Unit: 3

Recall: Fermat's Thm: If p is a prime, $p \nmid a$ (or $(a,p)=1$) then $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Theorem: If n is any +ve integer, $(a,n)=1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

(Since n is prime, $\phi(n) = n-1$).

Remarks: Euler's Theorem is the generalisation of Fermat's theorem.

Now the question is — is this $\phi(n)$ is least power of a such that $a^{\phi(n)} \equiv 1 \pmod{n}$.

e.g. By Euler's thm we have,

$$2^{\phi(7)} \equiv 1 \pmod{7}$$

$$\Rightarrow 2^6 \equiv 1 \pmod{7}.$$

But we have $2^3 \equiv 1 \pmod{7}$.

Order of an integer modulo n: Let $n>1$ and gcd $(a,n)=1$ the order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Remark: (1) If two integers are congruent modulo n, then they have the same order modulo n.

Let $a \equiv b \pmod{n}$ ① and order of a modulo n is k i.e $a^k \equiv 1 \pmod{n}$. But from ① implies that

$a^k \equiv b^k \pmod{n}$ so $b^k \equiv 1 \pmod{n}$

so order of b modulo n is also k.

Thm: Let the integer a have order K modulo n. Then $a^b \equiv 1 \pmod{n}$ if and only if $K \mid b$. in particular $K \mid \phi(K)$

Pf: Let $K \mid b$. Then $b = jk$ for $j \in \mathbb{Z}$

Since a have order k ie $a^K \equiv 1 \pmod{n}$

$$\Rightarrow (a^K)^j \equiv 1^j \pmod{n}$$

$$\Rightarrow a^{jK} \equiv 1 \pmod{n}$$

$$\Rightarrow a^b \equiv 1 \pmod{n}.$$

Conversely let b is any positive integer satisfying

$$a^b \equiv 1 \pmod{n}.$$

Since order of a is K modulo n. ie $a^K \equiv 1 \pmod{n}$

$\therefore b > K$. Now applying division algorithm we get, $\exists$ q and r such that $b = qk + r$, $0 \leq r < K$.

$$\therefore a^b = a^{qK+r} = (a^K)^q \cdot a^r$$

Since $a^b \equiv 1 \pmod{n}$ and $a^K \equiv 1 \pmod{n}$, this implies that $a^r \equiv 1 \pmod{n}$. Since $0 \leq r < K$, we end up with $r = 0$, otherwise, the choice of K as the smallest +ve integer such that $a^K \equiv 1 \pmod{n}$ is contradicted. Hence $b = qK$, and $K \mid b$.

As we know from Euler's theorem,

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

But order of a is K so $K \mid \phi(n)$

Remark: When attempting to find the order of an integer a modulo n, instead of considering all powers of a, the exponents can be restricted to the divisors of $\phi(n)$.

Thm: If a has order k modulo n, then $a^i \equiv a^j \pmod{n}$ if and only if $i \equiv j \pmod{k}$.

Pf: First suppose that $a^i \equiv a^j \pmod{n}$, where $i \geq j$.
Since a is relatively prime to n, so we have
$a^{i-j} \equiv 1 \pmod{n}$. But $a^k \equiv 1 \pmod{n}$.
$\therefore k \mid i-j$ thus $i \equiv j \pmod{k}$

Conversely let $i \equiv j \pmod{k}$ so $k \mid i-j$
$\Rightarrow i-j = qk$ for some integer q
$\Rightarrow i = j+qk$. But a has order k modulo n. so
$a^k \equiv 1 \pmod{n}$ —— (1)
$\therefore a^i \equiv a^{j+qk} \equiv a^j \cdot (a^k)^q \equiv a^j \pmod{n}$ ((1) $\Rightarrow$)
ie $a^i \equiv a^j \pmod{n}$ //

Corollary: If a has order k modulo n, then the integers $a, a^2, \ldots a^k$ are incongruent modulo n.

Pf: If $a^i \equiv a^j \pmod{n}$ for $1 \leq i \leq j \leq k$ then the above theorem implies that $i \equiv j \pmod{k}$ But this is impossible unless $i = j$.

Thm: If the integer a has order k modulo n, and $b > 0$, then a^b has order $\frac{k}{\gcd(b,k)}$ modulo n.

Pf: Let $d = \gcd(b, k)$.

$\therefore d|b$ and $d|k$

$\Rightarrow b = ds$ and $k = dt$ with $(s, t) = 1$

clearly, $(a^b)^t = (a^{ds})^{\frac{k}{d}} = (a^k)^s \equiv 1 \pmod n$ [Since a has order k]

If a^b is assumed to have order r modulo n, then $r|t$ — (i). On the other hand, since a has order k modulo n, the congruence,

$a^{br} \equiv (a^b)^r \equiv 1 \pmod n$ indicates that $k|br$.

i.e $dt|dsr \Rightarrow t|sr$ But $\gcd(t, s) = 1$ so $t|r$ — (ii)

(i), (ii) $\Rightarrow r = t = \frac{k}{d} = \frac{k}{\gcd(b, k)}$ //

Corollary: Let a have order k modulo n. Then a^b also have order k if and only if $\gcd(b, k) = 1$.

Primitive root: If $\gcd(a, n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a primitive root of n.

In other words, n has a as a primitive root if $a^{\phi(n)} \equiv 1 \pmod n$, but $a^k \not\equiv 1 \pmod n$ for all positive integers $k < \phi(n)$.

Remark: 1. Primitive root exist for any prime modulus.

2. Every integer does not possess a primitive roots. but there are some integers which have primitive roots but they are not prime.

Thm Let $\gcd(a,n)=1$ and let $a_1, a_2, \dots a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. If a is a primitive root of n, then

$a, a^2, \dots a^{\phi(n)}$ are congruent modulo n to $a_1, a_2 \dots a_{\phi(n)}$ in some order.

Pf: Since a is relatively prime to n, the same holds for all the powers of a, hence each a^k is congruent modulo n to some one of the a_i. The $\phi(n)$ numbers in the set $\{a, a^2, \dots a^{\phi(n)}\}$ are incongruent, [As we know, if a has order k modulo n, then the integers $a, a^2, \dots a^k$ are incongruent modulo n) hence these powers must represent (not necessarily in order of appearance) the integers $a_1, a_2, \dots a_{\phi(n)}$.

Corollary: If n has a primitive root, then it has exactly $\phi(\phi(n))$ of them.

Pf: Suppose that a is a primitive root of n. Thus, from the above theorem, any other primitive root of n is found among the members of the set $\{a, a^2, \dots a^{\phi(n)}\}$. But the number of powers a^k, $1 \le k \le \phi(n)$, which have order $\phi(n)$ is equal to the number of integers k for which $\gcd(k, \phi(n)) = 1$, there are $\phi(\phi(n))$ such integers, hence $\phi(\phi(n))$ primitive roots of n. //

Problems 8.1 (Burton).

1. Find the order of the integers 2, 3, 5 (a) modulo 17 (b) modulo 19 and (c) modulo 23.

Sol (a) $\phi(17) = 16$.

$\therefore$ divisors of 16 are 1, 2, 4, 8, 16.

$2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 1 \pmod{17}$

$3^2 \equiv 9$, $3^4 \equiv 13$, $3^8 \equiv 16$, $3^{16} \equiv 1 \pmod{17}$

$5^2 \equiv 8$, $5^4 \equiv 13$, $5^8 \equiv 16$, $5^{16} \equiv 1 \pmod{17}$

$\therefore$ order of $2 = 8 \pmod{17}$

order of $3 = 16 \pmod{17}$

order of $(5) \equiv 16 \pmod{17}$.

(b) modulo 19.

$\phi(19) = 18$, Divisors of 18 are 1, 2, 3, 6, 9, 18.

$2^2 \equiv 4$, $2^3 \equiv 8$, $2^6 \equiv 7$, $2^9 \equiv 18$, $2^{18} \equiv 1 \pmod{19}$

$\therefore$ ord $(2) = 18$.

$3^2 \equiv 9$, $3^3 \equiv 8$, $3^6 \equiv 7$, $3^9 \equiv 18$, $3^{18} \equiv 1 \pmod{19}$

$\therefore$ ord $(3) = 18$.

$5^2 \equiv 6$, $5^3 \equiv 11$, $5^6 \equiv 7$, $5^9 \equiv 1 \pmod{19}$

$\therefore$ ord $(5) = 9$.

(c) modulo 23.

HW Sol ord $(2) = 11$

ord $(3) = 11$

ord $(5) = 22$.

(2) Establish each of the statements below.

(a) If a has order hk modulo n, then a^h has order k modulo n.

Pf: Given that $a^{hk} \equiv 1 \pmod{n}$.

$$\Rightarrow (a^h)^k \equiv 1 \pmod{n}$$

If possible suppose $(a^h)^r \equiv 1 \pmod{n}$ s.t $0 < r < k$

$$\therefore 0 < hr < hk$$

Then a would not have order hk (since $hr < hk$ and $a^{hr} \equiv 1 \pmod{n}$.

Therefore a^h has order k modulo n //

(b) If a has order $2k$ modulo the odd prime p, then $a^k \equiv -1 \pmod{p}$.

