MTH 305: Practice assignment 4

1 Properties of congruences

Establish the following assertions.

(i) If $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

(ii) $7 \mid 111^{333} + 333^{111}$.

(iii) For $n \geq 1$,

(a) $13 \mid 3^{n+2} + 4^{2n+1}$

(b) $43 \mid 6^{n+2} + 7^{2n+1}$

(iv) Any set of n consecutive integers form a complete set of residues modulo n.

(v) For any integer a, $a^4 \equiv 0$ or $1 \pmod{5}$.

(vi) If an integer a is not divisible by 2 or 3, $a^2 \equiv 1 \pmod{24}$.

(vii) If p is a prime and $n < p < 2n$, then

$$\binom{2n}{n} \equiv 0 \pmod{p}.$$

(viii) If $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then $a \equiv b \pmod{n}$, where $n = \operatorname{lcm}(n_1, n_2)$.

(ix) If a is an odd integer, then for any $n \geq 1$

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

(x) If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, then $b \equiv c \pmod{n}$, where $n = \gcd(n_1, n_2)$.

2 Linear congruences

1. Reading assignment: Read the proof of Theorem 4.9 (page 81) from Burton.

2. Solve the following linear congruences.

   (i) $5x \equiv 2 \pmod{26}$

   (ii) $36x \equiv 8 \pmod{102}$

   (iii) $140x \equiv 133 \pmod{301}$

   (iv) $17x \equiv 3 \pmod{210}$

   (v) $3x - 7y \equiv 11 \pmod{13}$

3. Solve the following systems of linear congruences.

   (a) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$

   (b) $2x \equiv 1 \pmod{5}$, $3x \equiv 9 \pmod{6}$, $4x \equiv 1 \pmod{7}$, $5x \equiv 9 \pmod{11}$

   (c) $3x + 4y \equiv 5 \pmod{13}$, $2x + 5y \equiv 7 \pmod{13}$.

   (d) $2x \equiv 3 \pmod{5}$, $4x \equiv 2 \pmod{6}$, $3x \equiv 2 \pmod{6}$

   (e) $7x + 3y \equiv 6 \pmod{11}$, $4x + 2y \equiv 9 \pmod{11}$

   (f) $11x + 5y \equiv 7 \pmod{20}$, $6x + 3y \equiv 8 \pmod{20}$

4. Prove that the system of congruences

   $$x \equiv a \pmod{n} \text{ and } x \equiv b \pmod{m}$$

   admits a simultaneous solution if and only if $\gcd(n, m) \mid a - b$. Moreover, when a solution exists, show that it is unique modulo $\operatorname{lcm}(n, m)$.

5. If $x \equiv a \pmod{n}$, prove that either $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.