CHAPTER-1

1.4. It is generally believed that infinitely many primes have the form N2 + 1, although no one knows for sure.

(a) Do you think that there are infinitely many primes of the form $N^2 - 1$?

Answer: No.

For any N∈ Z and N≠ 1 ,

$N^2 - 1 = (N-1)(N+1)$

S0, we can always find two numbers N-1 and N+1, other than 1 and the number itself, which divide $N^2 - 1$. Therefore it cannot be prime number.

(b) Do you think that there are infinitely many primes of the form $N^2 - 2$?

(c) How about of the form $N^2 - 3$? How about $N^2 - 4$?

(d) Which values of a do you think give infinitely many primes of the form $N^2 - a$?

Answer: If a is not a square, we may not always find 2 or more than 2 numbers, other than 1 and $N^2 - a$, which divide $N^2 - a$. So we can expect infinitely many prime number of the form $N^2 - a$.

1.6. For each of the following statements, fill in the blank with an easy-to-check criterion:

(a&c) M is a triangular number if and only if _____ is an odd square.

Answer: If M is triangular number, then there exists some x in integer such that $M=\frac{x(x+1)}{2}$.

Also, if M is square, than there exists some y in integer such that $M= y^2$.

Therefore $\frac{x(x+1)}{2} = y^2$

⇨ $x^2 + x = 2y^2$

⇨ $x^2 + x - 2y^2 = 0$

Or $x = \frac{-1\pm\sqrt{1^2 - 4(1)(-2y^2)}}{2(1)} = \frac{-1\pm\sqrt{1+8y^2}}{2(1)}$ $\frac{-1\pm\sqrt{1+8M}}{2}$

Since x is an integer, $1 + 8M$ must be an odd square.

(b&c) N is an odd square if and only if _____ is a triangular number.

Answer: N is odd square if and only if there exist some x in integer such that $N = (2x+1)^2$

i.e. $N = 4x^2 + 1 + 4x$

or N-1 = 4x(x+1)

or $\frac{N-1}{8} = \frac{x(x+1)}{2}$ (triangular number)

N is an odd square if and only if $\frac{N-1}{8}$ is a triangular number.//

CHAPTER-3

3.3 Find a formula for all the points on the hyperbola $x^2 - y^2 = 1$ whose coordinates are rational numbers. [Hint. Take the line through the point (-1, 0) having rational slope m and find a formula in terms of m for the second point where the line intersects the hyperbola.]

Answer: Equation of the line passing through the point (-1, 0) and having slope m is given by

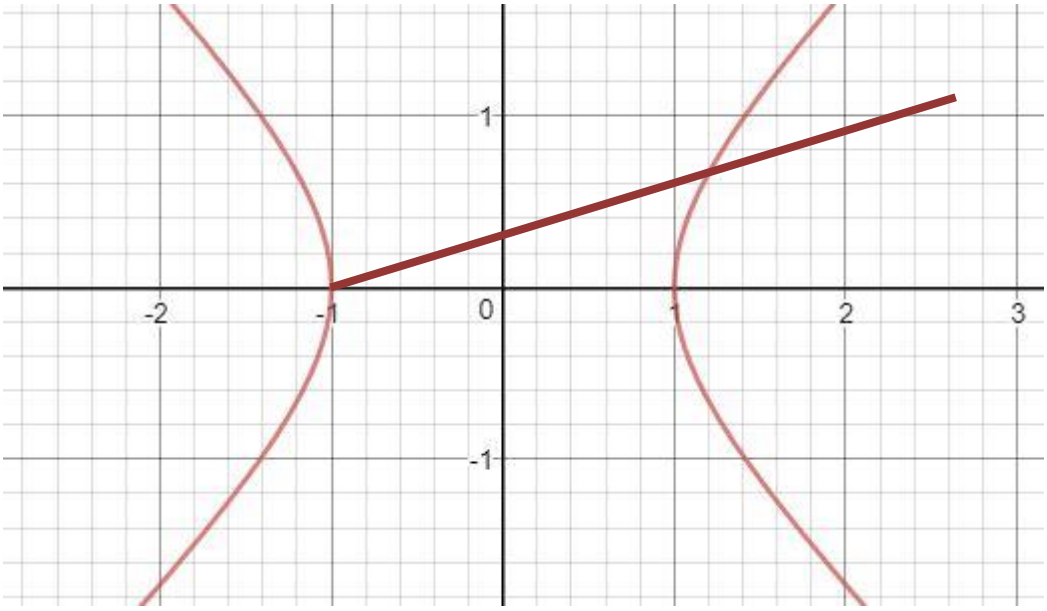
$y - y_1 = m(x-x_1)$

L: $y = m(x + 1)$ (since $x_1 = -1, y_1 = 0$)