Pf: Given that $a^{2k} \equiv 1 \pmod{p}$

If $p = 2$, a odd, then a has order $\phi(2) = 1 \neq 2k$

$\therefore$ Assume p is odd.

$$\therefore (a^k)^2 - 1 \equiv 0 \pmod{p}$$

$$\Rightarrow (a^k - 1)(a^k + 1) \equiv 0 \pmod{p}$$

$$\therefore p \mid (a^k - 1)(a^k + 1)$$

If $p \mid a^k - 1$ then $a^k \equiv 1 \pmod{p}$ so a would not have order $2k$ $\therefore p \nmid a^k - 1$ so $p \mid (a^k + 1)$

$$\therefore a^k + 1 \equiv 0 \pmod{p} \Rightarrow a^k \equiv -1 \pmod{p}$$ //

(c) If a has order $n-1$ modulo n, then n is prime.

Pf: Given that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{\phi(n)} \equiv 1 \pmod{n}$

If $\phi(n) < n-1$, then it would contradict that $n-1$ as the order of a.

$$\therefore \phi(n) = n - 1$$

If n were composite it would have a divisor d, $1<d<n$, n is also a divisor of n, so $\phi(n) \leq n-2$ But $\phi(n) = n-1$, so n is not composite.

$\therefore n$ is prime. //

10. (a) Verify that 2 is a primitive root of 19 but not of 17.

Soln Since $\phi(19) = 18$.

$2^6 = 64 \equiv 7 \pmod{19}$

$7^2 = 49 \equiv 11 \pmod{19}$

$7^3 \equiv 7 \cdot 7 = 4 \cdot 19 + 1 \equiv 1 \pmod{19}$

$\therefore 2^{18} = 2^{\phi(19)} \equiv 1 \pmod{19}$

Suppose order of $2 \pmod{19} = r$, $r < 18$.

$\therefore r \mid 18$, so $r \in \{1, 2, 3, 6, 9\}$.

$r \neq 1$, since $2^1 \neq 1 \pmod{19}$

$r \neq 2$, since $2^2 = 4 \neq 1 \pmod{19}$

$r \neq 3$, since $2^3 = 8 \neq 1 \pmod{19}$

$r \neq 6$, since $2^6 = 64 \equiv 7 \neq 1 \pmod{19}$

$r \neq 9$, since $2^9 = 2^3 \cdot 2^6 \equiv 8 \cdot 7 = 56 \equiv 18 \pmod{19}$

$\therefore 18 = \phi(19)$ is the smallest integer r for which $2^r \equiv 1 \pmod{19}$

$\therefore 2$ is a primitive root of 19.

For 17, $\phi(17) = 16$, let r be order of 2

$\therefore r \in \{1, 2, 4, 8, 16\}$

Clearly $r \neq 1, 2, 4$

$2^8 = 256 = 15(17) + 1 \equiv 1 \pmod{17}$

$\therefore 2^8 \equiv 1 \pmod{17}$, so order of 2 mod 17 is 8, not 16.

$\therefore$ 2 is not a primitive root of 17. //

12. (a) Find two primitive roots of 10.

Sol $\phi(10) = 4$. (relatively prime numbers are 1, 3, 7, 9.)

If 10 has a primitive root, then it has exactly $\phi(\phi(10)) = \phi(4) = 2$ primitive roots.

$3^4 = 81 \equiv 1 \pmod{10}$

and $3^1 \equiv 3 \pmod{10}$, $3^2 \equiv 9 \pmod{10}$, $3^3 \equiv 7 \pmod{10}$

$7^2 \equiv 9 \pmod{10}$, $\therefore 7^4 \equiv 81 \equiv 1 \pmod{10}$

$7^1 \equiv 7$, $7^2 \equiv 49 \equiv 9$, $7^3 \equiv 63 \equiv 3 \pmod{10}$

$\therefore$ 3, 7 are primitive roots of 10.

Note: $9^2 = 81 \equiv 1 \pmod{10}$ $\therefore$ 9 is not a primitive root, since $2 < 4$. ($9^4 \equiv 1 \pmod{10}$)

(b) Use the information that 3 is a primitive root of 17 to obtain the eight primitive roots of 17.

Note $\phi(\phi(17)) = \phi(16) = 2^4 - 2^3 = 8$

Since 3 has order $\phi(17) = 16 \pmod{17}$, then 3^r has order $16/\gcd(r,16)$

$\therefore$ When $\gcd(r,16) = 1$, 3^r will have order 16, and so be a primitive root of 17.

$\therefore$ For $\gcd(r,16) \Rightarrow r = 1, 3, 5, 7, 9, 11, 13, 15$.

$\therefore$ $3^3 \equiv 27 \equiv 10 \pmod{17}$

$3^5 \equiv 10 \cdot 3^2 \equiv 5 \pmod{17}$

$3^7 \equiv 3^5 \cdot 3^2 \equiv 5 \cdot 9 \equiv 45 \equiv 11 \pmod{17}$

$3^9 \equiv 3^7 \cdot 3^2 \equiv 11 \cdot 9 \equiv 85 \cdot 14 \equiv 14 \pmod{17}$

$3^{11} \equiv 3^9 \cdot 3^2 \equiv 14 \cdot 9 \equiv 126 \equiv 119 + 7 \equiv 7 \pmod{17}$

$3^{13} \equiv 3^{11} \cdot 3^2 \equiv 7 \cdot 9 \equiv 63 \equiv 51 + 12 \equiv 12 \pmod{17}$

$3^{15} \equiv 3^{13} \cdot 3^2 \equiv 12 \cdot 9 \equiv 108 \equiv 102 + 6 \equiv 6 \pmod{17}$

$\therefore$ Primitive roots of 17 are 3, 5, 6, 7, 10, 11, 12, 14. //

Primitive roots for primes.

Th^m (Lagrange) If p is a prime, and $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $a_n \not\equiv 0 \pmod p$ is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence $f(x) \equiv 0 \pmod p$ has atmost n incongruent solutions modulo p.

Pf: We prove this theorem by induction on n;

If $n=1$, $f(x) = a_1 x + a_0$, $a_1 \not\equiv 0 \pmod p$

ie $p \nmid a_1 \Rightarrow (a_1, p) = 1$

Hence the linear congruence $a_1 x \equiv -a_0 \pmod p$ has a unique solution [Since gcd (a_1, p) divides a_0]

So the result is true for $n=1$

Suppose the result is true for $n = k-1$, we have to prove the result is true for $n=k$.

Either $f(x) \equiv 0 \pmod p$ has no solution, or it has atleast one solution, say it is a.

If $f(x)$ is divided by $x-a$; then we have,

$$f(x) = (x-a) q(x) + r. \quad \text{---} (1)$$

Since a is a soln, so $x=a$ satisfy the eqn (1).

$$0 \equiv f(a) = (a-a) q(a) + r \equiv r \pmod p$$

[Since $f(x) \equiv 0 \pmod p$]

So, $f(x) \equiv (x-a) q(x) \pmod p$.

If b is another one of incongruent soln of $f(x) \equiv 0 \pmod p$ then $f(b) \equiv (b-a) q(b) \pmod p$ [since a and b are different soln so $a \not\equiv b \pmod p$]

But $f(b) \equiv 0 \pmod p$ and $(b-a) \not\equiv 0$ so

$$q(b) \equiv 0 \pmod p$$

$\therefore g(x) \equiv 0 \pmod p$ must be satisfied.

By induction hypothesis, $g(x)$ has atmost $k-1$ incongruent solution so

$f(x) \equiv 0 \pmod p$ has atmost k incongruent solutions.

Corollary: If p is a prime and $d \mid p-1$, then the congruence $x^d - 1 \equiv 0 \pmod p$ has exactly d solutions.

Pf: Since $d \mid p-1$ so $p-1 = dk$ for some $k \in \mathbb{Z}$.

Then $x^{p-1} - 1 = (x^d - 1) f(x)$ where ——— (2)

$f(x) = x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1$ has integral coefficients and is of degree $d(k-1) = dk - d$
$= p - 1 - d$.

Then by Lagranges theorem, $f(x)$ has atmost $p-1-d$ incongruent solutions modulo p.

By Fermat's theorem, $(a, p) = 1$ we have $a^{p-1} \equiv 1 \pmod p$

or $x^{p-1} - 1 \equiv 0 \pmod p$ has precisely $p-1$ incongruent sol'ns, ie $\{1, 2, 3, \cdots p-1\}$.

eg $p = 5$, $p-1 = 4$

To write $p-1 = dk$
$4 = 1, 4$

$d \mid p-1$
$d = 1$

$x^{p-1} - 1 = (x^d - 1) f(x)$
$x^4 - 1 = (x^1 - 1)(x^3 + x^2 + x + 1)$
or
$x^4 - 1 = (x^2 - 1)(x^2 + 1)$

Now from (2), $x^{p-1} - 1 = (x^d - 1) f(x)$

Now any solution $x = a$ of $x^{p-1} - 1 \equiv 0 \pmod p$ that is not a solution of $f(x) \equiv 0 \pmod p$ must satisfy $x^d - 1 \equiv 0 \pmod p$. ie if we put $x = a$ in ~~eqn (2) we get~~ in $x^{p-1} - 1 \equiv 0 \pmod p$ we get,

$a^{p-1} - 1 \equiv 0 \pmod p$

$\Rightarrow (a^d - 1) f(a) \equiv 0 \pmod p$ (using ②)

$\Rightarrow p \mid a^d - 1$ (As $x=a$ is not the soln of $f(x) \equiv 0 \pmod p$ so $p \nmid f(a)$.)

