60

Lemma: If p and q are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$ then

$$a^{pq} \equiv a \pmod{pq}$$

Proof:

61

Note: The Converse of Fermat's theorem is false, i.e if

$$a^{p-1} \equiv 1 \pmod{p} \not\Rightarrow p \text{ is a prime.}$$

e.g: $2^{560} \equiv 1 \pmod{561}$

but 561 is not a prime.

62

<u>Pseudoprime:</u> A composite integer n is called pseudoprime whenever $n \mid 2^n - 2$ or

$$2^n \equiv 2 \pmod{n}$$

→ There are infinitely many primes.

→ The smallest four being 341, 561, 645, 1105

→ A composite integer n for which $a^n \equiv a \pmod{n}$ is called a pseudoprime to the base a.

→ 91 is pseudoprime to the base 3, $3^{91} \equiv 3 \pmod{91}$

→ 217 is pseudoprime to the base 5, $5^{217} \equiv 5 \pmod{217}$

63

<u>Carmichael Number</u>: composite number n that are pseudoprime to ~~the~~ every base a, i.e,

$$a^n \equiv a \pmod n$$

$\forall\, a \in \mathbb{Z}$. These numbers are also called absolute pseudoprimes.

<u>e.g:</u> 561 is a Carmicheal number.

$$561 = 3 \cdot 11 \cdot 17$$

$$\gcd(a, 561) = 1$$

$$\Rightarrow \gcd(a, 3) = 1, \quad \gcd(a, 11) = 1$$

and $\gcd(a, 17) = 1$.

By Fermat's Theorem

$$a^{p-1} \equiv 1 \pmod p$$

$$a^{2} \equiv 1 \pmod{3}$$

$$a^{10} \equiv 1 \pmod{11}$$

$$a^{16} \equiv 1 \pmod{17}$$

$$a^{560} = \left(a^{2}\right)^{280} \equiv 1 \pmod{3}$$

$$a^{560} = \left(a^{10}\right)^{56} \equiv 1 \pmod{11}$$

$$a^{560} = \left(a^{16}\right)^{35} \equiv 1 \pmod{17}$$

$$\Rightarrow \quad a^{560} \equiv 1 \pmod{561}$$

$$\gcd(a, 561) = 1$$

$$\therefore \quad a^{561} \equiv a \pmod{561}$$

$\Rightarrow$ 561 is a Carmichael number.

65

Theorem: Let n be a composite square-free integer, say, $n = p_1 p_2 \ldots p_r$, where p_i are distinct primes. If $p_i - 1 \mid n-1$ for $i = 1, 2, \ldots r$, then n is absolute pseudoprime.

Proof: Let $a \in \mathbb{Z}$ s.t $(a, n) = 1$

$$\Rightarrow \quad (a, p_i) = 1 \quad \forall\, i,\ i = 1, 2, \ldots r$$

By Fermat's theorem

$$a^{p_i - 1} \equiv 1 \pmod{p_i}$$

ie $p_i \mid a^{p_i-1} - 1$

Also, $p_i - 1 \mid n-1 \quad \forall\, i = 1, 2, \ldots r$ (given)

66

$\Rightarrow \quad n-1 = t(p_i - 1)$ for some $t \in \mathbb{Z}$.

$$\therefore \quad a^{n-1} \equiv \left(a^{p_i - 1}\right)^t \pmod{p_i}$$
$$\equiv 1 \pmod{p_i}$$

$\Rightarrow \quad p_i \mid a^{n-1} - 1 \quad \forall\, i = 1, 2, \ldots r.$

$\Rightarrow \quad n \mid a^{n-1} - 1$

$\Rightarrow \quad a^{n-1} \equiv 1 \pmod{n}$

$\Rightarrow \quad a^n \equiv a \pmod{n}$

$\Rightarrow$ a is a Carmichael number.

67

Euler's Phi function: for $n \geq 1$, let $\phi(n)$ denotes the number of positive integers not exceeding n that are relatively prime to n, i.e,

$$\phi(n) = \{ x \in \mathbb{Z} \mid x < n \ \& \ \gcd(x, n) = 1 \}$$

$$\phi(30) = 8$$

$$\phi(1) = 1$$

→ $\phi(p) = p - 1$, p is a prime

→ $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$;
p is a prime

→ $\phi(mn) = \phi(m)\phi(n)$, $(m, n) = 1$

→ $=$

68

<u>Theorem:</u> If the integer $n>1$ has the prime factorization

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \text{ then}$$

$$\phi(n) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right) \cdots \left(p_r^{k_r} - p_r^{k_r-1}\right)$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$