21- Quadratic Reciprocity

CSE-D, CSE-E, CSE-F

Theorem (Euler's Criterion) – If p is prime, then

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

Theorem 1: (Law of Quadratic Reciprocity)- Let p and q be odd primes, then

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

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

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

Theorem 2: (Generalized Law of Quadratic Reciprocity)- Let a and b be odd positive integers, then

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

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

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

If $a = q_1 q_2 \ldots q_r$, then $\left(\frac{a}{b}\right) = \left(\frac{q_1}{a}\right)\left(\frac{q_2}{a}\right)\cdots\left(\frac{q_r}{a}\right).$

and if $b = p_1 p_2 \ldots p_r$, then $\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right).$

Q.1- Use the Law of Quadratic Reciprocity to compute the following Legendre symbols.

(a) $\left(\frac{85}{101}\right)$ **(b)** $\left(\frac{29}{541}\right)$ **(c)** $\left(\frac{101}{1987}\right)$ **(d)** $\left(\frac{31706}{43789}\right)$

Answer- (a) $\left(\frac{85}{101}\right)=\left(\frac{101}{85}\right)$ **since $101 \equiv 1 \pmod 4$**

$$\left(\frac{16}{85}\right)=\left(\frac{16}{5*17}\right)=\left(\frac{16}{5}\right)*\left(\frac{16}{17}\right)=\left(\frac{4^2}{5}\right)*\left(\frac{4^2}{17}\right)=1*1=1$$

[**If $b = p_1\ p_2\ ...p_r$, then** $\left(\frac{a}{b}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$

and $\left(\frac{a^2}{p}\right)=1$ **, where $p, p_1 , p_2 , ... , p_r$ are prime numbers**]

(b)

$$\left(\frac{29}{541}\right)=\left(\frac{541}{29}\right)=\left(\frac{19}{29}\right)=\left(\frac{29}{19}\right)=\left(\frac{10}{19}\right)=\left(\frac{2*5}{19}\right)$$

$$=\left(\frac{2}{19}\right)\left(\frac{5}{19}\right)=-\left(\frac{19}{5}\right)=-\left(\frac{4}{5}\right)=-\left(\frac{2^2}{5}\right)=-1$$

(c)

$$\left(\frac{101}{1987}\right)=\left(\frac{1987}{101}\right)=\left(\frac{68}{101}\right)=\left(\frac{2^2*17}{101}\right)=\left(\frac{2^2}{101}\right)\left(\frac{17}{101}\right)=1*\left(\frac{101}{17}\right)=\left(\frac{-1}{17}\right)=1$$

(d)

$$\left(\frac{31706}{43789}\right)=\left(\frac{2*15853}{43789}\right)=\left(\frac{2}{43789}\right)\left(\frac{15853}{43789}\right)=-\left(\frac{43789}{15853}\right)=-\left(\frac{12083}{15853}\right)$$

$$=-\left(\frac{15853}{12083}\right)=-\left(\frac{3770}{12083}\right)=-\left(\frac{2}{12083}\right)\left(\frac{1885}{12083}\right)=\left(\frac{12083}{1885}\right)=\left(\frac{773}{1885}\right)$$

$$=\left(\frac{1885}{773}\right)=\left(\frac{339}{773}\right)=\left(\frac{773}{339}\right)=\left(\frac{95}{339}\right)=\left(\frac{95}{3*113}\right)=\left(\frac{95}{3}\right)\left(\frac{95}{113}\right)=\left(\frac{2}{3}\right)\left(\frac{5*19}{113}\right)$$

$$=-\left(\frac{5}{113}\right)\left(\frac{19}{113}\right)=-\left(\frac{113}{5}\right)\left(\frac{113}{19}\right)=-\left(\frac{3}{5}\right)\left(\frac{-1}{19}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

Q.3-Let p be a prime number ($p \nmid 2$ and $p \nmid 5$), and let A be some given number. Suppose that p divides the number $A^2 - 5$. Show that p must be congruent to either 1 or 4 modulo 5.

Answer- $p \mid A^2 - 5$, so $A^2 - 5 \equiv 0 \pmod{p}$ or $A^2 \equiv 5 \pmod{p}$.

Therefore, $\left(\frac{5}{p}\right) = 1$ as 5 is QR (mod p)

or $\left(\frac{p}{5}\right) = 1$ $[5 \equiv 1 \pmod{4}]$

It means p is QR (mod 5). Therefore, p must be congruent to either 1 or 4 mod 5.

1^2	1
2^2	4
3^2	$9 \equiv 4$
4^2	$16 \equiv 1$

mod (5)

Q.7 Let p be a prime satisfying p ≡3 (mod 4) and suppose that a is a quadratic residue modulo p.

(a) Show that x = $a^{\left(\frac{p+1}{4}\right)}$ is a solution to the congruence $x^2 \equiv a \pmod p$. This gives an explicit way to find square roots modulo p for primes congruent to 3 modulo 4.

(b) Find a solution to the congruence $x^2 \equiv 7 \pmod{787}$. (Your answer should lie between 1 and 786.)

Answer- (a)

Euler's Criterion:

$$a^{\left(\frac{p-1}{2}\right)} \equiv \left(\frac{a}{p}\right) (\text{mod } p) \equiv 1 (\text{mod } p)$$ **[since a is QR (mod p)]**

$$x^2 = \left(a^{\left(\frac{p+1}{4}\right)}\right)^2 = a^{\left(\frac{p+1}{4}*2\right)} = a^{\left(\frac{p+1}{2}\right)} = a.a^{\left(\frac{p-1}{2}\right)} \equiv a(\text{mod } p)$$

This shows x = $a^{\left(\frac{p+1}{2}\right)}$ is solution to the congruence $x^2 \equiv a \pmod p$.

Q.8- Let p be a prime satisfying $p \equiv 5 \pmod 8$ and suppose that a is a quadratic residue modulo p.

(a) Show that one of the values $x = a^{(p+3)/8}$ or $x = 2a \cdot (4a)^{(p-5)/8}$ is a solution to the congruence $x^2 \equiv a \pmod p$. This gives an explicit way to find square roots modulo p for primes congruent to 5 modulo 8.

(b) Find a solution to the congruence $x^2 \equiv 5 \pmod{541}$. (Give an answer lying between 1and 540.)

(c) Find a solution to the congruence $x^2 \equiv 13 \pmod{653}$. (Give an answer lying between 1 and 652.)