Therefore $x^d - 1 \equiv 0 \pmod p$ must have at least $p-1-(p-1-d) = d$ solutions. Also this congruence can possess no more than d solutions (Lagranges Thm). Hence $x^d - 1 \equiv 0 \pmod p$ has exactly d solutions.

§2 Burton

1. If p is a prime (odd), prove

(a) The only incongruent solutions of $x^2 \equiv 1 \pmod p$ are 1 and $p-1$.

Pf: Since p is odd prime, $2 \mid p-1$.

∴ By corollary of Lagranges theorem, the congruence $x^2 - 1 \equiv 0 \pmod p$ has exactly 2 solutions.

clearly, 1 is a solution, since $1 \equiv 1 \pmod p$

And $p-1$ is also a solution, since,

$(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod p$

∴ 1 and $p-1$ are solutions and they are incongruent mod p. (Because $1 \equiv p-1 \pmod p \Rightarrow 1 \equiv -1 \pmod p$, whereas p is odd prime).

(b) The congruence $x^{p-2} + \cdots + x^2 + x + 1 \equiv 1 \pmod p$ has exactly $p-2$ incongruent solutions, and they are $2, 3, \cdots p-1$.

Pf: By Fermat's theorem, when $\gcd(x, p) = 1$,

Then $x^{p-1} \equiv 1 \pmod{p}$

Now $\gcd(x, p) = 1$ for $x = 1, 2, 3, \ldots p-1$ and these are all incongruent mod p.

$\therefore x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ solutions and they are $1, 2, 3, \ldots p-1$.

Moreover, $x^{p-1} - 1 = (x-1)(x^{p-2} + x^{p-3} + \cdots + x^2 + x + 1)$

Since p is odd, $p \geq 3$, so $p-2$ is a valid exponent.

Since $x - 1 \equiv 0 \pmod{p}$ has exactly one solution ($x \equiv 1$)

Then, $x^{p-2} + \cdots + x + 1$ has exactly $(p-1) - 1 = p-2$ solutions. Since $x \not\equiv 1 \pmod{p}$ for $x = 2, \ldots p-1$ and $x^{p-1} - 1 \equiv 0$ for $x = 2, 3, \ldots p-1$ then $x^{p-2} + \cdots + x + 1 \equiv 0$ for $x = 2, \ldots p-1$

Thus the $p-2$ solutions for $x^{p-2} + \cdots + x + 1 \equiv 0 \pmod{p}$ are $x = 2, 3, \ldots p-1$. ∎

2. verify that each of the congruences —

$x^2 \equiv 1 \pmod{15}$, $x^2 \equiv -1 \pmod{65}$,

$x^2 \equiv -2 \pmod{33}$ has four incongruent solutions, hence Lagranges theorem need not hold if the modulus is a composite number.

Pf: We know that if p and q are primes and $p \neq q$ and $p \mid c$ and $q \mid c$ then $pq \mid c$.

Now in above problems, if p, q are primes, $p \neq q$.

then if $x_1^2 \equiv a \pmod{p}$, $x_1^2 \equiv a \pmod{q}$ then $x_1^2 \equiv a \pmod{pq}$. [Since $p \mid x_1^2 - a$, $q \mid x_1^2 - a$ and so $pq \mid x_1^2 - a$].

Now strategy is to break up the congruence into two parts, solve each part and

Now find common congruent solutions.

$x^2 \equiv 1 \pmod{15} \Rightarrow x^2 \equiv 1 \pmod 3$

$x^2 \equiv 1 \pmod 5$

Now $x^2 \equiv 1 \pmod 3$

$\Rightarrow (x+1)(x-1) \equiv 0 \pmod 3$

$\Rightarrow x \equiv 1, 4, 7, 10, 13.$

$x \equiv -1, 2, 5, 8, 11, 14.$

$\therefore x \equiv 1, 4, 11, 14 \pmod{15}.$

$x^2 \equiv 1 \pmod 5$,

$\Rightarrow (x+1)(x-1) \equiv 0$,

$\Rightarrow x \equiv 1, 6, 11, 16$

$x \equiv -1, 4, 9, 14.$

$x^2 \equiv -1 \pmod{65} \Rightarrow$

$x^2 \equiv -1 \pmod 5$

$\Rightarrow x^2 \equiv 4 \pmod 5$

$\Rightarrow (x+2)(x-2) \equiv 0$

$\therefore x \equiv -2, 3, 8, 13, 18,$

$25, 28, 33, 38, 43.$

$x \equiv 2, 7, 12, 17, 22, 27, 32, 37,$

$42, 47, 52, 57$

$x^2 \equiv -1 \pmod{13}$

$\Rightarrow x^2 \equiv 12, x^2 \equiv 25$

$\Rightarrow (x+5)(x-5) \equiv 0$

$\therefore x \equiv -5, 8, 21, 34, 47, 60$

$x \equiv 5, 18, 31, 44, 57.$

$\therefore x \equiv 8, 18, 47, 57 \pmod{65}.$

$x^2 \equiv -2 \pmod{33} \Rightarrow$

$x^2 \equiv -2 \pmod 3$

$\Rightarrow x^2 \equiv 1 \pmod 3$

$\Rightarrow (x+1)(x-1) \equiv 0.$

$x \equiv -1, 2, 5, 8, 11, 14, 17, 20, 23, 26, 29$

$x \equiv 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31$

$\therefore x \equiv 8, 14, 19, 25 \pmod{33}.$

$x^2 \equiv -2 \pmod{11}$

$\Rightarrow x^2 \equiv 9 \pmod{11}$

$(x+3)(x-3) \equiv 0.$

$x \equiv -3, 8, 19, 30$

$x \equiv 3, 14, 25.$

Unit: 3

composite numbers having primitive roots:

Thm For $K \geq 3$, the integer 2^K has no primitive roots.

Pf: First we have to establish the following congruence $a^{2^{K-2}} \equiv 1 \pmod{2^K}$.

If $K=3$, then $a^2 \equiv 1 \pmod 8$ which is true as $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

For $K > 3$, we proceed by induction on K.

Assume that the congruence is true for K, ie $a^{2^{K-2}} \equiv 1 \pmod{2^K}$. which is equivalent to

$2^K \mid a^{2^{K-2}} - 1$

$\Rightarrow a^{2^{K-2}} - 1 = b2^K \quad b \in \mathbb{Z}$.

$\Rightarrow a^{2^{K-2}} = 1 + b2^K$

$\Rightarrow \left(a^{2^{K-2}}\right)^2 = 1 + 2b2^K + (b2^K)^2$

$\Rightarrow a^{2^{K-1}} = 1 + 2^{K+1}\left(b + b^2 2^{K-1}\right)$

$\equiv 1 \pmod{2^{K+1}}$.

$a^{2^{K-2}} \cdot a^{2^{K-2}} = a^{2^{K-2}+2^{K-2}} = a^{2 \cdot 2^{K-2}} = a^{2^{K-1}}$

$\therefore$ the congruence holds for $K+1$ and hence for all $K \geq 3$.

Now the integers which are relatively prime to 2^K are precisely the odd integers.

Also $\phi(2^K) = 2^{K-1}$.

Also we just proved that if a is an odd integer and $K \geq 3$, $a^{2^{K-2}} \equiv 1 \pmod{2^K}$.

$\Rightarrow a^{\frac{\phi(2^k)}{2}} \equiv 1 \pmod{2^k}$.

and hence there are no primitive roots of 2^k.

Th^n If $\gcd(m,n) = 1$, where $m > 2$ and $n > 2$, then the integer mn has no primitive roots.

Pf: Consider any integer a for which $\gcd(a, mn) = 1$ then $\gcd(a,m) = 1$ and $\gcd(a,n) = 1$.

Let $h = \text{lcm}(\phi(m), \phi(n))$ and

$d = \gcd(\phi(m), \phi(n))$.

Since $\phi(m)$ and $\phi(n)$ are both even (Th^m 7.4), so $d \geq 2$. Also we know that

$\text{lcm} \cdot \gcd = \phi(m) \cdot \phi(n)$

$\Rightarrow h \cdot d = \phi(m) \cdot \phi(n)$

$\Rightarrow h = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{2}$

Now from Euler's theorem, we have

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

Raising this equation to the $\frac{\phi(n)}{d}$ power, we get,

$\left(a^{\phi(m)}\right)^{\frac{\phi(n)}{d}} \equiv 1^{\frac{\phi(n)}{d}} \pmod{m}$

$\Rightarrow a^h \equiv 1 \pmod{m}$ ——— (1)

Similarly we can show that $a^h \equiv 1 \pmod{n}$ ——— (ii)

As $\gcd(m,n) = 1$, so from eqn^n (1) and (ii) implies that $a^h \equiv 1 \pmod{mn}$.

Thus order of a is h modulo mn. and $(a, mn) = 1$

Also $h \leq \frac{\phi(mn)}{2}$ thus mn has no primitive roots.

Corollary: The integer n fails to have a primitive root if either,

(i) n is divisible by two odd primes or

(ii) n is of the form $n = 2^m p^k$ where p is an odd prime and $m \geq 2$.

