pmod p.$$

Concluímos que, se $b^{n-1}\equiv 1 \pmod n$ e a ordem de b não é $n-1$, então existe algum divisor primo de $n-1$, tal que $b^{\frac{n-1}{p}}\equiv 1 \pmod p$.

Deste modo, dado inteiro n , se encontrarmos uma base b tal que

- $b^{n-1}\equiv 1 \pmod n$
- para todo divisor primo p de $n-1$ não vale $b^{\frac{n-1}{p}}\equiv 1 \pmod p$,

então b tem ordem $n-1$, o que mostra que n é primo.

O teste de Lucas consiste em encontrar uma tal base b .

Teste de Lucas

Seja n um inteiro positivo ímpar e b um inteiro tal que $2\le b\le n-1$. Se $b^{n-1}\equiv 1 \pmod n$ e se todo fator primo p de $n-1$ vale $b^{\frac{n-1}{p}}\not\equiv 1 \pmod p$, então n é primo.

Observe que o teste de Lucas é um teste que prova que n é primo. Os testes de Fermat e Miller-Rabin, apresentados anteriormente, podem provar que n é composto, mas não que n é primo.

Há duas dificuldades claras para a aplicação do teste de Lucas:

1ª) Temos que conseguir fatorar $n-1$.

2ª) É preciso encontrar a base b correta.

Em relação à primeira dificuldade: muitos primos n grandes interessantes são tais que $n-1$ pode ser fatorado facilmente, o que possibilita a aplicação do teste de Lucas.

Exemplo:

Seja $n=71$ e $b=11$. Temos que $11^{70}\equiv 1 \pmod{71}$. Como $70=2\cdot 5\cdot 7$, devemos testar as classes módulo 71 de 11 elevado aos expoentes $\frac{70}{2}=35$, $\frac{70}{5}=14$ e $\frac{70}{7}=10$.

Temos:

- $11^{35}\equiv 70 \not\equiv 1 \pmod{71}$.
- $11^{14}\equiv 54 \not\equiv 1 \pmod{71}$.
- $11^{35}\equiv 32 \not\equiv 1 \pmod{71}$.

Como nenhuma delas é congruente a 1 módulo 71, resulta que 11 tem ordem 70 e 71 é um inteiro primo.

O exemplo anterior é bastante artificial. É mais fácil provar que 71 é primo tentando dividi-lo pelos primos menores que $\sqrt{71}\approx 8{,}43$. No entanto, o teste de Lucas é muito eficiente para verificar a primalidade dos chamados números de Mersenne.

Já falamos deles, você se lembra? Os números de Mersenne são números da forma $M_n=2^n-1$.

Veja que, para que M_n seja primo, é necessário, mas não é suficiente, que n seja primo. Assim, temos que analisar apenas os inteiros da forma $M_p=2^p-1$ para p primo.

O teste de Lucas é muito eficiente quando aplicado a números desta forma, o que permite provar a primalidade de primos de Mersenne muito grandes. Esta é uma das razões pela qual os maiores primos conhecidos sejam os de Mersenne.

> Dos dez maiores primos conhecidos atualmente, sete deles são primos de Mersenne, incluindo os quatro primeiros. Você pode conferir os primos recordes no endereço http://primes.utm.edu/largest.html#biggest.

Texto 59 – Esquema de troca de chaves de Diffie-Hellman

O esquema de troca de chaves de Diffie-Hellman é um protocolo criptográfico que permite que dois participantes possam combinar uma chave secreta comunicando-se através de um canal inseguro. É baseado no problema do logaritmo discreto.

Foi publicado pela primeira vez em 1976 por Whitfield Diffie and Martin Hellman. No entanto havia sido descoberto, mas mantido em sigilo, anos antes pelo matemático Malcom Williamson, que trabalhava para o serviço secreto britânico.

A forma mais simples do esquema usa o grupo multiplicativo $\mathbb{Z}_p^*$ dos elementos inversíveis módulo p, onde p é primo. Já vimos que este grupo é cíclico. Seja g um elemento primitivo módulo p; podemos escrever:

$$\mathbb{Z}_p^* = \{g, g^2, g^3, \ldots, g^{p-1}\}.$$

Dizemos que g é um gerador para o grupo cíclico $\mathbb{Z}_p^*$. Qualquer raiz primitiva módulo p é um gerador do grupo.

O esquema de troca de chaves funciona da seguinte maneira: suponha que Alice e Bob estejam se comunicando por um canal inseguro e desejam combinar uma chave secreta para utilizar em algum sistema criptográfico simétrico.

1. Alice e Bob combinam usar um certo primo p e uma certa raiz primitiva g módulo p. Os atacantes podem conhecer p e g.
2. Alice escolhe um inteiro aleatório α e envia $g^\alpha \pmod p$ a Bob.
3. Bob escolhe um inteiro aleatório β e envia $g^\beta \pmod p$ a Alice.
4. Alice calcula $\left(g^\beta\right)^\alpha = g^{\alpha\beta} \pmod p$.
5. Bob calcula $\left(g^\alpha\right)^\beta = g^{\alpha\beta} \pmod p$.

Dessa forma, os dois conhecem o valor de $g^{\alpha\beta} \pmod p$. E qualquer atacante que interceptar toda essa comunicação terá acesso somente a g, g^α, g^β.

Para calcular $g^{\alpha\beta} \pmod p$, o atacante teria que conhecer também o valor de α ou de β, isto é, calcular o logaritmo discreto de $g^\alpha \pmod p$ ou de $g^\beta \pmod p$ na base g. Se o primo

p e os inteiros a e b são grandes o suficiente, então este problema é computacionalmente complexo.

O algoritmo pode ser implementado da mesma forma com qualquer grupo cíclico G e gerador g .

Repare que o esquema anterior não envolve uma forma de autenticação. O atacante poderia passar-se por Bob e combinar uma secreta com Alice. Aliás, poderia interceptar e modificar todas as comunicações, combinar chaves secretas distintas com Alice e Bob e passar a receber a mensagem de um deles, decifrá-la, modificá-la, criptografá-la novamente e enviá-la a outro.

Se for utilizado algum outro esquema para garantir autenticação, o sistema de troca de chaves de Diffie-Hellman é considerado bastante seguro. É importante que a ordem do grupo multiplicativo G utilizado seja um primo ou tenha algum fator primo grande; caso contrário é bem fácil resolver o problema do logaritmo discreto, tendo como base um gerador de G.

Se for utilizado $G=\mathbb{Z}_p^*$, em que p é primo, então G tem ordem $p-1$. Nesse caso, uma boa escolha são os chamados primos de Sophie German, que são da forma $p=2\mathrm{q}+1$, onde q _também é primo. Assim, $p-1=2\mathrm{q}$ tem um fator primo grande.