Answer- (a) For $x = a^{(p+3)/8}$, $x^2 = (a^{(p+3)/8})^2 = a^{(p+3)/4} \equiv a.a^{(p-1)/4} \pmod p$ ---(*)

For $x = 2a \cdot (4a)^{(p-5)/8}$,

$x^2 = (2a \cdot (4a)^{(p-5)/8})^2$

$$= 2^2.a^2.4^{\left(\frac{p-5}{4}\right)}.a^{\left(\frac{p-5}{4}\right)} = 2^{\left(\frac{p-1}{4}\right)}.a^{\left(\frac{p+3}{4}\right)} \equiv 2^{\left(\frac{p-1}{4}\right)}.a^{\left(\frac{p-1}{4}\right)}.a \pmod p$$

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

---(**)

Euler's Criterion:

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

Thus $a^{\left(\frac{p-1}{4}\right)} \equiv \pm 1(\text{mod } p)$

If $a^{\left(\frac{p-1}{4}\right)} = 1$, **then from (*),** $x = a^{\left(\frac{p+3}{8}\right)}$ **will be solution to the given congruence.**

And if $a^{\left(\frac{p-1}{4}\right)} = -1$, **then from (**),** $\text{x} = 2\text{a} \cdot (4\text{a})^{\left(\frac{(\text{p-5})}{8}\right)}$ **will be solution to the given congruence.**

(b) $x^2 \equiv 7 \pmod{787}$.

$a = 7$, $p = 787 \equiv 3 \pmod 4$

$$\left(\frac{7}{787}\right) = -\left(\frac{787}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$$

Thus 7 is QR (mod 787).

Therefore, $x = 7^{\left(\frac{787+1}{4}\right)}$ must be solution to the congruence **$x^2 \equiv 7 \pmod{787}$.**

i.e. $x = 7^{197} \pmod{787}$

$197 = (11000101)_2 = 1 + 4 + 64 + 128$.

$7^1 = 7 \equiv 7 \pmod{787}$

$7^2 = (7^1)^2 \equiv 49 \equiv 49 \pmod{787}$

$7^4 = (7^2)^2 \equiv (49)^2 \equiv 2401 \equiv 40 \pmod{787}$

$7^8 = (7^4)^2 \equiv (40)^2 \equiv 1600 \equiv 26 \pmod{787}$

$7^{16} = (7^8)^2 \equiv (26)^2 \equiv 676 \equiv 676 \pmod{787}$

$7^{32} = (7^{16})^2 \equiv (676)^2 \equiv 456976 \equiv 516 \pmod{787}$

$7^{64} = (7^{32})^2 \equiv (516)^2 \equiv 266256 \equiv 250 \pmod{787}$

$7^{128} = (7^{64})^2 \equiv (250)^2 \equiv 62500 \equiv 327 \pmod{787}$

$x \equiv 7*40*250*327 \pmod{787} \equiv 105 \pmod{787}$ ***Ans.***

(b) a= 5, p = 541.

First compute $5^{\left(\frac{541-1}{4}\right)} \pmod{541}$, if it is 1, then solution would be

$$x \equiv 5^{\left(\frac{541+1}{8}\right)} \pmod{541}.$$

else if $5^{\left(\frac{541-1}{4}\right)} \pmod{541}$ is -1, then solution would be

$$x = 2*5.(4*5)^{\left(\frac{541+3}{8}\right)} \pmod{541}$$

(c) Similar to (b) ☺

22-Proof of Quadratic Reciprocity

Let p be an odd prime, let a be any integer not divisible by p, and for convenience, let $P = \left(\frac{p-1}{2}\right)$.

We consider the list of numbers

a, 2a, 3a, ... , Pa,

and we reduce them modulo p into the range from -P to P. Some of the reduced values will be positive and some of them will be negative. Let

μ(a , p) = (number of integers in the list a, 2a, 3a, ... , Pa that become negative when the integers in the list are reduced modulo P into the interval from –P to P)

Example1:- Let p = 13 , a = 3. Then P = 6.

1.3 ≡ 3 (mod 13)

2.3 ≡ 6 ≡ 6 (mod 13)

3.3 ≡ 9 ≡ -4 (mod 13)

4.3 ≡ 12 ≡ -1 (mod 13)

5.3 ≡ 15 ≡ 2 (mod 13)

6.3 ≡ 18 ≡ 5 (mod 13)

Therefore, μ(3 , 13) = 2.

Theorem 1(Gauss's Criterion): Let p be an odd prime, let a be an integer that is not divisible by p, Then

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$$

Verification: let p = 13, a = 3.

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$\mu(3\ ,\ 13) = 2$

$1 = (-1)^2$ //

Lemma 2: When the numbers a, 2a, 3a, … , Pa are reduced modulo pinto the range from -P to P, the reduced values are ± 1, … , ±P in some order, with each number appearing once with either a plus sign or a minus sign.

Verification: In example 1, each number between 1 and 6 appears once either with plus sign or with minus sign (3,6,-4, -1,2, 5).

Lemma 3: Let p be an odd prime, let $P = \left(\frac{p-1}{2}\right)$, let a be an odd integer that is not divisible by p. Then

$$\sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a, p) (\bmod 2)$$

Verification: - In example 1, we have, p = 13, a = 3, and therefore P = 6.

μ(3 , 13) = 2,

Compute

$$\sum_{k=1}^{6} \left\lfloor \frac{k.3}{13} \right\rfloor = \left\lfloor \frac{1.3}{13} \right\rfloor + \left\lfloor \frac{2.3}{13} \right\rfloor + \left\lfloor \frac{3.3}{13} \right\rfloor + \left\lfloor \frac{4.3}{13} \right\rfloor + \left\lfloor \frac{5.3}{13} \right\rfloor + \left\lfloor \frac{6.3}{13} \right\rfloor$$

$$= 0 + 0 + 0 + 0 + 1 + 1$$

$$= 2$$

2 ≡ 2 (mod 2)//

Q.1- Compute the following values.

(a) $\left\lfloor -\frac{7}{3} \right\rfloor$ (b) $\left\lfloor \sqrt{23} \right\rfloor$ (c) $\left\lfloor \pi^2 \right\rfloor$ (d) $\left\lfloor \frac{\sqrt{73}}{\sqrt[3]{19}} \right\rfloor$

Answer- (a) $\left\lfloor -\frac{7}{3} \right\rfloor = \lfloor -2.33 \rfloor = -3$ **(b)** $\left\lfloor \sqrt{23} \right\rfloor = \lfloor 4.795 \rfloor = 4$

(c) $\left\lfloor \pi^2 \right\rfloor = \lfloor 9.86... \rfloor = 9$ **(d)** $\left\lfloor \frac{\sqrt{73}}{\sqrt[3]{19}} \right\rfloor = \left\lfloor \frac{8.54..}{2.66} \right\rfloor = \lfloor 3.201.. \rfloor = 3$

Q.3- This exercise asks you to explore some properties of the function

$$g(x) = \lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor,$$

where x is allowed to take any real number.