Lemma: 1 If p is an odd prime, then there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$

Proof: We know that if p is a odd prime then there exist a primitive root r of p. i.e $r^{\phi(p)} \equiv 1 \pmod{p}$.
If $r^{p-1} \not\equiv 1 \pmod{p^2}$ then there is nothing to prove.
If possible suppose $r^{p-1} \equiv 1 \pmod{p^2}$ —— (1)
Replace r by $r+p = r'$
$\therefore (r')^{p-1} \equiv (r+p)^{p-1}$

(Here $r+p$ is nothing but it is r only as $p \equiv 0 \pmod{p}$. so $r+p$ is also a primitive root of p)

Now applying binomial theorem,

$$(r')^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2}$$
(other terms containing p^2)
$$\equiv 1 + p^2 r^{p-2} - pr^{p-2} \pmod{p^2} \quad \text{(using (1))}$$
$$\equiv 1 - pr^{p-2} \pmod{p^2}$$
$$\Rightarrow (r')^{p-1} \equiv 1 - pr^{p-2} \pmod{p^2}$$
$$\not\equiv 1 \pmod{p^2}.$$

(Since r is a primitive root of p so $(r,p)=1$ ie $p \nmid r$ $\Rightarrow p \nmid r^{p-2}$ Thus $p^2 \mid p \cdot r^{p-2}$)

But we assume that $r^{p-1} \equiv 1 \pmod{p^2}$
Hence we have a contradiction and our assumption is wrong. Hence $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Corollary: If p is an odd prime, then p^2 has a primitive root; in fact for a primitive root r of p, either r or $r+p$ is a primitive root of p^2.

Pf: If r is a primitive root of p and p is an odd prime then ~~[illegible]~~ $r^{p-1} \not\equiv 1 \pmod{p^2}$ —— (*)
Also order of r modulo p^2 is either $p-1$ or

also $p(p-1) = \phi(p^2)$

But from ⊛, we have, if r has order $p-1$ modulo p^2, then $r+p$ will be a primitive root of p^2. ∎

Eg. we know that 3 is a primitive of 7.
⇒ 3 and $3+7=10$ are primitive roots of 7^2.

$r^{\phi(p^2)} \equiv 1 \pmod{p^2}$
$\Rightarrow r^{p(p-1)} \equiv 1 \pmod{p}$.
we know that order of r divides $\phi(p^2)$.

Lemma:2 Let p be an odd prime and let r be a primitive root of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then for each +ve integer $k \geq 2$,

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

Proof: We prove the above result by induction on k.

Let $k=2$, then $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$

$\Rightarrow r^{p(p-1)} \equiv r^{p-1} \not\equiv 1 \pmod{p^2}$ which is true.

Assume that the result is true for k and we have to show that the result is true for $k+1$.

Now since r is a primitive root of p so $(r,p)=1 \Rightarrow (r, p^{k-1}) = 1 \Rightarrow (r, p^k) = 1$

Now from Euler's theorem we have,

$$r^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}.$$

$\Rightarrow r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$.

$\Rightarrow r^{p^{k-2}(p-1)} = 1 + a \cdot p^{k-1}$, $a \in \mathbb{Z}$, $p \nmid a$

$\phi(p^{k-1}) = p^{k-1} - p^{k-2} = p^{k-2}(p-1)$

Raising powers to p on both sides,

$$r^{p^{k-1}(p-1)} = (1 + a p^{k-1})^p \equiv 1 + a p^k \pmod{p^{k+1}}$$

As $p \nmid a$, $\Rightarrow r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$ Hence proved ∎

Thm If p is an odd prime number and $K \geq 1$, then there exists a primitive root for p^K.

Pf: For a given prime p, let r be the primitive root of p. for which $r^{p^{K-2}(p-1)} \not\equiv 1 \pmod{p^K}$ (Lemma 2).

or $r^{p-1} \not\equiv 1 \pmod{p^2}$ when $K=2$ (Lemma 1)

Now we claim, r serves as primitive root for all powers of p.

Let n be the order of r modulo p^K. ie $r^n \equiv 1 \pmod{p^K}$, $K \geq 1$, and we know that order of r divides $\phi(p^K)$. ie $n \mid \phi(p^K)$

$\Rightarrow n \mid p^{K-1}(p-1)$ ——— ①

$\phi(p^K) = p^K - p^{K-1} = p^{K-1}(p-1)$

$\therefore n$ takes the form $p^m(p-1)$, $0 \leq m \leq K-1$

Also note that $r^n \equiv 1 \pmod{p^K}$, $K \geq 1$

$\Rightarrow r^n \equiv 1 \pmod{p}$

$\Rightarrow p-1 \mid n$.

$p^K \mid r^n - 1$

$\Rightarrow p \mid r^n - 1$

As r is a primitive root of p ie $r^{\phi(p)} \equiv 1 \pmod{p}$

$\Rightarrow r^{p-1} \equiv 1 \pmod{p}$

But here $r^n \equiv 1 \pmod{p}$

$\therefore p-1 \mid n$

Now from ①, we have, if $n \neq p^{K-1}(p-1)$ then $p^{K-2}(p-1)$ is divisible by n. (because n takes the form $p^m(p-1)$)

$\Rightarrow r^{p^{K-2}(p-1)} \equiv 1 \pmod{p^K}$

which is a contradiction to lemma 2.

And hence r act as primitive root of p^K //

Corollary: There are primitive roots for $2p^k$ where p is an odd prime and $k \geq 1$.

Pf: Let r be primitive root of p^k, Now we take r is an odd integer. (since if r is even, then $r+p$ is odd and $r+p$ is also act as primitive).

Now $\gcd(r, 2p^k) = 1$.

[If r is even then $(r, 2p^k) \neq 1$]

Also obviously order of r modulo $2p^k$ must divide $\phi(2p^k)$. Now if we assume that order of r is n then $n \mid \phi(2p^k)$

$$\Rightarrow n \mid \phi(2)\phi(p^k)$$

$$\Rightarrow n \mid \phi(p^k) \quad \text{---} (1) \quad [\because \phi(2) = 1]$$

Moreover since n is the order of r modulo $2p^k$ so

$$r^n \equiv 1 \pmod{2p^k}.$$

$$\Rightarrow r^n \equiv 1 \pmod{p^k}.$$

[Since r is a primitive root of p^k so $r^{\phi(p^k)} \equiv 1 \pmod{p^k}$.]

$$\therefore \phi(p^k) \mid n \quad \text{---} (ii)$$

$\therefore$ from (1), (ii) $\Rightarrow n = \phi(p^k) = \phi(2p^k)$

$\therefore$ r act as primitive root of $2p^k$. //

Remark: Let $n > 1$, $n = 2^{k_1} p_1^{k_2} p_2^{k_3} \cdots p_r^{k_r}$. where p_i are odd and $k_j \geq 0$., $1 \leq j \leq r$.

(i) If $n = 2$ then it has primitive root because it is a prime. ~~Moreover~~ Here $k_1 = 1$, $k_2 = 0$, $\cdots k_r = 0$

(ii) $n = 2^n = 4$ yes it has a primitive root.

(iii) $n = 2^k$, $k \geq 3$. [There is no primitive root].

(iv) $n = 2 \cdot p_2^{k_2}$, [yes, it has a primitive root].

(v) $n = 2 \cdot p_2 \cdot p_3$. [No primitive root]

[$(m, n) = 1$, $m > 2$, $n > 2$ mn has no primitive root]

(vi) $n = 2^k \cdot p_2^{k_2} \cdots p_r^{k_r}$. [No primitive roots, as $(p_2, p_3) = 1$]

(vii) $n = p^k$, $k \geq 0$, (yes it has primitive roots).

Eulers Criterion. Unit 3

Solution of Quadratic Congruence is Equivalent to solving linear congruence and a quadratic congruence of the form $x^2 \equiv a \pmod{p}$:

Let us consider the general quadratic congruence $ax^2+bx+c \equiv 0 \pmod{p}$ where p is an odd prime ①
and $a \not\equiv 0 \pmod{p}$. i.e $\gcd(a,p)=1$.

Since p is an odd prime so $\gcd(4a,p)=1$.
Thus the congruence is equivalent to

$$4a(ax^2+bx+c) \equiv 0 \pmod{p}$$

$$\Rightarrow (2ax+b)^2-(b^2-4ac) \equiv 0 \pmod{p}.$$

$$\Rightarrow (2ax+b)^2 \equiv (b^2-4ac) \pmod{p}$$

Now putting $y = 2ax+b$ and $d = b^2-4ac$ we get,

$$y^2 \equiv d \pmod{p} \quad \text{——— (II)}$$

If $x \equiv x_0 \pmod{p}$ is a solution of ① then $y \equiv 2ax_0+b \pmod{p}$ satisfies the congruence (II)
Conversely, if $y \equiv y_0 \pmod{p}$ is a solution of (II) then $2ax \equiv y_0-b \pmod{p}$ is a solution of ①.
Thus the problem of finding a solution to the quadratic congruence ① is equivalent to that of finding a solution to a linear congruence and a quadratic congruence of the form $x^2 \equiv a \pmod{p}$.

Note: To solve $ax^2+bx+c \equiv 0 \pmod{p}$ we have to solve $x^2 \equiv a \pmod{p}$.
Suppose x_0 is one solution, then other is $p-x_0$.
As it is a quadratic congruence so by Lagrange Theorem it has atmost 2 solutions.

Also x_0 is incongruent to $p - x_0$. If possible suppose $x_0 \equiv p - x_0 \pmod{p}$ then $2x_0 \equiv p \equiv 0 \pmod{p}$.

$\Rightarrow x_0 \equiv 0 \pmod{p}$.

