Lecture 12
Jan 30th, 2015
1st term test Friday Feb 6 9:10-10am
Ex300 (A-L)
Ex320 (M-Z)

Chapters 1-13

$\phi(n)=160=2^5\times 5$

$n=2^k 5^m p_1^{k_1}\cdots p_r^{k_r},\ p_i\neq 2,5$

$\phi(n)=2^{k-1}5^{m-1}\times 4p_1^{k-1}(p_1-1)\cdots p_r^{k_r-1}(p_r-1)$

$k_1=\cdots=k_r=1$

$p_i-1=2^5 5$ or 2^k, $m\leq 2$

Prime of the form $p-1=2^k$, $k\leq 5$ or $2^k 5$

3, 11, 17, 41, ... there are 12 different solutions.

Chapter 16

How would we complete $5^{10^{14}}$ mod 12830603

$12830603=3571\times 3593$ both are primes

$\phi(12830603)=3570\times 3592=12823440$

$5^{12823440}\equiv 1 \bmod 12830603$

$10^{14}=12830440\times 7798219+6546640$

$5^{10^{14}}\equiv 5^{6546640} \bmod 12830603$

Successive squaring method to compute $a^k \bmod m$.

$7^{327} \bmod 853$

Create a table giving the value, $7, 7^2, (7^2)^2, \cdots$ mod 852

$7\equiv 7 \bmod 853$

$7^2\equiv 49$

$(7^2)^2\equiv 2401\equiv 695 \bmod 853$

$7^8\equiv 227 \bmod 853$

Next make 327 as a sum of primes of 2 binary expansion.

$327=2^8+71=2^8+2^6+7=2^8+2^6+2^2+2^1+2^0$

$7^{327}=7^{2^8}7^{2^6}7^{2^2}7^{2^1}7^{2^0}=286 \bmod 853$

It takes $\log_2 k$ steps to compute a^k mod m, approximately equals to 3.332 times of the digits

Method of successive squaring to compute a^k mod m.

1. Write k as a sum of power of 2 (binary expansion of k)

   $k=u_0+u_1 2^1+u_2 2^2\cdots u_r 2^r,\ u_i=0$ or 1

2. Make a table of powers of a mod m using successive squaring

   $a^1\equiv A_0 \bmod m$

   $a^2\equiv A_0^2\equiv A_1$

$a^{2^2} \equiv A_1^2 \equiv A_2$
$a^{2^3} \equiv A_2^2 \equiv A_3$
$\cdots$
$a^{2^r} \equiv A_{r-1}^2 \equiv A_r$

3. $a^k = a^{u_0+u_1 2+\cdots+u_r 2^r} = a^{u_0}(a^2)^{u_1}\cdots(a^{2^r})^{u_r} \equiv A_0^{u_0} A_1^{u_1}\cdots A_r^{u_r} \mod m$

Note: This method wouldn't be tested because a calculator is needed then. So the only possible scenario in test is "to write the steps of it"

Method of checking whether a given number m is a prime or not.
Take any number a
If $d=\gcd(a,m)>1$, $d \mid m$ so m is not a prime.
If $\gcd(a,m)=1$, use successive squaring to compute $a^{m-1} \mod m$.
Fermat's Little Thm: if m is a prime, $a^{m-1} \equiv 1 \mod m$.
So if $a^{m-1} \not\equiv 1 \mod m$ then m is not a prime.
e.g. $2^{28397671080 3262} \equiv 2810196559097287 \mod 2839767 10803263$
So m is not a prime.
Suppose for any a, $\gcd(a,m)=1$, $a^{m-1} \equiv 1 \mod m$

Does this mean m is a prime? No!

There do exist composite number m such that $a^{m-1} \equiv 1 \mod m$, called Carmichael numbers.
e.g. $\gcd(a,m)=1$, $a^{80} \equiv 1 \mod m \rightarrow a^{560} \equiv 1 \mod 561$, $m=561=3\times11\times17$

Chapter 17
Compute k^{th} root mod m
$$x^k \equiv b \mod m$$
If $\gcd(k,\phi(m))=1$, then we can compute easily

$x^{131} \equiv 758 \mod 1073 = 29\times37$
$\phi(1073)=28\times36=1008$
$\gcd(131,1008)=1$ these exists u,v such that $131u-1008v=1$

$(x^{131})^u = x^{131u} = x^{1+1008v} = x(x^{1008})^v \equiv x$
$x^{1008} \equiv 1 \mod 1073$
$x \not\equiv 0 \mod 1073$
so $x \equiv 758^u \mod 1073$
use successive squaring
$1008\times36 - 131\times277 = 1$
$u = -277 + 1008 = 731$
$x \equiv 758^{731} \equiv 905 \mod 1073$