(a) Compute the following values of g(x).

g(0), g(0.25), g(0.5) , g(1), g(2), g(2.5), g(2.499).

Answer-

$$g(0) = \lfloor 0 \rfloor + \left\lfloor 0 + \frac{1}{2} \right\rfloor = 0 + 0 = 0$$

$$g(0.25) = \lfloor 0.25 \rfloor + \left\lfloor 0.25 + \frac{1}{2} \right\rfloor = 0 + 0 = 0$$

$$g(0.5) = \lfloor 0.5 \rfloor + \left\lfloor 0.5 + \frac{1}{2} \right\rfloor = 0 + 1 = 1$$

$$g(1) = \lfloor 1 \rfloor + \left\lfloor 1 + \frac{1}{2} \right\rfloor = 1 + 1 = 2$$

$$g(2) = \lfloor 2 \rfloor + \left\lfloor 2 + \frac{1}{2} \right\rfloor = 2 + 2 = 4$$

$$g(2.5) = \lfloor 2.5 \rfloor + \left\lfloor 2.5 + \frac{1}{2} \right\rfloor = 2 + 3 = 5$$

$$g(2.99) = \lfloor 2.499 \rfloor + \left\lfloor 2.499 + \frac{1}{2} \right\rfloor = 2 + 2 = 4$$

Looks like $g(x) = \lfloor 2x \rfloor$

(b)-**Using your results from (a), make a conjecture that g(x) = $\lfloor kx \rfloor$ for a particular value of k.**

Answer- k = 2.

(c) Prove that your conjecture in (b) is correct.

Proof- Let x = a + r , where a is integer and $0 \le r < 1$.

Then $\lfloor x \rfloor = \lfloor a + r \rfloor = a + \lfloor r \rfloor$

$$\left\lfloor x + \tfrac{1}{2} \right\rfloor = \left\lfloor a + r + \frac{1}{2} \right\rfloor$$

For $0 \le r < \frac{1}{2}$ **or** $0 \le 2r < 1$

We have

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = a + \lfloor r \rfloor + a + \left\lfloor r + \frac{1}{2} \right\rfloor = 2a + 0 = 2a + \lfloor 2r \rfloor$$

For $\frac{1}{2} \le r < 1$ **or** $1 \le 2r < 2$

we have

$$\lfloor x \rfloor + \left\lceil x + \frac{1}{2} \right\rceil = \lfloor a + r \rfloor + \left\lfloor a + r + \frac{1}{2} \right\rfloor$$

$$= a + 0 + a + 1 = 2a + 1 = 2a + \lfloor 2r \rfloor$$

Therefore ,

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor$$

23- Which Primes are Sums of Two Squares?

Prime	Can it be expressed as a sum of Two Squares?	
2	Yes	$(1^2 + 1^2)$
3	No	
5	Yes	$(1^2 + 2^2)$
7	No	
11	No	
13	Yes	$(2^2 + 3^2)$
17	Yes	$(1^2 + 4^2)$
19	No	
23	No	
29	Yes	$(2^2 + 3^2)$
31	No	
37	Yes	$(1^2 + 6^2)$
43	No	
47	No	

Theorem1 (Sum of Two Squares Theorem for Primes). Let p be a prime. Then p is a sum of two squares exactly when

$$p \equiv 1 (\text{mod } 4) \qquad\qquad (\text{or } p = 2).$$

Statement 1. If p is a sum of two squares, then $p \equiv 1 \pmod 4$.

Statement 2. If $p \equiv 1 \pmod 4$, then p is a sum of two squares.

Proof(Statement1) –

It is given that p is sum of two squares, say

$$p = a^2 + b^2$$

We also know that p is odd, so exactly one of a and b must be odd. Switching them if necessary, we may assume that a is odd and b is even, say

$a = 2m + 1,\ b = 2n.$

$$\begin{aligned} \text{then} \quad p &= (2m)^2 + (2n+1)^2 \\ &= 4m^2 + 4n^2 + 1 + 4n \\ &\equiv 1 \pmod 4).// \end{aligned}$$

Lemma- If two numbers that are sums of two squares are multiplied together, then the product is also a sum of two squares.

Proof- $(u^2 + v^2)(A^2 + B^2) = u^2 A^2 + u^2 B^2 + v^2 A^2 + v^2 B^2$

$$= u^2 A^2 + v^2 B^2 + 2uAvB + u^2 B^2 + v^2 A^2 + u^2 B^2 - 2uAvB$$

$$= (Au + Bv)^2 + (Av - Bu)^2 .$$

Proof(Statement2)- Fermat's Descent Procedure-

We assume that $p \equiv 1 \pmod 4$. We want to write p as a sum of two squares.

Quadratic Reciprocity tells us that $x^2 \equiv -1 \pmod p$ has a solution, say $x = A$ and then $A^2 + 1$ is a multiple of p.

So we begin with the knowledge that

$$A^2 + B^2 = Mp \quad \text{for some integers } A, B \text{ and } M.$$

Descent Procedure

p any prime ≡ 1 (mod 4)

Write

$A^2+B^2 = Mp$ with $M< p$

Choose numbers u and v with

$u \equiv A \pmod M$

$v \equiv B \pmod M$

$$-\frac{M}{2} \le u, v \le \frac{M}{2}$$

Observe that

$$u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \pmod M$$

So we can write

$u^2 + v^2 = Mr$

$A^2 + B^2 = Mp$ (for some $1 \le r < M$)

Multiply to get

$$(u^2 + v^2)(A^2 + B^2) = M^2rp$$

Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$

$$\left(\frac{uA+vB}{M}\right)^2 + \left(\frac{vA-uB}{M}\right)^2 = rp$$

This gives smaller multiple of p written as a sum of two squares.

Repeat this process until p itself can be written as a sum of two squares.

Q.2-If the prime p can be written in the form $p = a^2 + 5b^2$, show that $p \equiv 1$ or $9 \pmod{20}$.

(Of course, we are ignoring $5 = 0^2 + 5 \cdot 1^2$).

Answer- $20 = 4*5$, $\gcd(4,5)=1$.

Reducing p mod 5, we have

$$p \equiv a^2 + 5b^2 \pmod 5$$
$$\equiv a^2 + 0 \pmod 5$$
$$\equiv a^2 \pmod 5$$
$$a^2 \equiv p \pmod 5$$

This shows p is quadratic residue mod 5. Therefore p must be congruence to either 1 or 4 mod 5. [1 and 4 are QR mod 5.]

