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.

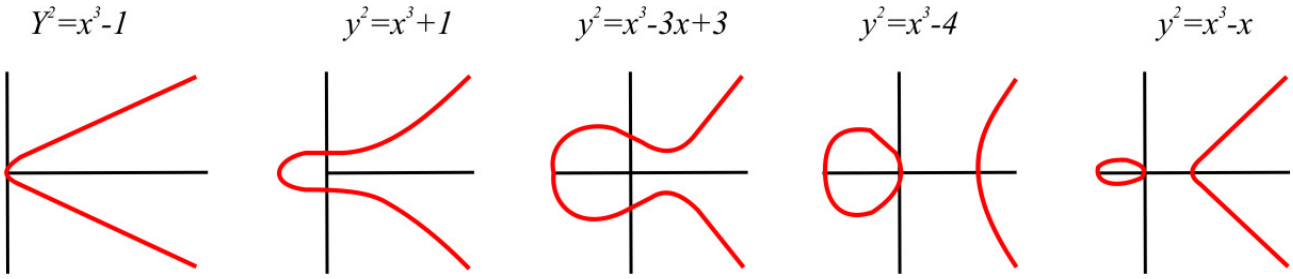
Pode-se mostrar que uma curva dada pela equação $y^2 = x^3 + ax + b$ é não-singular se, e somente se, o valor de

$$\Delta = 4\mathrm{a}^3 + 27\mathrm{b}^2$$

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 $-x$).

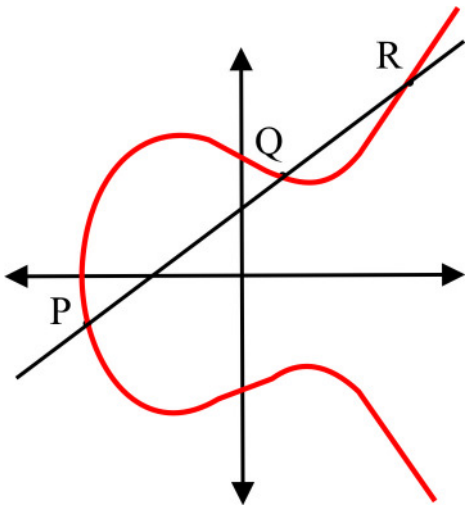
Nos sistemas criptográficos de Diffie-Hellman e ElGamal, há uma escolha inicial de um grupo cíclico G. Uma implementação simples desses sistemas usa $G=\mathbb{Z}_p^*$ ou um subgrupo cíclico dele. Os sistemas criptográficos de curva elíptica utilizam como grupo G o grupo dos pontos da curva.

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.

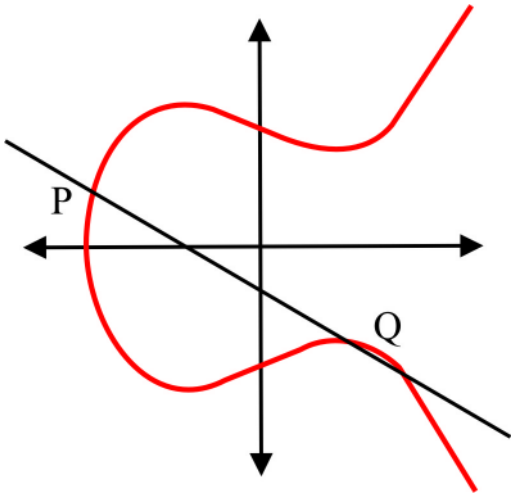
Observe a figura a seguir.



Se a reta que passa por P e Q for tangente à curva em algum dos pontos, esse será

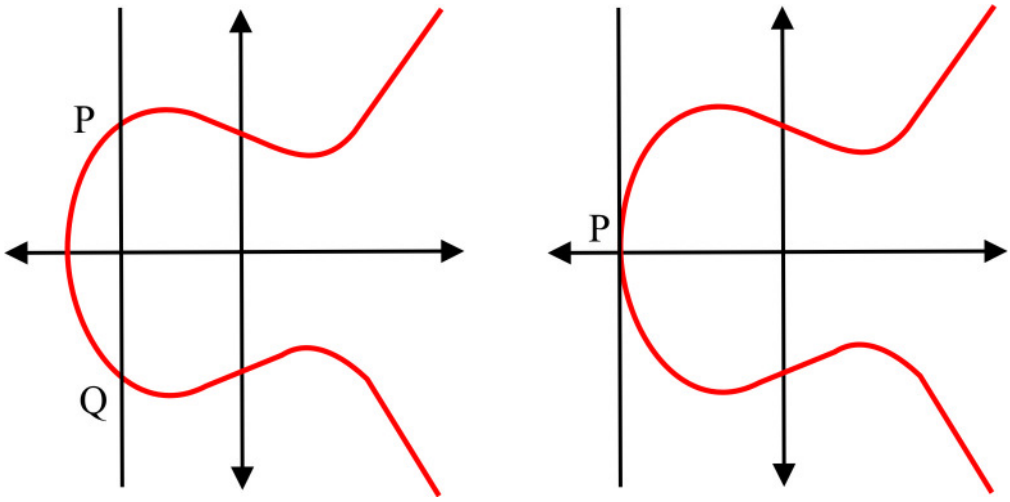
considerado o terceiro ponto de interseção R .

