Theorem 25 (Fermat's Little Theorem). If p is a prime and a is an integer such that p does not divide a, then

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

Proof: Consider the $(p-1)$ integers

$$a, 2a, 3a, 4a, \ldots, (p-1)a \qquad \text{---} (1)$$

We show that no two distinct members of the above $(p-1)$ integers are congruent to each other modulo p.

Suppose, if possible, $ra \equiv sa \pmod{p}$ where $1 \le s < r \le p-1$. Then $(r-s) \equiv 0 \pmod{p}$. Hence p divides $(r-s)a$. Since p is a prime, either p divides $r-s$ or p divides a. Now $1 \le s < r \le p-1$, Hence p does not divide $r-s$. Also from the hypothesis we find that p does not divide a. Hence $ra \not\equiv sa \pmod{p}$. Also we find that $ra \not\equiv 0 \pmod{p}$ for $r = 1, 2, 3, \ldots, p-1$. Hence $ra \equiv i \pmod{p}$ where i is an integer such that $0 < i \le p-1$.

Since no two distinct members are congruent to each other and there are $p-1$ distinct integers $a, 2a, \ldots, (p-1)a$, it follows that $p-1$ integers $a, 2a, \ldots, (p-1)a$ must be congruent modulo p to $1, 2, 3, \ldots, p-1$, taken in some order.

Hence $a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$

Then $(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$ $\cdots$ (2)

Since $\gcd(p, (p-1)!) = 1$, we can cancel $(p-1)!$ from both sides of (2) and obtain

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

Corollary 25: If p is a prime and a is any integer, then
$a^p \equiv a \pmod p$

Proof: If p divides a, then p divides $a^p - a$. Hence $a^p \equiv a \pmod p$
If p does not divide a, then from Theorem 25, we get

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

Hence $a^p \equiv a \pmod p$

Definition: Let n be a positive integer. The function ϕ from $\mathbb{N}$ to $\mathbb{N}$ defined by $\phi(n)$ = the number of positive integers not exceeding n and relatively prime to n is called the Euler phi-function. ($\mathbb{N}$ is the set of all positive integers)

Example: Let $n = 20$. The positive integers that do not exceed 20 and which are relatively prime to 20 are the followings: 1, 3, 7, 9, 11, 13, 17, 19

Hence $\phi(20) = 8$

Similarly $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$

$\phi(5) = 4$ $\phi(6) = 2$ $\phi(7) = 6$ $\phi(8) = 4$

$\phi(9) = 6$ etc.

Note: If p is a prime, $\phi(p) = p-1$

Lemma 26 Let a and n be two integers such that $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the distinct positive integers less than n and relatively prime to n, then

$aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Proof: Let i and j be two integers such that $1 \le i \ne j \le \phi(n)$. Then we show that $aa_i \not\equiv aa_j \pmod n$. Suppose $aa_i \equiv aa_j \pmod n$. Since $\gcd(a, n) = 1$, we can

applies cancellation property and get $a_i \equiv a_j \pmod{n}$. This contradicts our assumption that $0 < a_i, a_j < n$. Hence $aa_i \not\equiv aa_j \pmod{n}$. Now $\gcd(a, n) = 1$ and $\gcd(a_i, n) = 1$ imply that $\gcd(aa_i, n) = 1$. Hence n does not divide aa_i and for each fixed i, $1 \le i \le \phi(n)$, there exists a unique integer b_i such that $0 < b_i < n$ and $aa_i \equiv b_i \pmod{n}$. Since $\gcd(aa_i, n) = 1$ we find that $\gcd(b_i, n) = 1$. Hence b_i is a positive integer less than n and relatively prime to n. This implies that b_i is one of $a_1, a_2, \ldots, a_{\phi(n)}$.

Theorem 26 (Euler). Let a, n be integers such that $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$

Proof: For $n = 1$, the result follows trivially. So, assume that $n > 1$. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be distinct positive integers less than n and relatively prime to n. Then from the Lemma 25, $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order. Hence

$$(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}$$

i.e.,
$$a^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \quad \ldots (1)$$

Now $\gcd(a_i, n) = 1$ for $i = 1, 2, \ldots, \phi(n)$, imply that

$$\gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$$

Hence by cancellation property, we get from (1)

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

Theorem 27 (Wilson): If p is a prime, then

$$(p-1)! \equiv -1 \pmod{p}$$

Proof: Suppose $p = 2$ Then $(2-1)! = 1 \equiv -1 \pmod 2$

If $p = 3$, then $(3-1)! = 2! = 2 \equiv -1 \pmod 3$

Hence we find that the theorem is true for $p = 2$ and $p = 3$

Assume now that p is a prime greater than 3.

