Introdução à Algebra para Criptografia de Curvas Elipticas

Pedro Antonio Dourado de Rezende

Departamento de Ciência da Computação

Universidade de Brasilia

Abril 2003

ECC – Introdução: Grupos 1

Simbologia:

$\in$: pertencente a; $\forall$: para todo; $\exists$: existe; !: único

Definição: Grupo algébrico (G, •):

- G : conjunto de elementos contendo elemento neutro "e";
- • : operação binária inversível e associativa sobre G

[G1] *El. neutro*: $\exists\, e \in G\ \forall a \in G\ [\, a \bullet e = e \bullet a = a \,]$

[G2] *Inversível*: $\forall a \in G\ \exists\, x \in G\ [\, a \bullet x = e \,]$

[G3] *Associativa*: $\forall a, b, c \in G\ [\, a \bullet (b \bullet c) = (a \bullet b) \bullet c \,]$

Exemplos:

(Z , +); Z = {**...**-2, -1, 0, 1, 2 **...**}; e = 0; + adição de n. inteiros

(Q^*, *); Q^* = Q-{0}; Q = {n. racionais}; e = 1; * multiplicação

ECC – Introdução: Grupos 2

Definição: Grupo Abeliano

(G, •) é dito Abeliano se • for comutativa.

Comutatividade: $\forall a, b \in G \; [\, a \bullet b = b \bullet a \,]$

Nomeclatura: Usa-se representar • por "+" ou por "*"

Notação aditiva: (G, +) quando convém e G é abeliano

Notação multiplicativa: (G, *) quando convém

Inverso único: Decorre dos aximomas de grupo

$\forall a \in G \; \exists! \; x \in G \; [\; x \bullet a = a \bullet x = e \,]$

Em notação aditiva: $x = -a$; $(-a) + a = a - a = 0$

Em n. multiplicativa: $x = a^{-1}$; $(a^{-1}) * a = a a^{-1} = 1$

ECC – Introdução: Grupos 2

Exemplos úteis à criptografia:

$(Z_q, +)$; $Z_q = \{0, 1, 2, ...q\text{-}1\}$; $+$ = adição modulo $q \in Z$

$(Z_q^*, *)$; $Z_q^* = \{1, 2, ...q\text{-}1\}$; $*$ = multiplicação mod q

Aritmética Modular: mod q = resto da divisão inteira por q

$\forall q \in Z$ [$(Z_q, +)$ é grupo, $(Z_q^*, *)$ é grupo $\Leftrightarrow$ q é *primo*]

Z_7^*

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Z_8^*

*	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

* mod q satisfaz [G2] sobre Z_q^* se q = 7, mas não se q = 8

ECC – Introdução: Grupos 4

Divisão inteira: $d \mid b \Leftrightarrow \exists\, y\ [\ d*y = b\ ]$ (diz-se d *divide* b)

$\text{mdc}(a, b) = \max d\ [\ d \mid a, d \mid b\ ] =$ *max. divisor comum* de a e b

Propriedade da aritmética modular: Dados $(Z_q^*, *)$, $a \in Z_q^*$

a é *inversível* em $Z_q^* \Leftrightarrow \text{mdc}(a, q) = 1$ (a, q são *co-primos*)

a *divide zero* em $Z_q^* \Leftrightarrow \text{mdc}(a, q) \neq 1$ ($\exists\, y \in Z_q^*\ [\ a*y = 0\ ]$)

Z_7^*

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Z_8^*

*	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

$5^{-1} = 3 \bmod 7$; $4^{-1} = 2 \bmod 7$

$5^{-1} = 5 \bmod 8$; $4*2 = 0 \bmod 8$

ECC – Introdução: Grupos 5

Notação escalar:

Dados $a \in (G, \bullet)$, $n \in Z$; denota-se $a \bullet a \bullet \ldots \bullet a$ (n vezes)

