Teoria de números e corpos finitos

Gustavo Zambonin
Segurança em Computação (UFSC-INE5429)

(**1**) (a) O algoritmo de Euclides é um método eficiente para calcular o máximo divisor comum, ou *mdc*, de dois números inteiros. Baseia-se no princípio de que $mdc(a, b) = mdc(b, a \pmod b)$.

Demonstração. $a, b, q, r \in \mathbb{Z}$, $a \vee b \neq 0$ e $a = qb + r$ (Teorema da Divisão).
$mdc(a, b) \mid a \wedge mdc(a, b) \mid b \implies mdc(a, b) \mid (a - qb) = mdc(a, b) \mid r \implies mdc(a, b) \leq mdc(b, r)$.
$mdc(b, r) \mid b \wedge mdc(b, r) \mid r \implies mdc(b, r) \mid (qb + r) = mdc(b, r) \mid a \implies mdc(b, r) \leq mdc(a, b)$.
$mdc(a, b) \leq mdc(b, r) \wedge mdc(b, r) \leq mdc(a, b) \implies mdc(a, b) = mdc(b, r)$. □

É possível verificar que repetir essa computação diminuirá o número de maior ordem rapidamente, e o procedimento continuará equivalente, tomando o menor número e o resto da divisão anterior. Seja $a = 2147483647$ e $b = 541$:

$$
\begin{aligned}
2147483647 &= 541 \cdot 3969470 + 377 \\
541 &= 377 \cdot 1 + 164 \\
377 &= 164 \cdot 2 + 49 \\
164 &= 49 \cdot 3 + 17 \\
49 &= 17 \cdot 2 + 15 \\
17 &= 15 \cdot 1 + 2 \\
15 &= 2 \cdot 7 + 1 \\
2 &= 1 \cdot 2 + 0 \\
mdc(2147483647, 541) &= \mathbf{1}
\end{aligned}
$$

(b) De modo similar, o algoritmo de Euclides estendido computa todos os componentes desconhecidos da identidade de Bézout, ou seja, x, y e $mdc(a, b)$ em $ax + by = mdc(a, b)$. A inversa multiplicativa modular pode ser descoberta através da retro-substituição.

$$
\begin{aligned}
1 &= 2 - 1 \\
1 &= 2 - (15 - 7 \cdot 2) \\
1 &= 8 \cdot 2 - 15 \\
1 &= 8 \cdot (17 - 15) - 15 \\
1 &= 8 \cdot 17 - 9 \cdot 15 \\
1 &= 8 \cdot 17 - 9 \cdot (49 - 17 \cdot 2) \\
1 &= 26 \cdot 17 - 9 \cdot 49 \\
1 &= 26 \cdot (164 - 49 \cdot 3) - 9 \cdot 49 \\
1 &= 26 \cdot 164 - 87 \cdot 49 \\
1 &= 26 \cdot 164 - 87 \cdot (377 - 164 \cdot 2) \\
1 &= 200 \cdot 164 - 87 \cdot 377 \\
1 &= 200 \cdot (541 - 377) - 87 \cdot 377 \\
1 &= 200 \cdot 541 - 287 \cdot 377 \\
1 &= 200 \cdot 541 - 287 \cdot (2147483647 - 3969470 \cdot 541) \\
1 &= 1139238090 \cdot 541 - 287 \cdot 2147483647 \\
\mathbf{1139638090} &= 541^{-1} \pmod{2147483647} \\
\mathbf{257} &= 2147483647^{-1} \pmod{541}
\end{aligned}
$$

gustavo.zambonin@grad.ufsc.br src/

(**2**) (a) Um grupo G é um conjunto finito (ou infinito) de elementos equipados com uma operação binária[1]. Juntos, devem satisfazer algumas propriedades fundamentais:

i. associatividade: $\forall x, y, z \in G, (xy)z = x(yz)$.
ii. elemento de identidade: $\exists I \in G : Ix = xI = x, \forall x \in G$.
iii. elemento inverso: $\exists x^{-1} \in G : xx^{-1} = x^{-1}x = I, \forall x \in G$.

Um exemplo simples de grupo é o conjunto dos inteiros $\mathbb{Z}$ sobre a operação usual de adição, onde o elemento de identidade é chamado de zero, e os inversos são representados com um sinal negativo à frente do elemento. Um grupo onde sua operação binária é comutativa ($\forall x, y \in G, x + y = y + x$) é chamado de grupo abeliano.

