Lec. 7 Number Theory

- 1. Division
 - Let a and b be integers, and let m be a positive integer.

Then $a \equiv b \mod m$ if and only if $a \mod m = b \mod m$

pravf By the standard division algo.

$$a = q_1 m + r_1$$
 $p \le r_1 < m$ and $m = r_1$
 $b = q_2 m + r_2$ $p \le r_2 < m$ be mad $m = r_2$

by the standard division algo.

 $a = q_1 m + r_1$ $p \le r_1 < m$ and $a = r_2$

by the standard division algo.

 $a = q_1 m + r_1$ $p \le r_1 < m$ and $a = r_2$

by the standard division algo.

 $a = q_1 m + r_1$ $p \le r_1 < m$ and $a = r_2$

by the standard division algo.

 $a = q_1 m + r_1$ $p \le r_1 < m$ and $a = r_2$

by the standard division algo.

 $a = q_1 m + r_1$ $p \le r_1 < m$ and $a = r_2$

by the standard division algo.

 $a = q_1 m + r_1$ $p \le r_1 < m$ and $a = r_2$

by the standard division algo.

 $a = q_1 m + r_1$ $p \le r_1 < m$ and $a = r_2$

by the standard division algo.

 $a = q_1 m + r_1$ $p \le r_1 < m$ and $a = r_2$

the ship passibility is $a = r_1 < m$ and $a = r_2 < m$

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.
$$m|(z-d)$$
 \longrightarrow $m|(a-b)+(c-d)$ $(a+c)-(b+d)$

at $c \equiv btd \pmod{m}$

$$m(a-b)$$
 $m(a-b)c$ property (ii) $m(a-b)c+b(c-d)$
 $m(c-d)$ $m(c-d)$ $m(c-b)d$
 $ac-bd$
 $ac=bd$
 $ac=bd$
 $ac=bd$

- 4. Primes
- 5.

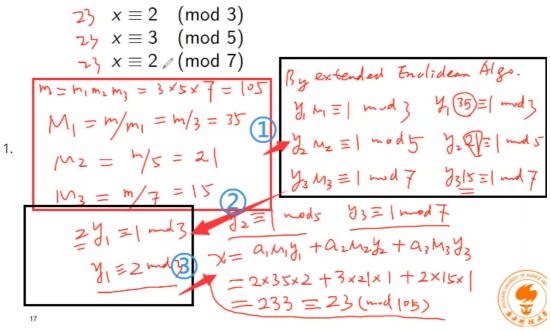
Lec 8

- 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 \leq a, and the # of prime factors of B is \leq 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) => <mark>inverse of a is s</mark> 3. 中国余数定理(Chinese Remainder Theorem)

Example



2.