Em notação aditiva: $a + a + \ldots + a = n \cdot a$ (mult. P/ escalar)

Em n. multiplicativa: $a * a * \ldots * a = a^n$ (exponenciação)

Observação:

Mesmo em estruturas distintas (G e Z), o sinal "-" comuta

Em notação aditiva: $(-n) \cdot a = n \cdot (-a)$; $0_Z \cdot a = 0_G$

Em n. multiplicativa: $a^{(-n)} = (a^{-1})^n$; $a^0 = 1_G$

Definição: ordem

$|G| = \#G =$ número de elementos de G (ordem de G)

$ord_G(a) = \text{Min } n>0 [\, n \cdot a = 0 \text{ (ou } a^n = 1) \,]$ (ou ∞ se não $\exists$ n)

ECC – Introdução: Grupos 6

Definições: gerador, grupo cíclico

$\langle g \rangle_G = \{ g^n \in G, n \in Z \}$ = subgrupo de G gerado por g

g é *gerador de* G se $\langle g \rangle_G = G$. Neste caso G é *cíclico,* $G = C_{|G|}$

Fatos: $\#\langle g \rangle_G \mid \#G$; Cíclico $\Rightarrow$ abeliano; nem todo G é cíclico.

Exemplos:

Seja $G = (Z_{23}^*, *)$; Então $\langle 5 \rangle_G = G$; $|\langle 2 \rangle_G| = 11$

$\langle 2 \rangle_G = \{2^n \bmod 23\} = \{ 1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$

Distributividade comutativa: (generalizando espaços vetoriais)

Dado (G, +) abeliano, a mult. escalar "•" de Z em G satizfaz:

[P1]: $(n +_Z m)\cdot a = n\cdot a +_G m\cdot a$; [P2]: $n\cdot(a +_G b) = n\cdot a +_G n\cdot b$

[P3]: $m\cdot(n\cdot a) = (m *_Z n)\cdot a$; [P4]: $m\cdot(n\cdot a) = n\cdot(m\cdot a)$

ECC – Anéis 1

Observações:

1- Se (G, +) for dado em termos de (Z , +), em [P1-P4] podemos identificar "$\cdot$" com "$*_Z$" e "$+_Z$"com "$+_G$" obtendo:

[A1]: $(n + m)\cdot a = n\cdot a + m\cdot a$; [A2]: $n\cdot(a + b) = n\cdot a + n\cdot b$

[A3]: $m\cdot(n\cdot a) = (m\cdot n)\cdot a$; [A4]: $m\cdot(n\cdot a) = n\cdot(m\cdot a)$

2- Em particular, se G = (Z , +) temos (Z , +, $\cdot$).

A comutatividade de $+_G$ é exigida em [A2], e a de "$\cdot$" em [A4].

(Z -{0}, $\cdot$) não é grupo, pois "$\cdot$" não é inversível em Z [G2]

Definição: Anel (generalizando a estrutura de Z)

(A, +, $\cdot$) satisfazendo [A1-A3], é chamado de *Anel (ring)*

(A, +, $\cdot$) satisfazendo [A1-A4] é um *anel comutativo.*

ECC – Anéis 2

Exemplos de anéis (A, +, ·)

1- $Z = \{...-2, -1, 0, 1, 2 ...\}$; + : adição; · : multiplicação.
obs: $N = \{0, 1, 2 ...\} \subseteq Z$ não é anel ($+_N$ não é inversível)

2-Q = {n. racionais}; R = {n. reais} ; C = {n. complexos}

3- $Z_q = \{0, 1, 2, ...q-1\} = \{n \bmod q , n \in Z \}$; + mod q; · mod q.