H: $x^2 - y^2 = 1$

C∩L: $x^2 - (m(x + 1))^2 = 1$

$x^2 (1 - m^2) - 2m^2x - (1 + m^2) = 0$ ---- (1)



Since (x + 1) is a factor of this quadratic equation, the other factor can be obtained by dividing this equation by (x + 1).

$$
\begin{array}{r|l}
 & x(1-m^2)-(1+m^2) \\
\hline
(x+1) & x^2(1-m^2)-2m^2x-(1+m^2) \\
 & x^2(1-m^2)-m^2x \\
\hline
 & -(1+m^2)x-(1+m^2) \\
 & -(1+m^2)x-(1+m^2) \\
\hline
 & 0
\end{array}
$$

$[\, x(1-m^2)-(1+m^2)] = 0$

$\Rightarrow [x(1-m^2)-(1+m^2)] = 0$

$\Rightarrow x = \frac{1-m^2}{1+m^2}$

Substituting x into L,

$y = m(x + 1)$

$= m(\frac{1-m^2}{1+m^2} + 1)$

$= \frac{2m}{1+m^2}$

Taking rational slope m, we can get all rational coordinates

$(x, y) = (\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2})$ **on hyperbola.**

3.4 The curve

$$y^2 = x^3 + 8$$

contains the points (1, -3) and (-7 / 4, 13 / 8). The line through these two points intersects the curve in exactly one other point. Find this third point. Can you explain why the coordinates of this third point are rational numbers?

Answer:

C: $y^2 = x^3 + 8$

L: $y - y_1 = m(x - x_1)$, where $m = \frac{y2-y1}{x2-x1} = -37/22$ $(x_1, y_1) = (1, -3)$ & $(x_2, y_2) = (-7/4, 13/8)$

L: $y = -3 - \frac{37}{22}(x - 1)$

To find the other point, substitute y from L into C

$$[-1 - \frac{37}{22}(x + 3)]^2 = x^3 + 8$$

Or $484x^3 - 1369x^2 - 2146x + 3031 = 0$.

We know that (x-1) and (x + 7/4) is a factor of this polynomial, we can we can find the third factor by dividing this polynomial of degree three by $(x - 1)(x + 7/4) = 4x^2 + 3x - 7$.

$$\begin{array}{r|l} & 121x - 433 \\ \hline 4x^2 + 3x - 7 & 484x^3 - 1369x^2 - 2146x + 3031 \\ & \underline{484x^3 + 363x^2 - 847x} \\ & -1732x^2 - 1299x + 3031 \\ & \underline{-1732x^2 - 1299x + 3031} \\ & 0 \end{array}$$

Other factor is : $(121x - 433)$

Equating to zero- $x = \frac{433}{121}$

Put this value into the L

$y = -\frac{9765}{1331}$

So the third point is : $(x,y) = (\frac{433}{121}, -\frac{9765}{1331})$.

CHAPTER- 6: LINEAR EQUATIONS AND GREATEST COMMON DIVISORS

2. Describe all integer solutions to each of the following equations.
(a) 105x + 121y = 1

Answer-

a=105, b=121

We can always find the solution (x_1, y_1) in integers to the equation ax +by = gcd(a, b)=g.

Find g= gcd(105, 121)
121 = 1*105 + 16
105 = 6*16 + 9
16 = 1*9 + 7
9 = 1*7 + 2
7 = 3*2 + 1 =g
2 = 1*2 + 0

So, we need to find the solution of the equation 105x +121y =1=g
16= 121 – 1*105 = b-1*a = -a + b
9= 105 – 6*16 = a -6*(b-a) = 7a-6b
7= 16 – 1*9 = (-a +b)-1*(7a-6b) = -8a +7b
2= 9-1*7 = (7a-6b)-1*(-8a +7b) = 15a -13b
1 = 7-3*2 = (-8a + 7b)-3*(15a – 13b) = -53a + 46b
(x_1 = -53, y_1 = 46)

We know that every solution to the equation can be obtained by substituting integers k into the formula

$\left(x_1 + k*\frac{b}{g}, y_1 - k*\frac{a}{g} \right)$; $\frac{b}{g} = \frac{121}{1} = 121$ and $\frac{a}{g} = \frac{109}{1} = 105$.