O esquema de Diffie-Hellman é bastante utilizado na prática, sendo inserido em alguns protocolos criptográficos.

Antes de finalizar esta seção, vamos fazer um exemplo prático, ainda que com números artificialmente pequenos.

Exemplo

1. Alice e Bob escolhem o primo $p=31$ e a raiz primitiva módulo 31 dada por $g=3$.
   Verifique que $g=3$ de fato é raiz primitiva módulo 31 . Esta verificação pode ser feita usando o programa GP/Pari. O comando $znorder(x)$ dá a ordem de x módulo n . **Verifique** que $znorder(Mod(3,31))=30.$

2. Alice escolhe o inteiro $a=10$ e envia $3^{10}\equiv 25\ (mod\ 31)$. Usando GP/Pari, **verifique** que $Mod(3\ \hat{}\ 10,31)=Mod(25,31)$.

3. Bob escolhe o inteiro $b=17$ e envia $3^{17}\equiv 22 \pmod{31}$. Utilizando GP/pari, **verifique** esta congruência.

4. Alice calcula $22^{10} \mod 31 = 5 \mod 31$.

5. Bob calcula $25^{17} \mod 31 = 5 \mod 31$.

A chave secreta combinada entre os dois é 5.

Texto 60 – ElGamal

O algoritmo ElGamal é um algoritmo criptográfico assimétrico baseado no esquema de troca de chaves de Diffie-Hellman, proposto pelo criptógrafo egípcio Taher Elgamal em 1984.

Este algoritmo vem sendo muito utilizado atualmente. Faz parte de diversos sistemas criptográficos, incluindo o software livre GNU privacy guard, e de várias implementações do PGP.

Assim como no esquema de troca de chaves de Diffie-Hellman, o algoritmo começa com a escolha de um grupo cíclico G, de ordem n, e de um gerador g de G. Uma escolha simples, mas não a mais segura, é escolher um p primo e $G=\mathbb{Z}_p^*$, o grupo das classes inversíveis módulo p. O gerador g pode ser qualquer raiz primitiva módulo p. O grupo G tem ordem $p-1$.

Confira os passos do algoritmo a seguir.

Processo de geração de chaves

1. Alice escolhe um grupo cíclico G, de ordem n, e um gerador g do grupo.

2. Alice escolhe, de forma aleatória, um inteiro x, $0\leq x\leq n-1$.

3. Alice calcula $h=g^x$. A chave pública de Alice é (G,n,g,h), isto é, o grupo G, sua ordem n, o gerador escolhido g e o elemento $h\in G$. A chave secreta de Alice é o inteiro x.

Processo de cifragem de uma mensagem

4. Bob quer enviar a mensagem M para Alice. Bob codifica a mensagem como um elemento de G, de uma forma bem conhecida por todos, e consegue a chave pública de Alice.

5. Bob escolhe aleatoriamente um inteiro y, $0 \leq x \leq n-1$ e calcula
$c_1 = g^y \quad e \quad c_2 = M \cdot h^y$

6. Bob envia o texto cifrado (c_1, c_2) para Alice.

Processo de decifragem da mensagem

7. Alice usa sua chave secreta x e calcula $c_{2\text{left}}(¿)^{-1}$. Este é o texto claro original, porque:

$$c_{2\text{left}}(¿)^{-1} = (M \cdot h^y) \cdot \left((g^y)^x\right)^{-1} = \frac{M \cdot h^y}{g^{xy}} = \frac{M \cdot (g^x)^y}{g^{xy}} = \frac{M \cdot g^{xy}}{g^{xy}} = M$$

Como só Alice conhece a chave secreta x, só ela pode calcular $c_{2\text{left}}(¿)^{-1}$.

A segurança do algoritmo ElGamal reside na dificuldade do problema do logaritmo discreto para um grupo cíclico G, que é o de calcular o expoente x, dados gerador $g \in G$ e um elemento $h = g^x$. Há vários modos de escolher o grupo G. A escolha $G = \mathbb{Z}_p^*$, com p primo, não é considerada segura.

Uma opção interessante é um subgrupo de $\mathbb{Z}_p^*$. Se o primo p é escolhido de forma que $p = 2q + 1$, com q primo, é possível optar por um elemento $g \in \mathbb{Z}_p^*$, que tenha ordem q, e usar o subgrupo $G = \{g, g^2, \ldots, g^q\}$, com q elementos.

O sistema ElGamal é tipicamente utilizado para combinar uma chave entre duas partes. Esta chave será utilizada por um sistema simétrico, que é muito mais rápido. Trata-se, então, de um sistema de criptografia híbrido:

- usa criptografia assimétrica para combinar a chave;
- e utiliza criptografia simétrica para cifrar e decifrar a mensagem.

Texto 61 – Algoritmo de assinatura digital

Há diversos sistemas de assinatura digital de chave pública que estão baseados na dificuldade do problema do logaritmo discreto. Um sistema que merece atenção especial é o DSA – *Digital Signature Algorithm* – que passamos a descrever agora.

O DSA é um padrão de assinatura digital adotado pelo governo americano. Foi proposto pelo NIST (National Institute of Standards and Technology) em 1991, adotado como padrão em 1993 e confirmado como padrão, com pequenas modificações, em 1996 e 2000.

O sistema usa um par de chaves, uma pública outra privada. Como todo sistema de assinatura digital, divide-se em três partes:

- geração das chaves pública e privada;
- assinatura de uma mensagem;
- verificação da assinatura.

Vamos agora descrever o sistema.

Suponha que nossa velha conhecida, a expert em criptografia Alice, queira enviar uma mensagem M ao seu correspondente usual Bob, sempre disposto a testar novos sistemas criptográficos.

Geração das chaves

Para a geração das chaves, Alice deve fazer os seguintes procedimentos:

1. Escolher um primo p de L bits, ou seja, $2^{L-1} < p < 2^L$, onde L é um múltiplo de 64 entre 512 e 1024. Quanto maior o valor de L, maior será a segurança do sistema. Hoje, recomenda-se usar apenas o valor $L = 1024$.

2. Selecionar um primo q de 160 bits que seja divisor de $p-1$. É claro que, para que isso possa ser feito, o primo p deve ter sido escolhido de tal forma que $p-1$ tenha um divisor primo de 160 bits.

3. Escolher o inteiro h, $1 < h < p-1$, tal que $h^{\frac{p-1}{q}} \bmod p > 1$. Seja $g = h^{\frac{p-1}{q}} \bmod p$.

4. Escolher o inteiro x tal que $0 < x < q$.

5. Calcular $y = g^x \bmod p$.

A chave pública de Alice é (p, q, g, y). Sua chave privada é x .

