Conceitos e algoritmos da Teoria dos Números
Parte II

Teorema Chinês do Resto

Problema 1 *Encontre os inteiros x que, ao serem divididos por 3, 5, e 7 dão resto 2, 3 e 2 respectivamente.*

- Resposta: $x = 23$ é uma solução.
- Resposta melhor: $x = 23 + 105k$ para todo $k \in \mathbb{Z}$.

Como encontrar essas respostas sistematicamente?

Para que serve isso?

Teorema Chinês do Resto

Teorema 1 *Seja* $n = n_1 \times n_2 \times \ldots \times n_k$ *onde* $\text{MDC}(n_i, n_j) = 1$ *para* $1 \leq i < j \leq k$. *Considere o mapeamento*

$$a \leftrightarrow (a_1, a_2, \ldots, a_k), \tag{1}$$

onde $a \in \mathbb{Z}_n, a_i \in \mathbb{Z}_{n_i}$ *e*

$$a_i = a \bmod n_i, \ \forall \ i = 1, \ldots, k.$$

Então, (1) é uma bijeção de $\mathbb{Z}_n$ *no produto cartesiano* $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \mathbb{Z}_{n_k}$.

- Operações entre elementos de $\mathbb{Z}_n$ podem ser substituídas por operações equivalentes nas suas imagens (k-tuplas).
- O resultado das operações pode ser mapeado de volta para um elemento da pré-imagem, usando o mapeamento inverso.

Teorema Chinês do Resto

Dados a e b, onde

$$a \leftrightarrow (a_1, a_2, \ldots, a_k)$$

$$b \leftrightarrow (b_1, b_2, \ldots, b_k),$$

temos

- $(a + b) \bmod n \leftrightarrow$
  $((a_1 + b_1) \bmod n_1, (a_2 + b_2) \bmod n_2, \ldots, (a_k + b_k) \bmod n_k)$.
- $(a - b) \bmod n \leftrightarrow$
  $((a_1 - b_1) \bmod n_1, (a_2 - b_2) \bmod n_2, \ldots, (a_k - b_k) \bmod n_k)$.
- $(ab) \bmod n \leftrightarrow$
  $((a_1 b_1) \bmod n_1, (a_2 b_2) \bmod n_2, \ldots, (a_k b_k) \bmod n_k)$.

Teorema Chinês do Resto

Demonstração Defina

- $m_i = n/n_i \; \forall \; i = 1, \ldots, k$;
- $c_i = m_i(m_i^{-1} \bmod \; n_i) \; \forall \; i = 1, \ldots, k$;
- $a \equiv (a_1c_1 + a_2c_2 + \ldots + a_kc_k) \pmod{n}$.

e verifique a bijeção.

Teorema Chinês do Resto

Corolário 1 *Se* $n = n_1.n_2.\ldots.n_k$, *onde* $\text{MDC}(n_i, n_j) = 1$ *para todo* $1 \leq i < j \leq k$, *então para todos inteiros* $a_1, a_2, \ldots, a_k$, *o sistema de equações:*

$$x \equiv a_i \pmod{n_i}, \forall i = 1, \ldots, k,$$

tem uma **única** *solução* **módulo** n.

Corolário 2 *Se todo par de inteiros do conjunto* $\{n_1, n_2, \ldots, n_k\}$ *é primo relativo e* $n = n_1.n_2.\ldots.n_k$, *então para todo par de inteiros* x *e* a,

$$x \equiv a \pmod{n_i}, \forall i = 1, \ldots, k \Leftrightarrow x \equiv a \pmod{n}.$$

Teorema Chinês do Resto

Exemplo 1

$$a \equiv 2 \pmod{5},$$

$$a \equiv 3 \pmod{13},$$

$a \bmod 65$?

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	40	15	55	30	5	45	20	60	35	10	50	25
1	26	1	41	16	56	31	6	46	21	61	36	11	51
2	52	27	2	42	17	57	32	7	47	22	62	37	12
3	13	53	28	3	43	18	58	33	8	48	23	63	38
4	39	14	54	29	4	44	19	59	34	9	49	24	64

Potências de um Elemento

Potências de a mod n onde $a \in \mathbb{Z}_n^*$.

Exemplo 2 $a = 3$ e $n = 7$

i	0	1	2	3	4	5	6	7	8	9	10	11...
3^i mod 7	1	3	2	6	4	5	1	3	2	6	4	5 ...