Now from ②, $0 \equiv a \pmod{p}$ which is a contradiction. $\gcd(a, p) = 1$, $p \nmid a$.

$\Rightarrow a \not\equiv 0 \pmod{p}$

Eg: Solve $5x^2 - 6x + 2 \equiv 0 \pmod{13}$ —— ①

To obtain the solution, one replaces this congruence by the simpler one

$y^2 \equiv 9 \pmod{13}$. —— ④

Now by hit and trial method, if we put $y = 3$ then from ④, $9 \equiv 9 \pmod{13}$ i.e. ④ is satisfied.

If we get one solution then we can easily get another soln which is say $y_2 = p - 3 = 13 - 3 = 10$.

$\therefore$ 3, 10 are incongruent solutions of ④.

Now we have to find the solutions of ①. For finding the solutions of ①, we write,

$$2ax \equiv y - b \pmod{p}.$$

For $y = 3$; $10x \equiv 9 \pmod{13}$

$\therefore$ It is not difficult to solve these two linear congruence and we get the solns which are $x \equiv 10, 12 \pmod{13}$ and these two solutions satisfy eqn ①.

$y^2 \equiv d \pmod{p}$

Here $d = b^2 - 4ac$

$= 25 \cdot 9$

$y = 2ax + b$

$= 2.5x - 6$

$= 10x - 6$.

when $y = 10$,

$10x \equiv 16 \pmod{13}$

Def^n: Let p be an odd prime and $\gcd(a, p) = 1$. If the congruence $x^2 \equiv a \pmod{p}$ has a solution then a is said to be a quadratic residue of p. Otherwise a is called a quadratic non-residue of p.

Let p - odd prime and $\gcd(a, p) = 1$

If $x^2 \equiv a \pmod{p}$ — solvable, then a is quad. residue of p.
— not solvable, then a is non-quad. residue of p.

[If $\gcd(a, p) \neq 1$ then, $p \mid a$ and then $a \equiv 0 \pmod{p}$.
And then $x^2 \equiv a \pmod{p}$ and $a \equiv 0 \pmod{p}$ implies that $x^2 \equiv 0 \pmod{p}$. then $x = 0$ is the trivial soln.
But we only interested to find non trivial soln.
Therefore we consider $\gcd(a, p) < 1$]

Eg: Let $p = 13$. Then how to find the quadratic residue of 13. To find out how many of the integers $1, 2, 3, \dots 12$ are quadratic residues of 13, we must know which of the integer congruences $x^2 \equiv a \pmod{13}$ are solvable when a runs through the set $\{1, 2, \dots 12\}$. Modulo 13, the squares of the integers $1, 2, 3, \dots 12$ are

$1^2 \equiv 1 \pmod{13}$ $\quad 7^2 \equiv 10 \pmod{13}$
$2^2 \equiv 4 \pmod{13}$ $\quad 8^2 \equiv 12 \pmod{13}$
$3^2 \equiv 9 \pmod{13}$ $\quad 9^2 \equiv 3 \pmod{13}$
$4^2 \equiv 3 \pmod{13}$ $\quad 10^2 \equiv 9 \pmod{13}$
$5^2 \equiv 12 \pmod{13}$ $\quad 11^2 \equiv 4 \pmod{13}$
$6^2 \equiv 10 \pmod{13}$ $\quad 12^2 \equiv 1 \pmod{13}$

That is $1^2 \equiv 12^2 \equiv 1 \pmod{13}$
$2^2 \equiv 11^2 \equiv 4 \pmod{13}$
$3^2 \equiv 10^2 \equiv 9 \pmod{13}$
$4^2 \equiv 9^2 \equiv 3 \pmod{13}$
$5^2 \equiv 8^2 \equiv 12 \pmod{13}$
$6^2 \equiv 7^2 \equiv 10 \pmod{13}$

Now we see that x can take values from 1 to 12 But a only takes the values, $a = 1, 3, 4, 9, 10, 12$, and these 6 values of a are called the quadratic residue of 13. And the remaining integers i.e 2, 5, 6, 7, 8, 11 are called quadratic non-residue of 13.

Notice that number of quadratic residue and number of quadratic non-residue are equal.

Euler's criterion: Let p be an odd prime and $\gcd(a,p) = 1$. Then a is a quadratic residue of p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

[Remark: Euler's criteria is used to check whether any a is a quadratic residue of p or not.

e.g Let $p=13$, $a=2$; then

$2^{\frac{13-1}{2}} \equiv 2^6 = 64 \equiv 12 \equiv -1 \pmod{13}$ so 2 doesn't satisfy the Euler's criteria, so 2 is not a quadratic residue of 13.]

Let $p=13$, $a=3$ then

$3^{\frac{13-1}{2}} = 3^6 \equiv (3^3)^2 = 27^2 \equiv 1^2 \equiv 1 \pmod{13}$

$\therefore$ 3 is a quadratic residue of 13.

Pf: Let a is a quadratic residue of p. so by definition, $x^2 \equiv a \pmod{p}$ has a solution (say x_1)

$\therefore x_1$ satisfy the congruence $x_1^2 \equiv a \pmod{p}$. Also since $\gcd(a,p) = 1$ so $\gcd(x_1, p) = 1$. We have to show that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

[If $(x_1, p) \neq 1$ then $p \mid x_1 \Rightarrow x_1 \equiv 0 \pmod{p} \Rightarrow x_1^2 \equiv 0 \pmod{p}$

$\Rightarrow a \equiv 0 \pmod{p} \Rightarrow (a,p) \neq 1$, a contradiction

Hence $(x_1, p) = 1$.

Now by applying Fermat's Theorem; as $(x_1, p) = 1$,

$$x_1^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow (x_1^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$ //

Conversely, let $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. We have to show that a is a quadratic residue of p.

Let r be a primitive root of p. (Since p is a prime so it has primitive root).

[If we consider power of primitive root ie $r^1, r^2, \dots r^{\phi(p)}$ they are congruent to 1 in some order, to integers 1, 2, ... $p-1$, ie if $(a, p) = 1$ then $a \in \{1, 2, \dots, p-1\}$]

Then $a \equiv r^K \pmod{p}$ for some $K \in \mathbb{Z}$, $1 \le K \le p-1$. ①

$$\Rightarrow r^{\frac{K(p-1)}{2}} \equiv a^{\frac{(p-1)}{2}} \equiv 1 \pmod{p}$$

$$\Rightarrow r^{\frac{K(p-1)}{2}} \equiv 1 \pmod{p}.$$

Since r is a primitive root, ie $r^{\phi(p)} \equiv 1 \pmod{p}$ ie order of r is $\phi(p) = p-1$

$\therefore \phi(p) \mid \frac{K(p-1)}{2}$

$$\Rightarrow \frac{K(p-1)}{2} = \phi(p) \cdot l, \quad l \in \mathbb{Z}$$

$$\Rightarrow \frac{K(p-1)}{2} = (p-1) \cdot l.$$

$$\Rightarrow \frac{K}{2} = l. \Rightarrow K = 2 \cdot l.$$

$\therefore$ ① $\Rightarrow r^K \equiv a \pmod{p} \Rightarrow r^{2l} \equiv a \pmod{p}$

$$\Rightarrow (r^l)^2 \equiv a \pmod{p}.$$

$\therefore$ For $x = r^l$, the congruence $x^2 \equiv a \pmod{p}$ is solvable.

$\therefore a$ is quadratic residue of p. //

Corollary: Let p be an odd prime and $\gcd(a,p)=1$. Then, a is quadratic residue of p if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ and a is quadratic non-residue of p if $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

Proof: Given $(a,p)=1$. Now by Fermat's theorem, we get,

$a^{p-1} \equiv 1 \pmod p \Rightarrow a^{p-1} - 1 \equiv 0 \pmod p$.

$\Rightarrow (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p$.

$\Rightarrow$ Either $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$ or $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$

If $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ then by Euler's criterion, we have, a is quadratic residue of p

And if $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ then a is quadratic non-residue of p.

Eg: If $p=13$, $a=2$ then by above corollary we have, $2^{\frac{13-1}{2}} \equiv -1 \pmod{13}$ so 2 is quadratic non-residue

and if $p=13$, $a=3$ then by again above corollary we have $3^{\frac{13-1}{2}} \equiv 1 \pmod{13}$ so 3 is quadratic residue of 13.

Remark: Euler's criterion is difficult to use for bigger prime number. As we have to calculate large powers. To reduce these calculations we introduce Legendre symbol.

Note: But the concept of quadratic residue is very much important, as the general quadratic congruence $ax^2+bx+c \equiv 0 \pmod p$ can be solved only by the quadratic congruence $x^2 \equiv a \pmod p$ and a linear congruence $y = 2ax+b$. and $d = b^2 - 4ac$ etc.

Legendre Symbol: Let p be an odd prime and $\gcd(a,p)=1$. The Legendre Symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{if } a \text{ is a quadratic residue of } p.\\ -1 & \text{if } a \text{ is a quadratic non-residue of } p.\end{cases}$$

Basic properties of Legendre Symbol:

Th^m Let p be an odd prime and a and b be integers which are relatively prime to p. Then the Legendre symbol has the following properties:

(i) If $a\equiv b \pmod p$ then $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

(ii) $\left(\frac{a^2}{p}\right)=1$

(iii) $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$.

(iv) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(v) $\left(\frac{1}{p}\right)=1$ and $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ (vi) $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)=\left(\frac{a}{p}\right)$.

