Number Theory

Notes for B.Sc

By Prof. Asghar Ali

Number Theory

Divisibility

Divisibility:

Let 'a' and 'b' be any two integers. We say that 'a' divides 'b' or 'b' is divisible by 'a' denoted by a|b. when there exist integer 'c' such that b = ca. If a does not divides b then a∤b.

Perfect Number:

A number is said to be a perfect number if it is equal to the sum of its all +ve integral divisors. i.e 6|1 , 6|2 , 6|3 without itself 1+2+3=6

Theorem: let a,b and c be integers, then

(1) If a|b, then a|kb, for any integer k

If a|b, then ∃ integer k_1 s.t $b=ak_1$..... (1) multiplying equation (1) by integer k

$kb=ak\ k_1$, where $k_1, k \in Z$, so $kk_1 = k_2 \in Z$

$kb=ak_2 \rightarrow a|bk$

(2) If a|b, and b|a, then a=±b

If a|b, b|a, then ∃ integer k_1, k_2 s.t

$b= k_1a$..... (1) $a= k_2b$.... (2) use (2) in (1)

$b= k_1 k_2 b$, $k_1 k_2=1$, which is only possible

when both $k_1=1$, $k_2=1$ or $k_1 =-1$, $k_2=-1$ use in (1) and (2)

b = a..... (3), a= - b..... (4)

combine (3), and (4) a=±b

(3) For any non-zero integer k, a|b iff ka|kb

If a|b then ∃ integer k_1 s.t

$b= k_1a$ multiplying by k

$bk=ka(k_1) \rightarrow$ ka|bk

conversely

ka|bk, so ∃ integer k_2 s.t

$bk= k_2(ka)$ cancel out k

$b= k_2a \rightarrow$ a|b

Proposition

Let a,b,c be the integers then prove the following axioms.

(1)

- a|0
  0 = 0.a where 0,a be the integers. So a|0
- 1|a
  Since a = 1.a 1, a be the integer. So 1|a
- -1|a
  Since a = - (-1)(a) → -1|a -1, a be integers. So -1|a

(2) If a|b and b|c then a|c.

As a|b so there exist an integer k_1 s.t b = k_1a ……. (1)

Similarly if b|c there exist an integer k_2 s.t c = k_2b……...(2)

c = k_1k_2a using (1) $k_1, k_2 \in Z$, so we take $k_1k_2 = k$

c = ka → a|c.

(3) If a|b and a|c then a|bx+cy for every integer x or y.

If a|b then ∃ an integer k_1 s.t b = k_1a ……(1)

if a|c then ∃ an integer k_2 s.t c = k_2a……..(2)

then bx+cy = ak_1x + ak_2y

= a (k_1x + k_2y) as k_1, k_2, x, y∈ Z ,Let k_1x + k_2y = k ∈ Z

bx +cy = ak

→ a|bx + cy

Assignment: **If a|b and a|c then a|b + c and a|b - c.**

Proof:

If a|b so ∃ an integer k_1 s.t b = k_1a …….. (1)

if a|c so ∃ an integer k_2 s.t c = k_2a ……. .(2) (1) + (2)

b + c = k_1a + k_2a

= a($k_1 + k_2$) k_1, k_2 ∈ Z ,$k_1 + k_2$ = k ∈ Z

b + c = ak

→ a|b + c

Now (1) - (2)

b - c = k_1a - k_2a

= a(k_1-k_2) k_1, k_2 ∈ Z , k_1 - k_2 = k ∈ Z

b - c = ka → a|b – c Hence prove.

Division Algorithm

a = qd + r

a = 26, q = 8, d = 3, r = 2

26 = (8)(3) + (2)

26 = 26

Division Algorithm. Given integers a and b, with b>0, there exist unique integers q and r satisfying

$$a = qb + r \qquad 0 \le r < b$$

The integers q and r are called,respectively,the quotient and remainder in the division of a by b.