Consider the following $p-1$ consecutive integers.

$$1, 2, 3, \ldots, p-1$$

If a is any of these integers, then $\gcd(a, p) = 1$

Hence we find that the congruence

$$ax \equiv 1 \pmod p$$

has a unique solution modulo p (using the result: If a, b and m be integers with $m > 0$ and $\gcd(a, m) = 1$, then the congruence $ax \equiv b \pmod m$ has a unique solution)

Hence there exists a unique integer b such that $0 \le b \le p-1$ and $ab \equiv 1 \pmod p$

Now $b = a$ if and only if $a^2 \equiv 1 \pmod p$

i.e., if and only if $(a-1)(a+1) \equiv 0 \pmod p$

i.e., if and only if either $(a-1) \equiv 0 \pmod p$

or $a+1 \equiv 0 \pmod p$

i.e., if and only if either $a = 1$ or $a = p-1$

(since $0 \le a \le p-1$)

Thus we find that only for $a = 1$ and $a = p-1$

$$1 \cdot 1 \equiv 1 \pmod p \quad \text{and} \quad (p-1)(p-1) \equiv 1 \pmod p$$

If $a \ne 1, p-1$, there exists b such that $b \ne a$, $1 < b < p-1$ and $ab \equiv 1 \pmod p$

Let us now group the integers $2, 3, 4, \ldots, p-2$ into pairs (a, b) such that $ab \equiv 1 \pmod{p}$

Then we obtain $\frac{p-3}{2}$ distinct pairs (a,b) and hence $\frac{p-3}{2}$ congruences $ab \equiv 1 \pmod{p}$

We multiply all these congruences and rearrange the factors. Then we obtain $2.3.4\ldots(p-2) \equiv 1 \pmod{p}$

Hence $1.2.3.4.\ldots.(p-2)(p-1) \equiv (p-1) \pmod{p}$

i.e., $(p-1)! \equiv (p-1) \pmod{p}$

But $p-1 \equiv -1 \pmod{p}$. So, it follows that $(p-1)! \equiv -1 \pmod{p}$. This completes the proof of the theorem.

Theorem 28 If p be a prime and k be a positive integer, then $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$

Proof: The positive integers $\leq p^k$ which are not prime to p^k are $p, 2p, 3p, \ldots, (p^{k-1})p$

Therefore the number of positive integers less than p^k and prime to p^k is $p^k - p^{k-1}$

Hence $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$

We state a theorem without proof:

Theorem 29 If m and n are relatively prime integers then $\phi(mn) = \phi(m)\phi(n)$

Using this theorem we can show that if $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ where $p_1, p_2, \ldots p_r$ are prime $k_1, k_2, \ldots k_r$ are positive integer, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

worked out examples: 1. Show that for any positive integer n, $\frac{n^7}{7} + \frac{n^3}{3} + \frac{11n}{21}$ is an integer

Solution: We have $n^7 \equiv n \pmod 7$ and $n^3 \equiv n \pmod 3$

Hence $n^7 - n$ is a multiple of 7 and $n^3 - n$ is a multiple of 3.

Then there exists integers r and t such that

$$n^7 - n = 7r \quad \text{and} \quad n^3 - n = 3t$$

Hence $$\frac{n^7}{7} + \frac{n^3}{3} + \frac{11n}{21} = \frac{7r+n}{7} + \frac{3t+n}{3} + \frac{11n}{21}$$

$$= r + t + \frac{n}{7} + \frac{n}{3} + \frac{11n}{21}$$

$$= r + t + \frac{21n}{21} \equiv r + t + n$$

$$= \text{an integer.}$$

2. Find the remainder when 10^{515} is divided by 7.

Solution: If we find an integer r such that $0 \le r < 7$ and $10^{515} \equiv r \pmod 7$, then r will be the required remainder.