Proof: (i) Consider $x^2\equiv a \pmod p$ ——— (1), $x^2\equiv b \pmod p$ ——— (2)

Since it is given that

$$a\equiv b \pmod p$$

$$\Rightarrow x^2\equiv a\equiv b\equiv x^2 \pmod p. \quad ((1),(2)\Rightarrow).$$

Hence either both congruence is solvable or both congruence is not solvable. ie either ~~both~~ $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ take the value 1 or both take the value -1. ie in both the situation

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

(ii) Consider $x^2\equiv a^2 \pmod p$.

Now this trivially true for $x=a$.

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{if } a \text{ is a quad residue of } p.\\ -1 & \text{if } a \text{ is a quad non residue of } p\end{cases}$$

But $\left(\frac{a^2}{p}\right)=\begin{cases}1 & \text{if } a^2 \text{ is a quadratic residue of } p.\end{cases}$

$\Rightarrow$ given congruence is always solvable.

$\therefore \left(\frac{a^2}{p}\right) = 1$

(iii) We know that $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p. \\ -1 & \text{if } a \text{ is a quad. non residue of } p. \end{cases}$ ①

By Euler's criteria,

a is a quadratic residue of p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ ④

①, ④ $\Rightarrow \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

Also by Corollary to Euler's criteria,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

(iv) Using part (iii), $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

$\therefore \left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod p$.

$\equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod p$

$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$.

$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$

$+1 \quad +1 \quad -1$

$1 \equiv -1 \pmod p \Rightarrow 2 \equiv 0 \pmod p \Rightarrow p \mid 2$ which is not possible as p is odd.

(v) Using part (iv), $\left(\frac{1}{p}\right) \equiv 1^{\frac{p-1}{2}} \pmod p$

$\equiv 1 \pmod p$.

As p is odd $p-1$ is even. so $\frac{p-1}{2}$ is an integer.

$\therefore \left(\frac{1}{p}\right) = 1$.

Also, $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. (by part (iv) again)

corollary of part (v) If p is an odd prime then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Pf: As we know that

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{(4k+1-1)}{2}} \equiv (-1)^{\frac{4k}{2}} \equiv (-1)^{2k} \equiv 1 \pmod p$$

when $p = 4k+1$.

and $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{(4k+3-1)}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$.

(vi) Using part (iv), $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)$

$= \left(\frac{a}{p}\right)$ $\left(\text{since } \left(\frac{b^2}{p}\right) = 1\right)$.

Eg: check whether $x^2 \equiv -46 \pmod{17}$ is solvable or not

Method 1 $\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right)$. $\left(\text{since } \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right)$

$= 1 \cdot \left(\frac{46}{17}\right)$. $\left[\text{since } \left(\frac{-1}{p}\right) = 1 \text{ if } p = 4k+1\right.$

$\left. = -1 \text{ if } 4k+3\right]$

$= \left(\frac{46}{17}\right)$ since $17 = 4.4+1$.

$= \left(\frac{12}{17}\right)$. $\left(\text{since } 46 \equiv 12 \pmod{17} \Rightarrow \left(\frac{46}{17}\right) = \left(\frac{12}{17}\right)\right)$.

$= \left(\frac{2^2 \cdot 3}{17}\right)$

$= \left(\frac{2^2}{17}\right)\left(\frac{3}{17}\right)$.

$= 1 \cdot \left(\frac{3}{17}\right) = \left(\frac{3}{17}\right)$

Now $\left(\frac{3}{17}\right) \equiv 3^{\frac{17-1}{2}} = 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1 \pmod{17}$.

$\therefore x^2 \equiv -46 \pmod{17}$ is not solvable.

Alternative method. $\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right) = \left(\frac{46}{17}\right)$

$= \left(\frac{2 \cdot 23}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{23}{17}\right)$

$= \left(\frac{2}{17}\right)\left(\frac{6}{17}\right)$, (since $23 \equiv 6 \pmod{17}$)

Now $\left(\frac{2}{17}\right) = 2^{\frac{17-1}{2}} \equiv 2^8 \equiv 2^4 \cdot 2^4 \equiv (-1)(-1) \equiv 1 \pmod{17}$.

$\left(\frac{6}{17}\right) = 6^{\frac{17-1}{2}} \equiv 6^8 \equiv (6^2)^4 \equiv (36)^4 \equiv 2^4 \pmod{17}$

$\equiv -1 \pmod{17}$.

$\therefore \left(\frac{-46}{17}\right) \equiv -1$.

$\therefore x^2 \equiv -46 \pmod{17}$ is not solvable. //

Theorem: If p is an odd prime, then $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

Hence there are precisely $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues of p.

pf: Eg: $p = 13$.

$a = \{1, 3, 4, 9, 10, 12\} \rightarrow$ quadratic residues.

$\{2, 5, 6, 7, 8, 11\} \rightarrow$ quadratic non residues.

Def^n of Legendre symbol says that $\left(\frac{a}{p}\right)$ has only two values ie.

$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is quadratic residue.} \\ -1 & \text{if } a \text{ is quadratic non-residue.} \end{cases}$

$\therefore \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{12}{p}\right)$.

$= 1 - 1 + 1 - \cdots + 1$.

$= 0$. //

Also, p is an odd prime so $p-1$ is even and hence $\frac{p-1}{2}$ is an integer. ie there are equal number of integers.

Proof of theorem: Let r be a primitive root of p. We know that, modulo p, the powers $r, r^2, \cdots r^{\phi(p)=p-1}$ are just a permutation of the integers $1, 2, 3, \cdots p-1$. Thus for any a between 1 and $p-1$, there exist a unique positive integer k $(1 \le k \le p-1)$ s.t $a \equiv r^k \pmod p$.

Therefore $\left(\frac{a}{p}\right) = \left(\frac{r^k}{p}\right)$

[if $a \equiv b \pmod p$ $\Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.]

$= \left(r^k\right)^{\frac{p-1}{2}}$

$= \left(r^{\frac{p-1}{2}}\right)^k$

$\equiv (-1)^k \pmod p$.

[$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$.]

Here we choose -1 because r is a primitive root ie $r^{\phi(p)=p-1} \equiv 1 \pmod p$, but $r^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. Hence $\left(\frac{a}{p}\right) =$ ~~± 1~~ -1 only choice. (As Legendre symbol has only two choice, 1 and -1).

$\therefore \left(\frac{a}{p}\right) = \left(\frac{r^k}{p}\right) \equiv (-1)^k \pmod p$.

[if k is even then $\left(\frac{a}{p}\right) = 1$. if k is odd then $\left(\frac{a}{p}\right) = -1$.]

$\therefore \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{r^k}{p}\right) = \sum_{k=1}^{p-1} (-1)^k = 0$.

→ Since $p-1$ is even so there are equal number of $+1$ and -1 and hence total sum is zero.

//

Corollary: The quadratic residues of an odd prime p are congruent modulo p to the even powers of a primitive root r of p; the quadratic non-residues are congruent to the odd powers of r.

Example Let $p=13$, $\phi(\phi(13)) = \phi(12) = 4$.

$\therefore$ There are 4 primitive roots of 13.

And the primitive roots are 2, 6, 7, 11.

For $r=2$, From the previous theorem, $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

Also we know that $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{K=1}^{p-1} \left(\frac{r^K}{p}\right) = (-1)^K$.

Now let us consider the only even powers of r, —

$2^2 \equiv 4$ $\quad 2^8 \equiv 9$

$2^4 \equiv 3$ $\quad 2^{10} \equiv 2^6 \cdot 2^4 \equiv 10$

$2^6 \equiv 12$ $\quad 2^{12} \equiv 1$.

And we know $\{1, 3, 4, 9, 10, 12\}$ are the quadratic residues of 13.

Again let us consider the only the odd powers of r, then we get quadratic non-residues of 13. ie

$2^1 \equiv 2$, $2^3 \equiv 8$, $2^5 \equiv 6$, $2^7 \equiv 11$, $2^9 \equiv 5$, $2^{11} \equiv 7$. $\rightarrow$ $\{2, 5, 6, 7, 8, 11\}$ are the quadratic non-residues of 13.

Let's verify the result for another primitive root $r=6$

$6^2 \equiv 36 \equiv 10$

$6^4 \equiv 6^2 \cdot 6^2 \equiv 36 \cdot 36 \equiv 10 \cdot 10 \equiv 9$.

$6^6 \equiv 6^4 \cdot 6^2 \equiv 9 \cdot 10 \equiv 90 \equiv -1 \equiv 12$

$6^8 \equiv 6^4 \cdot 6^4 \equiv 9 \cdot 9 \equiv 81 \equiv 3 \pmod{13}$

$6^{10} \equiv 6^8 \cdot 6^2 \equiv 3 \cdot 10 \equiv 30 \equiv 4 \pmod{13}$

$6^{12} \equiv 6^{10} \cdot 6^2 \equiv 4 \cdot 10 \equiv 40 \equiv 1 \pmod{13}$

$\therefore \{1, 3, 4, 9, 10, 12\}$ are the quadratic residues of 13.

