Aritmética em Corpos Finitos

Ranieri Althoff

[1]Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
Segurança em Computação

1. Algoritmo de Euclides

O algoritmo de Euclides é um método simples de encontrar o máximo divisor comum (GCD) entre dois números inteiros diferentes de zero. Foi desenvolvido pelo matemático homônimo por volta de 300 a.C. e é baseado no princípio de que o GCD entre dois números não muda quando um é subtraído pelo outro.

É fácil verificar esta propriedade: suponha dois números a e b com um máximo divisor comum n ($gcd(a, b) = n$, então $a = kn$ e $b = ln$, sendo todas as variáveis números inteiros. Ao subtrair a por b, temos que $a - b = kn - ln = (k - l)n$, ou seja, o resultado continua sendo múltiplo de n.

De forma análoga, é possível encontrar que $r = a - qb$, ou seja, subtraímos de a a maior quantidade possível de b (pela propriedade acima descrita $gcd(a, b) - gcd(b, a\%b)$ e usamos o resto r para aplicar o GCD utilizando valores menores. Esse procedimento é repetido até que um dos valores seja zero, indicando que o outro é o GCD entre a e b.

A versão extendida do algoritmo, além de calcular o GCD, também encontra dois inteiros α e β tal que $gcd(a, b) = a\alpha + b\beta$, chamados de coeficientes da **identidade de *Bézout***. Esse algoritmo é útil para encontrar o inverso multiplicativo de um número: se a e b são relativamente primos, $a\alpha \equiv 1 \pmod{b}$ e $b\beta \equiv 1 \pmod{a}$.

1.1. Exemplos

a) Algoritmo de Euclides para $gcd(9907321467, 941)$.

$$\begin{aligned} 9907321467 &= 941 \times 10528503 + 144 \\ 941 &= 144 \times 6 + 77 \\ 144 &= 77 \times 1 + 67 \\ 77 &= 67 \times 1 + 10 \\ 67 &= 10 \times 6 + 7 \\ 10 &= 7 \times 1 + 3 \\ 7 &= 3 \times 2 + 1 \\ 3 &= 1 \times 3 + 0 \end{aligned}$$

Sendo no próximo passo $b = 0$, o valor final de a e, portanto, o GCD entre os dois números, 1. É possível ver que, logo no primeiro passo, o maior número diminuiu por várias ordens de grandeza.

b) A identidade de *Bézoit* pode ser encontrada se revertendo os passos do algoritmo de Euclides, encontrando a inversa multiplicativa de a e b módulo b e a, respectivamente:

$$
\begin{aligned}
1 &= 7 + 3 \times (-2) \\
1 &= 7 + (10 - 7) \times (-2) \\
1 &= 7 \times 3 + 10 \times (-2) \\
1 &= (67 + 10 \times (-6)) \times 3 + 10 \times (-2) \\
1 &= 67 \times 3 + 10 \times (-20) \\
1 &= 67 \times 3 + (77 - 67) \times (-20) \\
1 &= 67 \times 23 + 77 \times (-20) \\
1 &= (144 - 77) \times 23 + 77 \times (-20) \\
1 &= 144 \times 23 + 77 \times (-43) \\
1 &= 144 \times 23 + (941 + 144 \times (-6)) \times (-43) \\
1 &= 144 \times 281 + 941 \times (-43) \\
1 &= (9907321467 + 941 \times (-10528503)) \times 281 + 941 \times (-43) \\
1 &= 9907321467 \times \mathbf{281} + 941 \times (\mathbf{-2958509386})
\end{aligned}
$$

Usando uma linguagem de programação, é fácil verificar que $9907321467 * 281 \equiv 1 \pmod{941}$ e $941 * -2958509386 \equiv 1 \pmod{9907321467}$.

2. Grupos, anéis e corpos

2.1. Grupo

Um grupo G é um conjunto, finito ou infinito, de elementos acompanhado de uma operação binária $*$ (chamada de operação do grupo) que satisfazem as seguintes propriedades fundamentais [Weisstein 1999c]:

Associatividade: o agrupamento dos fatores não altera o resultado da operação.

$$\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$$

Identidade: existe um elemento identidade e ou 1 em G tal que todo elemento a em G aplicado com e resulte no próprio a.

$$\forall a \in G, \quad a * e = e * a = a.$$

Inversa: existe uma inversa a^{-1} para cada elemento tal que todo elemento a em G aplicado com sua inversa resulte na identidade e.

$$\forall a \in G, \quad a * a^{-1} = a^{-1} * a = e$$

Um exemplo de grupo pode ser o conjunto $0, 1$ sob a operação lógica $\wedge$.