(b) Um anel R é um conjunto de elementos equipados com duas operações binárias $(+, \cdot)$, geralmente interpretadas como adição e multiplicação, respectivamente. R é um grupo abeliano sobre a operação de adição, e satisfaz também as seguintes propriedades:

i. distributividade da multiplicação sobre adição à esquerda e à direita: $\forall x, y, z \in R, x \cdot (y + z) = (x \cdot y) + (x \cdot z) \wedge (y + z) \cdot x = (y \cdot x) + (z \cdot x)$.
ii. associatividade da multiplicação[2]: $\forall x, y, z \in R, (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
iii. elemento identidade da multiplicação[3]: $\exists I \in R : I \cdot x = x \cdot I = x, \forall x \in R$.

Um dos anéis mais conhecidos é, novamente, o conjunto dos inteiros $\mathbb{Z}$. Seus elementos identidade são 0 e 1 para adição e multiplicação, respectivamente. Este anel, e muitos outros, são comutativos sobre a operação de multiplicação ($\forall x, y \in R, (x \cdot y) = (y \cdot x)$).

(c) Um corpo é um anel não-trivial[4] cujos elementos formam um grupo abeliano sobre a operação de multiplicação. Então, um corpo satisfaz vários axiomas (associatividade, comutatividade, distributividade, elemento identidade e elemento inverso, para adição e multiplicação) e emula apropriadamente as noções de adição, subtração, multiplicação e divisão. Um corpo de Galois, ou corpo finito, é um corpo que contém um número finito de elementos, como o conjunto das classes de congruência de inteiros módulo n, onde n é primo, denotado $\mathbb{Z}/n\mathbb{Z}$.

(**3**) (a) Um corpo primo é um corpo que não contém subcorpos próprios[5]. O conjunto dos números racionais com as operações usuais de adição e multiplicação $(\mathbb{Q}, +, \cdot)$ forma um corpo primo[6].

(b) Corpos finitos de ordem $2^m, m \geq 1$ são chamados de corpos binários. Os elementos de $GF(2^m)$ são geralmente polinômios cujos coeficientes são 0 ou 1, com grau máximo de $m-1$. Estes corpos são particularmente adequados para utilização em computadores, pois suas operações podem ser simuladas por deslocamentos de bits e portas lógicas `XOR`. O corpo $GF(2^3)$ contém os seguintes polinômios: $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.

(**4**) (a) Um polinômio irredutível é um polinômio não-constante que não consegue ser fatorado para o produto de outros dois polinômios não-constantes. Esta propriedade depende do corpo ou anel que os polinômios pertencem.

(b) A adição é realizada entre termos do mesmo grau. Porém, já que os polinômios pertencem ao corpo finito $GF(2^m)$, os coeficientes devem pertencer às classes de congruência módulo 2. A multiplicação utiliza a propriedade usual da distributividade, e o resultado final deve ser reduzido para o grau máximo $m-1$ com uma operação de divisão pelo polinômio primitivo do corpo finito, além da redução de coeficientes.

(c) Tomando o polinômio primitivo $x^8+x^4+x^3+x+1$, deseja- se resolver $(x^7+x^5+x^4+x^2+x)\cdot(x^6+x^4+x+1)$ sobre $GF(2^8)$.

$$
\begin{aligned}
&(x^7 + x^5 + x^4 + x^2 + x) \cdot (x^6 + x^4 + x + 1) = \\
&= x^{13} + 2x^{11} + x^{10} + x^9 + 3x^8 + 2x^7 + 2x^6 + 3x^5 + x^4 + x^3 + 2x^2 + x \\
&\quad = x^{13} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^3 + x \pmod{x^8 + x^4 + x^3 + x + 1} = \boldsymbol{x^5 + x^4 + x^2 + x}
\end{aligned}
$$

(**5**) (a) $9x \equiv 8 \pmod 7$
$= 9x \equiv 1 \pmod 7$
$= \mathbf{4 + 7n}, n \in \mathbb{Z}$

(b) $x \equiv 5 \pmod 3$
$= x \equiv 2 \pmod 3$
$= \mathbf{2 + 3n}, n \in \mathbb{Z}$

[1] operação que combina dois elementos de um conjunto não-vazio S de modo a produzir, unicamente, outro elemento $xy \in S \; \forall x, y \in S$.
[2] não necessariamente requerida, mas extremamente utilizada.
[3] alguns autores definem anéis sem esta propriedade.
[4] o anel trivial contém apenas um elemento: a identidade aditiva, que também é multiplicativa, neste caso.
[5] um subcorpo é estritamente menor, ou seja, de menor cardinalidade, que o corpo onde está contido.
[6] https://proofwiki.org/wiki/Rational_Numbers_form_Prime_Field