Para se comunicar com outras pessoas, Alice pode usar os mesmos valores (p, q, g) e utilizar outros valores de x e de $y = g^x \bmod p$.

Assinatura

Para assinar uma mensagem M , Alice deve:

1. Gerar um inteiro aleatório k , $1 < k < q$. Esse inteiro será usado apenas uma vez por mensagem.

2. Calcular $r = (g^k \bmod p) \bmod q$.

3. Calcular $s = (k^{-1}(H(M) + x \cdot r)) \bmod q$, onde M é a mensagem a ser enviada, e $H(M)$ é o hash de M , obtido pelo uso da função de hash SHA-1.

A assinatura é o par (r, s).

Alice envia para Bob a mensagem M e a assinatura (r, s), usando algum sistema criptográfico. Por exemplo, Alice pode usar o RSA, utilizando a chave pública de Bob.

Bob recebe estes valores, decodifica e tem acesso a M , r e s . Agora, ele deve verificar a assinatura de Alice.

Verificação

Para verificar a assinatura (r,s) de Alice, Bob precisa:

1. Calcular $w=(s)^{-1} \, mod \, q$.
2. Calcular $u_1=(H(M)\cdot w) \, mod \, q$, onde $H(M)$ é o hash da mensagem M usando a função SHA-1.
3. Calcular $u_2=(r\cdot w) \, mod \, q$.
4. Calcular $v=((g^{u_1}\cdot y^{u_2}) \, mod \, p) \, mod \, q$.

A assinatura será válida se $v=r$.

Bastante trabalho, não é? Por que funciona?

Para começar, como $g = h^{\frac{p-1}{q}} \, mod \, p$, então:

$$g^q \equiv h^{q\cdot\frac{p-1}{q}} \equiv h^{p-1} \equiv 1 \, mod \, p,$$

em que usamos o pequeno teorema de Fermat. Como q é primo e $g^q \equiv 1 \, mod \, p$, então g tem ordem q módulo p .

Como $s=(k^{-1}(H(M)+x\cdot r)) \, mod \, q$, então ao multiplicar os dois lados da congruência por $k\cdot s^{-1}$, temos

$$(k\cdot s^{-1})s \equiv (k\cdot s^{-1})(k^{-1}(H(M)+x\cdot r)) \, mod \, q \Rightarrow k \equiv H(M)s^{-1}+x\cdot r\cdot s^{-1} \, mod \, q.$$

Substituindo $w \equiv s^{-1} \, mod \, q$, obtemos

$$k \equiv H(M)\cdot w + x\cdot r\cdot w \mod q.$$

Como g tem ordem q e $k \equiv H(M)\cdot w + x\cdot r\cdot w \mod q$, então

$$
\begin{aligned}
g^k &\equiv g^{H(M)\cdot w + x\cdot r\cdot w} \mod q \\
&\equiv g^{H(M)\cdot w} \cdot g^{x\cdot r\cdot w} \mod q \\
&\equiv \left(g^{H(M)\cdot w} \cdot y^{r\cdot w} \mod p\right) \mod q \\
&\equiv \left(g^{u_1} \cdot y^{u_2} \mod p\right) \mod q
\end{aligned}
$$

Como $v=((g^{u_1}\cdot y^{u_2}) mod\ p) mod\ q$ e $r=(g^k mod\ p) mod\ q$, então a congruência anterior nos informa que, se a assinatura for correta, então $v=r$.

Iniciamos esta aula com o teste de primalidade de Lucas e depois apresentamos três sistemas criptográficos de chave pública que usam o problema do logaritmo discreto:

- o sistema de troca de chaves de Diffie-Hellman;
- o sistema de criptografia de mensagens ElGamal;
- e, por último, o sistema de assinatura digital DSA.

Na próxima aula, você vai estudar as curvas elípticas e verá que todos estes sistemas criptográficos descritos possuem versões que as utilizam.

Atividades

1) Usando o teste de Lucas com a base $b=3$, prove que $n=31$ é primo.

2) Alice e Bob querem combinar uma chave secreta usando o esquema de Diffie-Hellman. Eles escolhem o primo $p=23$ e o gerador $g=5$. Alice escolhe o inteiro $a=9$ e Bob escolhe o inteiro $b=7$. Cada um mantém sua escolha em segredo. Como ocorre a troca de chaves e qual é a chave combinada?

Aula 15 – Criptografia com o uso de Curvas Elípticas

Chegamos ao último tópico desta disciplina: as curvas elípticas. Este estudo é de grande importância na Teoria dos Números e vem sendo muito pesquisado atualmente.

A utilização de curvas elípticas em criptografia foi proposta inicialmente pelos matemáticos Neal Koblitz e Victor Miller, em 1985. Como veremos, sistemas como ElGamal, Diffie-Hellman e o Algoritmo de Assinatura Digital podem ser modificados para o uso de curvas elípticas.

A vantagem desta utilização é que por ela se consegue o mesmo nível de segurança, com chaves menores, do que o obtido nos sistemas de chaves públicas tradicionais. A desvantagem é que a implementação é mais complexa.

Nesta aula, vamos definir curvas elípticas, mostrar a existência de um grupo formado por certos pontos da curva e, em seguida, falar sobre as aplicações em criptografia.

Texto 62 – Curvas Elípticas

Uma curva elíptica é uma curva plana definida por uma equação do tipo

$$y^2 = x^3 + ax + b$$

e que seja não-singular. Isso significa que seu gráfico não tem auto-interseção e não possui as chamadas cúspides, que são pontos onde o gráfico da curva não é suave, existindo uma "quina".

Assim, nem toda curva de equação $y^2 = x^3 + ax + b$ é um curva elíptica. Para alguns valores de a e b, a curva é singular, isto é, seu gráfico não é suave sem auto-interseção.

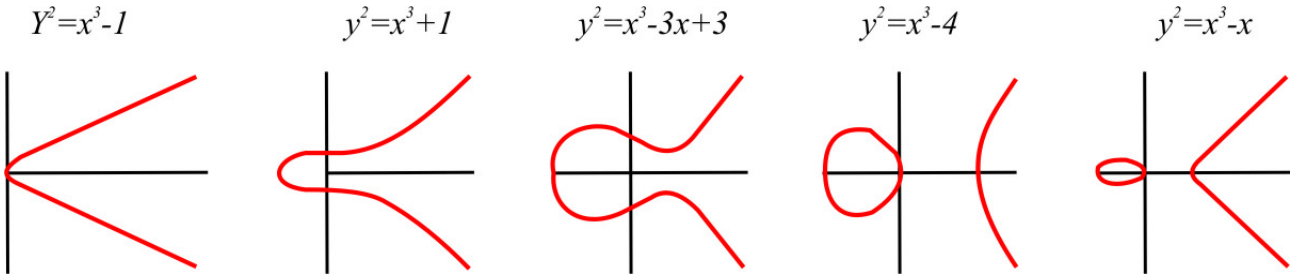
Pode-se mostrar que uma curva dada pela equação $y^2 = x^3 + ax + b$ é não-singular se, e somente se, o valor de

$$\Delta = 4\mathrm{a}^3 + 27\mathrm{b}^2$$

for diferente de 0.