Proof. We begin by proving that the set

$$S = \{a - xb | x\ an\ integer; a - xb \ge 0\}$$

is non empty. To do this, it suffices to exhibit a value of x making $a - xb$ nonnegative. Because the integers $b \ge 1$, we have $|a|b \ge |a|$, and so

$$a - (-1|a|)b = a + |a|b \ge a + |a| \ge 0$$

For the choice $x = -|a|$, then, $a - xb$ lies S. This paves the way for an application of the well-ordering principle, from which we infer that the set S contains a smallest integers; call it r. By the definition of S, there exists an integers q satisfying

$$r = a - qb \qquad 0 \le r$$

We argue that $r < b$. If this were not the case then $r \ge b$ and

$$a-(q+1)b=(a-qb)-b=r-b\geq 0$$

The implication is that the integers $a-(q+1)b$ has the proper form to belong to the set S. But $a-(q+1)b=r-b<r$, leading to a contradiction of the choice of r as the smallest member of S. Hence, $r<b$.

Next we turn to the task of showing the uniqueness of q and r. Suppose that a has two representations of the desired form, say,

$$a=qb+r=q'b+r'$$

Where $0\leq r<b, 0\leq r'<b. then\, r'-r=b(q-q')$ and, owing to the fact that the absolute value of a product is equal to the product of the absolute values,

$$|r'-r|=b|q-q'|$$

Upon adding the two inequalities $-b<-r\leq 0\ and\ 0\leq r'<b$, we obtain

$-b<r'-r<b$ or,in equivalent terms, $|r'-r|<b$. thus, $b|q-q'|<b$, which yeilds

$$0\leq |q-q'|<1$$

Because $|q-q'|$ is a nonnegative integers, the only possibility is that $|q-q'|=0$, where $q=q'$; this,in turn, gives $r=r'$, ending the proof.

Mathmatical Induction

It is a method which is often used to prove the divisibility based result. It is most powerful tool to prove the result in exponent form. To prove the result with the help of mathematical induction, we have to follow the following steps:

- First , we will check the result at n = 1
- In the second step , we suppose that the result is true for n = k
- Now with the help of above supposition, we have to prove that the result is true for n = k+1

Remark :

If a result fulfilled the above three steps, then that result is true mathematically.

Quesion: Show that: a - b|a^n - b^n ∀ a,b Є Z, n is +ve

Proof: we prove the result by induction method.

Step 1:

Let n = 1 then,a - b | $a^1 - b^1$ ……(1) which is true for n=1.

Step 2:

Now we suppose it is true for n = k → a - b|$a^k - b^k$ ……(2)

Step 3:

Now we want to prove that for n = k + 1 is also satisfy a - b|$a^{k+1} - b^{k+1}$

a^{k+1}-b^{k+1} = $aa^k - bb^k$

$=aa^k - a^kb - bb^k + a^kb$ +ing and –ing a^kb

$=a^k(a-b) + b(a^k - b^k)$

From eq (1) a – b | a – b and a – b | $a^k - b^k$ by hypothesis

and we know that, If a|b and a|c then a|bx + cy ∀ x,y Є Z

Hence a – b |a^k(a - b) + b($a^k - b^k$) = $a^{k+1} - b^{k+1}$

→a - b | $a^{k+1} - b^{k+1}$

So a - b | $a^n - b^n$ ∀ a,b Є Z, by mathematical induction.

***Question :* if n is odd , prove that a + b | $a^n + b^n$ ∀ *a,b Є Z*.**

Proof :

We will prove above result by induction method.

Let n = 1 then a + b|$a^1 + b^1$ ……..(1) which is true for n=1.