Hence we say that the result doesn't depend on the primitive root. It only depends on the powers of primitive roots. If we consider even power

then we get quadratic residue and if we consider odd powers then we get quadratic non-residue. Once we get the set of quadratic residue then no need to calculate quadratic non-residues one by one. Because, the remaining integers definitely become the quadratic non-residues //

Gauss Lemma: Let p be an odd prime, let $\gcd(a,p)=1$. Then $\left(\frac{a}{p}\right) = (-1)^n$ where n denotes the number of integers in the set $S=\{a, 2a, 3a, \cdots, \left(\frac{p-1}{2}\right)a\}$ whose remainders upon division by p exceeds $p/2$.

e.g. $p=13$, $a=5$. $\left(\frac{p-1}{2} = \frac{13-1}{2} = 6\right)$

$S = \{5, 2.5, 3.5, 4.5, 5.5, 6.5\}$

$= \{5, 10, 15, 20, 25, 30\}$.

$\equiv \{5, 10, 2, 7, 12, 4\} \pmod{13}$.

these are the remainders and the number of remainders which are greater than $p/2$ are 7, 10, 12 ie only 3 numbers //

[Here $p/2 = \frac{13}{2} = 6.5$, $p/2 \geq 7$]

$\therefore \left(\frac{5}{13}\right) = (-1)^3 = -1$

$\therefore$ 5 is quadratic non-residue of 13 //

Proof: Here $\gcd(a,p)=1$, and $S=\{a, 2a, 3a, \cdots, \left(\frac{p-1}{2}\right)a\}$.

None of the $\frac{p-1}{2}$ integers in S is congruent to zero.

[If possible, $ja \equiv 0 \pmod p \Rightarrow j \equiv 0 \pmod p$ or $a \equiv 0 \pmod p$
Not possible $\Rightarrow p \mid a$.
$1 \leq j \leq \frac{p-1}{2}$. Not possible

None of elements of S are congruent to each other. [If possible $ra \equiv sa \pmod p$, $1 \leq r, s \leq \frac{p-1}{2}$

$\Rightarrow r \equiv s \pmod p$ (since $(a,p)=1$)

Not possible

so we may say $S = \{a, 2a, \cdots (\frac{p-1}{2})a\}$

$\equiv \{a_1, a_2, \cdots a_{\frac{p-1}{2}}\} \pmod p$, $0 < a_i < p$.

Let $r_1, r_2, \cdots r_m$ be the those remainder upon division by p.
and $0 < r_i < p/2$.

Let $\{s_1, s_2, \cdots s_n\}$ be those remainder s.t. $p > s_i > p/2$.

$\therefore m + n = \frac{p-1}{2}$.

$\therefore r_1, r_2, \cdots r_m$ and $p - s_1, \cdots p - s_n$ are all +ve and less than $p/2$. and none of them are congruent to each other,

on contrary, suppose $p - s_i \equiv r_j$

$\Rightarrow p = s_i + r_j$

$\therefore (u+v)a \equiv s_i + r_j = p \equiv 0 \pmod p$

$\Rightarrow u + v \equiv 0 \pmod p$ which is not possible as $u + v \le p-1$.

$s_i \equiv ua \pmod p, 1 \le u \le \frac{p-1}{2}$

$r_j \equiv va \pmod p, 1 \le v < \frac{p-1}{2}$

$u + v \le p-1$

So now, $\{1, 2, \cdots \frac{p-1}{2}\}$ in some order is congruent to

$\{r_1, r_2, \cdots r_m, p-s_1, \cdots p-s_n\}$

$\therefore (\frac{p-1}{2})! \equiv (r_1 r_2 \cdots r_m)(p-s_1, p-s_2 \cdots p-s_n) \pmod p$

$\equiv (r_1 r_2 \cdots r_m)(-s_1 \cdot -s_2 \cdots -s_n) \pmod p$

$\equiv (-1)^n (r_1 r_2 \cdots r_m)(s_1 s_2 \cdots s_n) \pmod p$.

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

$\equiv (-1)^n \cdot a^{\frac{p-1}{2}} \cdot (\frac{p-1}{2})! \pmod p$.

since $((\frac{p-1}{2})!, p) = 1$

$\Rightarrow 1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod p$.

$\Rightarrow (-1)^n \equiv a^{\frac{p-1}{2}} \pmod p$.

$\Rightarrow (-1)^n \equiv (\frac{a}{p}) \pmod p$.

$\Rightarrow (\frac{a}{p}) = (-1)^n$. //

Theorem: If p is an odd prime, then,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}.$$

Pf: According to Gauss Lemma,

$\left(\frac{2}{p}\right) = (-1)^n$, where n is the number of integers in the set, $S = \{2, 2.2, 3.2, \ldots, \left(\frac{p-1}{2}\right).2\}$ which upon division by p, have remainders greater than $p/2$. The members of S are all less than p, so that it suffices to count the number that exceed $p/2$.

The elements of S are all less than p.

To find $\left(\frac{2}{p}\right) = (-1)^n$. where n = number of elements of S — number of elements of S whose remainder is less than $p/2$.

and notice that in the set $S = \{2, 2.2, 3.2 \ldots \left(\frac{p-1}{2}\right)2\}$ all the elements of the form $2K$ where $1 \le K \le \frac{p-1}{2}$

Now we want those elements ~~would~~ whose remainder is less than $p/2$: ie $2K < p/2 \Rightarrow K < p/4$

and hence $n = \frac{p-1}{2} - [p/4]$. integers which are greater than $p/2$.

where $[\,]$ denotes the greatest integer function, then there are $[p/4]$ integers in S less than $p/2$.

Now we have four possibilities, for any odd prime has one of the forms - $8k+1$, $8k+3$, $8k+5$, or $8k+7$. A simple calculations shows that

(i) if $p = 8k+1$, $n = \frac{8k+1-1}{2} - \left[\frac{8k+1}{4}\right]$

$= 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k.$

$\therefore \left(\frac{2}{p}\right) = (-1)^{2k} = +1.$

(ii) if $p = 8k+3$, $n = \frac{8k+3-1}{2} - \left[\frac{8k+3}{4}\right]$

$= 4k+1 - 2k = 2k+1$

$\therefore \left(\frac{2}{p}\right) = (-1)^{2k+1} = -1.$

(iii) if $p = 8k+5$, $n = \frac{8k+5-1}{2} - \left[\frac{8k+5}{4}\right]$

$= 4k+2 - \left[2k+1+\frac{1}{4}\right]$

$= 4k+2 - (2k+1) = 2k+1.$

$\therefore \left(\frac{2}{p}\right) = (-1)^{2k+1} = -1.$

(iv) if $p = 8k+7$, $n = \frac{8k+7}{2} - \left[\frac{8k+7}{4}\right]$

$= 4k+3 - \left[2k+1+\frac{3}{4}\right]$

$= 4k+3 - (2k+1) = 2k+2$

$\therefore \left(\frac{2}{p}\right) = (-1)^{2k+2} = 1.$

Hence if p is of the form, $8k+1$ or $8k+7$ then $\left(\frac{2}{p}\right) = 1$ and if p is of the form $8k+3$ or $8k+5$ then $\left(\frac{2}{p}\right) = -1.$ //

Corollary: If p is an odd prime, then

$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$

Pf: From the previous theorem we have,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p = 8k \pm 1 \\ -1 & \text{if } p = 8k \pm 3. \end{cases}$$

Now $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{8k^2 \pm 2k}$

$= 1$.

when $p = 8k \pm 1$.

$(p^2-1)/8 = \frac{(8k\pm1)^2 - 1}{8}$

$= \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$

Now if $p = 8k \pm 3$, then $\frac{p^2-1}{8} = \frac{(8k\pm3)^2 - 1}{8}$

$= \frac{64k^2 \pm 48k + 8}{8}$

$= 8k^2 \pm 6k + 1$

$\therefore \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$.

Hence the proved. ∎

Germain Prime, Safe prime and its primitive root:

An odd prime p such that $2p+1$ is also a prime is called a Germain Prime. and its corresponding integer $2p+1$ is also prime and is called safe prime.

Thm: If p and $2p+1$ are both odd primes, then the integer $(-1)^{\frac{p+1}{2}} \cdot 2$ is a primitive root of $2p+1$.

(Actually the integer $(-1)^{\frac{p+1}{2}} \cdot 2$ is either 2 or -2 depending on $\frac{p+1}{2}$ (odd/even)).

Pf: Let p be an odd prime of the form $4k+1$ or $4k+3$.

And let us consider $q = 2p+1$ (say). To prove that $(-1)^{\frac{p-1}{2}} \cdot 2$ is a primitive root of q.

Case 1 Let $p = 4k+1$, then $q = 2p+1 = 2(4k+1)+1 = 8k+3$.

Then the integer $(-1)^{\frac{p-1}{2}} \cdot 2 = (-1)^{\frac{4k+1-1}{2}} \cdot 2 = 2$. ie we have to show that 2 is a primitive root of q. ie to show, $2^{\phi(q)} \equiv 1 \pmod{q}$ ie to show that $\phi(q)$ is the order of 2 modulo q.

If possible suppose, consider the order of 2 as $1, 2, p, 2p$. as these are the divisors of $\phi(q) = q-1 = 2p+1-1 = 2p$.

When order of 2 is 1: $2^1 \equiv 1 \pmod{q}$ which is not possible as q is odd prime.

When order of 2 is 2: $2^2 \equiv 1 \pmod{q}$ which is not possible as q is odd prime since $q = 2p+1$ since p is odd. so $p \geq 3$, so $q \geq 7$.

When order of 2 is p: $2^p \not\equiv 1 \pmod{q}$ because

Using Legendre Symbol, we get,-

$$\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \pmod{q}$$

$$\equiv 2^p \pmod{q}$$

$$\Rightarrow -1 \equiv 2^p \pmod{q}.$$

$q = 2p+1$

$\Rightarrow \frac{q-1}{2} = p$.