O parâmetro Δ é chamado discriminante da curva.

As figuras a seguir mostram os gráficos de algumas curvas elípticas.



Figuras elaboradas com o uso do software Mathematica

(Fonte: http://mathworld.wolfram.com/EllipticCurve.html. Acesso em: 25 ago. 2005)

Como você pode observar, o gráfico de uma curva elíptica pode ter um ou dois “pedaços”.

Os gráficos anteriores são de curvas definidas para os reais, ou seja, os valores dos parâmetros a e b são números reais e os valores das variáveis x e y na equação são reais. No entanto, uma curva elíptica pode estar definida sobre qualquer corpo. Em criptografia, estamos interessados em curvas elípticas definidas sobre corpos finitos.

Mas o que é um corpo finito?

Texto 63 - Corpos Finitos

Um corpo é um conjunto com duas operações — normalmente soma e multiplicação — que satisfazem às propriedades usuais da soma e da multiplicação de números reais.

A soma deve ser comutativa, associativa, ter elemento neutro (zero) e elemento simétrico (para todo x no conjunto deve existir um $-x$).

A multiplicação tem de ser comutativa, associativa, possuir elemento neutro (um) e todo elemento não-nulo deve possuir uma inversa (para todo $x \neq 0$ deve existir o elemento $1/x$). Além disso, precisa ser válida a propriedade da distributividade da multiplicação em relação à soma ($x \cdot (y+z) = x \cdot y + x \cdot z$).

O conjunto dos racionais $\mathbb{Q}$, dos reais $\mathbb{R}$ e dos complexos $\mathbb{C}$ são exemplos de corpos.

> Um corpo finito é formado por um número finito de elementos.

Você já trabalhou bastante com um corpo finito: para p primo, o conjunto $\mathbb{Z}_p$, as operações de soma e de produto de classes são um corpo finito com p elementos.

Se F é um corpo finito com q elementos, então q é uma potência de algum primo p, ou seja, $q = p^m$, para algum primo p e inteiro m. Além disso, todos os corpos com q elementos são equivalentes de certa maneira. Esta "equivalência" é dada pela noção de isomorfismo.

> Dois corpos finitos com mesmo número de elementos q são isomorfos. Isso significa que existe uma aplicação bijetiva entre estes corpos que preserva a soma e a multiplicação.

Por causa dessa equivalência, é comum falar-se no corpo finito de p^m elementos, como se houvesse apenas um. Este corpo é denotado $GF(p^m)$ ou F_{p^m}.

A notação $GF(p^m)$ vem da expressão em inglês "Galois Field" que, em português, significa "corpo de Galois"[1], em homenagem ao matemático francês Évariste Galois, que fez contribuições relevantes para a teoria dos corpos.

Galois morreu aos 20 anos em um duelo, aparentemente, para defender a honra de uma mulher. Existe um ramo muito bonito da álgebra chamado Teoria de Galois, que trata dos corpos e soluções de polinômios.

Agora, vamos voltar ao estudo das curvas elípticas.

1 A estrutura algébrica corpo é chamada em inglês de "field".

Texto 64 – Grupo de uma Curva Elíptica

Um aspecto importante sobre as curvas elípticas é a possibilidade de definir uma operação de soma nos pontos da curva. O conjunto de pontos obtido com esta operação é um grupo.

> Lembre-se que um **grupo** é um conjunto com uma operação (tipicamente soma ou multiplicação) que é comutativa, associativa, possui elementos neutro (zero) e simétrico (para todo x no conjunto há um $-x$).

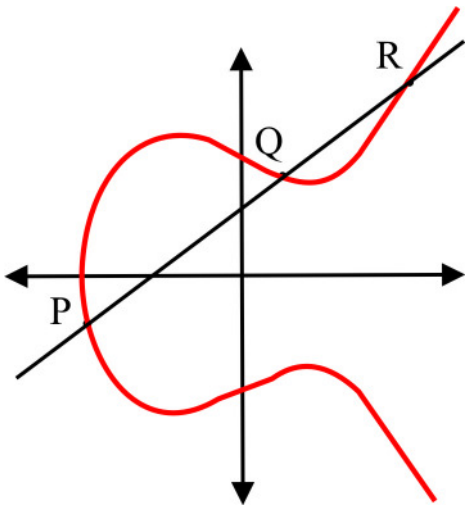
Nos sistemas criptográficos de Diffie-Hellman e ElGamal, há uma escolha inicial de um grupo cíclico G. Uma implementação simples desses sistemas usa $G=\mathbb{Z}_p^*$ ou um subgrupo cíclico dele. Os sistemas criptográficos de curva elíptica utilizam como grupo G o grupo dos pontos da curva.

Antes de ingressar na criptografia, é preciso que você compreenda este grupo de pontos da curva. Por isso, vamos descrevê-lo para seu melhor entendimento.

Descrição do grupo de pontos

Dados dois pontos P e Q em uma curva elíptica, podemos identificar de maneira única um ponto R como o terceiro ponto de interseção da reta que passa por P e Q com a curva.

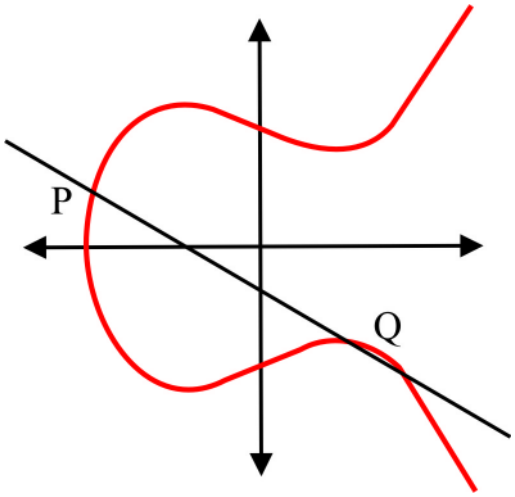
Observe a figura a seguir.