Reducing p mod 4, we have

$$p \equiv a^2 + 4b^2 + b^2 \pmod 4$$
$$\equiv a^2 + 0 + b^2 \pmod 4$$
$$\equiv a^2 + b^2 \pmod 4$$

Since p is odd prime, exactly one of a and b must be odd,

say $a = 2x$, $b = 2y + 1$.

$$p \equiv (2x)^2 + (2y+1)^2 \pmod 4 \equiv 4x^2 + 4y^2 + 1 + 4y \pmod 4 \equiv 1 \pmod 4$$

Numbers that are congruent to 1 or 4 mod 5:

{...., 1,4,6,9,11,14,16,19,...}

Numbers that are congruent to 1 mod 4:

{...,1,5,9,13,17,...}

Therefore p must be congruent to either 1 or 9 (mod 5*4=20).//

Q.3- Use the Descent Procedure twice, starting from the equation $557^2 + 55^2 = 26.\ 12049$, to write the prime 12049 as a sum of two squares.

Answer-

p = 12049 ≡ 1(mod 4)

Write $557^2 + 55^2 = 26.\ 12049$

$A = 557,\ B = 55,\ M = 26.$

Choose numbers with

11 ≡ 557 (mod 26)

3 ≡ 55 (mod 26)

$$-\frac{26}{2} \leq 11{,}3 \leq \frac{26}{2}$$

Observe that $11^2 + 3^2 \equiv 557^2 + 55^2 \equiv 0 \pmod{26}$

So we can write $11^2 + 3^2 = 26*5$

$557^2 + 55^2 = 26*12049$

Multiply to get $(11^2 + 3^2)(557^2 + 55^2) = 26^2*5*12049$

Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$
$(11*557 + 3*55)^2 + (557*3 - 55*11)^2 = 26^2*5*12049$ $242^2 + 41^2 = 5*12049$
Set $A = 242$, $B = 41$, $M = 5$
Choose numbers with $2 \equiv 242 \pmod 5$ $1 \equiv 41 \pmod 5$ $\quad -\frac{5}{2} \leq 2,1 \leq \frac{5}{2}$
We can write $2^2 + 1^2 = 5*1$ $242^2 + 41^2 = 5*12049$
Multiply to get $(2^2 + 1^2)(242^2 + 41^2) = 5^2*1*12049$
Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$
$(242*2 + 41*1)^2 + (242*1 - 41*2)^2 = 5^2*1*12049$ $\left(\frac{(242*2+41*1)}{5}\right)^2 + \left(\frac{(242*1-41*2)}{5}\right)^2 = 12049$ $105^2 + 32^2 = 12049$

4. (a) Start from $259^2 + 1^2 = 34 \cdot 1973$ and use the *Descent Procedure* to write the prime 1973 as a sum of two squares.

Answer-

p = 1973

$259^2 + 1^2 = 34 * 1973$

A = 259, B = 1, M = 34

Choose numbers with

$-13 \equiv 259 \pmod{34}$

$1 \equiv 1 \pmod{34}$

$$-\frac{34}{2} \le -13, 1 \le \frac{34}{2}$$

Observe that

$(-13)^2 + 1^2 \equiv 259^2 + 1^2 \equiv 0 \pmod{34}$

So we can write

$(-13)^2 + 1^2 = 34*5$

$259^2 + 1^2 = 34 * 1973$

Multiply to get

$((-13)^2 + 1^2)(259^2 + 1^2) = 34^2*5*1973$

$$(259*(-13) + 1*1)^2 + (259*1 - 1*(-13))^2 = 34^2*5*1973$$

$(-99)^2 + 8^2 = 5*1973$ (OR) $99^2 + 8^2 = 5*1973$

p = 1973

$992 + 8^2 = 5*1973$

A = 99, B = 8, M = 5

Choose numbers with

$-1 \equiv 99 \pmod 5$

$-2 \equiv 8 \pmod 5$

$$-\frac{5}{2} \le -1, -2 \le \frac{5}{2}$$

Observe that

$(-1)^2 + (-2)^2 \equiv 99^2 + 8^2 \equiv 0 \pmod 5$

So we can write

$(-1)^2 + (-2)^2 \equiv 5*1$

$99^2 + 8^2 \equiv 5*1973$

Multiply to get

$((-1)^2 + (-2)^2)(99^2 + 8^2) = 5^2 *1*1973$

$$\left(\frac{(-1)\times 99 + 8\times(-2)}{5}\right)^2 + \left(\frac{99\times(-2) - 8\times(-1)}{5}\right)^2 = 1973$$

$(-23)^2 + (-38)^2 = 1973$

$23^2 + 38^2 = 1973$

(b) Start from $261^2 + 947^2 = 10 \cdot 96493$ and use the Descent Procedure to write the prime 96493 as a sum of two squares.

Answer-

p = 96493

$261^2 + 947^2 = 10 \cdot 96493$;   A = 261, B = 947, M = 10

Choose numbers with

$1 \equiv 261 \pmod{10}$

$-3 \equiv 947 \pmod{10}$

$$-\frac{10}{2} \le 1, -3 \le \frac{10}{2}$$

Observe that

$1^2 + (-3)^2 \equiv 261^2 + 947^2 \equiv 0 \pmod{10}$

So we can write

$1^2 + (-3)^2 = 10*1$

$261^2 + 947^2 = 10 * 96493$

Multiply to get

$(1^2 + (-3)^2)(261^2 + 947^2) = 10^2 * 1 * 96493$

Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$

$$(261 \times 1 + 947 \times (-3))^2 + (261 \times (-3) - 947 \times 1)^2 = 10^2 \times 96493$$

$$\left(\frac{-2580}{10}\right)^2 + \left(\frac{-1730}{10}\right)^2 = 96493$$

$$258^2 + 173^2 = 96493$$

24-Which Numbers are sums of Two Squares?

$(u^2 + v^2)(A^2 + B^2) = (uA + vB)2 + (vA - uB)^2$ -----------(*)

Step-by-step strategy for expressing a number **m** as a sum of two squares-

Divide: Factor m into a product of primes $p_1\, p_2 \cdots p_r$.

Conquer: Write each prime p_i as a sum of two squares.

Unify: Use the identity (*)repeatedly to write **m** as a sum of two squares.

Example- m = 26

- **$26 = 2 * 13$**
- **$2*13 = (1^2 + 1^2)(2^2 + 3^2)$**
- **$26 = (1^2 + 1^2)(2^2 + 3^2) = (1*2 + 1*3)^2 + (1*2 - 1*3)^2 = 5^2 + 1^2$.**

Theorem1 (Sum of Two Squares Theorem). Let m be a positive integer.

(a) Factor m as $m = p_1 p_2 \cdots p_r M^2$

with distinct prime factors $p_1, p_2, \ldots, p_r$. Then m can be written as a sum of two squares exactly when every p_i is either 2 or is congruent to 1 modulo 4.

