Aritmética Modular

Faculdade de Informática - PUCRS
Prof. Dr. Avelino Francisco Zorzo

Pano de fundo

- Teoria dos números é usada para:
  - Protocolos de troca de chaves
  - Assinaturas digitais
  - Criptografia pública

Mais informações: http://shoup.net/ntb/ntb-v2.pdf

Notação

- N representa um número positivo inteiro.
- p representa um número primo.
- Notação: $Z_N = \{0, 1, 2, \ldots, N-1\}$
- Podemos fazer soma e multiplicação com módulo N?

Aritmética modular

- Exemplos: Seja N = 12

  $9 + 8 = 5$ em Z_{12}

  $5 \times 7 = 11$ em Z_{12}

  $5 - 7 = 10$ em Z_{12}

- Aritmética em Z_N funciona como esperado,
  - *e.g.* $x \cdot (y+z) = x \cdot y + x \cdot z$ em Z_N

Maior Divisor Comum

- **Def**: Para inteiros x,y: **mdc(x, y)** é o maior divisor comum de x,y
  - Exemplo: mdc(12, 18) = 6
- **Fato**: para todos inteiros x,y existem inteiros a,b tal que $\mathbf{a \cdot x + b \cdot y = mdc(x,y)}$
  - Exemplo: $2.12 - 1.18 = 6$
- a,b podem ser encontrados eficientemente usando o algoritmo estendido de Euclides.
- Se mdc(x,y)=1 dizemos que x e y são **primos relativos**

Inverso modular

- Nos números racionais, o inverso de 2 é ½ .
- Como fica em Z_N?
- **Def**: O **inverso** de x em Z_N é um elemento y em Z_N tal que $x.y = 1$ em Z_N
  - y é representado por x^{-1} .
- Exemplo:
  - $Z_7 = \{ 0,1,2,3,4,5,6 \} \rightarrow 3^{-1} = 5$ em Z_7 pois $3x5 = 1$ em Z_7
  - Seja N um inteiro ímpar.
  - O inverso de 2 em Z_N é $(N+1)/2$.

    $2.((N+1)/2) = N+1 = 1$ em Z_N

Inverso modular

- Quais elementos tem um inversos em Z_N?
- **Lema**: x em Z_N tem um inverso se e somente se mdc(x,N) = 1 (x é um primo relativo de N)
- Prova:
  - mdc(x,N) = 1 $\Rightarrow \exists$ a,b: $a \cdot x + b \cdot N = 1$ em Z_N
    $\Rightarrow a \cdot x = 1$ em $Z_N \Rightarrow x^{-1} = a$ em Z_N
  - mdc(x,N)>1 $\Rightarrow \forall$ a: mdc(a · x, N)>1 $\Rightarrow a \cdot x \neq 1$ em Z_N
  - Exemplo:
    - mdc(x,N)=2 $\Rightarrow \forall$ a: a.x é par $\Rightarrow$ a.x (par) $\neq$ b.N (par) + 1 em Z_N

Mais notações

- **Def:** Z_N^* = (conjunto de elementos invertíveis em Z_N)
  $= \{ x \in Z_N : mdc(x,N) = 1 \}$
- Exemplos:
  1. Para p primo, $Z_p^* = Z_p - \{0\} = \{1, 2, \ldots, p-1\}$
  2. $Z_{12}^* = \{1, 5, 7, 11\}$
- Para x em Z_N^*, podemos encontrar x^{-1} usando o algoritmo estendido de Euclides.

Resolvendo equações lineares

- Resolva: $\mathbf{a \cdot x + b = 0}$ **em** $\mathbf{Z_N}$
- Solução: $\mathbf{x = -b \cdot a^{-1}}$ **em** $\mathbf{Z_N}$
- Encontre a^{-1} em Z_N usando o algoritmo estendido de Euclides.
- Tempo de execução: $O(\log^2 N)$

Teorema de Fermat (1640)

- **Teorema:** Seja p um número primo
  $\forall x \in (Z_p)^* : x^{p-1} = 1$ em Z_p
- Exemplo: p = 5. $3^4 = 81 = 1$ em Z_5
- Assim:
  $x \in (Z_p)^* \Rightarrow x \cdot x^{p-2} = 1 \Rightarrow x^{-1} = x^{p-2}$ em Z_p
- Outra forma de calcular inversos, mas menos eficiente que Euclides

Aplicação: gerar aleatoriamente primos

- Suponha que queiramos gerar aleatoriamente um grande primo com 1024 bits (i.e. $p \approx 2^{1024}$)
  - Passo 1: escolha um inteiro aleatório
    $p \in [2^{1024}, 2^{1025}-1]$
  - Passo 2: teste se $2^{p-1} = 1$ em Z_p
    Se sim, imprima p e pare.
    Senão, vá para o Passo 1.
- Algoritmo simples (não o melhor).
- Probabilidade[p não primo] $< 2^{-60}$

A estrutura de $(Z_p)^*$

- **Teorema** (Euler):
  $(Z_p)^*$ é um **grupo cíclico**, ou seja
  $\exists g \in (Z_p)^*$ tal que $\{1, g, g^2, g^3, \ldots, g^{p-2}\} = (Z_p)^*$
- g é chamado um **gerador** de $(Z_p)^*$
- Exemplo:
  - p=7.
  - $\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (Z_7)^*$
- Nem todo elemento é um gerador:
  - $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

Ordem

- Para $g \in (Z_p)^*$ o conjunto $\{1, g, g^2, g^3, \ldots\}$ é chamado de **grupo gerado por g**, ou $<g>$
- **Def**: a ordem de $g \in (Z_p)^*$ é o tamanho de $<g>$
  - $ord_p(g) = |<g>| = $ (menor $a>0$ t.q. $g^a = 1$ em Z_p)
- Exemplos:
  - $ord_7(3) = 6$; $ord_7(2) = 3$; $ord_7(1) = 1$
- **Thm** (Lagrange): $\forall g \in (Z_p)^*$: $ord_p(g)$ divide $p-1$

Euler: generalização de Fermat

- **Def**: Para um inteiro N defina $\phi(N) = |(Z_N)^*|$ (Função ϕ de Euler)
- Exemplos:
  - $\phi(12) = |\{1,5,7,11\}| = 4$; $\phi(p) = p-1$
  - Para $N=p \cdot q$: $\phi(N) = N-p-q+1 = (p-1)(q-1)$
- **Thm** (Euler): $\forall x \in (Z_N)^*$: $x^{\phi(N)} = 1$ em Z_N
  - Exemplo: $5^{\phi(12)} = 5^4 = 625 = 1$ em Z_{12}
- Generalização de Fermat. Base do RSA.

MDC

```
mdc(a,b) {
  if (b == 0) return a
  else
   return gcd(b, a mod b);
}
```

```
mdc(a,b) {
  while (a != b)
    if (a > b)
      a = a - b
    else b = b - a;
  return a;
}
```


Algoritmo estendido de Euclides

```
/* retorna (d,a,b) onde:
   d = mdc(x,y) e d == x*a + y*b */

ExtendedEuclid (x,y) {
  if (y == 0) return (x,1,0) ;
  (d1,a1,b1) = ExtendedEuclid(y, x mod y);
  d = d1;
  a = b1;
  b = a1 - (x div y) * b1;
  return (d,a,b);
}
```