4- $M_{nxn}[A] = \{[a_{i,j}] , a_{i,j} \in A, 0 \geq i, j \geq n \in N \}$; A anel, etc.,
$M_{nxn}[A]$ é o *anel das matrizes nxn sobre* A,

5- $A[X] = \{ f(X) = a_nX^n + ... + a_1X + a_0 ; n \in N , a_n,..,a_o \in A, a_n \neq 0 \}$
A anel, X variável; $+_{A[X]}$ adição e $\cdot_{A[X]}$ mult. de polinômios,
A[X] é o *anel dos polinômios em X sobre* A, n = *grau* de f

ECC – Anéis 3

Definição: D.I.

A é *Domínio de Integridade* $\Leftrightarrow \forall a,b \in A\ [a \cdot b = 0 \Rightarrow a \text{ ou } b = 0]$

Exemplos: Z é D.I.; Z_q é D.I. $\Leftrightarrow$ q é primo

A é D.I. $\Rightarrow$ A[X] é D.I.; $n>1 \Rightarrow M_{nxn}[Z]$ não é D.I.

Definições: D.F.U., Corpo (generalizando a divisão inteira)

1- Dado D.I. A, $u \in A$ é *inversível* se $u \mid 1$ $[\ \exists u^{-1},\ 1 = u \cdot u^{-1}\ ]$

$p \in A$ é *irredutível* se $\forall u \in A\ [\ u \mid p \Leftrightarrow$ u é inversível $]$

$p \in A$ é *primo* se $\forall a, b \in A\ [\ p \mid a \cdot b \Rightarrow p \mid a \text{ ou } p \mid b\ ]$

2- A é *Domínio de Fatoração Única (DFU)* se

$\forall a \in A^*\ [a = u \cdot p_1 \cdot p_2 \ldots \cdot p_n$, u inversível, p_i irred. e "únicos"$]$

3- A é *Anel de Divisão* se $(A^*,*)$ é grupo; se abeliano, A é *Corpo*

ECC – Anéis e Corpos 1

Exemplos de D.F.U.s, Corpos

1- Z é D.F.U. [$q \in Z$ é irredutível $\Leftrightarrow q \in Z$ é primo]

2-Q ,R , C , F_q são corpos, onde $\#F_q = q$ [q primo $\Rightarrow F_q \approx Z_q$]

3- F corpo $\Rightarrow$ F[X], F[X,Y], etc. são D.F.U.s

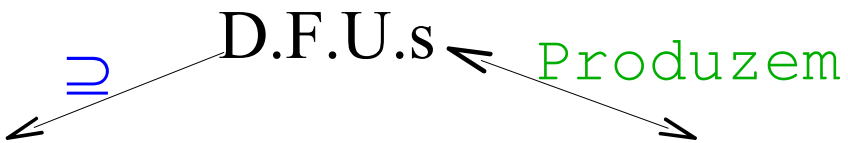
4- F corpo, $n>1 \Rightarrow U_{nxn}[F]$ é Anel de Divisão (não comutativo),
onde $U_{nxn}[F] = \{ [a_{i,j}] \in M_{nxn}[F],\ \det([a_{i,j}]) \neq 0 \}$

5- F corpo, $f = f(X) \in F[X]$ irred. $\Rightarrow$ F[X]/(f) é corpo
onde $F[X] / (f) = \{g \bmod f , g \in F[X] \}$; $+ \bmod f$; $\cdot \bmod f$

Notação: $F[X]/(f) = F[X] / f \cdot F[X]$; $Z_q = Z / q \cdot Z$,
$f \cdot F[X]$, $q \cdot Z$, $p \cdot A = \{ p \cdot a, a \in A \}$ *ideal* do anel A gerado por p

ECC – Anéis e Corpos 2

Resumo das definições algébricas:



Definições: Característica, Extensão

F corpo, $\text{char}(F) = \text{Min}\ \ n>0 \in N\ \ [\ n \cdot 1_F = 0\ ]$ (ou 0 se não $\exists$ n)

Fato 1: $\text{char}(F) \neq 0 \Rightarrow \text{char}(F) = p$ pimo (*característica* de F)

Fato 2: $\#F = p^m \Rightarrow \exists\ f \in Z_p[X]$ irred grau m. $[\ F \approx Z_p[X]/(f)\ ]$

Fato 3: Se α representa uma raiz de f(X) de grau m, i.e.,$f(\alpha) = 0$,
$\{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$ é uma base de F como e. vetorial sobre Z_p.