Now by Fermat's theorem,

$$10^{7-1} \equiv 1 \pmod 7 \quad \text{i.e.,} \quad 10^6 \equiv 1 \pmod 7 \quad \text{---(1)}$$

Notice that $515 = 85 \cdot 6 + 5$. Hence from the congruence (1),

$$(10^6)^{85} \equiv 1^{85} \pmod 7$$

i.e., $$10^{85 \cdot 6} \equiv 1 \pmod 7 \quad \text{---(2)}$$

Again $$10 \equiv 3 \pmod 7$$

Then $$10^5 \equiv 3^5 \pmod 7 \quad \text{---(3)}$$

Now $$3^5 = 243 \equiv 5 \pmod 7 \quad \text{---(4)}$$

Hence from (2) $$10^{85 \cdot 6} \cdot 10^5 \equiv 10^5 \pmod 7$$

i.e., $$10^{515} \equiv 3^5 \pmod 7 \quad \text{(by (3))}$$

$$\equiv 5 \pmod 7 \quad \text{(by (4))}$$

So, the remainder is 5.

3. Find the remainder when 17! is divided by 19

Solution: 19 is a prime number. Hence by Wilson's theorem $(19-1)! \equiv -1 \pmod{19}$

i.e., $18! \equiv -1 \pmod{19}$

Now $-1 \equiv 18 \pmod{19}$

Hence $18! \equiv 18 \pmod{19}$

i.e. $18(17!) \equiv 18 \pmod{19}$

Since $\gcd(18, 19) = 1$, it follows from the above congruence that $17! \equiv 1 \pmod{19}$

Hence the remainder is 1

4. Find $\phi(191)$

Solution: we first examine whether 191 is prime or not. For this we find all primes p such that $p^2 \leq 191$

They are 2, 3, 5, 7, 11, 13. But none of these primes divide 191. Hence 191 is a prime

So, $\phi(191) = 191 - 1 = 190$

5. Find $\phi(260)$

Solution $260 = 2^2 \cdot 5 \cdot 13$

Hence $\phi(260) = 260\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{13}\right)$

$= 260 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{12}{13}$

$= 96$

Exercises: 1. Find the remainder when $2^{1000000}$ is divided by 17.

2. Find $\phi(380)$

3. Find $\phi(293)$

Application of Congruences : Divisibility Test.

Let m be a positive integer. Then $m = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$

$= (a_k a_{k-1} \cdots a_1 a_0)_{10}$

where $a_1, a_2, \ldots, a_k$ are integers such that $a_k \neq 0$ and $0 \leq a_i < 10$ for $i = 0, 1, 2, \ldots, k$

Test for divisibility by power of 2 : Let $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$

Then $f(10) = m$ and $f(0) = a_0$. We observe that $10 \equiv 0 \pmod 2$

Hence by our previous result, $f(10) \equiv f(0) \pmod 2$. This shows that $m \equiv a_0 \pmod 2$. It follows that m is divisible by 2 if and only if a_0 is divisible by 2. Next observe that $10^i \equiv 0 \pmod 4$ for $i \geq 2$

Hence $a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 \equiv 0 \pmod{2^2}$

and $a_1 10 + a_0 \equiv (a_1 10 + a_0) \pmod{2^2}$

From these two congruences, we get

$$m = a_0 + a_1 10 + a_2 10^2 + \cdots + a_{k-1} 10^{k-1} + a_k 10^k \equiv (a_1 10 + a_0) \pmod{2^2}$$

i.e., $m \equiv (a_1 a_0)_{10} \pmod{2^2}$. Hence m is divisible by 2^2 if and only if $a_1 a_0$ is divisible by 2^2. Likewise we can prove that m is divisible by 2^3 if and only if the number $a_2 a_1 a_0$ is divisible by 8.

Next we develop the divisibility test for 3, 9 and 11

Theorem 30 Let $m = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$, where $a_0, a_1, a_2, \ldots, a_k$ are integers such that $a_k \neq 0$ and $0 \leq a_i < 10$ for $i = 0, 1, 2, \ldots, k$. Let

$S = a_0 + a_1 + \cdots + a_k$ and $T = a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$

Then (i) m is divisible by 3 if and only if S is divisible by 3

(ii) m is divisible by 9 if and only if S is divisible by 9

(iii) m is divisible by 11 if and only if T is divisible by 11

Proof: Let $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$

(i) Now $f(10) = m$, $f(1) = S$. Since $10 \equiv 1 \pmod 3$, so by our previous result $f(10) \equiv f(1) \pmod 3$. Hence m is divisible by 3 if and only if S is divisible by 3.