Now suppose that above result is true for n = k (k is odd)

→ a + b|$a^k + b^k$ ……..(2)

Now we have to prove that the result is true for n = k + 2(k is odd) → a + b|$a^{k+2} + b^{k+2}$

$a^{k+2} + b^{k+2} = a^k a^2 + b^k b^2 + a^k b^2 - a^k b^2$ +ing and –ing $a^k b^2$

$= a^k a^2 - a^k b^2 + b^k b^2 + a^k b^2$

$= a^k(a^2 - b^2) + b^2(a^k + b^k)$

Since a + b|$a^2 - b^2$ also a + b|$a^k + b^k$ by hypothesis.

And we know that if a|b , a|c then a|bx + cy ∀ x,y Є Z

Hence a + b | $a^{k+2} + b^{k+2} = a^k(a^2 - b^2) + b^2(a^k + b^k)$

→ the result is true for n = k + 2 & ∀ n by mathematical induction.

Question : Prove that the product of any three consecutive integers is divisible by 6.

Proof:

Let n, n+1, n+2 be three consecutive integers. Then product of three consecutive integer is n (n + 1) (n + 2)

Now we have to prove that 6|n (n + 1) (n + 2) ……(1).We prove it by induction method.

Step 1:

Put n=1

Then 6|1 (1 + 1) (1 + 2) = 6 → 6|6 so it is true for n=1.

Step 2:

Now we suppose that the result is true for n=k

→ 6|k (k + 1) (k + 2)…….. (2)

Now we prove it that the result is true for n = k + 1

n (n + 1) (n + 2) = (k + 1) (k + 2) (k + 3) = k (k + 1) (k + 2) + 3 (k + 1) (k + 2)

By hypothesis factor k (k + 1) (k + 2) is divisible by 6 i.e 6| k (k + 1) (k + 2) .

Now we show that 6|3 (k + 1) (k + 2)

Here we have two cases.

1st : If k is even say k = 2m, m is integer then

6|3 (2m + 1) (2m + 2)

6|6 (2m + 1) (m + 1) which is true

2nd: If k is odd say k = 2m + 1, m is integer then

6|3 (2m + 1 + 1) (2m + 1 + 2) = 3 (2m + 2) (2m + 3)

6|6 (m+1) (2m+3) which is true.

We know that if a|b and a|c then a|bx + cy ∀ x , y Є Z

So 6|k (k + 1) (k + 2) + 3 (k + 2) (k + 3) = (k + 1) (k + 2) (k + 3) = n (n + 1) (n + 2)

→ 6|k (k + 1) (k + 2) (k + 3)

Hence It is proved that product of three consecutive integer is divisible by 6.

Question : **Prove that if n is +ve even integer then a + b|$a^n - b^n$.**

Proof:

We prove it by mathematical induction.

Step 1:

Put n=2 because n is +ve even .

→ a + b | $a^2 - b^2$ …….. (1)

→ a + b | (a + b) (a - b) which is tue for n=2.

Step 2:

Now we suppose that the result is true for n = 2k because n is even. k is integer

→ a + b | $a^{2k} - b^{2k}$ …….(2)

Now we have to prove that the result is true for n=2k+2 because n is +ve even.

→ a + b | $a^{2k+2} - b^{2k+2}$

$a^n - b^n = a^{2k+2} - b^{2k+2}$

$= a^{2k}a^2 - b^{2k}b^2 - a^{2k}b^2 + a^{2k}b^2$ +ing and –ing $a^{2k}b^2$

$= a^{2k}a^2 - a^{2k}b^2 + a^{2k}b^2 - b^{2k}b^2$

$= a^{2k}(a^2 - b^2) + b^2(a^{2k} - b^{2k})$

Fom eq (1) a + b | $a^2 - b^2$ and by hypothesis a + b| $a^{2k} - b^{2k}$

So we know that if a|b and a|c then a| bx+cy for every integers x, y

So a + b | $a^{2k}(a^2 - b^2) + b^2(a^{2k} - b^{2k}) = a^{2k+2} - b^{2k+2}$

Hence it is prove that if n is +ve even integer then a + b |$a^n - b^n$.

