NTL3 – Modular Arithmetic

Theorem 5.1 (Properties of Modulus)

Let a, b and m be integers, with $m \neq 0$. We say that a and b are congruent modulo m, denoted by

$$a \equiv b(\text{mod } m)$$

if $m \mid a - b$.

1. *Reflexivity: $a \equiv a(\text{mod } m)$*
2. *Transitivity: If $a \equiv b(\text{mod } m)$ and $b \equiv c(\text{mod } m)$, then $a \equiv c(\text{mod } m)$*
3. *Symmetry: If $a \equiv b(\text{mod } m)$, then $b \equiv a(\text{mod } m)$*
4. *Addition: If $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, then $a + c \equiv b + d(\text{mod } m)$ and $a - c \equiv b - d(\text{mod } m)$.*
5. *If $a \equiv b(\text{mod } m)$, then for any integer k, $ka \equiv kb(\text{mod } m)$.*
6. *Multiplication: If $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, then $ac \equiv bd(\text{mod } m)$*
   In general, if $a_i \equiv b_i(\text{mod } m), i = 1, \dots, k$ then $a_1 \dots a_k \equiv b_1 \dots b_k(\text{mod } m)$
   In particular, if $a \equiv b(\text{mod } m)$, then for any positive integer k, $a^k \equiv b^k(\text{mod } m)$.
7. *We have $a \equiv b(\text{mod } m_i),\ i = 1, \dots, k$ if and only if $a \equiv b\left(\text{mod } \text{lcm}(m_1, \dots, m_k)\right)$*
   In particular, if $m_1, \dots, m_k$ are pairwise relatively prime, then $a \equiv b(\text{mod } m_i), i = 1, \dots, k$ if and only if $a \equiv b(\text{mod } m_1 \dots m_k)$.
8. *Division: If $ac \equiv bc(\text{mod } m)$, then $a \equiv b\left(\text{mod } \frac{m}{\gcd(m,c)}\right)$*
   In particular, if $ac \equiv bc(\text{mod } m), \gcd(c, m) = 1$, then $a \equiv b(\text{mod } m)$
9. *If $a \equiv b(\text{mod } m)$, and $d \mid m$, then $a \equiv b\ (\text{mod } d)$.*
10. *If $a \equiv b(\text{mod } m)$ and $d \neq 0$, then $da \equiv db\ (\text{mod } dm)$.*

Example 1. (Russia 2001) Find all primes p and q such that $p + q = (p - q)^3$.

Definition 5.1 (Residue Classes or Congruence Classes)

Pick a natural number n, and a non-negative number $r < n$. Then the r^{th} residue class is the set of integers a that satisfy $a \equiv r\ (\text{mod } n)$. Equivalently, it is the set of all integers that leave r as a remainder when divided by n.
These integers are

$$\{\dots, r - 2n, r - n, r, r + n, r + 2n, r + 3n, \dots\}$$

Definition 5.2 (Complete System of Residues Modulo n)

By the division algorithm, any integer is just congruent to one of the numbers $0,1,\dots,n-1$ modulo n, the n numbers $0,1,\dots,n-1$ are not congruent each other modulo n. Therefore, there are totally n different classes modulo n. They are

$$M_i = \{x \mid x \in \mathbb{Z}, x = i \ (mod\ n)\}, i = 0,1,\dots,n-1.$$

$0,1,\dots,n-1$ *is a complete system of residues modulo n.*

Theorem 5.2 (Modular Contradictions)

Let n be an integer. Then

1. $n^2 \equiv 0 \ or\ 1 \ (mod\ 3)$
2. $n^2 \equiv 0 \ or\ 1 \ (mod\ 4)$
3. $n^2 \equiv 0 \ or \pm 1 \ (mod\ 5)$
4. $n^2 \equiv 0 \ or\ 1 \ or\ 4 \ (mod\ 8) \ or\ odd^2 \equiv 1 (mod\ 8)$
5. $n^3 \equiv 0 \ or \pm 1 \ (mod\ 7)$
6. $n^3 \equiv 0 \ or \pm 1 \ (mod\ 9)$
7. $n^4 \equiv 0 \ or\ 1 \ (mod\ 16)$

Proof: By Checking complete system of residue classes.

Example 2. Prove that the sum of the squares of 3, 4, 5, or 6 consecutive integers is not a perfect square.

Example 3. Assume that integers x, y and z satisfy

$$(x-y)(y-z)(z-x) = x+y+z.$$

Prove that $x+y+z$ is divisible by 27.