(b) The number m can be written as a sum of two squares $m = a^2 + b^2$ with $\gcd(a, b) = 1$ if and only if it satisfies one of the following two conditions:

(i) m is odd and every prime divisor of m is congruent to 1 modulo 4.

(ii) m is even, m/2 is odd, and every prime divisor of m/2 is congruent to 1 modulo 4.

Theorem 2 (Pythagorean Hypotenuse Proposition). A number c appears as the hypotenuse of a primitive Pythagorean triple (a, b, c) if and only if c is a product of primes each of which is congruent to 1 modulo 4.

Q.1- For each of the following numbers m, either write m as a sum of two squares or explain why it is not possible to do so.

(a) 4370 (b) 1885 (c) 1189 (d) 3185.

Answer- (a) m = 4370 = $2 \times 5 \times 19 \times 23$

$$p_1 = 2, p_2 = 5, p_3 = 19, p_4 = 23$$

p_3 and p_4 are not congruent to 1 (mod 4). So this number can't be written as a sum of two squares.

(b) m = 1885 $= 5 \times 13 \times 29$

$$p_1 = 5 \equiv 1 (\text{mod } 4),\ p_2 = 13 \equiv 1 (\text{mod } 4),\ p_3 = 29 \equiv 1 (\text{mod } 4)$$

$$= (1^2 + 2^2)(2^2 + 3^2)(2^2 + 5^2)$$

$$= ((1 \times 2 + 2 \times 3)^2 + (2 \times 2 - 1 \times 3)^2)(2^2 + 5^2)$$

$$= (8^2 + 1^2)(2^2 + 5^2)$$

$$= (8 \times 2 + 1 \times 5)^2 + (1 \times 2 - 8 \times 5)^2$$

$$= 21^2 + 38^2$$

(c) $m = 1189 = 29 \times 41$

$$p_1 = 29, p_2 = 41$$

$$= (2^2 + 5^2)(4^2 + 5^2)$$

$$= (2 \times 4 + 5 \times 5)^2 + (5 \times 4 - 2 \times 5)^2$$

$$= 33^2 + 10^2$$

(d) $m = 3185 = 5 \times 13 \times 7^2$

$$(p_1 = 5, p_2 = 13, M = 7)$$

$$= (1^2 + 2^2)(2^2 + 3^2) \times 7^2$$

$$= ((1 \times 2 + 2 \times 3)^2 + (2 \times 2 - 3 \times 1)^2) \times 7^2$$

$$= (8^2 + 1^2) \times 7^2$$

$$= (8 \times 7)^2 + (1 \times 7)^2$$

$$= 56^2 + 7^2$$

Q.2- For each of the following numbers c, either find a primitive Pythagorean triple with hypotenuse c or explain why it is not possible to do so.

(a) 4370 (b) 1885 (c) 1189 (d) 3185

Answer-

(a) c = 4370 and even number. 4370 cannot be hypotenuse of a PPT.

(b) c = 1885 = 21^2+38^2

$$a=st, b=\frac{s^2-t^2}{2}, c=\frac{s^2+t^2}{2}; s\geq t>1, \gcd(s,t)=1,$$ **s and t are odd.**

$$2c=s^2+t^2$$

$$2c=2\times(21^2+38^2)=(1^2+1^2)(21^2+38^2)$$

$$=(1\times21+1\times38)^2+(1\times21-1\times38)^2$$

$$=59^2+17^2$$

$$s=59, t=17$$

$$a=st=59\times17=1003, b=\frac{s^2-t^2}{2}=\frac{59^2-17^2}{2}=1596, c=1885$$

$$(a,b,c)=(1003,1596,1885)$$

(c) c = 1189 = 29×41

$$= 33^2 + 10^2$$

$$2c = 2 \times (33^2 + 10^2)$$

$$= (1^2 + 1^2)(33^2 + 10^2)$$

$$= (1 \times 33 + 1 \times 10)^2 + (1 \times 10 - 1 \times 33)^2$$

$$= 43^2 + 23^2$$

$$s = 43, t = 23$$

$$a = st = 989$$

$$b = \frac{s^2 + t^2}{2} = 660$$

$$(a, b, c) = (989,660,1189)$$

(d) c = 3185 = $5 \times 13 \times 7^2$

7 is not congruent to 1 (mod 4), therefore c can't be hypotenuse of a Primitive Pythagorean Triple. (Theorem 2)

Q.3- Find two pairs of relatively prime positive integers (a, c) such that $a^2 + 5929 = c^2$. Can you find additional pairs with gcd(a, c) > 1?

Answer- $a^2 + 77^2 = c^2 \Rightarrow c^2 - a^2 = 77^2$

$$(c-a)(c+a) = 7^2 \times 11^2$$

// **If gcd(c-a,c+a)=1, then gcd(a,c)=1((a,b,c) is ppt).**

Proof-

Let d be the common factor of a and c.

Then d|a and d|c. ⇨ d|(c-a and d|c+a. But c-a and c+a are relatively prime.

Therefore d must be 1.//

(i) c-a = 1 and c+a = $7^2 * 11^2$

$2c = 1 + 7^2 * 11^2 = 5930$

c = 2965

a = 2964

(a,b,c) = (2964, 2965)

(ii) c-a = 7^2, c+a = 11^2

2c = 170

c = 85, a = 36

(a,c) = (36, 85)

For additional pair with gcd(a,c) >1,

we have to choose a-c and a+c such that

gcd(c-a,c+a)>1 and (a-c)(a+c) = $7^2 * 11^2$.

(iii) c-a = 7, c+a = $7 * 11^2$

(a,c) = ?

(iv) c-a = 11, c+a = $7^2 * 11$

(a,c)= ?

Q.4 In this exercise you will complete the proof of the first part of the Sum of Two Squares Theorem (Theorem 1). Let m be a positive integer and factor m as $m = p_1, p_2, \dots, p_r M^2$ with distinct prime factors $p_1, p_2, \dots, p_r$. If some p_i is congruent to 3 modulo 4, prove that m cannot be written as a sum of two squares.

Answer- Let $p_i \equiv 3 \pmod 4$ and p_i divides m

and suppose that m can be written as a sum of two squares, say

$m = a^2 + b^2$.

Then $m \equiv 0 \pmod{p_i}$ or $a^2 + b^2 \equiv 0 \pmod{p_i}$

$$a^2 \equiv -b^2 \pmod{p_i}$$

i.e. $$\left(\frac{-b^2}{p_i}\right) = 1$$

$$\left(\frac{-1}{p_i}\right)\left(\frac{b^2}{p_i}\right) = 1$$

$$-1 \times \left(\frac{b^2}{p_i}\right) = 1$$

$$\left(\frac{b^2}{p_i}\right) = -1$$

But we know that $\left(\frac{b^2}{p_i}\right) = 1$, it means our supposition was wrong i.e. m cannot be written as a sum of two squares.