Na próxima figura, o terceiro ponto de interseção é o próprio Q .



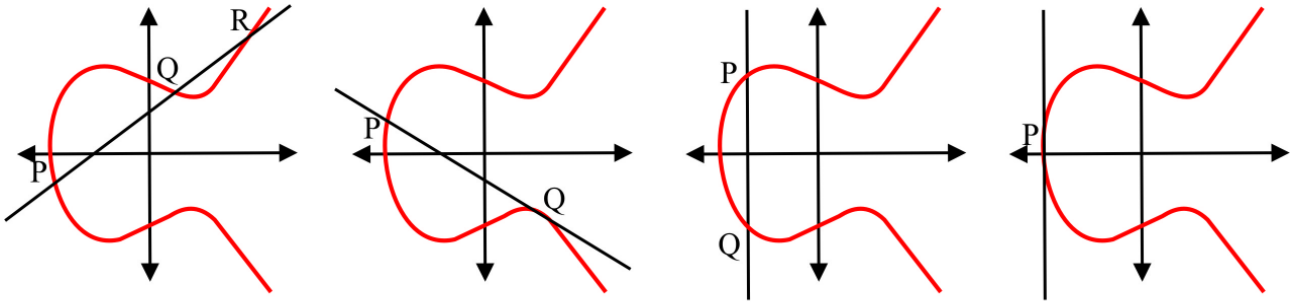
Se a reta que passa por P e Q é vertical, então definimos o terceiro ponto de interseção como o “ponto no infinito”. Essa noção de ponto no infinito é importante para podermos definir o grupo dos pontos na curva. Esse ponto ocupa o papel do 0 (elemento neutro) do grupo.

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:



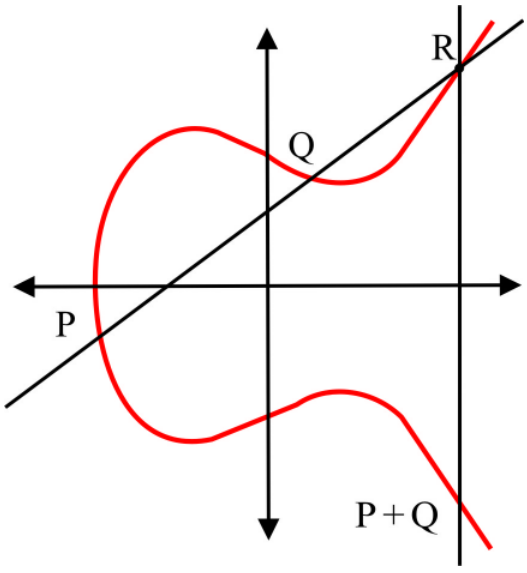
(Fonte: http://en.wikipedia.org/wiki/Elliptical_curve. Acesso em: 25 ago. 2005)

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

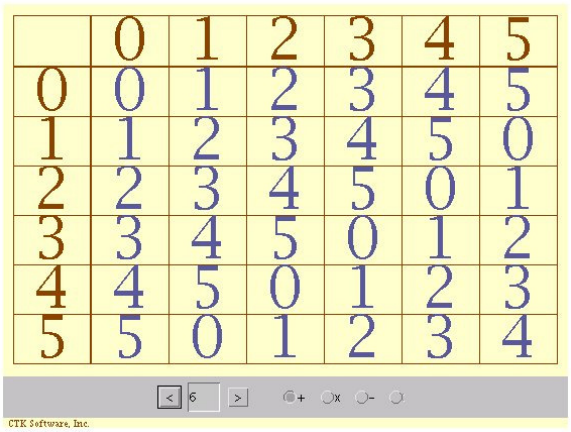
2)
   a) $mdc(35,12)=1 \ \ e \ \ mmc(35,12)=420.$
   b) $mdc(-30,18)=6 \ \ e \ \ mmc(-30,18)=90.$
   c) $mdc(315,250)=5 \ \ e \ \ mmc(315,250)=15750.$

Aula 3

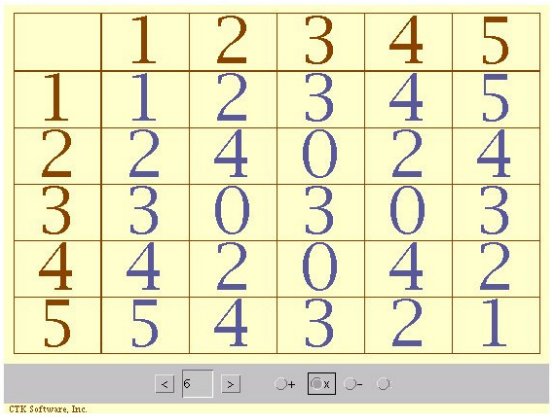
1) a) $mdc(a,b)=7$ e $mmc(a,b)=11011$
   b) $mdc(a,b)=33$ e $mmc(a,b)=17325$

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.

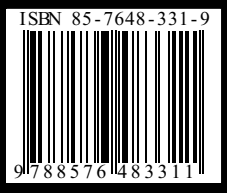
Universidade de Lisboa. Departamento de Educação. Faculdade de Ciências. **Página dos Números Primos**. Disponível em: <http://www.educ.fc.ul.pt/icm/icm98/icm12/Mat_kz.htm#Marin%20Mersenne>. Acesso em 25 ago. 2005.

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