Lecture 7

$a = bq + r_0$

$0 \le r_0 < b$

$0 \le |r_0| < \frac{b}{2}$

Last time: Fermat's Little Thm

$p \nmid a$, $a^{p-1} \equiv 1 \bmod p$

This can be used to show that a number is not a prime without factoring it.

$2^{1234566} \equiv 899557 \bmod 1234567$

if 1234567 is a prime, $2^{123456} \equiv 1 \bmod 1234567$

so 1234567 is not a prime.

$m = 10^{100} + 37$

$2^{m-1} \bmod m$, $2^{m-1} \not\equiv 1 \bmod m \Rightarrow m$ is not a prime.

$(p-1)!$ $\quad a^{p-1}(p-1)! \equiv (p-1)! \bmod p$

$p \nmid \underset{(p-1)\cdots 1}{\underset{\parallel}{(p-1)!}} \Rightarrow a^{p-1} \equiv 1 \bmod p$

$(p-1)! \bmod p \equiv -1 \bmod p$ (always) can be proved by induction.

$\underbrace{1 \cdot 2 \cdots (p-2)}_{\underset{1 \bmod p}{\equiv}}(p-1) \equiv p-1 \equiv -1 \bmod p$

Chapter 10 Euler's formula (generalization of Fermat)

$a^{p-1} \equiv 1 \bmod p$ is no longer true if m is not a prime.

$5^5 \bmod 6 \equiv (-1)^5 \equiv -1 \bmod 6$ (NOT 1 here)

$5 \equiv -1 \bmod 6$

$a^{\square} \equiv 1 \bmod m$

$\square$ is $\phi(m)$ makes the equation hold for any int m.

Suppose $a^k \equiv 1 \bmod m$

$a^k = 1 + my$ for some y

$a \cdot \boxed{a^{k-1}} - my = 1$

$\Rightarrow \gcd(a, m) = 1$ We need to look at the set of numbers that are relatively prime to m.

$S_m = \{a : 1 \le a \le m, \gcd(a, m) = 1\}$

m	S_m
1	$\{1\}$
2	$\{1\}$
3	$\{1, 2\}$
4	$\{1, 3\}$
$\vdots$	
12	$\{1, 5, 7, 11\}$

if m is a prime, $S_p = \{1, 2, \cdots, p-1\}$

$\phi(m)$ Euler phi-function

$= \# S_m = |S_m|$

Euler's formula

$\gcd(a,m)=1$
$a^{\phi(m)} \equiv 1 \bmod m$

(Mimic the proof of Fermat's little theorem)

$\{1,2,\cdots,p-1\}$
$\{a,2a,\cdots,a(p-1)\}$] → are the same mod p

Let $1 \le b_1 < b_2 < \cdots < b_{\phi(m)} \le m$
$S_m = \{b_1, b_2, \cdots, b_{\phi(m)}\}$
Claim: $\{b_1 a, b_2 a, \cdots, b_{\phi(m)} a\} = \{b_1, b_2, \cdots, b_{\phi(m)}\} \bmod m$ They may be in a different order.

Proof of the claim: If $\gcd(b,m)=1$, then $\gcd(a\cdot b, m)=1$
So for each i, $b_i a \equiv b_j \bmod m$ for some j (switch)
So we only need to show $b_i a \not\equiv b_j a \bmod m$ if $i \ne j$ (distinct)
proof by contradiction.
Suppose $b_i a \equiv b_j a \bmod m$
$m \mid (b_i - b_j)a \Rightarrow m \mid (b_i - b_j)$ because $\gcd(m,a)=1$
but $|b_i - b_j| < m \Rightarrow b_i - b_j = 0$
Now $(b_1 a)(b_2 a)\cdots(b_{\phi(m)} a) \equiv b_1 b_2 \cdots b_{\phi(m)} \bmod m$
$a^{\phi(m)}(b_1 \cdots b_{\phi(m)}) \equiv b_1 b_2 \cdots b_{\phi(m)} \bmod m$
$\gcd(b_1 \cdots b_{\phi(m)}, m) = 1$
So $a^{\phi(m)} \equiv 1 \bmod m$

What is $b_1 b_2 \cdots b_{\phi(m)} \bmod m$? (HW)

* It can happen that $a^{m-1} \equiv 1 \bmod m$ even though m is not a prime.
(the smallest such # is 561)
$m = 561 = 3 \times 11 \times 17$
$\phi(m) = \phi(3)\phi(11)\phi(17) = 2 \times 10 \times 16 = 320$
$a^{320} \equiv 1 \bmod 561 \rightsquigarrow a^{560} \equiv 1 \bmod 561$
*561 is called a Carmichael number (∞ many)

Last two digits of $3^{1000} = 3^{1000} \bmod 100$
$\phi(100) = 40$
$3^{40} \equiv 1 \bmod 100$
$1000 = 40 \times 25$
$3^{1000} = (3^{40})^{25} \equiv 1 \bmod 100$