Se a reta que passa por P e Q for tangente à curva em algum dos pontos, esse será

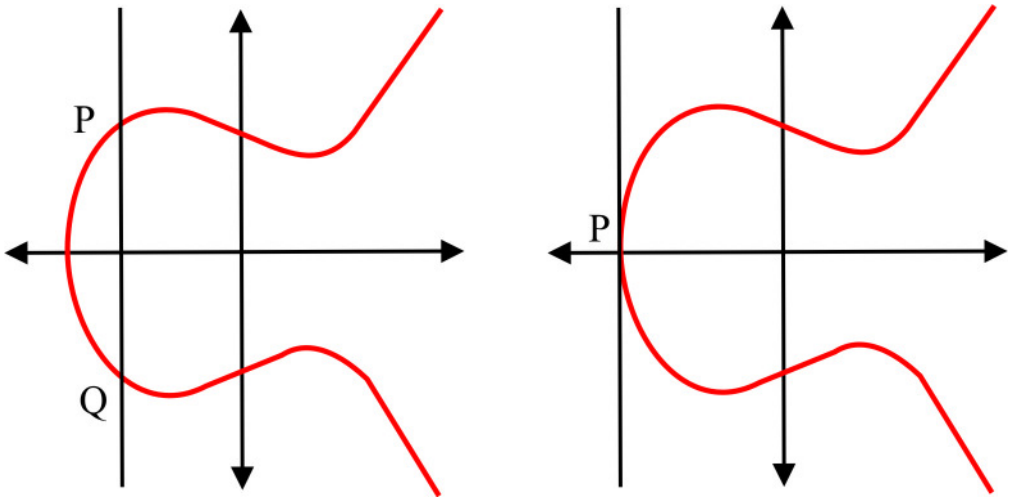
considerado o terceiro ponto de interseção R .

Na próxima figura, o terceiro ponto de interseção é o próprio Q .



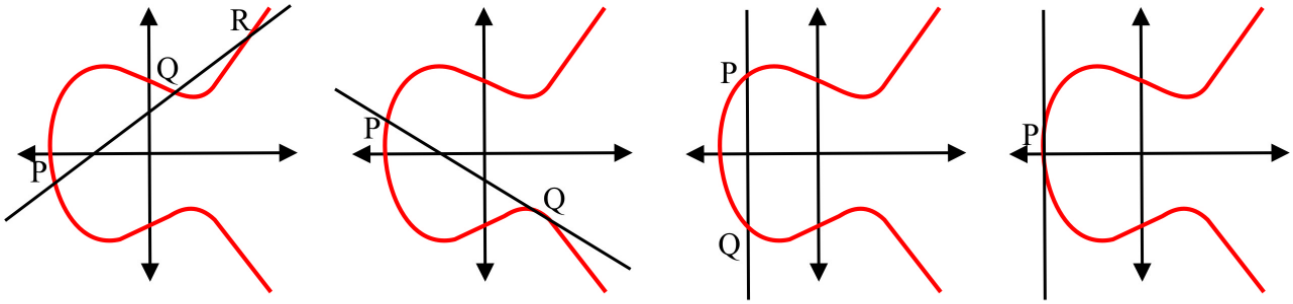
Se a reta que passa por P e Q é vertical, então definimos o terceiro ponto de interseção como o “ponto no infinito”. Essa noção de ponto no infinito é importante para podermos definir o grupo dos pontos na curva. Esse ponto ocupa o papel do 0 (elemento neutro) do grupo.

Dessa forma, toda reta vertical (paralela ao eixo y) passa pelo ponto no infinito. As figuras, a seguir, mostram os dois casos em que o terceiro ponto de interseção é o ponto no infinito.



Podemos, assim, definir uma operação de soma ($+$) nos pontos da curva da seguinte forma: consideramos o ponto no infinito como o elemento neutro 0 da soma e dizemos que $P+Q+R=0$, quando P , Q e R são pontos da curva e estão em uma mesma reta.

Nas quatro figuras anteriores, temos as seguintes somas:



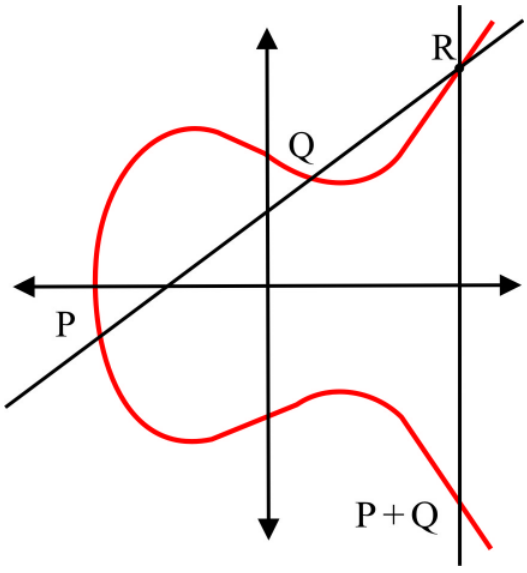
(Fonte: http://en.wikipedia.org/wiki/Elliptical_curve. Acesso em: 25 ago. 2005)

Desse modo, se P , Q e R estão na mesma reta, então $P+Q+R=0$, ou seja, $R=-(P+Q)$.

Caso $R_1 e R_2$ estejam em uma reta vertical, então $R_1+R_2+0=0$, ou seja, $R_2=-R_1$. O resultado é que, dados pontos P e Q , para encontrar o ponto $P+Q$ devemos traçar a reta que passa por P e Q .

O terceiro ponto de interseção com a curva é o ponto $R=-(P+Q)$. Em seguida, traçamos a vertical que passa por R . O ponto em que essa vertical corta a curva é o ponto $-R=P+Q$.

Veja na figura a seguir:



Agora que definimos a soma de dois pontos P e Q, podemos definir $k \cdot P$, para k inteiro positivo, como a soma $P+P+\ldots+P$ com k fatores.

Assim:

$$2\mathrm{P} = P + P$$
$$3\mathrm{P} = P + P + P$$

e assim por diante.

Esse mesmo grupo pode ser definido algebricamente. Não é difícil encontrar uma fórmula que, dadas as coordenadas dos pontos P e Q, forneça as coordenadas do ponto $P+Q$.

Agora que possuímos um grupo para pontos de uma curva elíptica, vamos voltar à nossa criptografia.

Texto 65 – Criptografia de Curvas Elípticas

No texto anterior, definimos uma operação de soma para pontos de uma curva elíptica. Em criptografia usam-se curvas elípticas definidas sobre corpos finitos.

Uma curva elíptica E, definida sobre um corpo finito $GF(q)$, é dada por uma equação não-singular $y^2 = x^3 + a\,x + b$, em que $a, b \in GF(q)$. Aqui, o interesse está no conjunto dos pontos (x, y) da curva com $x, y \in GF(q)$. Esse conjunto, com a operação de soma de pontos que definimos, forma um grupo.