25- Euler's Phi Function and Sums of Divisors

Q.1- A function f(n) that satisfies the multiplication formula $f(mn) = f(m)f(n)$ for all numbers m and n with $\gcd(m, n) = 1$ is called a multiplicative function. For example, we have seen that Euler's phi function $\varphi(n)$ is multiplicative and that $F(n) = \sum_{d/n} \Phi(n)$ is multiplicative.

Now suppose that f(n) is any multiplicative function, and define a new function

$$g(n) = f(d_1) + f(d_2) + \cdots + f(d_r),$$

where $1 = d_1 < d_2 < \cdots < d_{r-1} < d_r = n$ are the divisors of n.

Prove that g(n) is a multiplicative function.

Proof. If gcd(m, n) = 1, and

the divisors of m are $d_1, d_2, \ldots, d_r$,

and

the divisors of n are $e_1, e_2, \ldots, e_s$,

then $\gcd(d_i, e_j) = 1$ for all i,j, and the divisors of mn are $d_i e_j$ for $i = 1,2,\ldots,r$ and $j = 1,2,\ldots,s$. So

$$g(mn) = \sum_{i=1}^{r}\sum_{j=1}^{s} f(d_i e_j)$$

$$= \sum_{i=1}^{r}\sum_{j=1}^{s} f(d_i) f(e_j) \quad \text{(since } f(mn) = f(m)f(n) \text{)}$$

$$= \sum_{i=1}^{r} f(d_i) \sum_{j=1}^{s} f(e_j)$$

$= g(m)g(n)$ //

Q.2- Define $\lambda(n)$ by factoring n into a product of primes, $n = p_1^{k1}\ p_2^{k2} \cdots p_l^{kl}$, with $p_1 < p_2 < \cdots < p_l$ prime, and then setting $\lambda(n) = (-1)^{k1+k2+\cdots+kl}$, with $\lambda(1) = 1$. For example, since $1728 = 2^6 * 3^3$, we have $\lambda(1728) = (-1)^{6+3} = (-1)^9 = -1$.

(a) Compute $\lambda(30)$ and $\lambda(504)$.

Ans. We have $30 = 2^1 * 3^1 * 5^1$ and $504 = 2^3 * 3^2 * 7^1$, so $\lambda(30) = (-1)^{1+1+1} = -1$

and $\lambda(504) = (-1)^{3+2+1} = 1$.

(b) Prove that $\lambda(n)$ is a multiplicative function.

Proof. Write $m = p_1^{k_1}\ p_2^{k_2} \ldots p_r^{k_r}$ and $n = q_1^{l_1}\ q_2^{l_2} \ldots q_s^{l_s}$.

$$mn = p_1^{k_1}\ p_2^{k_2} \ldots p_r^{k_r}\ q_1^{l_1}\ q_2^{l_2} \ldots q_s^{l_s}.$$

Then $\lambda(m)\lambda(n) = (-1)^{(k_1 + k_2 + \ldots + k_r)}\ (-1)^{(l_1 + l_2 + \ldots + l_s)} = (-1)^{(k_1+k_2+\ldots+k_r+l_1+l_2+\ldots+l_s)} = \lambda(mn)$.

(Note there's no requirement that m and n are relatively prime!)

(c) We now define a new function G(n) by the formula $G(n) = \lambda(d_1) + \lambda(d_2) + \cdots + \lambda(d_r)$, where $1 = d_1 < d_2 < \cdots < d_{r-1} < d_r = n$ are the divisors of n. Explicitly compute G(n) for each $1 \le n \le 18$.

Ans.

n	λ(n)	G(n)
1	1	1
2	-1	0
3	-1	0
4	1	1
5	-1	0
6	1	0
7	-1	0
8	-1	0
9	1	1

n	λ(n)	G(n)
10	1	0
11	-1	0
12	-1	0
13	-1	0
14	1	0
15	1	0
16	1	1
17	-1	0
18	-1	0

It looks like G(n) = 1 if n is a perfect square, and 0 otherwise.

(d) Use your computations to make a guess as to the value of G(n). Use your guess to find the value of G(62141689) and G(60119483).

Ans. It looks like G(n) = 1 if n is a perfect square, and 0 otherwise. IF this is the case, then since 62141689 is a perfect square, but 60119483 is not, G(62141689) should be 1, and G(60119483) should be 0.

(e) Prove that your guess in (d) is correct.

Ans. Since λ(n) is multiplicative, so is G(n). [From Q.1]

So if $n = p_1^{k_1}\, p_2^{k_2} \ldots p_r^{k_r}$, then

$G(n) = G(p_1^{k_1}\, p_2^{k_2} \ldots p_r^{k_r}) = G(p_1^{k_1})\, G(p_2^{k_2}) \ldots G(p_r^{k_r})$

Now, $G(p^k) = \lambda(1) + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^k) = 1 + (-1)^1 + (-1)^2 + \ldots + (-1)^k$

$$= \begin{cases} 0 & \text{if } k \text{ is odd,} \\ 1 & \text{if } k \text{ is even.} \end{cases}$$

So G(n) is 0 whenever at least one k_i is odd (i.e. when n is not a perfect square) and is 1 otherwise (when n is a perfect square).

26- Powers Modulo p and Primitive Roots

Define: Fix p, and let a be an integer with gcd(a,p)=1. The order of a (mod p), written $e_p(a)$, is the smallest positive integer e such that $a^e \equiv 1$ (mod n).

Facts:

(1) $e_p(a) = 1$ if and only if $a = 1$

(2) $1 \le e_p(a) \le p-1$

(3) $e_p(a)$ divides p-1

* We call **a** a primitive root (mod p) if $e_p(a) = ø(p) = p-1$.

p = 5
$1^1 \equiv 1 \pmod{5}$
$2^4 \equiv 1 \pmod{5}$
$3^4 \equiv 1 \pmod{5}$
$4^2 \equiv 1 \pmod{5}$

p = 7
$1^1 \equiv 1 \pmod{7}$
$2^3 \equiv 1 \pmod{7}$
$3^6 \equiv 1 \pmod{7}$
$4^3 \equiv 1 \pmod{7}$
$5^6 \equiv 1 \pmod{7}$
$6^2 \equiv 1 \pmod{7}$

p = 11
$1^1 \equiv 1 \pmod{11}$
$2^{10} \equiv 1 \pmod{11}$
$3^5 \equiv 1 \pmod{11}$
$4^5 \equiv 1 \pmod{11}$
$5^5 \equiv 1 \pmod{11}$
$6^{10} \equiv 1 \pmod{11}$
$7^{10} \equiv 1 \pmod{11}$
$8^{10} \equiv 1 \pmod{11}$
$9^5 \equiv 1 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$

Smallest Power of a that Equals 1 Modulo p

Example:

$$e_5(1) = 1, e_5(2) = 4, e_5(3) = 4, e_5(4) = 2.$$

$$e_7(1) = 1, e_7(2) = 3, e_7(3) = 6, e_7(4) = 3, e_7(5) = 6, e_7(6) = 2.$$

$$e_{11}(1) = 1, e_{11}(5) = 5, e_{11}(7) = 10, e_{11}(9) = 5.$$

Theorem1(Order Divisibility Property) - Let a be an integer not divisible by the prime p, and suppose that $a^n \equiv 1 \pmod{p}$. Then the order $e_p(a)$ divides n.