Example : Show that ∀ n (>0) Є Z, 24 |$2.7^n + 3.5^n - 5$

Proof :

We prove it by M.I

Step 1:

Put n = 1

24 | $2.7^1 + 3.5^1 - 5 = 2.7 + 3.5 - 5 = 24$ →24|24 which is true.

Step 2:

Now we suppose that result is true for n = k then,

24 |$2.7^k + 3.5^k - 5$ ……..(1)

Step 3:

Now we show that result is true for n = k + 1

$2.7^{k+1} + 3.5^{k+1} - 5 = 2.77^k + 3.55^k - 5$

$= 14.7^k + 15.5^k - 5$

$= 2.7^k + 12.7^k + 3.5^k + 12.5^k - 5$

$= (2.7^k + 3.5^k - 5) + 12.7^k + 12.5^k$

$= (2.7^k + 3.5^k - 5) + 12(7^k + 5^k)$

By hypothesis 24 | $2.7^k + 3.5^k - 5$. Now we will prove that 24 |$12(7^k + 5^k)$

Since 7^k and 5^k are odd and sum of two odd numbers is even , so the sum of 5^k and 7^k is even number.

So, 24 | 12 ($5^k + 7^k$)

Thus 24 | ($2.7^k + 3.5^k - 5$) + 12($5^k + 7^k$)

we know that if a|b and a|c then a| bx+cy for every integers x, y

Hence, It is proved that ∀ n (>0) Є Z, 24 | $2.7^n + 3.5^n - 5$.

Assignment: Show that ∀ n (>0) ∈ Z, $9|10^n + 3.4^{n+2} + 5$.

Proof: **(do yourself).**

Theorem: **Every odd integer can be written in the form of 4k + 1 or 4k + 3, 4n + 1or 4n – 1.**

Proof :

Let a be an odd integer . We want to write in the form of 4n+1 or 4n-1

We prove it by division algorithm method. As a is an odd integer. Let d = 4 then ∃ unique integer "n" and "r" s.t

a = 4n + r $\quad 0 \leq r < d$. as d=4 so r=0,1,2,3

if r = 0 , then ,

a = 4n ……..(1)

if r = 1,2,3 ,then ,

a = 4n + 1 ……(2)

a = 4n + 2 ……(3)

a = 4n + 3 ……(4)

where a=4n , a = 4n + 2 , both are even numbers .

but we given that a is odd so we take a = 4n + 1 , a = 4n + 3 ,i.e , 4n - 1

Hence , Every odd integer can be written in the form 4n + 1 or 4n - 3.

G.C.D (Greatest Common Divisor)or (H.C.F)

Definition:

A +ve integer d is called G.C.D of 'a' and 'b' if the following are holds

- $d \geq 0$
- d|a and d|b
- if some other integer c exists s.t c|a and c|b , then c|d or $c \leq d$

gcd of a, b is denoted such as gcd(a, b)=d or simply we can write (a, b)=d

Example: Find gcd(24 , 16) find prime factors of 24 and 16

24 = (2) (2) (2) (3)

16 = (2) (2) (2) (2)

gcd (24 , 16) = (2) (2) (2)

gcd (24 , 16) = 8

Question : ***if c is a common divisor of a, b then c|(a, b) .also prove that d is unique.***

Proof :

Let (a, b)=d, then there exists some integers x, y s.t $\quad ax+by=d$…….(1)

Since c|a and c|b

We know If a|b and a|c then a|bx+cy for every integer x or y

So c|ax+by→ $\quad c|d \quad$ from (1)

Now we will prove that gcd of a, b is unique. For this suppose d_1, d_2 be two gcd's of a, b

Then $d_1 \leq d_2$ as d_1 is common divisor and d_2 is a gcd. Similarly $d_2 \leq d_1$ as d_2 is common divisor and d_1 is a gcd. So that $d_1 = d_2$.