Potências de um Elemento

Teorema 2 (Euler) *Para todo inteiro* $n > 1$,

$$a^{\phi(n)} \equiv 1 \pmod{n}, \forall a \in \mathbb{Z}_n^*.$$

Teorema 3 (Fermat) *Para todo* p *primo, temos*

$$a^{p-1} \equiv 1 \pmod{p}, \forall a \in \{1, 2, \ldots, p-1\}.$$

Definição 1 Se $g \in \mathbb{Z}_n^*$ e $\text{ord}(g) = \phi(n)$, então todo elemento de $\mathbb{Z}_n^*$ é uma potência de g módulo n e g é uma **raiz primitiva** ou **gerador** de $\mathbb{Z}_n^*$. Se $\mathbb{Z}_n^*$ tiver uma raiz primitiva, então é **cíclico**.

Exemplo 3 3 é raiz primitiva de $\mathbb{Z}_7^*$.

Potências de um Elemento

Teorema 4 *Os valores de $n > 1$ para os quais $\mathbb{Z}_n^*$ é cíclico são: 2, 4, p^e e $2p^e$ para todo primo* **ímpar** *e todo inteiro positivo e.*

Definição 2 Se g é uma **raiz primitiva** de $\mathbb{Z}_n^*$ e a é um elemento qualquer deste grupo, então existe um z tal que $g^z \equiv a \pmod{n}$. Este z é o **logaritmo discreto** ou índice de a módulo n na base g, também denotado por $\text{ind}_{n,g}(a)$.

Teorema 5 *Se g é uma raiz primitiva de $\mathbb{Z}_n^*$ então $g^x \equiv g^y \pmod{n}$ se e somente se $x \equiv y \pmod{\phi(n)}$.*

Potências de um Elemento

Teorema 6 *Se p é primo* **ímpar** *e $e \geq 1$, então $x^2 \equiv 1 \pmod{p^e}$ tem somente 2 soluções dadas por $x = 1$ e $x = -1$.*

Definição 3 $x^2 \equiv 1 \pmod{n}$ e $x \neq \pm 1$ então x é uma **raiz não trivial de 1, módulo** n.

Exemplo 4 Exemplo: 9 é raiz não trivial de 1, módulo 80.

Corolário 3 *Se existe uma raiz não trivial de 1 módulo n, então n é um número composto.*

Exponenciação Modular

Para a e b inteiros não negativos e n inteiro positivo, qual seria um método eficiente para calcular $a^b \bmod n$?

EXPONENCIAÇÃO-MODULAR(a, b, n)

1. $c \leftarrow 0$
2. $d \leftarrow 1$
3. seja $\langle b_k, b_{k-1}, \ldots, b_1, b_0 \rangle$ a representação binária de b;
4. **Para** $i \leftarrow k$ **até** 0 **faça**
5. $\quad c \leftarrow 2c$;
6. $\quad d \leftarrow (d.d) \bmod n$;
7. $\quad$ **Se** $b_i = 1$ **então**
8. $\quad\quad c \leftarrow c + 1$;
9. $\quad\quad d \leftarrow (d.a) \bmod n$;
10. **Retorne** d.

Exponenciação Modular

Corretude:

- na iteração i, c é o inteiro representado pelo prefixo $\langle b_k, b_{k-1}, \ldots, b_i \rangle$ ...
- invariante: $d = a^c \bmod n$ ...

Exemplo 5 $a = 7$, $b = 560$ e $n = 561$.

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
d	7	49	157	526	160	241	298	166	67	1

RSA revisitado

Criação das chaves

Passo 1: Escolher dois números primos p e q bem **grandes**.

Passo 2: Calcular $n = pq$.

Passo 3: Escolher um inteiro ímpar e pequeno tal que
$\text{MDC}(e, \phi(n)) = 1$.

Passo 4: Calcular d o inverso multiplicativo de e módulo $\phi(n)$:

$$de \equiv 1 \pmod{\phi(n)}.$$

Passo 5: Tornar pública a chave (e, n).

Passo 6: Manter secreta a chave d.

RSA revisitado

As funções $\textsc{Enc}_e()$ **e** $\textsc{Dec}_d()$

- $y \leftarrow \textsc{Enc}_e(x)$: $x^e \bmod n$
- $x \leftarrow \textsc{Dec}_d(y)$: $y^d \bmod n$

Complexidades: para $|e| = O(1)$ e $|d| = |n| = \beta$,

- $\textsc{Enc}_e(x)$: $O(\beta^2)$
- $\textsc{Dec}_e(x)$: $O(\beta^3)$

Teorema 7 *O sistema criptográfico RSA é correto.*

Demonstração mais tarde, no curso.