Lec. 7 Number Theory

1. Division

2. Let a and b be integers, and let m be a positive integer. Then $a \equiv b \bmod m$ if and only if $a \bmod m = b \bmod m$

   Proof. By the standard division algo.

   $a = q_1 m + r_1 \quad 0 \le r_1 < m \quad a \bmod m = r_1$

   $b = q_2 m + r_2 \quad 0 \le r_2 < m \quad b \bmod m = r_2$

   "only if" $m \mid (a-b) = (q_1 - q_2)m + (r_1 - r_2) \quad m \mid (r_1 - r_2) \quad -m < r_1 - r_2 < m$

   the only possibility is $r_1 - r_2 = 0$

   "if" $r_1 = r_2$ then $a - b = (q_1 - q_2)m$ a multiple of m $m \mid a-b$

   "

3. Let m be a positive integer. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$.

   Proof. $m \mid (a-b)$, $m \mid (c-d)$ $\longrightarrow$ $m \mid (a-b)+(c-d) = (a+c)-(b+d)$ Property (i)

   $a + c \equiv b + d \pmod m$

   $m \mid (a-b)$ $\quad m \mid (a-b)c$

   $m \mid (c-d)$ $\quad m \mid b(c-d)$ $\quad$ Property (ii) $\quad m \mid (a-b)c + b(c-d) = ac - bd$

   $ac \equiv bd \pmod m$

4. Primes

5.

Lec 8

1. Goldbach's Conjecture (1 + 1): Every even integer n > 2, is the sum of two primes.

   "a+b" "every large even integer is the sum of two integer A and B, where the number of prime factors of A is <= a, and the # of prime factors of B is <= b"

2. 线性同余:

1. An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *inverse* of a modulo m.

2. 找inverse的方法:
   1. gcd(a,m) = 1 => sa + tm=1 (Extended Eulidean Algo) => inverse of a is s

3. 中国余数定理(Chinese Remainder Theorem)

- **Example**

  23 $x \equiv 2 \pmod{3}$

  23 $x \equiv 3 \pmod{5}$

  23 $x \equiv 2 \pmod{7}$

1. $m = m_1 m_2 m_3 = 3 \times 5 \times 7 = 105$

   $M_1 = m/m_1 = m/3 = 35$

   $M_2 = m/5 = 21$

   $M_3 = m/7 = 15$

   ① By extended Euclidean Algo.

   $y_1 M_1 \equiv 1 \bmod 3$ $\quad y_1 \cdot 35 \equiv 1 \bmod 3$

   $y_2 M_2 \equiv 1 \bmod 5$ $\quad y_2 \cdot 21 \equiv 1 \bmod 5$

   $y_3 M_3 \equiv 1 \bmod 7$ $\quad y_3 \cdot 15 \equiv 1 \bmod 7$

   ② $y_2 \equiv 1 \bmod 5$ $\quad y_3 \equiv 1 \bmod 7$

   $2y_1 \equiv 1 \bmod 3$

   $y_1 \equiv 2 \bmod 3$ ③

   $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

   $= 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1$

   $= 233 \equiv 23 \pmod{105}$

   17

2.