

ACOL1002: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Number Theory and Cryptography

Primes and GCD

- Worst-case time complexity of simple operations. In each of the cases the input size is denoted by $n = |a| + |b|$.

Operation	Time complexity
$a \pm b$	$O(n)$
$a \cdot b$	$O(n^2)$
$a \text{ (div } b)$	$O(n^2)$
$a \text{ (mod } b)$	$O(n^2)$
$a^{-1} \text{ (mod } b)$ for relatively prime a, b	$O(n^3)$

Number Theory and Cryptography

Primes and GCD

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \dots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \dots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Number Theory and Cryptography

Primes and GCD

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \dots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \dots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

- Proof of existence:
 - Let $M_k = m/m_k$ and let y_k denote the inverse of M_k modulo m_k (i.e., $M_k \cdot y_k \equiv 1 \pmod{m_k}$).
 - Claim: $x = \sum_i a_i \cdot M_i \cdot y_i$ is a solution modulo m .

Number Theory and Cryptography

Primes and GCD

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \dots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \dots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

- Proof of uniqueness:
 - Lemma: Let p, q be relatively prime positive integers. For any integers a, b , if $a \equiv b \pmod{p}$ and $a \equiv b \pmod{q}$, then $a \equiv b \pmod{pq}$.

Number Theory and Cryptography

Primes and GCD

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \dots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \dots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

- Let $m_1, \dots, m_n$ be relatively prime and let $m = m_1 \dots m_n$. Consider the following two sets:
 - $A = \mathbb{Z}_m$
 - $B = \{(x_1, \dots, x_n) \mid \forall i (x_i \in \mathbb{Z}_{m_i})\}$.
- Claim: Consider $f : A \rightarrow B$ defined as

$$f(x) = (x \pmod{m_1}, x \pmod{m_2}, \dots, x \pmod{m_n}).$$

Then f is a bijection.

Number Theory and Cryptography

Primes and GCD

- Suppose we have to multiply the following two numbers:

$$x = 1682593 \quad \text{and} \quad y = 176234$$

- Let $m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19, m_5 = 23, m_6 = 29, m_7 = 31, m_8 = 37, m_9 = 41$. So, $m = m_1 \dots m_9 = 1448810778701$.

r	$x \pmod{r}$	$y \pmod{r}$	$xy \pmod{r}$
11	0	3	?
13	3	6	?
17	1	12	?
19	10	9	?
23	5	8	?
29	13	1	?
31	6	30	?
37	18	3	?
41	35	16	?

Number Theory and Cryptography

Primes and GCD

- Suppose we have to multiply the following two numbers:

$$x = 1682593 \quad \text{and} \quad y = 176234$$

- Let $m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19, m_5 = 23, m_6 = 29, m_7 = 31, m_8 = 37, m_9 = 41$. So, $m = m_1 \dots m_9 = 1448810778701$.

r	$x \pmod{r}$	$y \pmod{r}$	$xy \pmod{r}$
11	0	3	0
13	3	6	5
17	1	12	12
19	10	9	14
23	5	8	17
29	13	1	13
31	6	30	25
37	18	3	17
41	35	16	27

- Can we construct xy using the table above?

Read the chapter on the application of congruences.

End