Como você se recorda, os sistemas criptográficos de chave pública de Diffie-Hellman, ElGamal, algoritmo de assinatura digital (DSA), entre outros, utiliza um grupo cíclico G. A segurança desses sistemas está na dificuldade do problema do logaritmo discreto. Recordando, este problema é o seguinte: dados o grupo cíclico G e um gerador g deste grupo, e dado $h = g^x$, como calcular x.

Seja agora P um ponto de uma curva elíptica E, definida sobre um corpo finito $GF(q)$.

Lembre-se que definimos:

$$2\mathrm{P} = P + P,$$
$$3\mathrm{P} = P + P + P$$
etc.

Ou seja, definimos uma operação $k \cdot P$ para qualquer k inteiro.

Como estamos trabalhando em um corpo finito, na seqüência $P, 2\mathrm{P}, 3\mathrm{P}, \ldots, kP$, em algum momento, existirão elementos repetidos, pois há apenas um número finito de pontos (x, y) possíveis.

Dessa forma, temos $iP = jP$, para $i \neq j$, o que mostra que $(i-j) \cdot P = 0$. O menor n tal que $n \cdot P = 0$ é a ordem do ponto P no grupo dos pontos da curva.

Isso resulta que o conjunto

$$\{P, 2\mathrm{P}, 3\mathrm{P}, \ldots, (n-1)P, nP\}$$

é um grupo cíclico de ordem n gerado por P.

Em aplicações criptográficas, um grupo como este é utilizado no lugar dos subgrupos cíclicos de $\mathbb{Z}_n^*$, que são usados nos sistemas de chave pública tradicionais.

O problema do logaritmo discreto para curvas elípticas é o seguinte: dados pontos P e $Q = k \cdot P$ em uma curva elíptica sobre um corpo finito, como determinar o valor do inteiro k ? Acredita-se que esse problema seja mais complexo que o do logaritmo discreto.

Ao utilizar o grupo de uma curva elíptica, podemos formular sistemas de chave pública com curvas elípticas modificando os sistemas usuais.

O sistema de troca de chaves de Diffie-Hellman, com o uso de curvas elípticas, funciona da seguinte maneira:

1. Alice e Bob escolhem uma curva elíptica E e um ponto P de E . Esta informação não é secreta.

2. Alice escolhe, aleatoriamente, um inteiro k_A e envia o ponto $k_A \cdot P$ para Bob. O inteiro

k_A é a chave secreta de Alice, enquanto que o ponto $k_A \cdot P$ é sua chave pública.

3. Bob escolhe, de forma aleatória, um inteiro k_B e envia o ponto $k_B \cdot P$ para Alice.

4. Alice calcula o ponto $k_A(k_B P) = (k_A \cdot k_B) P$. Esse ponto é a chave secreta combinada entre os dois.

5. Bob calcula o ponto $k_B(k_A P) = (k_A \cdot k_B) P$.

Realizar as operações necessárias para os cálculos citados anteriormente — soma de pontos em curvas elípticas — é um processo mais lento do que efetuar a exponenciação módulo um primo, que é a operação utilizada nos sistemas tradicionais.

No entanto, como o problema do logaritmo discreto para curvas elípticas é mais complexo, o mesmo nível de segurança pode ser conseguido com uma chave menor.

> Uma chave menor implica em operações mais rápidas, o que na prática compensa a maior complexidade das operações.

A mesma adaptação simples, vista anteriormente, do sistema de Diffie-Hellman para usar curvas elípticas pode ser feita com outros sistemas de chave pública.

> Essencialmente todo sistema de chave pública pode ser adaptado para o uso de curvas elípticas. Basta substituir a operação de exponenciação módulo p por soma de pontos em um grupo cíclico de uma curva elíptica.

Assim, há versões para curvas elípticas dos algoritmos ElGamal, Diffie-Hellman e para o RSA. Existem também vários algoritmos utilizados para assinatura digital que usam curvas elípticas.

Por sua complexidade, vários detalhes na implementação destes sistemas não serão discutidos neste momento. Como exemplo, as escolhas da curva elíptica E e do ponto P devem atender à exigência de que P tenha como ordem um primo grande.

Em fevereiro de 2005, a agência de segurança americana NSA (National Security Agency) anunciou a adoção da criptografia de curva elíptica como parte dos padrões de segurança do governo norte-americano.

A NSA adotou um conjunto de sistemas criptográficos que foi chamado de Suite B . Nesse modelo consta:

1. Um algoritmo de troca de chaves denominado Menezes-Qu-Vanstone de curva elíptica (ECMQV). Na sigla, as iniciais EC vêm de Elliptic Curve.

2. O algoritmo de troca de chaves Diffie-Hellman de curva elíptica (ECDH).

3. O algoritmo de assinatura digital de curva elíptica (ECDSA - Elliptic curve digital signature algorithm).

4. O algoritmo simétrico AES.

5. A função de Hash SHA (secure hashing algorithm).

Na última aula desta disciplina, abordamos um ponto bastante recente e importante da criptografia de chave pública: o uso de curvas elípticas.

O uso de curvas elípticas permite um grau muito maior de segurança para chaves de mesmo tamanho que os sistemas de chave pública usuais. Dessa forma, oferece a mesma segurança que os sistemas usuais, mas com a utilização de chaves menores, o que favorece implementações mais rápidas destes algoritmos.

A matemática envolvida, como você deve ter notado, é mais complexa que a matemática do RSA e dos sistemas baseados no problema do logaritmo discreto (como Diffie-Hellman e ElGamal). Vários tópicos relacionados aos assuntos abordados nesta aula são focos de ativas pesquisas matemáticas atuais.

Enfim, o assunto é complexo. O importante é compreender o que é uma curva elíptica e como elas são utilizadas nos modernos sistemas criptográficos de chave pública.

Há ainda outras aplicações das curvas elípticas que interessam à criptografia, como algoritmos de fatoração de inteiros.

Atividades

1) Defina curva elíptica.

2) Como se define a operação de soma de pontos em uma curva elíptica? Qual é o zero desta soma?

3) Como o grupo dos pontos de uma curva elíptica é usado em sistemas criptográficos?

4) Quais são as vantagens do uso de sistemas criptográficos de curvas elípticas?

Complemente seu estudo

Leituras

Na última aula, você estudou as curvas elípticas. Para saber mais sobre este tema e sua utilização em criptografia, indicamos duas interessantes referências.

- HANKERSON, Darrel; MENEZES, Alfred J.; VANSTONE, Scott. **Guide to elliptic curve cryptography**. Berlim: Springer Verlag, 2004.

- WASHINGTON, Lawrence C. **Elliptic curves:** number theory and cryptography. Boca Raton, FL.: Chapman & Hall/CRC, 2003.

