Abstract II Spring 2010
Fermat's and Euler's theorems-Section 20

Goal:
In this section we will concentrate on the ring $\mathbb{Z}_n$ and learn tools that will help us to do some crazy arithmetic.
Motivation: Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove that if p is prime then

$$a^p \equiv a \mod p \text{ for all } a \in \mathbb{Z}.$$

Theorem 0.1. *(Fermat's Little Theorem) If $a \in \mathbb{Z}$ and p is a prime not dividing a, then*

$$a^{p-1} \equiv 1 \mod p, \text{ for } a \neq 0 \mod p$$

Applications:

1. Compute the remainder of 3^{47} when it is divided by 23.

2. Show that $2^{11,213} - 1$ is not divisible by 11.

Euler's generalization to Fermat's theorem
We will not be restricted to the ring $\mathbb{Z}_p$ for p prime.

Theorem 0.2. *The set of G_n of nonzero elements of $\mathbb{Z}_n$ that are not zero divisors form a group under multiplication modulo n.*

Proof:

Definition 0.3. *Let n be a positive integer. The function $\phi\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ defined as $n \mapsto \phi(n)$=the number of positive integers less than or equal to n and relatively prime to n is called Euler phi-function.*

Theorem 0.4. *(Euler's Theorem) If a is an integer relatively prime to n then*

$$a^{\phi(n)} \equiv 1 \mod n$$

Proof:

Solving congruences $ax \equiv \mod m$

Theorem 0.5. *Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in $\mathbb{Z}_m$.*

Proof:

Theorem 0.6. *Let m be a positive integer and let $a, b \in \mathbb{Z}_m$. Let $gcd(a, m) = d$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and onlt if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$.*

Proof:

Describe all the solutions to the given congruences.

1. $36x \equiv 15 \mod 24$

2. $45x \equiv 15 \mod 24$