Theorem 6.1 (Two Special Equal Sets)

Let p be a prime and consider $S = \{0,1,2,\dots,(p-1)\}$ to be the set of non-zero remainder modulo p. Let a be any integer coprime to p. Then

$$aS \equiv S \ (mod\ p)$$

where, aS means the set obtained on multiplying each element of S by a.

Theorem 6.2 (Fermat's Little Theorem)

Let a be any number relatively prime to a prime p. Then

$$a^{p-1} \equiv 1 (mod\ p).$$

Alternatively,

Let a be any number. Then

$$a^p \equiv a\ (mod\ p)$$

Theorem 6.3 (General Equal Sets)

Let n be any integer. Let S be the set of integers less than n and relatively prime to n. Let a be any integer coprime to n. Then

$$aS \equiv S\ (mod\ n)$$

Definition 5.3 (Reduced System of Residues Modulo n)

Let n be any integer. Let S be the set of integers less than n and relatively prime to n. The set S is called a reduced residue system modulo n. We denote the number of reduced congruence classes modulo n by $\phi(m)$, and is called Euler's function. For example, $\phi(p) = p - 1$

Theorem 6.4 (Euler's Totient Theorem)

Let a be any number relatively prime to n. Then

$$a^{\phi(n)} \equiv 1 (mod\ n)$$

Example 4. Find 2^{98} $(mod\ 33)$.

Theorem 7.1 (Inverses)

Let p be a prime and a be an integer coprime to p. Then there always exists an integer x such that

$$ax \equiv 1\ (mod\ p)$$

This integer is called the inverse of a.

Note. If $ax \equiv b\ (mod\ p)$, then $x \equiv \frac{b}{a} \equiv b\ \cdot a^{-1} (mod\ p)$

Theorem 7.2 (General Inverses)

Let $n \geq 2$ be any positive integer. Then every number with $gcd(a, n) = 1$ has an inverse, that is a number x such that

$$ax \equiv 1\ (mod\ n).$$

We write $x = a^{-1}$

Theorem 7.3 (Inverses don't always exist)

If n is a natural number, and a is an integer, then a has an inverse modulo n if and only if $gcd(a, n) = 1$. In particular, if $gcd(a, n) > 1$, a does not have an inverse.

Theorem 7.4 (Inverses add like fractions)

Let $b, d \not\equiv 0 \ (mod\ p)$. Then for any a, c, we have

$$\frac{a}{b} + \frac{c}{d} \equiv a \cdot b^{-1} + c \cdot d^{-1} \equiv (ad + bc) \cdot (bd)^{-1} \equiv \frac{ad + bc}{bd} \ (mod\ p)$$

just like normal fractions.

Theorem 7.4 (Inverses multiply like fractions)

Let $b, d \not\equiv 0 \ (mod\ p)$. Then for any a, c, we have

$$\frac{a}{b} \cdot \frac{c}{d} \equiv (a \cdot b^{-1}) \cdot (c \cdot d^{-1}) \equiv (ac) \cdot (bd)^{-1} \equiv \frac{ac}{bd} \ (mod\ p)$$

just like normal fractions.

Example 5. Check the following whether they are true or not.

$$(i) \quad \frac{2}{3} \equiv 2 \cdot 3^{-1} \equiv 3 \ (mod\ 7)$$

$$(ii) \quad \frac{3}{8} \equiv 3 \cdot 8^{-1} \equiv 3 \ (mod\ 7)$$

$$(iii) \quad \frac{2}{3} + \frac{3}{8} \equiv \frac{16 + 9}{24} \equiv \frac{25}{24} \ (mod\ 7)$$

$$(iv) \quad \frac{2}{3} \cdot \frac{3}{8} \equiv \frac{1}{4} \ (mod\ 7)$$

Example 6. (AIME 1983) Let $a_n = 6^n + 8^n$. Determine the remainder on dividing a_{83} by 49.

Theorem 7.5 (Chinese Remainder Theorem)

The system of linear congruences

$$x \equiv a_1 (mod\ b_1)$$

$$x \equiv a_2 (mod\ b_2)$$

$$\ldots$$

$$x \equiv a_n (mod\ b_n),$$

where $b_1, b_2, \ldots, b_n$ are pairwise relatively prime (aka $\gcd(b_i, b_j) = 1$ iff $i \neq j$) has one distinct solution for x modulo $b_1 b_2 \ldots b_n$.

Example 7. (AIME II 2012) For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is $3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, \ldots$. Find the number of positive integers less than or equal to 10000 which are simultaneously 7-safe, 11-safe, and 13 safe.