

CRYPTOGRAPHY HANDOUT 14

SUMMARY: KEY NUMBER THEORY DEFINITIONS AND RESULTS

1. DIVISIBILITY AND CONGRUENCES

Definition. Let a and b be integers with $a \neq 0$. We say a **divides** b if there is an integer k such that $b = ak$. This is denoted $a \mid b$.

Definition. Suppose a, b, n are integers with $n > 0$. We say a **and** b **are congruent modulo** n if and only if $n \mid (a - b)$ or $a \equiv b \pmod{n}$. Alternatively, we can think of $a - b$ as a multiple of n , or $a - b = kn$ for some integer k .

Definition. The **greatest common divisor** of a and b is the largest positive integer dividing both a and b . This is denoted $\gcd(a, b)$.

Euclidean Algorithm. Suppose a and b are integers and $a > b$.

1. Divide a by b to get

$$a = q_1b + r_1$$

where q_1 is the quotient and r_1 is the remainder.

2. If $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$. If $r_1 \neq 0$, then divide b by r_1 to get

$$b = q_2r_1 + r_2.$$

3. Continue in this way until the remainder is 0.

$$a = q_1b + r_1$$

$$b = q_2r_1 + r_2$$

$$r_1 = q_3r_2 + r_3$$

$$\vdots$$

$$r_{k-1} = q_{k+1}r_k$$

The conclusion is that $\gcd(a, b) = r_k$.

Theorem 1. *Let a and b be integers not both 0. There exist integers x and y such that $ax + by = \gcd(a, b)$.*

Corollary. *If p is a prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Theorem 2. *Let a and n be integers with $n > 0$. If $\gcd(a, n) = 1$, then a^{-1} exists modulo n .*

2. CHINESE REMAINDER THEOREM

Definition. Let a and n be integers. If $\gcd(a, n) = 1$, then we say a and n are **relatively prime**.

Chinese Remainder Theorem. Suppose $\gcd(m, n) = 1$ for two integers m and n . Given integers a and b , there exists exactly one solution $x \pmod{mn}$ to the simultaneous congruences:

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

3. FERMAT'S LITTLE THEOREM AND EULER'S THEOREM

Definition. Let a and n be integers where $n > 0$. The smallest natural number k such that

$$a^k \equiv 1 \pmod{n}$$

is the **order of a modulo n** and is denoted $k = \text{ord}_n(a)$.

Fermat's Little Theorem. Let p be a prime number and let a be an integer such that $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Definition. For a natural number n , the Euler phi-function $\varphi(n)$ is equal to the number of natural numbers less than or equal to n that are relatively prime to n .

Euler's Theorem. Let a and n be integers with $n > 0$ such that $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

4. PRIMITIVE ROOTS

Definition. Let p be a prime. An integer g such that $\text{ord}_p(g) = p - 1$ is a **primitive root modulo p** .

Theorem 3. *Every prime p has a primitive root.*

Theorem 4. *Every prime p has $\varphi(p - 1)$ primitive roots.*

5. SQUARE ROOTS AND SQUARES

Definition. If a is an integer, p is a prime, and $a \equiv b^2 \pmod{p}$ for some integer b , then a is called a **quadratic residue modulo p** . If a is not congruent to any square modulo p , then a is a **quadratic non-residue modulo p** .

Theorem 5. *Let p be a prime. Half the numbers not congruent to 0 mod p in a complete residue system mod p are quadratic residues and half are quadratic non-residues.*

Definition. For an odd prime p and a natural number a with p not dividing a , the **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined to be:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue mod } p \\ -1 & a \text{ is a quadratic non-residue mod } p \end{cases}$$

Theorem 6. *Suppose p is an odd prime and p does not divide the numbers a or b . Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

Euler's Criterion (Theorem). Suppose p is an odd prime and p does not divide the natural number a . Then a is a quadratic residue mod p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$, and a is a quadratic non-residue mod p if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Quadratic Reciprocity. Let p and q be odd primes. Then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & p \equiv q \equiv 3 \pmod{4} \end{cases}$$