2.2. Anel

Mais restritivo que um grupo, um anel é um conjunto G acompanhado de duas operações $+$ e $*$ (interpretados como adição e multiplicação) que satisfazem as seguintes propriedades fundamentais [Weisstein 1999d]:

Associatividade aditiva: tal qual como a associatividade em grupos, o agrupamento dos fatores não altera o resultado da adição.

$$\forall a, b, c \in G, \quad (a + b) + c = a + (b + c)$$

Comutatividade aditiva: a ordem dos fatores não altera o resultado da adição.

$$\forall a, b \in G, \quad a + b = b + a$$

Identidade aditiva: tal qual a identidade em grupos, existe um elemento 0 tal que todo elemento a em G adicionado a 0 resulte no próprio a.

$$\forall a \in G, \quad a + 0 = 0 + a = a$$

Inversa aditiva: tal qual a inversa em grupos, existe uma inversa a^{-1} para cada elemento tal que todo elemento a em G adicionado a sua inversa resulte na identidade 0.

$$\forall a \in G, \quad a + (-a) = (-a) + a = 0$$

Distributividade: a operação de multiplicação deve ser distributiva sobre a operação de adição.

$$\forall a, b, c \in G, \quad a * (b + c) = (a * b) + (a * c) \wedge (b + c) * a = (b * a) + (c * a)$$

Associatividade multiplicativa: a operação de multiplicação também é associativa:

$$\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$$

Um exemplo de anel infinito é o conjunto de números inteiros $\mathbb{Z}$, já que há a operação de adição e multiplicação que satisfaz todas as condições acima sobre esse conjunto.

2.3. Corpo

Um corpo é um conjunto G, satisfazendo todas as condições de um anel e adicionalmente todo elemento $a \in G$ diferente de zero possui inversa multiplicativa. Essa característica é conhecida como álgebra de divisão, porque é a propriedade que permite que um certo conjunto possua uma operação de divisão [Weisstein 1999a].

Um corpo com uma quantidade finita de elementos é conhecido como um **corpo de Galois** [Weisstein 1999b]. Os exemplos mais usados de corpos finitos são os conjuntos de números relativamente primos a n, denotados $\mathbb{Z}_n$.

3. Corpos primos e binários

Corpos finitos sempre tem um número de elementos primo ou potência de um primo, e para cada potência de primo p^n existe apenas um (considerando corpos isomórficos como iguais) corpo finito $\mathbb{F}_{p^n}$.

3.1. Corpo primo

Um corpo finito $\mathbb{F}_p$, onde p é um número primo, é chamado de corpo primo de ordem p e contém as classes de congruencia módulo p, sendo os p elementos denominados $0, 1, \ldots, p-1$. $a = b$ em $\mathbb{F}_p$ significa $a \equiv b \pmod{p}$ [Weisstein 1999b].

O corpo finito $\mathbb{F}_2$ é um corpo primo que consiste dos elementos 0 e 1 e satisfaz as seguintes operações:

$+$	0	1
0	0	1
1	1	1

$*$	0	1
0	0	0
1	0	1

3.2. Corpo binário

Um corpo finito de ordem 2^m, onde $m \geq 1$, é chamado de corpo binário. Em geral, são corpos cujos elementos são polinômios, cujos coeficientes são 0 ou 1 com grau máximo $m-1$ (*e.g.* $x^4 + x^3 + x^1 + 1$ para $m = 5$).

O corpo finito $\mathbb{F}_{2^3}$ é composto pelos seguintes polinômios:

$$\{x^2 + x + 1, x^2 + x, x^2 + 1, x^2, x + 1, x, 1, 0\}$$

4. Polinômios irredutíveis

Um polinômio é dito irredutível se não puder ser fatorado em polinômios não-triviais em um mesmo grupo. A irredutibilidade de um polinômio depende do grupo no qual está sendo trabalhado, portanto.

No corpo finito $\mathbb{F}_{2^3}$, o polinômio $x^2 + x + 1$ é irredutível, mas $x^2 + 1$ não é, pois $(x+1)(x+1) = x^2 + 2x + 1 \equiv x^2 + 1 \pmod{2}$.