Notação: $Z_p[X]/(f) \approx Z_p(\alpha)$ dita a *extensão* de Z_p por α ($\approx: X \rightarrow \alpha$)

ECC – Anéis e Corpos 3

Exemplo de extensão de corpo finito:

f(X) irredutíveis de grau 2 sobre Z_3: X^2+1, X^2+X-1, X^2-X-1

Escolhendo $f(X) = X^2-X-1$ sobre Z_3 temos * de $Z_3[X] / (f)$ dado por

Z_3^*

*	1	2
1	1	2
2	2	1

F_9^*

* (f)	1	2	α	1+α	2+α	−α	1−α	2−α
1	1	2	α	1+α	2+α	−α	1−α	2−α
2	2	1	−α	2−α	1−α	α	2+α	1+α
α	α	−α	1+α	1−α	1	2−α	2	2+α
1+α	1+α	2−α	1−α	2				
2+α	2+α	1−α	1					
−α	−α	α	2−α					
1−α	1−α	2+α	2					
2−α	2−α	1+α	2+α					

Obs:

Em Z_3, $2 = -1$

Z_3 subcorpo de F_9

$Z_3[X]/(f) \approx Z_3(\alpha)$:

(EXERCÍCIO: completar a tabela, usando $\alpha^2-\alpha-1 = 0$)

ECC – Anéis e Corpos 4

Exemplo (cont):

Escolhido f(X) = X^2-X-1 sobre Z_3 e α rep. raiz de f (X), podemos também representar $Z_3(\alpha)$ como espaço vetorial sobre Z_3, $Z_3(\alpha) = Z_3 \times Z_3$, base $\{1, \alpha\}$ (onde $\alpha^2 = \alpha+1$). EXERCÍCIO: completar .

F_9^*

x	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
$1 \rightarrow$ (0,1)	(0,1)	(0,2)	(0,1)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
$2 \rightarrow$ (0,2)	(0,2)	(0,1)	(2,0)	(2,2)	(2,1)	(1,0)	(1,2)	(1,1)
$\alpha \rightarrow$ (1,0)	(1,0)	(2,0)	(1,0)	(2,1)	(0,1)	(2,2)	(0,2)	(0,2)
$1+\alpha \rightarrow$ (1,1)	(1,1)	(2,2)	(2,1)	(0,2)				
$2+\alpha \rightarrow$ (1,2)	(1,2)	(2,1)	(0,1)					
$-\alpha \rightarrow$ (2,0)	(2,0)	(1,0)	(2,2)					
$1-\alpha \rightarrow$ (2,1)	(2,1)	(1,2)	(0,2)					
$2-\alpha \rightarrow$ (2,2)	(2,2)	(1,1)	(0,2)					

ECC – Anéis e Corpos 5

Cont: A extensão escolhida para construir $F = Z_3(\alpha)$, onde $\alpha^2-\alpha-1 = 0$, permite ainda representar F via $<\alpha>_{F^*} = F^*$

$\alpha^1 = \alpha$; $\alpha^2 = \alpha+1$; $\alpha^3 = -\alpha+1$; $\alpha^4 = -1$;

$\alpha^5 = -\alpha$; $\alpha^6 = -\alpha-1$; $\alpha^7 = \alpha-1$; $\alpha^8 = \alpha^0 = 1$;