Also $\left(\frac{2}{q}\right) = \begin{cases} 1 & \text{if } q = 8k \pm 1 \\ -1 & \text{if } q = 8k \pm 3. \end{cases}$

ie $2^p \not\equiv 1 \pmod{q}$.

so now only possibility is order of 2 is $2p$.

But we know from Fermat's theorem that if $(2,q)=1$ where q is a prime

$$2^{\phi(q)} \equiv 1 \pmod{q}$$

$$\Rightarrow 2^{q-1} \equiv 1 \pmod{q} \Rightarrow 2^{2p} \equiv 1 \pmod{q}.$$

$\therefore$ order of 2 is $2p$.

Case II If $p = 4k+3$. then $q = 2p+1 = 2(4k+3)+1$
$= 8k+6+1$
$= 8k+7$

Then the integer $(-1)^{\frac{p-1}{2}} \cdot 2 = -2$ ie we have to show show that -2 is a primitive root of q ie to show $(-2)^{\phi(q)} \equiv 1 \pmod{q}$ ie to show $\phi(q)$ is the order of -2 modulo q.

If possible, consider the order of -2 as 1, 2, p, $2p$ as these are the divisors of $\phi(q) = q-1 = 2p$.

when order of -2 is 1 : $(-2)^1 \equiv 1 \pmod{q}$ which is not possible as $q \geq 7$.

order of -2 is 2 : $(-2)^2 \equiv 1 \pmod{q}$ which is not possible as $q \geq 7$

order of -2 is p : $(-2)^p \not\equiv 1 \pmod{q}$ because

Using the Legendre Symbol, we have,

$$\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) \pmod{q}$$

$$\Rightarrow (-2)^{\frac{q-1}{2}} = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) \pmod{q}$$

$\Rightarrow (-2)^p \equiv \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) \pmod q$

$\Rightarrow (-2)^p \equiv (-1)(+1) \pmod q$

$\Rightarrow (-2)^p \equiv -1 \pmod q$.

ie $(-2)^p \not\equiv 1 \pmod q$.

$\left(\frac{-1}{q}\right) = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3. \end{cases}$

$\left(\frac{2}{q}\right) = \begin{cases} 1 & \text{if } q = 8k \pm 1 \\ -1 & \text{if } q = 8k \pm 3 \end{cases}$

As $q = 8k+7$
$= 4k+3$.
Also $q = 8k+7$.
$= 8k-1$.

so now only possibility is order of -2 is $2p$. So again by Fermat's theorem

$(-2)^{\phi(q)} \equiv 1 \pmod q$

$\Rightarrow (-2)^{q-1} \equiv 1 \pmod q \Rightarrow (-2)^{2p} \equiv 1 \pmod q$.

$\therefore$ order of -2 is $2p = \phi(q)$

Hence 2 and -2 is the primitive root of $q = 2p+1$.

L-9

Theorem: There are infinitely many primes of the form $4k+1$.

Pf: Suppose that there are finite number of primes, say $p_1, p_2, \dots p_n$. and consider the integer,

$N = (2p_1 p_2 \cdots p_n)^2 + 1$

Clearly N is odd and it is of the form $4k+1$.

So by Division Algorithm, there exists an odd prime p such that $p \mid N$. which implies -

$(2p_1 p_2 \cdots p_n)^2 + 1 \equiv 0 \pmod p$

$\Rightarrow (2p_1 p_2 \cdots p_n)^2 \equiv -1 \pmod p$

Now the above congruence hold if

$\left(\frac{-1}{p}\right) = 1.$

$x^2 \equiv a \pmod p$ solvable if $\left(\frac{a}{p}\right) = 1$

Thus p is of the form $4k+1$.

Now as $p \mid N$, so p must be one of p_i, $1 \le i \le n$, and $p = p_k$.

$\therefore p_k \mid p_1 p_2 \cdots p_n$, and also $p_k = p \mid N$

$\Rightarrow p_k \mid (2p_1 p_2 \cdots p_n)^2 + 1$

$\Rightarrow p_k \mid 1$ which is a contradiction as p_k is a prime and $p_k > 1$.

so there exists infinitely many primes of the form $4k+1$.

$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3 \end{cases}$

$(2p_1 p_2 \cdots p_n)^2 + 1 \equiv 0 \pmod{p_k}$

$\Rightarrow 1 \equiv 0 \pmod{p_k}$

$\Rightarrow p_k \mid 1$

Th^m: There are infinitely many primes of the form $8k+1$.

pf: Suppose there exist finite number of primes of the form $8k-1$, say $p_1, p_2, \cdots, p_n$.

Consider $N = (4p_1 p_2 \cdots p_n)^2 - 2$

Now N is of the form $16q - 2$

Now by Division algorithm, there exist atleast one odd prime divisor p of N

so that $(4p_1 p_2 \cdots p_n)^2 \equiv 2 \pmod{p}$

In view of Legendres symbol, the above congruence is solvable if $\left(\frac{2}{p}\right) = 1$. ie if $p = 8k \pm 1$.

$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p = 8k+1 \\ -1 & \text{if } p = 8k+3 \end{cases}$

So when $p = 8k+1$, As we have $p \mid N$ ie $N \equiv 0 \pmod{p}$ and it is obvious that $p \equiv 0 \pmod{p}$

$\therefore$ If p is of the form $8k+1$ then N is also of the form $8q+1$ which is not true as N is of the form $16q-2$

$\therefore$ p is of the form $8k-1$. Also $p \mid N$ so there exists an odd prime p such that $p = 8k-1$ and $p \mid N$
But we already assume that there are finite number of primes of the form $8k-1$ i.e $p_1, p_2, \cdots, p_m$
thus p must be one of above say $p = p_k$ for some k, where $1 \le k \le n$.

$\therefore$ $p = p_k \mid N \Rightarrow p_k \mid (4(p_1 p_2 \cdots p_m))^2 - 2$ and $p_k \mid p_1 p_2 \cdots p_m$

$\therefore$ $p_k \mid 2$ which is a contradiction as
p_k is a odd prime so $p_k \ge 3$, or $p_k > 2$
Therefore there exist an infinitly many primes of the form $8k-1$.

Lemma: If p is an odd ~~integer~~ prime and a an odd integer, with $\gcd(a, p) = 1$ then, —

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{p-1} \left[\frac{ka}{p}\right]}$$

pf:

Quadratic Reciprocity Law: If p and q are distinct odd primes then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Pf:

Corollary: If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

pf: As p and q are odd so $p-1$ and $q-1$ are even.

Now By quadratic reciprocity law we have,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \quad \text{——— (*)}$$

If p is of the form $4k+1$ then from (*) we have,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{4k+1-1}{2}\cdot\frac{q-1}{2}} = (-1)^{2k\cdot\frac{q-1}{2}} = 1 \quad \left[\text{as } 2k\cdot\frac{q-1}{2} \text{ is even}\right]$$

Moreover, if q is of the form $4K+1$ then again from (*) we have,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{4k+1-1}{2}} = (-1)^{\frac{p-1}{2}\cdot 2k} = 1.$$

Now if $p = 4k+3$ and $q = 4k+3$ then from (*) we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = (-1)^{\frac{4k+3-1}{2}\cdot\frac{4k+3-1}{2}} = (-1)^{(2k+1)(2k+1)} = -1 \quad \left[\begin{matrix}\text{odd} \times \text{odd} \\ = \text{odd}\end{matrix}\right]$$

Thus $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if either } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$

Corollary 2: If p and q are distinct odd primes then,

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

pf: Since from Corollary 1 we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Now if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = \left(\frac{q}{p}\right)$$

$$\Rightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \left[\left(\frac{q}{p}\right)^2 = 1\right]$$

Similarly, if $p \equiv q \equiv 3 \pmod 4$ then,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$$

$$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 \equiv -\left(\frac{q}{p}\right)$$

$$\Rightarrow \left(\frac{p}{q}\right) \equiv -\left(\frac{q}{p}\right) \quad \left[\text{Since } \left(\frac{q}{p}\right)^2 = 1\right]$$

(d) $\left(\frac{1234}{4567}\right)$ Here $1234 = 2.617$.

$4567 \equiv 3 \pmod 4$, $617 \equiv 1 \pmod 4$

$$\therefore \left(\frac{1234}{4567}\right) \equiv \left(\frac{2}{4567}\right)\left(\frac{617}{4567}\right)$$

$$= (1)\left(\frac{4567}{617}\right) \quad \text{as } 4567 \equiv 7 \pmod 8$$

$$= \left(\frac{248}{617}\right) \equiv \left(\frac{2^3 \cdot 31}{617}\right) = \left(\frac{2}{617}\right)\left(\frac{31}{617}\right)$$

$$= (1)\left(\frac{31}{617}\right) \quad \text{as } 617 \equiv 1 \pmod 8$$

$$= \left(\frac{617}{31}\right) \equiv \left(\frac{28}{31}\right) = \left(\frac{4.7}{31}\right) = \left(\frac{7}{31}\right)$$

$$= -\left(\frac{31}{7}\right) \quad \text{as } 7 \equiv 3 \pmod 4,\ 31 \equiv 3 \pmod 4$$

$$= -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

$$\therefore \left(\frac{1234}{4567}\right) = 1.$$