4.1. Aritmética em corpos finitos

Para se realizar aritmética em corpos finitos, se realiza a operação entre os termos de mesmo grau, depois dividindo por um polinômio irredutível que define o corpo [Stallings 2002]. Por exemplo:

$$p = x^3 + x + 1$$
$$q = x^3 + x^2$$
$$p + q = 2x^3 + x^2 + x + 1$$

No entanto, para corpos binários, a operação de adição convenientemente é equivalente a operação de ou-exclusivo sobre os bits do polinômio. Pelo mesmo exemplo, convertendo os termos dos polinômios para 0 ou 1 no corpo $\mathbb{F}_{2^3}$.

$$p = 1011_2$$
$$q = 1100_2$$
$$p + q = p \oplus q \equiv 0111_2 \pmod{1011} = x^2 + x + 1 \pmod{x^3 - x - 1}$$

A operação de multiplicação em um corpo finito é a multiplicação módulo um polinômio irredutível que define o corpo, o que também pode ser feito se convertendo os termos para uma representação binária, o que facilita o uso por computadores [Stallings 2002]:

$$p * q = x^6 + x^5 + x^4 + 2x^3 + x^2 = 1110100_2$$
$$p * q = 1110100_2 \equiv 110_2 \pmod{1011} = x^2 + x \pmod{x^3 - x - 1}$$

5. Encontrando x

a) $9x \equiv 8 \pmod 7$
$= 9x \equiv 1 \pmod 7$
$x = 4 + 7n$

b) $x \equiv 5 \pmod 3$
$= x \equiv 2 \pmod 3$
$x = 2 + 3n$

c) $x \equiv 5 \pmod{-3}$
$= x \equiv -1 \pmod{-3}$
$x = -1 - 3n$

d) $x \equiv -5 \pmod 3$
$= x \equiv 1 \pmod 3$
$x = 1 + 3n$

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

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

g) $x \equiv -24140 \pmod{40902} = x \equiv 16762 \pmod{40902}$ $x = 16762 + 40902n$

6. Inversas multiplicativas do conjunto $\mathbb{Z}_{11}$

O conjunto Z_n é o conjunto dos números relativamente primos a n. Como 11 é um número primo, todos os números inferiores a ele são relativamente primos, portanto o conjunto compreende $1, 2, \ldots, 10$. As inversas multiplicativas podem ser encontradas se multiplicando os números deste conjunto de forma a encontrar $ab = 1 \pmod{11}$, sendo a a inversa multiplicativa de b e vice-versa [Stallings 2002].

$*$	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

É possível concluir, portanto, que os pares de inversas multiplicativas de $\mathbb{Z}_{11}$ são $(1, 1)$, $(2, 6)$, $(3, 4)$, $(5, 9)$ e $(10, 10)$.

7. Aritmética polinomial em $\mathbb{Z}_{10}$

a) $(7x + 2) - (x^2 + 5) = -x^2 + 7x - 3 = \mathbf{9x^2 + 7x + 7}$

b) $(6x^2 + x + 3) \times (5x^2 + 2) = 30x^4 + 5x^3 + 27x^2 + 2x + 6 = \mathbf{5x^3 + 7x^2 + 2x + 6}$

8. Polinômios em corpos finitos

a) $gcd(x^3 + x + 1, x^2 + x + 1)$ sobre GF(2)

$x^3 + x + 1$ é irredutível em GF(2), portanto o único divisor comum com outros polinômios do mesmo grupo é **1**.

b) $gcd(x^3 - x + 1, x^2 + 1)$ sobre GF(3)

$x^2 + 1$ é irredutível em GF(3), portanto o único divisor comum com outros polinômios do mesmo grupo é **1**.

9. Tabela aditiva e multiplicativa para GF(2^4)

Para o polinômio irredutível $x^4 + x + 1$, as tabelas de adição e multiplicação do corpo finito GF(2^4) são:

$+$	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

$*$	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

Utilizando os números como representação dos polinômios como explicado em seções anteriores.

10. Inverso multiplicativo em GF(2^4)

Para o polinômio irredutível $x^4 + x + 1$, utilizando as tabelas acima, se encontra que o inverso multiplicativo de $x^3 + x + 1$, que pode ser representado como 1011_2 ou B_{16}, é $x^2 + 1$ (101_2 ou 5_{16}).

Referências

Stallings, W. (2002). *Cryptography and Network Security: Principles and Practice*. Pearson Education, 3rd edition.

Weisstein, E. (1999a). Field axioms. Wolfram MathWorld. Disponível em: `http://mathworld.wolfram.com/FieldAxioms.html`. Acesso em: 25 mai 2016.

Weisstein, E. (1999b). Finite field. Wolfram MathWorld. Disponível em: `http://mathworld.wolfram.com/FiniteField.html`. Acesso em: 25 mai 2016.

Weisstein, E. (1999c). Group. Wolfram MathWorld. Disponível em: `http://mathworld.wolfram.com/Group.html`. Acesso em: 25 mai 2016.

Weisstein, E. (1999d). Ring. Wolfram MathWorld. Disponível em: `http://mathworld.wolfram.com/Ring.html`. Acesso em: 25 mai 2016.