Website

Há implementações de muitos algoritmos criptográficos com código aberto disponível na internet. A biblioteca de programas “Crypto++” possui implementação de diversos algoritmos simétricos e assimétricos, incluindo algoritmos de curvas elípticas. Para acessar esses programas, o endereço é http://www.eskimo.com/~weidai/cryptlib.html .

Soluções das atividades

Aula 1

1) $D(10)=\{\pm1,\pm2,\pm5,\pm10\} \subset \{\pm1,\pm2,\pm4,\pm5,\pm10,\pm20\}=D(20)$

2) 3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31. É interessante que não se sabe se há infinitos primos gêmeos.

3) Há o caso 3, 5 e 7. É o único caso possível, pois dados 3 inteiros n, n+2 e n+4 é fácil ver que um deles deve ser múltiplo de 3.

4) 4 = 2+2, 6 = 3+3, 8 = 3+5, 10 = 5+5 etc. Um dos problemas não-resolvidos mais antigos na Teoria dos Números é a chamada conjectura de Goldbach, que afirma que todo inteiro par pode ser escrito como soma de dois primos. Esta conjectura foi proposta em 1742, em uma carta de Goldbach para Euler.

Aula 2

1) a) q = 2e r = 11
   b) q = -2 e r = 6
   c) q = 1 e r = 75

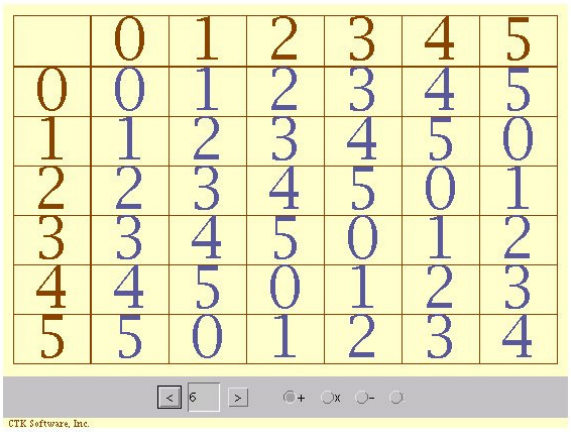
2)
   a) $mdc(35,12)=1 \ \ e \ \ mmc(35,12)=420.$
   b) $mdc(-30,18)=6 \ \ e \ \ mmc(-30,18)=90.$
   c) $mdc(315,250)=5 \ \ e \ \ mmc(315,250)=15750.$

Aula 3

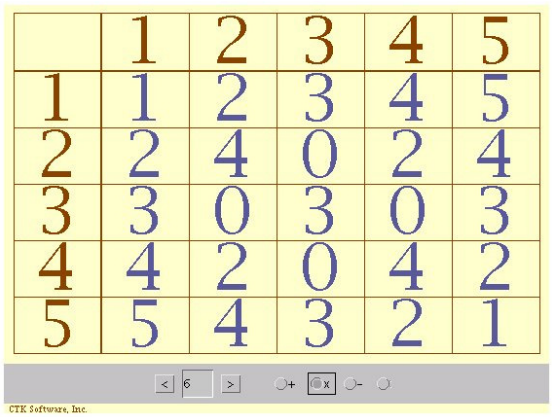
1) a) $mdc(a,b)=7$ e $mmc(a,b)=11011$
   b) $mdc(a,b)=33$ e $mmc(a,b)=17325$

Aula 6

1) As tabelas são as seguintes:



	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4



	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

2) Um inteiro a é divisível por 8 se, e somente se, o número formado por seus três últimos algarismos for divisível por 8.

3)

a) O resto da divisão de 2^{303} por 15 é 8.

b) O resto da divisão de 7^{250} por 48 é 1.

c) O resto da divisão de 5^{61} por 7 é 5.

Aula 7

1) $\mathbb{Z}_9^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$, $\mathbb{Z}_{20}^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{17}, \bar{19}\}$.

2)

a) A equação $3x \equiv 8 \, mod \, 15$ não tem solução, pois $mdc(3,15) = 5 \nmid 8$.

b) A equação $2x \equiv 20 \, mod \, 32$ tem duas soluções, porque $mdc(2,32) = 2 | 20$. As soluções são $x \equiv 10 \, mod \, 32$ e $x \equiv 26 \, mod \, 32$.

c) A equação $5x \equiv 7 \, mod \, 11$ possui uma única solução, pois $mdc(5,11) = 1$. A solução é $x \equiv 9 \, mod \, 11$.

3)

a) $a = 35 \;\; e \;\; b = 65$; $mdc(35,65) = 5$ e $2 \cdot 35 - 1 \cdot 65 = 5$.

Aula 4

1) a) 229 é primo. Como curiosidade, é o 50º primo.
b) 1223 é primo. Este é o 200º primo.
c) 481 não é primo (é divisível por 13).

2) $\pi(200)=46.$

Aula 5

1)

1. R_1 é relação de equivalência: é reflexiva, simétrica e transitiva. É a relação de igualdade.
2. R_2 não é reflexiva, não é simétrica, mas é transitiva.
3. R_3 é reflexiva, não é simétrica e não é transitiva.
4. R_4 não é reflexiva, é simétrica e não é transitiva.
5. R_5 é reflexiva, não é simétrica, mas é transitiva.

2)

a) Verdadeira.
b) Verdadeira.
c) Falsa.
d) Verdadeira.
e) Verdadeira.

b) $a=15 \ e \ b=23$; $mdc(15,23)=1$ e $-3\cdot 15+2\cdot 23=1$.

4) A inversa de 45 módulo 91 é 89 .

Aula 8

1)
a) 16
b) 12
c) 4

2) $x^2+y^2-8z=6 \Rightarrow x^2+y^2\equiv 6 \, mod \, 8.$ Verifique que não há inteiros x e y , tais que $x^2+y^2\equiv 6 \, mod \, 8.$

Aula 9

1) $4^{14}=\left(4^2\right)^7=16^7\equiv 1 \ (mod \, 15)$

2) $7^{24}=\left(7^2\right)^{12}=49^{12}\equiv(-1)^{12}\equiv 1 \ (mod \, 15)$

3) Temos que calcular $3^{90} \ (mod \, 91).$ Sabemos que $3^4=81\equiv -10 \ (mod \, 91).$
Multiplicando essa congruência por 3^2 obtemos $3^6\equiv -90\equiv 1 \ (mod \, 91).$
Logo $3^{90}=\left(3^6\right)^{15}\equiv 1 \ (mod \, 91)$.

4) Como $24=2^3\cdot 3$, temos que calcular as três potências 7^3 , $7^{2\times 3}$ e $7^{2^2\times 3}$ módulo 25.

