NZM 2: Congruence

Michael Lee

1 Congruences

Definition If an integer m, not zero, divides the difference $a - b$, we say that a is congruent to b modulo m and write $a \equiv b(\text{mod m})$. If $a - b$ is not divisible by m say tt a is not conguent to b modulo $m \not\equiv b \pmod{m}$.

Theorem 1.1 *Let a, b, c, d, x, y denote integers*

1. *$a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $(a-b) \equiv 0 \pmod{m}$ are equivalent statements.*
2. *If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.*
3. *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ax + by \equiv bx + dy \pmod{m}$.*
4. *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.*
5. *If $a \equiv b \pmod{m}$ and $d \mid m$, $d>0$, then $a \equiv b \pmod{m}$.*
6. *If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$, for $c>0$.*

Theorem 1.2 *Let f denote a polynomial with integral coefficients. If $a \equiv b \pmod{m}$ then $f(a) \equiv f(b) \pmod{m}$.*

Theorem 1.3

1. *$ax \equiv ay \pmod{m}$ if and only if $x \equiv y \pmod{\frac{m}{(a,m)}}$*
2. *If $ax \equiv ay \pmod{m}$ and $(a, m) = 1$, then $a \equiv y \pmod{m}$.*

Definition If $x \equiv y \pmod{m}$ then y is called a residue of x modulo m. A set $x_1, x_2, \ldots x_m$ is called a complte residue system modulo m if for every integer y, there is one and only one x_j such that $y \equiv x_j \pmod{m}$.

Theorem 1.4 *If $x \equiv y \pmod{m}$, then $(x, m) = (y, m)$.*

Proof We have $x - y = mz$ for some integer z. Since $(x, m) \mid x$ and $(x, m) \mid m$, we have $(x, m) \mid y$ and hend $(x, m) \mid (y, m)$, therefore $(x, m) = (y, m)$.

Definition A reduced residue system modulo m is a set of integers r_i such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, and such that every x prime to m is congruent modulo m to some member r_i of the set.

Theorem 1.5 *The number $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.*

Theorem 1.6 *Let $(a, m) = 1$. Let $r_1, r_2, \ldots, r_n$ be a complete, or a reduced, residue system modulo m. Then $ar_1, ar_2, \ldots, ar_n$ is a complete, or a reduced, residue system, modulo m.*

Theorem 1.7 *Fermat's Theorem. Let p denote a prime. If $p \nmid a$ then $a^{p-1} \equiv 1$ (mod p). For every integer a, $a^p \equiv a$ (mod p).*

Theorem 1.8 *Euler generalization of Fermat's theorem. If $(a, m) = 1$, then*

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

Corollary 1.9 *If $(a, m) = 1$, then $ax \equiv b$ (mod m) has a solution $x = x_1$. All solutions are given by $x = x_1 + jm$ where $j = \pm 1, \pm 2, \ldots$.*

Theorem 1.10 *Wilson's Theorem. If p is a prime, then $(p-1)! \equiv -1$ (mod p).*

Theorem 1.11 *Let p denote a prime. Then $x^2 \equiv -1$ (mod p) has solutions if and only if $p = 2$ or $p \equiv 1$ (mod 4).*

Assignment NZM 2.1: 3, 9, 10, 14, 17, 18, 19, 24, 26

2 Solutions of Congruences

Definition Let $r_1, r_2, \ldots, r_m$ denote a complete residue system modulo m, The number of solutions $f(x) \equiv 0 \pmod{m}$ is the number of the r_i such that $f(r_i) \equiv 0 \pmod{m}$.

Definition Let $f(X) = a_0x^n + a_1x^{n-1} + \ldots a_n$. IF $a_0 \equiv 0 \pmod{m}$ the degree of the congruence $f(x) \equiv 0 \pmod{m}$ is n. If $a_0 \equiv 0 \pmod{m}$, let j be the smalelst positive integer such that $a_j \not\equiv 0 \pmod{m}$; then the degree of the congurnece is $n - j$. IF there is no such integer j, thjat is all the coefficients of $f(x)$ are multiples of m, no degree is assigned to the congruence.

Theorem 2.1 *If $d \mid m$, and if u is a solution of $f(x) \equiv 0$ (mod m), then u is a solution of $f(x) \equiv 0$ (mod d).*

Assignment None

3 Chinese Remainder Theorem

Theorem 3.1 *The congurnece* $ax \equiv b \pmod{m}$ *has exactly one solution if* $(a, m) = 1$. *More generally, if* g *denotes the greatest common divisor* (a, m), *the congruence is solvable if and only if* $g \mid b$. *IF* $g \mid b$ *the cognruence has exactly* g *solutions* $x \equiv x_0 + tm \pmod{m}$ *for* $t = 0, 1, \ldots, g-1$, *where* x_0 *is any solution of* $(\frac{a}{g})x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$

Theorem 3.2 *Given a cognruence* $ax \equiv b \pmod{m}$, *reduce it to* $my \equiv -b \pmod{a}$. *If* y_0 *is a solution of the reduced congruence, then* x_0 *defined by* $x_0 = \frac{my_0+b}{a}$ *is a solution of the original congruence.*

Theorem 3.3 *Chinese remainder theorem. Let* $m_1, m_2, \ldots, m_r$ *denote* r *positive integers that a rrelatively prime in pairs, and let* $a_1, a_2, \ldots, a_r$ *denote any* r *integers. Then the congruences* $x \equiv a_i \pmod{m_i}$, $i = 1, 2, \ldots, r$ *have common solutions. Any two solutions are congruent modulo* $m_1 m_2 \ldots m_r$.