In particular, the order $e_p(a)$ always divides p - 1.

Proof- $a^{e_p(a)} \equiv 1 \pmod{p}$

We are assuming that $a^n \equiv 1 \pmod{p}$.

We divide n by $e_p(a)$ to get a quotient and remainder,

$n = e_p(a)q + r$ with $0 \le r < e_p(a)$.

Then

$$1 \equiv a^n \equiv a^{e_p(a)q + r} \equiv (a^{e_p(a)})^q . a^r \equiv a^r \pmod{p}.$$

But $r < e_p(a)$, and by definition, $e_p(a)$ is the smallest positive exponent e that makes $a^e \equiv 1 \pmod{p}$, so we must have $r = 0$. Therefore $n = e_p(a)q$, which shows that $e_p(a)$ divides n.//

Theorem 2 (Primitive Root Theorem). Every prime p has a primitive root. More precisely, there are exactly $\phi(p - 1)$ primitive roots modulo p.

Q.2- For any integers a and m with gcd(a, m) = 1, we let $e_m(a)$ be the smallest exponent $e \geq 1$ such that $a^e \equiv 1 \pmod{m}$. We call $e_m(a)$ the order of a modulo m.

(a) Compute the following values of $e_m(a)$:

(i) $e_9(2)$ (ii) $e_{15}(2)$ (iii) $e_{16}(3)$ (iv) $e_{10}(3)$

(b) Show that $e_m(a)$ always divides $\phi(m)$.

Answer- (a)

(i)&(ii)

a = 2, m = 9, 15
$2^6 \equiv 1 \pmod{9}$
$2^4 \equiv 1 \pmod{15}$

(iii)&(iv)

a = 3, m = 16, 10
$3^4 \equiv 1 \pmod{16}$
$3^4 \equiv 1 \pmod{10}$

$e_9(2) = 6$, $e_{15}(2) = 4$

$e_{16}(3) = 4$, $e_{10}(3) = 4$

(b)Answer- $a^{e_m(a)} \equiv 1 \pmod{m}$

Euler's formula: $a^{\phi(m)} \equiv 1 \pmod{m}$.

We divide m by $e_m(a)$ to get a quotient and remainder,

$m = e_m(a)q + r$ with $0 \le r < \Phi(m)$.

Then

$$1 \equiv a^{\phi(m)} \equiv a^{e_m(a)q + r} \equiv (a^{e_m(a)})^q . a^r \equiv a^r \pmod{m}.$$

But $r < e_m(a)$, and by definition, $e_m(a)$ is the smallest positive exponent e that makes $a^e \equiv 1 \pmod{m}$, so we must have $r = 0$.

Therefore $\phi(m) = e_m(a)q$, which shows that $e_m(a)$ divides $\phi(m)$.//

Q.5- (a) If g is a primitive root modulo 37, which of the numbers $g^2, g^3, \ldots, g^8$ are primitive roots modulo 37?

(b) If g is a primitive root modulo p, develop an easy-to-use rule for determining if g^k is a primitive root modulo p, and prove that your rule is correct.

(c) Suppose that g is a primitive root modulo the prime p = 21169. Use your rule from (b) to determine which of the numbers $g^2, g^3, \ldots, g^{20}$ are primitive roots modulo 21169.

Answer-

(a) g^5 and g^7. //First read (b)//

(b) g^k will be primitive root if and only if gcd(k, p-1) =1.

Proof- Let d = gcd(k, p-1). Then d|k and d|p-1.

If G>1, Then

$$\left(g^k\right)^{\frac{p-1}{d}} = \left(g^{p-1}\right)^{\frac{k}{d}} \equiv (1)^{\frac{k}{d}} \equiv 1 \pmod{p}$$

It means order of g^k is $\frac{p-1}{d}$ which is less than p-1.

So g^k cannot be a primitive root.

Let us assume that d = 1 i.e. $\gcd(k,p-1) = 1$.

Then the equation $kx - (p-1)y = 1$ has solution in positive integers.

Let the solution be (u,v). Then $ku - (p-1)v = 1$ or $ku = 1 + (p-1)v$ ---(1)

Suppose that $(g^k)^n \equiv 1 \pmod p$. Then

$$g^{kn} \equiv 1 \pmod p$$

$$(g^{kn})^u \equiv 1^u \pmod p$$

$$g^{kun} \equiv 1 \pmod p$$

$$g^{(1+(p-1)v)n} \equiv 1 \pmod p$$

$$g^n (g^{p-1})^{vn} \equiv 1 \pmod p$$

$$g^n \equiv 1 \pmod p$$

Since g is primitive root modulo p, p-1 must divide n. Therefore order of g^k is p-1. [Order cannot exceed p-1].

(c) If g is primitive root, then g^k will be primitive root if and only if gcd(k, p-1) = 1.

p = 21169

p-1 = 21168 = $2^4 \times 3^3 \times 7^2$

So we need to find integers between 2 and 20 that are relatively prime to 21168.

As 2,3 and 7 are the only prime divisors of 21198,

numbers between 2 and 20 that are relatively prime to 21168:

5, 11, 13, 17, 19.

Therefore g^5, g^{11}, g^{13}, g^{17}, and g^{19} are primitive root modulo 21169.

27- Primitive Roots and Indices

Let p be a prime number with primitive root g. If a is positive integer with gcd(a,p)=1 , then the unique integer x with $1 \le x \le p-1$ and $g^x \equiv a \pmod{p}$ is called *the index of a to the base g modulo p*, denoted by I(a) or $I_g(a)$.