Temos:

$$7^3=7\cdot 7^2=7\cdot 49\equiv 7\cdot(-1)\equiv -7 \ (mod \, 25).$$
$$7^{2\times 3}=\left(7^3\right)^2\equiv(-7)^2\equiv 49\equiv -1 \ (mod \, 25).$$
$$7^{2^2\times 3}=7^{2\times 2\times 2}=\left(7^{2\times 3}\right)^2\equiv(-1)^2\equiv 1 \ (mod \, 25).$$

Logo 25 é pseudoprimo forte para a base 7.

Aula 10

1)

a) $\phi(90)=24$

b) $\phi(250)=100$

c) $\phi(1620)=432$

3)

a) o resto é 17.

b) o resto é 11.

Aula 11

1) $x \equiv 67 \pmod{165}$.

2) $x \equiv 85 \pmod{630}$.

3) $x \equiv 41 \pmod{168}$

Aula 12

1) Temos $n=143=11\cdot 13$. Então $\phi(n)=\phi(11\cdot 13)=\phi(11)\phi(13)=10\cdot 12=120.$ Como $e=23$, a chave privada d é a inversa de 23 módulo 120 que é 47 (use o algoritmo de Euclides estendido).

A mensagem original é $P=C^d=2^{23} \bmod 143=85 \bmod 143$.

Aula 13

1) Como $\phi(18)=6$. As raízes primitivas módulo 18 os inteiros que têm ordem 6 módulo 18.

Calculando as ordens, obtemos:

- a ordem de 1 módulo 18 é 1.
- a ordem de 5 módulo 18 é 6.

- a ordem de 7 módulo 18 é 3.
- a ordem de 11 módulo 18 é 6.
- a ordem de 13 módulo 18 é 2.
- a ordem de 17 módulo 18 é 2.

Assim, as raízes primitivas módulo 18 são 5 e 11.

2)

a) a ordem de 3 módulo 8 é 2.

b) a ordem de 5 módulo 16 é 4.

c) a ordem de 7 módulo 20 é 4.

3)

x	1	2	3	4	5	6	7	8	9	10	11	12
$ind_{2,13}(x)$	0	1	4	2	9	5	11	3	8	10	7	6

Aula 14

1) Basta verificar que $3^{30} \equiv 1 \ mod \ 31$ e que nenhuma das potências $3^{\frac{30}{2}} = 3^{15}$, $3^{\frac{30}{5}} = 3^{6}$ e $3^{\frac{30}{3}} = 3^{10}$ é congruente a 1 módulo 31. Verifique que $3^{15} \equiv 30 \ mod \ 31$, $3^{6} \equiv 16 \ mod \ 31$ e $3^{10} \equiv 25 \ mod \ 31$.

2) A combinação de chaves se dará da seguinte forma: Alice envia $5^{9} \equiv 11 \ mod \ 23$ para Bob. Este envia $5^{7} \equiv 17 \ mod \ 23$ para Alice. Para calcular a chave secreta, Alice faz $17^{9} \equiv 7 \ mod \ 23$, enquanto Bob faz $11^{7} \equiv 7 \ mod \ 23$. A chave combinada é 7.

Aula 15

1) Uma curva elíptica é uma curva dada por uma equação $y^2 = x^3 + a\,x + b$, em que $4\,a^3 + 27\,b^2 \neq 0$.

2) Dados pontos P e Q . O ponto $P + Q$ é obtido da seguinte forma: traçamos a reta que

passa por P e Q . Esta reta corta a curva em um terceiro ponto R (caso a reta seja tangente à curva, o ponto de tangência é contado duas vezes). Traçamos a reta vertical passando por R . O outro ponto onde esta vertical corta a curva é o ponto $P+Q$.

3) Em sistemas criptográficos que usam o problema do logaritmo discreto, este é substituído pelo problema do logaritmo discreto para curvas elípticas: dada uma curva elíptica E , dados pontos P e Q em E , sendo $Q=k\cdot P$, encontrar o valor de k .

4) Sistemas criptográficos de curvas elípticas oferecem o mesmo nível de segurança que sistemas usuais utilizando chaves significativamente menores.

Referências

Livros e publicações

COUTINHO, S.C. **Números inteiros e criptografia RSA**. Rio de Janeiro: IMPA/SBM, 1997.

KOBLITZ, Neal. **Algebraic aspects of cryptography**. 2.ed. Berlim: Springer Verlag, 1999.

MENEZES, A. J. et al. **Handbook of applied cryptography**. Boca Raton, FL.: CRC Press, 1997.

SANTOS, José Plínio de O. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, 1998.

STALLINGS, William. **Cryptography and network security:** principles and practice. 2.ed. N. Jersey: Prentice Hall, 1999.

Websites

Elliptic curve. **Math World.** Disponível em: <http://mathworld.wolfram.com>. Acesso em 25 ago. 2005.

Elliptic curve. **Wikipédia, enciclopédia livre.** Disponível em: <http://en.wikipedia.org/wiki/Elliptical_curve>. Acesso em 25 ago. 2005

Paul Erdös. **Wikipédia, enciclopédia livre.** Disponível em:<http://pt.wikipedia.org/wiki/Paul_Erd%C3%B6s>. Acesso em 24 ago. 2005.

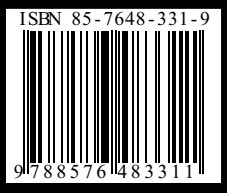
Universidade de Lisboa. Departamento de Educação. Faculdade de Ciências. **Página dos Números Primos**. Disponível em: <http://www.educ.fc.ul.pt/icm/icm98/icm12/Mat_kz.htm#Marin%20Mersenne>. Acesso em 25 ago. 2005.

Autor

Luiz Manoel Silva de Figueiredo

Professor adjunto da Universidade Federal Fluminense (UFF), onde leciona desde 1992. Bacharel em Física pela Universidade Federal do Rio de Janeiro (UFRJ), o prof. Luiz Manoel Figueiredo é Mestre em Matemática pelo Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, e Doutor em Matemática pela University of Cambridge (Reino Unido). Sua área de doutorado é em teoria dos números e atualmente trabalha com Criptografia.

ISBN 85-7648-331-9



UENF
Universidade Estadual
do Norte Fluminense

UERJ
UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO

Universidade Federal Fluminense
uff

UNIVERSIDADE DO BRASIL

Universidade Federal Rural
do Rio de Janeiro

UNIRIO

FAPERJ
Fundação Carlos Chagas Filho de Amparo
à Pesquisa do Estado do Rio de Janeiro

GOVERNO DO
Rio de Janeiro
SECRETARIA DE
CIÊNCIA E TECNOLOGIA

UAB
UNIVERSIDADE
ABERTA DO BRASIL

Ministério
da Educação

BRASIL
UM PAÍS DE TODOS
GOVERNO FEDERAL