Lesson 26

pseudo primes
Euler's φ function

Equivalent form of Fermat's little th:
If p is prime $a^p \equiv a \mod p$

1) If $(p, a) = 1$ we can multiply

$$a^{p-1} \equiv_p 1 \quad \text{by } a$$
$$a \cdot a^{p-1} \equiv_p a$$

2) If $(a, p) \neq 1$ then $(a, p) = p$

therefore $a^p_p \equiv_p a \equiv 0$

Is the converse true?
If $a^p \equiv_p a$ then p is prime?

No
Def If n is composite and $a^n \equiv_n a$
n is called a pseudoprime in base n

Pseudoprimes are rare.

Example $\quad 91 = 13 \cdot 7 \qquad (3, 91) = 1$

$3^{90} \mod 91$

$90 = 64 + 16 + 8 + 2$

$3^2 = 9 \mod 91$

$3^4 = 81 \mod 91$

$3^8 = 81^2 \equiv 9 \mod 91$

$3^{16} = 81 \mod 91$

$3^{32} \equiv 9 \mod 91$

$3^{64} \equiv 81 \mod 91$

$3^{90} = 3^2 \cdot 3^8 \cdot 3^{16} \cdot 3^{64} \equiv 9 \cdot 9 \cdot 81 \cdot 81 \equiv 1 \mod 91$

So 91 is a pseudoprime to base 3

Different calculation of $3^{90} \bmod 91$

$91 = 13 \cdot 7$

$3^{90} \bmod 7$: $(3^6)^{15} \equiv 1^{15} \equiv 1 \bmod 7$

$3^{90} \bmod 13$: $(3^{12})^7 \cdot 3^6 \quad \cdot (27)^2 \equiv 1 \cdot 1^2 \equiv 1 \bmod 13$

so 7 div $3^{90} - 1$ and 13 div $3^{90} - 1$

therefore $3^{90} - 1 = 7h = 13k$ for some

$h, k \in \mathbb{Z}$ so 7 div $13 \cdot k$ and

since $(7, 31) = 1$ 7 div k so $k = 7 \cdot \ell$

$3^{90} - 1 = 13 \cdot 7 \cdot \ell$ for some $\ell \in \mathbb{Z}$

so $3^{90} \equiv 1 \bmod 91$

Idea for a primality test:

Is n prime?

Compute $2^n \bmod n$ if $\neq 2$ n is composite

if 2 n is probably prime, to further check

Compute $3^n \bmod n$ if $\neq 3$ n is composite

....

There are composite numbers that are pseudoprime to any base a

Def: Given $a \in \mathbb{Z}_m$, if there is an integer k s.t $a^k = 1$ in $\mathbb{Z}_m$ then the order of a is defined to be the smallest positive integer j s.t $a^j = 1$.

If no power of a is equal to 1 the order of a is not defined

The function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ such that $\phi(n) =$ the number of positive integers which are $\leq n$ and are relatively prime to n is called the Euler's ϕ function.

Example $\phi(10) = 4$

because of the numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

4 of them: 1, 3, 7, 9 are relatively prime to 10 i.e $(10, a) = 1$

Facts about φ

1) If p is prime then $\phi(p) = p - 1$

2) If p and q are primes then $\phi(p \cdot q) = (p-1)(q-1)$

(it is true in general that if (m,n)=1 then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$)

3) Euler 's theorem: If (a,n)=1 then $a^{\phi(n)} \equiv 1$ mod n

Proof of Euler's th:

Consider all the elements of Z_n; exactly $\phi(n)$ of them are relatively prime to n, call them $a_1, a_2, \cdots a_{\phi(n)}$. Multiply each element by a : $a \cdot a_1, a \cdot a_2, \cdots a \cdot a_{\phi(n)}$ are all distinct in Z_n (i.e no two of them are congruent mod n) and they are also all relatively prime to n , therefore (why ?) they must each be congruent to one of $a_1, a_2, \cdots a_{\phi(n)}$. So

$$a_1 \cdot a_2 \cdot \cdots a_{\phi(n)} \equiv a \cdot a_1 \cdot a \cdot a_2 \cdots a_{\phi(n)} \text{ mod n}$$

or

$$a_1 \cdot a_2 \cdot \cdots a_{\phi(n)} \equiv a^{\phi(n)} \cdot a_1 \cdot a_2 \cdots a_{\phi(n)} \text{ mod n}$$

Since the elements a_i are all relatively prime to n they can be cancelled and we get

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