The general solution is (-53 + k*121, 46 – k*105) with k integers.

(b) 12345x+67890y = gcd(12345,67890)

Answer-

a= 12345 , b= 67890;

We can always find the solution (x_1, y_1) in integers to the equation ax +by = gcd(a, b)=g.

Find g= gcd(12345, 67890)

67890 = 5*12345 + 6165
123456 = 2*6165 + 15
6165 = 411*15 + 0

6165 = 67890 – 5*12345 = b – 5* a = -5a + b
15 = 12345 – 2*6165 = a – 2*(-5a + b) = 11a -2b

(x_1 = 11, y_1 = -2)

$\frac{b}{g} = \frac{67890}{15} = 4526$ and $\frac{a}{g} = \frac{12345}{15} = 823$.

The general solution is (-11 + k*4526, 46 – k*823) with k integers.

(c) **54321x+9876y = gcd(54321,9876)**

Answer-

a = 54321, b = 9876;

We can always find the solution (x_1, y_1) in integers to the equation ax +by = gcd(a, b)=g.

Find g= gcd(a, b)

54321 = 5* 9876 + 4941
9876 = 1* 4941 + 4935
4941 = 1*4935 + 6
4935 =822*6 + 3
6 = 2*3 + 0

4941 = 54321 – 5*9876 = a-5b
4935 = 9876 -1*4935 = b-1*(a-5b) = -a + 6b
6 = 4941 – 1*4935 = (a - 5b) - 1*(-a + 6b) = 2a -11b
3 = 4935 – 822*6 = (-a + 6b) – 822*(2a – 11b) = -1645a + 9048b

(x_1 = -1645, y_1 = 9048)

$\frac{b}{g} = \frac{9876}{3} = 3292$ and $\frac{a}{g} = \frac{54321}{3} = 18107$.

The general solution is (-1645 + k*3292, 9048 – k*18107) with k integers.

5. Suppose that gcd(a, b) = 1. Prove that for every integer c, the equation ax + by = c has a solution in integers x and y. [Hint. Find a solution to au+ bv = 1 and multiply by c.] Find a solution to 37x + 47y = 103. Try to make x and y as small as possible.

Answer-

We know that we can always find the solution to the equation au + bv = gcd(a, b).
So, let us try to find the solution to the equation 37u +47v = gcd(37, 103). We can find the solution to the equation 37x + 47y = 103 if 103 is a multiple of gcd(37, 47).

a =37 , b = 47;

47 = 1*37 + 10

37 = 3*10 + 7

10 = 1*7 + 3

7 = 2*3 + 1

3 = 3*1 + 0

10 = 47 – 1*37 = b – 1*a = – a + b

7 = 37 – 3*10 = a – 3*(-a + b) = 4a – 3b

3 = 10 – 1*7 = (-a + b) – 1*(4a -3b) = -5a + 4b

1 = 7 -2*3 = (4a – 3b)-2*(-5a + 4b) = 14a – 11b

(u_1 = 14, v_1 = -11)

$37u_1 + 47v_1 = 1 = \gcd(37, 47)$ (since (u_1, v_1) is the solution to the equation $37u + 47v = 1$) Multiply both sides by 103.

$37(u1*103) + 47(v_1*103) = 103$.

Therefore ($x_1 = u1*103$, $y_1 = v_1*103$) would be the solution to the original equation $37x + 47y = 103$.

So, the solution is: (1442, -1133).

CHAPTER- 7: FACTORIZATION

2. Suppose that gcd(a, b) = 1, and suppose further that a divides c and that b divides c. Show that the product ab must divide c.

Answer:

METHOD-1:

Since gcd(a, b) = 1, we have LCM(a, b) = $\frac{ab}{\gcd(a,b)} = \frac{ab}{1}$ = ab.

LCM(a, b) * gcd(a, b) = a*b

Also, a divides c and b divides c, so c must be a common multiple of a and b.