Example- Let p = 7, we know that 3 is primitive root modulo 7.

p = 7
$1^1 \equiv 1 \pmod{7}$
$2^3 \equiv 1 \pmod{7}$
$3^6 \equiv 1 \pmod{7}$
$4^3 \equiv 1 \pmod{7}$
$5^6 \equiv 1 \pmod{7}$
$6^2 \equiv 1 \pmod{7}$

a	1	2	3	4	5	6
$I_3(a)$	6	2	1	4	5	3

$3^1 \equiv 3 \pmod{7}$

$3^2 \equiv 3*3 = 9 \equiv 2 \pmod{7}$

$3^3 \equiv 3*2 = 6 \equiv 6 \pmod{7}$

$3^4 \equiv 3*6 = 18 \equiv 4 \pmod{7}$

$3^5 \equiv 3*4 = 12 \equiv 5 \pmod{7}$

$3^6 \equiv 3*5 = 15 \equiv 1 \pmod{7}$

$$3^{I(a)} \equiv a \pmod{7}$$

$I_3(1) = 6$

$I_3(2) = 2$

$I_3(3) = 1$ **etc.**

Theorem-1(Rules for Indices)-

Indices satisfy the following rules:

(a) $I(ab) \equiv I(a) + I(b) \pmod{p-1}$ [Product Rule]

(b) $I(a^k) \equiv kI(a) \pmod{p-1}$ [Power Rule]

Proof- (a) compute

$$g^{I(ab)} \equiv ab \equiv g^{I(a)} . g^{I(b)} \equiv g^{I(a) + I(b)} \pmod{p}.$$

$$g^{I(ab) - I(a) - I(b)} \equiv 1 \pmod{p}$$

But g is primitive root, so I(ab) must be multiple of p-1

i.e. p-1 divides $I(ab) - I(a) - I(b)$

or $I(ab) \equiv I(a) + I(b) \pmod{p-1}$ //

Proof-(b) $g^{I(a^k)} \equiv a^k \equiv (g^{I(a)})^k \equiv g^{kI(a)} \pmod{p}$

This implies that $I(a^k) - kI(a)$ is a multiple of p-1//

Q.1 Use the table of indices modulo 37 to find all solutions to the following congruences.

(a) $12x \equiv 23 \pmod{37}$ (b) $5x^{23} \equiv 18 \pmod{37}$

(c) $x^{12} \equiv 11 \pmod{37}$ (d) $7x^{20} \equiv 34 \pmod{37}$

Answer-

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$I_2(a)$	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7

18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
17	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8	19	18

(a) $\mathbf{12x \equiv 23 \pmod{37}}$

$$I(12x) \equiv I(23) \pmod{36}$$

$$I(12) + I(x) \equiv I(23) \pmod{36}$$

$$28 + I(x) \equiv 15 \pmod{36}$$

$$I(x) \equiv 15 - 28 \equiv -13 \equiv 23 \pmod{36}$$

$$x \equiv 5 \pmod{37} \textit{ Ans.}$$

(b) $5x^{23} \equiv 18 \pmod{37}$

$I(5x^{23}) \equiv I(11) \pmod{36}$

$I(5) + I(x^{23}) \equiv I(18) \pmod{36}$

$23 + 23I(x) \equiv 17 \pmod{36}$

$23I(x) \equiv -6 \equiv 30 \pmod{36}$

$A = 23$, $B = 36$, $c = 30$, $g = \gcd(23,36) = 1$ divides 30.

$36 = 1*23 + 13$	$13 = B - A$
$23 = 1*13 + 10$	$10 = A - (B-A) = 2A - B$
$13 = 1*10 + 3$	$3 = (B - A) - (2A - B) = -3A + 2B$
$10 = 3*3 + 1$	$1 = (2A - B) - 3(-3A + 2B)$
$3 = 3*1 + 0$	$1 = 11A - 7B$

$u_0 = 11$, $v_0 = 7$

$I(x_0) = 30*11/1 = 330$

$I(x) \equiv 319 \equiv 6 \pmod{36}$. Therefore $x \equiv 27 \pmod{37}$

(c) $x^{12} \equiv 11 \pmod{37}$

$I(x^{12}) \equiv I(11) \pmod{36}$

$12\, I(x) \equiv 30 \pmod{36}$

$\gcd(12, 36) = 12$ does not divide 30. So there are no solutions to this congruence.

(d) $7x^{20} \equiv 34 \pmod{37}$

$I(7x^{20}) \equiv I(34) \pmod{36}$

$I(7) + 20I(x) \equiv 8 \pmod{36}$

$32 + 20I(x) \equiv 8 \pmod{36}$

$20I(x) \equiv -24 \pmod{36} \equiv 12 \pmod{36}$

$A = 20$, $B = 36$, $C = 12$, $g = \gcd(20,36) = 4$.

$36 = 1*20 + 16 \qquad 16 = B - A$

$20 = 1*16 + 4 \qquad 4 = A - (B - A) = 2A - B$

$16 = 4*4 + 0 \qquad u_0 = 2,\ v_0 = 1$

$I(x_0) = 12*2/4 = 6.$

$I(x) \equiv [6 + k*36/4] \pmod{36}$; $k = 0,1,2,3$.

$I(x) \equiv 6, 15, 24, 33 \pmod{36}$

Therefore **$x \equiv 27, 23, 10, 14 \pmod{37}$** ***Ans.***

Q.3 Create a table of indices modulo 17 using the primitive root 3.

(a) Use your table to solve the congruence $4x \equiv 11 \pmod{17}$.

(c) Use your table to find all solutions to the congruence $5x^6 \equiv 7 \pmod{17}$.

Answer- (a)

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$I_3(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

$I(4x) \equiv I(11) \pmod{16}$

$I(4) + I(x) \equiv I(11) \pmod{16}$

$12 + I(x) \equiv 7 \pmod{16}$

$I(x) \equiv 7-12 \pmod{16}$

$I(x) \equiv -5 \pmod{16} \equiv 11 \pmod{16}$

$x \equiv 7 \pmod{17}$ *Ans.*

(b)

$5x^6 \equiv 7 \pmod{17}$

$I(5x^6) \equiv I(7) \pmod{16}$

$I(5) + I(x^6) \equiv I(7) \pmod{16}$

$5 + 6I(x) \equiv 11 \pmod{16}$

$6I(x) \equiv 6 \pmod{16}$

$A = 6$, $B = 16$, $C = 6$, $g = \gcd(A, B) = 2$.

$16 = 2*6 + 4 \quad 4 = B - 2A$

$6 = 1*4 + 2 \quad 2 = A - (B - 2A) = 3A - B$

$4 = 2*2 + 0 \quad u_0 = 3$, $v_0 = 1$

$I(x_0) = 6*3/2 = 9$.

$I(x) \equiv [9 + k*16/2] \pmod{16}$, $k = 0,1$.

$I(x) \equiv 9, 1 \pmod{16}$

$x \equiv$ **3, 14 (mod 17)** ***Ans.***