Number Theory Reminder

Cryptography and Protocols

Andrei Bulatov

Divisibility, Primes, etc.

- Divisibility, residues
- Prime numbers
- Primality tests
- Prime decomposition
- Greatest common divisor
- Relatively prime numbers
- Euler totient function
- Multiplicative group
- Primitive roots
- Quadratic residues
- Complexity of arithmetic

Residues

For a positive integer n, we denote

- $\mathbb{Z}_n$ the set {0,1,2,…,n –1}
- $\mathbb{Z}_n^+$ the set {1,2,…,n –1}
- $+, \times, x^y$ addition, multiplication and exponentiation modulo n

$\mathbb{Z}_n$ with these operations is called the set of residues modulo n

Every integer m, positive or negative, has a corresponding residue — $m \bmod n$

For example,

$$17 \bmod 5 = 2, \quad 20 \bmod 5 = 0, \quad -1 \bmod 5 = 4$$

Modular Arithmetic

- We define addition, subtraction, and multiplication of residues:

  Let $a,b \in \mathbb{Z}_n$. Then

  $a + b \pmod{n}$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a + b \pmod{m}$

  $a - b \pmod{n}$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a - b \pmod{m}$

  $a \cdot b \pmod{n}$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a \cdot b \pmod{m}$

- Example. Construct operation tables for $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Divisors of Zero

- It is not hard to see that the operation tables of addition looks similar for all m
- It is not the case for multiplication. Consider

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- A proper divisor of 0 modulo m is a residue a such that there is $b \not\equiv 0 \pmod{m}$ with $a \cdot b \equiv 0 \pmod{m}$. $\mathbb{Z}_4$ has a proper divisor of zero. $\mathbb{Z}_5$ does not.

Inverse

- A residue a modulo m is called an inverse of a residue b if $a \cdot b \equiv 1 \pmod{m}$, denoted b^{-1}
- 3 is the inverse of 2 modulo 5
- 2 does not have an inverse modulo 4
- **Theorem**

  Let a be residue modulo m. The following conditions are equivalent:

  (i) a has an inverse;

  (ii) a is not a proper divisor of 0;

  (iii) a is relatively prime with m.

Fermat's Little Theorem

- **Fermat's Little Theorem.**
  If p is prime and a is an integer not divisible by p, then
  $$a^{p-1} \equiv 1 \pmod{p}$$

- Clearly, it suffices to consider only residues modulo p.

$\mathbb{Z}_5$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Fermat's Little Theorem (cntd)

- Fermat's Little Theorem was improved by Euler
- **Fermat's Little Theorem improved**

  For any integers m and a such that they are relatively prime

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

where $\varphi(m)$ denotes the Euler totient function, the number of numbers $0 < k < m$ relatively prime with m

- Example: $\mathbb{Z}_8$

Multiplicative Groups

- The set of invertible elements from $\mathbb{Z}_n$ is denoted by $\mathbb{Z}_n^*$
- It is called the multiplicative group modulo n, because it is equipped with multiplication modulo n
- If a and b are invertible then $a \cdot b$ is also invertible, so $\mathbb{Z}_n^*$ is closed under multiplication
- We also know that every member of $\mathbb{Z}_n^*$ has an inverse.
- Example: $n = 8$

Primitive Roots

- Let p be a prime. Then $\mathbb{Z}_p^*$ contains p – 1 element
- There is always a number g such that
$$\{1,2,\dots,p-1\} = \{g, g^2, g^3, \dots, g^{p-1}\}$$
- It is called a primitive root modulo p
- Note that p – 1 is the smallest number with $g^{p-1} \equiv 1 (mod\ p)$
- We say that p – 1 is the order of g
- Other members of $\mathbb{Z}_p^*$ may have different orders
- Example: p = 11
- For $\mathbb{Z}_n^*$ the set $\{a, a^2, \dots, a^{n-1}\}$ is called the subgroup generated by a
- It is not hard to see that the number of primitive roots is φ(p – 1)
- Primitive roots exist for $n = 2,4,p^k,2p^k$, p is an odd prime

Quadratic Residues

- A residue $q \in \mathbb{Z}_n$ is called a quadratic residue modulo n if $q \equiv x^2 (\mathrm{mod}\, n)$ for some $x \in \mathbb{Z}_n$
- Modulo an odd prime p there are (p + 1)/2 quadratic residues. (Why?)
- Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \text{ divides } a, \\ 1, & \text{if } a \text{ is a quadratic residue and } p \text{ doesn't divide } a \equiv x^2 (\mathrm{mod}\, n) \\ -1, & \text{if } a \text{ is not a quadratic residue} \end{cases}$$

Complexity of Arithmetic

Given two integers, a and b, we can compute

- a + b in O(max(log a, log b))
- a $\times$ b in O(log a $\times$ log b)

a^b cannot be computed in polynomial time, because the size of this number is b log(a)

It is possible modulo n

Let $b_0 b_1 b_2 \dots b_k$ be the binary representation of b (k = log b)

Then $b = b_0 2^0 + b_1 2^1 + \cdots + b_k 2^k$ that implies

$$a^b (mod\ n) = a^{b_0 2^0} \cdot a^{b_1 2^1} \cdot \dots \cdot a^{b_k 2^k}$$

First, we consecutively compute $a^{2^0}, a^{2^1}, \dots, a^{2^k}$ in $O(k \log^2 n)$

Then we compute the product again in $O(k \log^2 n)$