Since c is a common multiple and ab= LCM is the least among all common multiples, ab ≤ c and ab must divide c.

METHOD-2:

Since a|c and b|c there are k, l ∈ Z satisfying ak = c and bl = c.

And since gcd(a,b) = 1, we have an integer solution to ax + by = 1.

Multiplying both sides by k, we get

k = akx + bky

= cx + bky **since ak = c,**

= blx + bky **since c = bl,**

= b(lx + ky).

So

c = ak = ab(lx + ky).

Therefore, since lx + ky ∈Z, we have ab|c.

2. This exercise asks you to continue the investigation of the E-Zone. Remember as you work that for the purposes of this exercise, odd numbers do not exist!

(a) Describe all E-primes.

Answer- E-primes- { 2, 6, 10, 14, 18,...}

$\frac{2}{2}$ = 1(odd), $\frac{6}{2}$ = 3(odd), $\frac{10}{2}$ = 5(odd), $\frac{14}{2}$ **= 7(odd),....**

While $\frac{4}{2}$ = 2 (even), $\frac{8}{2}$ = 4 (even), $\frac{12}{2}$ = 6 (even), ...

If m is E-prime, then $\frac{m}{2}$ = odd number.

So E-primes are exactly all those even numbers for which $\frac{m}{2}$ is odd.

(b) Show that every even number can be factored as a product of E-primes. [Hint. Mimic our proof of this fact for ordinary numbers.]

Answer- **Let n be an even number.**

If n is E-prime, we are done.

If n is not an E-prime, we can write n as a product of two even integers.

Say n= p*q.

If p or q (or both p and q) are E-primes, leave as they are, else factor them.

Keep on doing the same thing to each non- E-prime factors, we can write an even number as a product of E-primes.

(c) We saw that 180 has three different factorizations as a product of E-primes. Find the smallest number that has two different factorizations as a product of E-primes. Is 180 the smallest number with three factorizations? Find the smallest number with four factorizations.

Answer- A number of the form **$4x^2$** with odd prime number x will have two different factorization, namely $2(2x^2)$ and $(2x)(2x)$.The smallest such odd number is 3. If we take odd prime number x= 3, then we will have two different factorization- 2* 18 and 6*6. (Note- 2, 6 and 18 all are distinct E-primes).

Similarly a number of the form $4x^2y$ with odd prime number x and y will have three different factorization. Three different factors are $(2x^2)(2y)$, $(2x)(2xy)$ and $(2)(2x^2y)$. If we take x= 3 and y =5, we will have three different factorization- 18*10, 6*30 and 2*90.

A number of the form $4x^3y$ with odd primes x and y will have four different factorization. Three factors will be $2*2x^3y$, $2x*2x^2y$, $2x^2*2xy$ and $2x^3*2y$. Take x=3 and y=5. The smallest such number is 420.

(Can you find other form of such number? If YES, try to find.)

(d) **The number 12 has only one factorization as a product of E-primes: 12 = 2 · 6. (As usual, we consider 2 · 6 and 6 · 2 to be the same factorization.) Describe all even numbers that have only one factorization as a product of E-primes.**

Answer- There are only three possibilities-

1- $2x$, with x odd,

2- 2^k , with integer $k \geq 1$,

3- $(2^k)*p$ with integer $k \geq 1$ and p odd prime.

CHAPTER- 8: CONGRUENCES

5. Find all incongruent solutions to each of the following linear congruences.

- **(a)** $8x \equiv 6 \pmod{14}$ $\quad ax \equiv c \pmod{m}$

Answer. **a= 8, c= 6, m= 14.**

Since g = gcd (8, 14) = 2 and 2|6, there are exactly 2 incongruent solutions.

First solve 8u + 14v = gcd (8, 14) = 2, a solution is u_0 =2, v_0 = -1. $\quad$ **Au + Bv = gcd(A, B)**

Euclidian Algorithm to find gcd	Use intermediate quotients and remainders to find solution of the linear equation 8u + 14v = gcd (8, 14) = 2
A = 8, B= 14 14 = 1*8 + 6 8 = 1*6 + 2 6 = 3*2 + 0	6 = 14 – 1*6 = b – 1*a = b - a 2 = 8 – 1*6 = A – 1*(B – A) = A(2) + B(-1) OR A(2) + B(-1) = 2 = gcd (8, 14) ➔ (u_o = 2, v_0 = 1)

$x_0 = \frac{cu_0}{g} = \frac{6*2}{2} = 6$, and a complete set of *incongruent* solutions is given by

$x \equiv x_0 + k\frac{m}{g} \pmod{m}$ for k = 0, 1, 2, … , g-1.

