Lecture 9

Euler's formula : $\gcd(a,m)=1$

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

$m = p_1^{k_1} \cdots p_r^{k_r}$, p_i distinct primes

$$\phi(m) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r})$$
$$= (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_k^{k_r-1})$$
$$= m \prod_{p \mid m} (1 - \frac{1}{p})$$

For those who study group theory.

$$f(m) = LCM(p_1^{k_1} - p_1^{k_1-1}, \cdots, p_r^{k_r} - p_r^{k_r-1})$$
$$a^{f(m)} \equiv 1 \mod m$$

e.g. $\gcd(a, 561) = 1$

$$a^{80} \equiv 1 \mod 561$$
$$a^{560} \equiv (a^{80})^7 \equiv 1 \mod 561$$
$$m = 561 = 3 \times 11 \times 17$$
$$\phi(m) = 2 \times 10 \times 16 = 320$$
$$f(m) = LCM(2, 10, 16) = 80$$

Any composite number m which satisfies $a^{m-1} \equiv 1 \mod m$ is called Carmichael number.

Ex: Last 2 digits of 3^{1000}, 2^{1000}

$$\log 3^{1000} = 1000 \log 3 \quad \text{(either base e or 10)}$$
$$= 1000 \cdot 0.48$$

$3^{1000} \mod 100 = 10^2 = 2^2 \times 5^2$ (for last 2 digits)

$$\phi(100) = \phi(2^2)\,\phi(5^2) = 2 \times (5^2 - 5) = 40$$
$$3^{40} \equiv 1 \mod 100$$

$3^{1000} = (3^{40})^{25} \equiv 1 \mod 100 \Rightarrow$ last 2 digits is "01"

$2^{1000} \mod 100$ (we cannot apply Euler's formula, since $2 \mid 100$)
so, we need some trick

$\boxed{\text{my version}}$: $2^{20} \equiv 1 \mod 25$ (by Euler)

$$2^{1000} = (2^{20})^{50} \equiv 1 \mod 25$$
$$2^{1000} \equiv 0 \mod 4$$

$$\left.\begin{aligned} x &\equiv 1 \mod 25 \\ x &\equiv 0 \mod 4 \end{aligned}\right\} \Longrightarrow CRT \rightarrow x \equiv 76 \mod 100$$

last 4 digits of 2^{1000} are 9376

Chapter 12 Twin Prime Conjecture

Goldbach Problem:

Any even # is a sum of two primes.

Solved: — Ternary Goldbach Problem.

Any odd # > 5, is sum of 3 primes

Euclid: There are inf. many primes.

Proof: Suppose there are only finitely many primes. $p_1, \cdots, p_r$.

Let $A = p_1 \cdots p_r + 1$.

A cannot be prime since $A > p_i$, $\forall i$

Let q be the smallest prime dividing A.

Claim: q can't be p_i for any i

Suppose q is p_i for some i, $q \mid (p_1 \cdots p_r + 1) \Rightarrow q \mid 1$, contradiction

$\{2\}$ $A = 2+1$

$A = 2+1 = 3$

$\langle 2,3 \rangle$

$A = 2 \times 3 + 1 = 7$

$\langle 2,3,7 \rangle$

$A = 2 \times 3 \times 7 + 1 = 43$

$\langle 2,3,7,43 \rangle$

$\vdots$

* 2 is the only even prime

$\Rightarrow p > 2$ is odd, only two kinds $\begin{cases} p \equiv 1 \bmod 4 \\ p \equiv 3 \bmod 4 \end{cases}$

$\Rightarrow$ Dirichlet's Theorem on Arithmetic Progression

primes are evenly distributed.

Proof: requires complex analysis.

We prove a weak result

Prime 3 (mod 4) Theorem, there are infinitely many prime, that are congruent to 3 mod 4

Proof: Sps there are only fin. many primes $\equiv 3 \bmod 4$.

$3 p_1 \cdots p_r$

Let $A = 4p_1 \cdots p_r + 3 > p_r$ thus A is not prime.

$A \equiv 3 \bmod 4$

$A = q_1 \cdots q_s$ (prime factorization)

Claim (1): One of q_i is $\equiv 3 \bmod 4$

(2): $q_i \neq p_j$ for any j, $q_i \neq 3$

(1). If not $q_i \equiv 1 \bmod 4$ $\forall i$

$\Rightarrow A \equiv 1 \bmod 4$ contradiction.

(2). $q_i \mid A = 4p_1 \cdots p_r + 3$, if $q_i = p_j$ for some j or $q_i \neq 3$ $\Rightarrow$ contradiction

sps $p_j \nmid A$

$3 \nmid A$

$\langle 7 \rangle$: $A = 4 \times 7 + 3 = 31$

$\langle 7,31 \rangle$: $A = 4 \times 7 \times 31 + 3 = 871 = 13 \times 67$

$67 \equiv 3 \bmod 4$. $\langle 7, 31, 67 \rangle$