MATH 8
HANDOUT 23: LINEAR CONGRUENCES

Linear Congruences

Solving the congruence $ax \equiv b \mod m$ is equivalent to solving $ax - my = b$. We already know we can use Euclid's algorithm to solve this type of equations.
Let $d = gcd(a, m)$. If $d \not| b$ then the linear congruence $ax \equiv b \mod m$ has no solutions. If $d|b$ then the linear congruence $ax \equiv b \mod m$ has exactly d solutions (by solution we mean different congruence classes modulo m). The solutions are of the form $x = x_0 + (\frac{m}{d})t$, where t takes integer values, 0, 1,...,d-1.

Inverse modulo m

An inverse of $a \mod m$ is any integer such that $a \cdot c \equiv 1 \mod m$. We can also write it as $a^{-1} \mod m = c$. An inverse of $a \mod m$ exists if and only if gcd(a, m)=1.

Problems

1. For the following equations, find at least one solution (if exists; if not, explain why)

$$5x \equiv 1 \mod 19$$
$$9x \equiv 1 \mod 24$$
$$9x \equiv 6 \mod 24$$

2. Show that the equation $ax \equiv 1 \mod m$ has a solution if and only if $\gcd(a, m) = 1$. Such an x is called the inverse of a modulo m. [Hint: Euclid's algorithm!]

3. Find the following inverses
inverse of 2 mod 5
inverse of 5 mod 7
inverse of 7 mod 11
inverse of 11 mod 41

4. Show that if $a \equiv 1 \mod n$ and $a \equiv 1 \mod m$ and gcd(m,n)=1 then $a \equiv 1 \mod mn$.

5. Given integers m, n,
(a) Prove that $(m+1)^n \equiv 1 \mod m$
(b) Given some integer k, determine the value of $(m+1)^0 + (m+1)^1 + (m+1)^2 + ... + (m+1)^k \mod m$
(c) Determine the value of $1111 \mod 9$
(d) Given some integer a written in base 10, determine a method for finding the value of a mod 9.

6. Given a prime p, let a_1, a_2, ..., a_k be a set of positive integers each less than p. Prove that the product $a_1 a_2 ... a_k$ cannot be divisible by p.

7. For a positive number n, let $\tau(n)$ (this is Greek letter "tau") be the number of all divisors of n (including 1 and n itself).
Compute
$\tau(10)$
$\tau(77)$
$\tau(p^a)$, where p is prime (the answer, of course, depends on a)
$\tau(p^a q^b)$, where p, q are different primes
$\tau(10000)$
$\tau(p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})$, where p_i are distinct primes.