$x \equiv 6 + k\frac{14}{2} \pmod{14}$ for k = 0, 1 **(since g-1 = 2-1 = 1)**

$x \equiv 6 + k * 7 \pmod{14}$ for k = 0, 1

i.e. $x \equiv 6 \pmod{14}$

and $x \equiv 13 \pmod{14}$

- **(b)** $66x \equiv 100 \pmod{121}$ $\quad ax \equiv c \pmod{m}$

Answer. **Since gcd(66,121) = 11 and 11†100, there are no solutions.**

❖ **(c)** $21x \equiv 14 \pmod{91}$ $ax \equiv c \pmod{m}$

Answer. a= 21, c= 14, m= 91.

Since g= gcd(21,91) = 7 and 7| 14, there are exactly 7 incongruent solutions.

First solve $21u + 91v = \gcd(21, 91) = 7$, a solution is $u_0 = -4$, $v_0 = 1$. $Au + Bv = \gcd(A, B)$

Euclidian Algorithm to find gcd		Using intermediate quotients and remainders to find solution of the linear equation $21u + 91v = \gcd(21, 91) = 7$
A =21, B= 91 $91 = 4*21 + 7$ $21 = 3*7 + 0$		$7 = 91 - 4*21 = B - 4A = (-4)A + (1)B$ ➔ $(u_0 = -4, v_0 = 1)$

$x_0 = \frac{cu_0}{g} = \frac{14*(-4)}{7} = -8$.

One solution is $x \equiv -8 \pmod{91}$ or $x \equiv 83 \pmod{91}$ *(since $-8 \equiv -8 + 91 \pmod{91}$)*

and a complete set of *incongruent* solutions is given by

$x \equiv x_0 + k\frac{m}{g} \pmod{m}$ for k = 0, 1, 2, … , g-1.

$x \equiv -8 + k\frac{91}{7} \pmod{91}$ for k = 0, 1, 2,..., 6 (since g-1 = 7-1 = 6)

$x \equiv -8 + k * 13 \pmod{91}$ for k = 0, 1, … , 6

i.e.

$x \equiv -8 \pmod{91}$ ⟷ $\equiv$ { ….,190, -99, -8, 83, 174, …. }(mod 91)

$x \equiv 5 \pmod{91}$ ⟷ $\equiv$ { ….,-177, -86, 5,96, 187, …. }(mod 91)

$x \equiv 18 \pmod{91}$ ⟷ $\equiv$ { ….,-164, -73, 18, 109, 200, …. } (mod 91)

$x \equiv 31 \pmod{91}$ ⟷ $\equiv$ { ….,-151, -60, 31, 122, 213, …. }(mod 91)

$x \equiv 44 \pmod{91}$ ⟷ $\equiv$ { ….,-138, -47, 44, 135, 226, …. } (mod 91)

$x \equiv 57 \pmod{91}$ ⟷ $\equiv$ { ….,-125, -34, 57, 148, 239, …. } (mod 91)

$x \equiv 70 \pmod{91}$ ⟷ $\equiv$ { ….,-112, -21, 70, 161, 252, …. } (mod 91)

6. Determine the number of incongruent solutions for each of the following congruences. You need not write down the actual solutions.

(a) $72x \equiv 47 \pmod{200}$

Answer. **Since gcd(72, 200) = 8 and 8 †47, there are no solutions.**

(b) $4183x \equiv 5781 \pmod{15087}$

Answer. **a= 4183, c= 5781, m= 15087**

First find gcd of 'a' and 'm'.

15087 = 3*4183 + 2538

4183 = 1*2538 + 1645

2538 = 1*1645 + 893

1645 = 1*893 + 752

893 = 1*752 + 141

752 = 5*141 + 47 ⇨ **g = gcd(a=4183, m=15087)**

141 = 3*47 + 0

Since g = 47 and 47 | 5781, there are exactly 47 incongruent solutions.

(c) $1537x \equiv 2863 \pmod{6731}$

Since g=gcd(1537, 6731) = 53 and 53 † 2863, there are no solutions.