(ii) $10 \equiv 1 \pmod 9$ So, $f(10) \equiv f(1) \pmod 9$. So, m is divisible by 9 if and only if S is divisible by 9.

(iii) $10 \equiv -1 \pmod{11}$. So, $f(10) \equiv f(-1) \pmod{11}$. So, $m \equiv T \pmod{11}$ as $f(-1) = T$. So m is divisible by 11 if and only if T is divisible by 11

We now develop divisibility test for 7 and 13

Theorem 31 Let $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$, where $a_k, a_{k-1}, \ldots, a_0$ are integers such that $a_k \neq 0$ and $0 \leq a_i \leq 9$ for $i = 0, 1, \ldots, k$. Let

$$t = (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - \cdots$$

Then (i) n is divisible by 7 if and only if t is divisible by 7

(ii) n is divisible by 13 if and only if t is divisible by 13

Proof: $n = (a_k a_{k-1} \cdots a_0)_{10} = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0$

$= (a_0 + a_1 10^1 + a_2 10^2) + (a_3 10^3 + a_4 10^4 + a_5 10^5) + (a_6 10^6 + a_7 10^7 + a_8 10^8) + \cdots$

$= (a_2 10^2 + a_1 10^1 + a_0) + 10^3 (a_5 10^2 + a_4 10^1 + a_3) + 10^6 (a_8 10^2 + a_7 10^1 + a_6) + \cdots$

$= (a_2 10^2 + a_1 10^1 + a_0) + (1000)^1 (a_5 10^2 + a_4 10^1 + a_3) + (1000)^2 (a_8 10^2 + a_7 10^1 + a_6) + \cdots$

Now $1000 \equiv -1 \pmod 7$ and $1000 \equiv -1 \pmod{13}$

Then $(1000)^i \equiv 1 \pmod 7$ if i is even.

$\equiv -1 \pmod 7$ if i is odd.

Similarly, $(1000)^i \equiv 1 \pmod{13}$ if i is even.

$\equiv -1 \pmod{13}$ if i is odd.

Hence $n \equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - \cdots \pmod 7$

i.e. $n \equiv t \pmod 7$. So n is divisible by 7 if and only if t is divisible by 7.

Similarly, we can prove that $n \equiv t \pmod{13}$. So n is divisible by 13 if and only t is divisible by 13.

Examples : 1. Determine whether the integers 761215122 and 51956124 are divisible by 9 or 11 or 3

Solution : Let $n = 761215122$

Now $S = 7+6+1+2+1+5+1+2+2 = 27$. Since 9 divides 27, so 9 divides n Hence 3 also divides n

Again $T = 2-2+1-5+1-2+1-6+7 = -3$

Since 11 does not divide -3, so n is not divisible by 11.

Next let $n = 51956124$

For this n, $S = 5+1+9+5+6+1+2+4 = 33$

Since 3 divides 33 and 9 does not divide 33, it follows that n is divisible by 3 but not divisible by 9

Again $T = 4-2+1-6+5-9+1-5 = -11$ which is divisible by 11

So, 11 divides n.

2. Which of the following integers are divisible by 13?

(a) 501121301 (b) 271111111202201

Solution: (a) Let $n = 501121301$. For this integer

$t = 301 - 121 + 501 = 681$. Now 13 does not divide 681

So, n is not divisible by 13

(b) Let $n = 271111111202201$. For this integer

$t = 201 - 202 + 111 - 111 + 27 = 26$. Since 13 divides 26,

So, n is divisible by 13.

3. Find the highest power of 2 dividing each of the following integers (a) $(1001100)_2$ (b) $(10111011)_2$

Solution: (a) Let $n = (1001100)_2$. Then

$$n = 2^6.1 + 2^5.0 + 2^4.0 + 2^3.1 + 2^2.1 + 2^1.0 + 0$$
$$= 2^2(2^4 + 2 + 1)$$

Hence n is divisible by 2^2 but 2^3 does not divide n.

Therefore 2 is highest power of 2 dividing n.

(b) Let $n = (10111011)_2$

Then $n = 2^7.1 + 2^6.0 + 2^5.1 + 2^4.1 + 2^3.1 + 2^2.0 + 2^1.1 + 1$

So, n is not divisible by 2. So 0 is the highest power of 2 dividing n.

4. Let $n = (a_k a_{k-1} \cdots a_1 a_0)_b$ be an integer in the base b. If d is a positive integer such that d divides $b-1$,