THEOREMS ABOUT CONGRUENCES

1. (Linear Congruences). Suppose that $a,\ b \in \mathbf{Z}$ and that m is a positive integer. Assume that $gcd(a, m) = 1$. Then the congruence

$$ax \equiv b \pmod{m}$$

has infinitely many solutions where $x \in \mathbf{Z}$. If x_0 is one solution, then all the solutions are described by

$$x \equiv x_0 \pmod{m} \ .$$

2. (Linear Congruences). Suppose that $a,\ b \in \mathbf{Z}$ and that m is a positive integer. Let $d = gcd(a, m)$. Then the congruence

$$ax \equiv b \pmod{m}$$

has solutions where $x \in \mathbf{Z}$ if and only if $d \big| b$. If x_0 is one solution, then all the solutions are described by

$$x \equiv x_0 \pmod{m/d} \ .$$

3. (Chinese Remainder Theorem.) Let $t \geq 1$. Suppose that $m_1, ..., m_t$ are positive integers which are pairwise relatively prime. Suppose that $a_1, ..., a_t$ are arbitrary integers. Consider the set of congruences

$$x \equiv a_1 \pmod{m_1}, \ \ . \ \ . \ \ . \ \ . \ \ , \ \ x \equiv a_t \pmod{m_t} \ . \tag{1}$$

Let m be the product of the integers $m_1, ..., m_t$. Then there exists an integer a such that (1) is equivalent to the single congruence

$$x \equiv a \pmod{m} \ . \tag{2}$$

Consequently, the set of congruences (1) has infinitely many solutions x and any two solutions are congruent to each other modulo m.

MORE THEOREMS ARE ON THE BACK OF THIS HANDOUT

4. Suppose that $a \in \mathbf{Z}$, that m is a positive integer, and that $gcd(a, m) = 1$. Then there exists a positive integer k such that $a^k \equiv 1 \pmod{m}$.

Definition: Assume that $gcd(a, m) = 1$. The smallest positive integer e such that

$$a^e \equiv 1 \pmod{m}$$

is called the *order of a modulo m*. The integer e is denoted by $ord_m(a)$.

5. Suppose that m is a positive integer and that a is an integer such that $gcd(a,\ m) = 1$. Let $e = ord_m(a)$.

(a) Let $k \geq 0$. Then $a^k \equiv 1 \pmod{m}$ if and only if $e|k$.

(b) Let $k_1,\ k_2 \geq 0$. Then $a^{k_1} \equiv a^{k_2} \pmod{m}$ if and only if $k_1 \equiv k_2 \pmod{e}$.

6. (Fermat's Little Theorem.) Suppose that p is a prime and that a is an integer which is not divisible by p. Then $a^{p-1} \equiv 1 \pmod{p}$.

7. (Euler's Theorem.) Suppose that m is a positive integer and that a is an integer such that $gcd(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

8. Suppose that p is a prime and that a is an integer which is not divisible by p. Then $ord_p(a)$ divides $p - 1$.

9. Suppose that m is a positive integer and that a is an integer such that $gcd(a, m) = 1$. Then $ord_m(a)$ divides $\varphi(m)$.

10. (The Primitive Root Theorem.) Let p be a prime. Then there exists an integer a such that $ord_p(a) = p - 1$. Furthermore, for any positive integer d which divides $p - 1$, there exists an integer b such that $ord_p(b) = d$.

11. Suppose that p is a prime. The congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.