(c) $x \equiv 5 \pmod{-3}$
$= x \equiv -4 \pmod{-3}$
$= \mathbf{-1}$

(d) $x \equiv -5 \pmod{3}$
$= x \equiv 1 \pmod{3}$
$= \mathbf{1 + 3n}, n \in \mathbb{Z}$

(e) $x \equiv -5 \pmod{-3}$
$= \mathbf{-2}$

(f) $x \equiv 1234^{-1} \pmod{4321}$

$$\begin{aligned} 4321 &= 1234 \cdot 3 + 619 \\ 1234 &= 619 \cdot 1 + 615 \\ 619 &= 615 \cdot 1 + 4 \\ 615 &= 4 \cdot 153 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

$mdc(4321, 1234) = \mathbf{1}$

$$\begin{aligned} 1 &= 4 - 3 \\ 1 &= 4 - (615 - 4 \cdot 153) \\ 1 &= 4 \cdot 154 - 615 \\ 1 &= (619 - 615) \cdot 154 - 615 \\ 1 &= 154 \cdot 619 - 155 \cdot 615 \\ 1 &= 154 \cdot 619 - 155 \cdot (1234 - 619) \\ 1 &= 309 \cdot 619 - 155 \cdot 1234 \\ 1 &= 309 \cdot (4321 - 3 \cdot 1234) - 155 \cdot 1234 \\ 1 &= 309 \cdot 4321 - 1082 \cdot 1234 \\ x &= 4321 - 1082 = \mathbf{3239} \end{aligned}$$

(g) $x \equiv -24140 \pmod{40902}$
$= x \equiv 16762 \pmod{40902}$
$= \mathbf{16762 + 40902n}, n \in \mathbb{Z}$

(**6**) Tabela multiplicativa para inteiros em $\mathbb{Z}_{11}$, com as inversas dos elementos destacadas:

·	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

(**7**) (a) $(7x + 2) - (x^2 + 5)$ em $\mathbb{Z}_{10}[x]$
$= -x^2 + 7x - 3$
$= \mathbf{9x^2 + 7x + 7}$

(b) $(6x^2 + x + 3) \cdot (5x^2 + 2)$ em $\mathbb{Z}_{10}[x]$
$= 30x^4 + 5x^3 + 27x^2 + 2x + 6$
$= \mathbf{5x^3 + 7x^2 + 2x + 6}$

(**8**) (a) Verifica-se que $x^3 + x + 1$ é um polinômio irredutível sobre $GF(2)$ [1], então $mdc(x^3 + x + 1, x^2 + x + 1) = \mathbf{1}$.

(b) O polinômio $x^2 + 1$ é irredutível sobre $GF(3)$. Portanto, $mdc(x^3 - x + 1, x^2 + 1) = \mathbf{1}$.

(c) Todos os coeficientes são reduzidos módulo 101, e inversas multiplicativas são utilizadas onde necessário.

$$\begin{aligned} x^5 + 88x^4 + 73x^3 + 83x^2 + 51x + 67 &= (x^2 - 9x + 906) \cdot (x^3 + 97x^2 + 40x + 38) + (90x^2 + 8x + 80) \\ x^3 + 97x^2 + 40x + 38 &= 55x + 22 \cdot (90x^2 + 8x + 80) + (9x + 96) \\ 90x^2 + 8x + 80 &= (10x + 85) \cdot (9x + 96) + 0 \end{aligned}$$

$mdc(x^5 + 88x^4 + 73x^3 + 83x^2 + 51x + 67, x^3 + 97x^2 + 40x + 38)$ sobre $GF(101) = \mathbf{9x + 96}$.

(**9**) Tabela aditiva para $GF(2^4), P = x^4 + x + 1$.

$+$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Tabela multiplicativa para $GF(2^4), P = x^4 + x + 1$.

$\cdot$	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

(**10**) Considerando a tabela multiplicativa acima, verifica-se que $(x^3 + x + 1)^{-1} = \boldsymbol{x^2 + 1}$ sobre $GF(2^4)$.

Referências

[1] William Stallings. *Cryptography and Network Security: Principles and Practice.* Pearson Education, 3rd edition, 2002.