F_9^*

$< >$	α^0	α^4	α^1	α^2	α^7	α^5	α^3	α^6
$1 = \alpha^0 = \alpha^8$	1	α^4	α	α^2	α^7	α^5	α^3	α^6
$2 = \alpha^4$	α^4	1	α^5	α^6	α^3	α	α^7	α^2
$\alpha = \alpha^1$	α	α^5	α^2	α^3	1	α^6	α^4	α^7
$1+\alpha = \alpha^2$	α^2	α^6	α^3	α^{2+2}				
$2+\alpha = \alpha^7$	α^7	α^3	1					
$-\alpha = \alpha^5$	α^5	α	α^6					
$1-\alpha = \alpha^3$	α^3	α^7	α^4					
$2-\alpha = \alpha^6$	α^6	α^2	α^7					

ECC – Anéis e Corpos 6

Definição: **Primitividade, completude**

Se $\langle\alpha\rangle_{F(\alpha)^*} = F(\alpha)^*$; $F(\alpha) = F[X] / (f)$, f é *primitivo* em F[X]

F é dito *completo* se $\forall\ f \in F[X]$ [f irrdutível $\Rightarrow$ grau(f) = 1]

Exemplo:

$f = X^2+1$ é irred. em R[X], $R[X]/(f) \approx R(i) = C$ é completo.

Definição: Isomorfismo de anéis, corpos (etc.)

F e K são *isomorfos* ($F \approx K$) se $\exists\ \varphi: F. \rightarrow K$ satisfazendo:

1) $\forall a, b \in F$ [$\varphi(a \cdot_F b) = \varphi(a) \cdot_K \varphi(b)$; $\varphi(a +_F b) = \varphi(a) +_K \varphi(b)$]

2) $\varphi(f) = 1_K \Rightarrow f = 1_F$; $\varphi(f) = 0_K \Rightarrow f = 0_F$ [φ é bijetora]

ECC – Corpos

Fatos sobre Corpos Finitos

1- $\#F \in N \Rightarrow (F^*, *)$ é grupo cíclico.

2- $\#F = \#K \in N \Rightarrow F \approx K$. (justifica-se a notação F_q , $q = \#F$)

3- $F = F_q \Rightarrow q = p^m$ onde $p = \text{char}(F)$ é primo, $m > 0$, e

$F \approx Z_p[X]/(f)$ para qualquer f irred. de grau m Sobre Z_p

Definição: Corpos de Decomposição

Diz-se que F *decompõe* $f \in F[X]$ se todos os fatores irredutíveis de f em F[X] tem grau 1 (i.e., se F contém todas as raízes de f)

Observações:

F_q decompõe $X^q - X$; F é completo se decompõe todo $f \in F[X]$

ECC – Corpos e Criptografia

Fatos relevantes para a criptografia

1- F_q subcorpo de $F_r \Rightarrow q = p^m$, $r = p^n$ e $m \mid n$, $p = \text{char}(F_{q,,r})$

2- Z_p é subcorpo de F_q , $p = \text{char}(F_q)$, dito o *corpo primo* de F_q

3- Desconhece-se algoritmo eficiente p/ achar gerador de $(F_q^*, *)$

Observações:

1- Devido ao fato 3 acima, para se trabalhar com uma representação cíclica de F_q (via gerador de $(F_q^*, *)$ com q "grande"), busca-se f primitivo em $F_q[X]$.

2- A estrutura de qualquer F_q é determinada por $\#F_q = p^m$
Tal não ocorre com grupos (exceto #G primo), nem entre os abelianos: $C_2 \times C_2 \times C_2$, $C_2 \times C_4$, C_8 $(\# = 2^3)$ não são isomorfos

Próxima Leitura

- **Barreto, Paulo**

  “Curvas Elípticas e Criptografia:

  Conceitos e Algoritmos”

  http://planeta.terra.com.br/informatica/paulobarreto/ECC

Bibliografia

- **Koblitz, Neal**

  “A course in Number Theory and Cryptography”

  GTM 114, Springer-Verlag, 1994

- **Silverman, Joseph**

  “The Arithmetic of Elliptic Curves”

  GTM 106, Springer-Verlag, 1986