Theorem: ***If d = gcd(a , b) then 'd' can be expressed as a linear combination of 'a' and 'b' i.e d = ax + by: where x, y are some integers and a, b not both of which are zero.***

Proof :

Let 'S' be set defined as S = {au+bv |au+bv > 0 ,u,v ∈ Z}

1st we will prove that 'S' is non-empty set.

Let b=0 then
$|a| = au+b(0)$ choosing $u = 1$
$|a| = a(1) \in S$
If $u = -1$ then 'a' is $(-a)$
$\rightarrow |a| = (-a)(-1) \in S$ So 'S' is non-empty.
{By using well order principle WELL ORDERING PRINCIPLE that Every non – empty set S of Non – negative integer contains a least element that is there is some integer a in S s.t $a \leq b, \forall b \in S$}
So S has least element say 'd'.
Then for some integer x,y we have
$d = ax+by$ ……..(1)
we have to prove that gcd (a,b) = d.
by using division algorithm . $\exists$ unique integers q & r s.t
$a = qd+r$ ……(2) where $0 \leq r < d$.
$a = q(ax+by) + r$ from (1)
$a = aqx + qby + r$
$a-aqx-qby = r$
$a(1-qx) + b(-qy) = r$ ……(3) $\because$ 1,q,x,y ∈ Z ,(1-qx) , (-qy) are also integers.
Let $1-qx = t$, $-qy = m$ put in (3)
Then $at+bm = r$
$\rightarrow at + bm \in S \rightarrow r \in S$.
If r is the +ve integer $r \neq 0$ .Then $0 < r < d$. $\rightarrow r \in S$ this shows r is the least element of S. But we consider 'd' is also least element so we take r = 0 then eq (2) becomes
$a = qd+0$, $a = qd \rightarrow d|a$
similarly we can show that d|b.
now we will prove 'd' is gcd of a and b for this let 'c' be another common divisor of a,b
$\rightarrow c|a$, $c|b$
we know that if a|b and a|c then a| bx+cy for every integers x, y.
so $c|ax+by$; $x,y \in Z$
c|d from eq (1)
$\rightarrow |c| \leq |d|$
Hence 'd' is the gcd of a,b So gcd (a,b) = ax+by.

Assignment : Find gcd also write it as linear combination

(1) ***gcd (49,105)***
$105 = 2\times49+7 \rightarrow$ $105 - 2\times49 = 7$
$49 = 7\times7 +0 \rightarrow$ $49 - 7\times7 = 0$ gcd (49,105) = 7
$7 = 105 - 2\times49 = 1\times105 + (-2)\times49$
Where x = 1 , y = -2 and a=49, b=105

(2) Find gcd and write it as linear combination form (321 , -86)
Take a=321, b=86 we ignore minus sign when find gcd
$321 = 3\times86 + 63 \rightarrow$ $321 - 3\times86 = 63$
$86 = 1\times63 + 23 \rightarrow$ $86 - 1\times63 = 23$
$63 = 2\times23 + 17 \rightarrow$ $63 - 2\times23 = 17$
$23 = 1\times17 + 6 \rightarrow$ $23 - 1\times17 = 6$
$17 = 2\times6 + 5 \rightarrow$ $17 - 2\times6 = 5$
$6 = 1\times5 + 1 \rightarrow$ $6 - 1\times5 = 1$
$5 = 5\times1 + 0 \rightarrow$ $5 - 5\times1 = 0$

$1 = 6-1\times5$
$1 = 6+(-1)\times5$
$1 = 6+(-1)(17-2\times6)$
$1 = 1\times6+(-1)\times17+2\times6$
$1 = -1\times17+3\times6$
$1 = -1\times17+3\times\{23-1\times17\}$
$1 = -1\times17+3\times23-3\times17$
$1 = 3\times23-4\times17$
$1 = 3\times23-4\times\{63-2\times23\}$
$1 = 3\times23-4\times63+8\times23$
$1 = -4\times63+11\times23$
$1 = -4\times63+11\times\{86-1\times63\}$
$1 = -4\times63+11\times86-11\times63$
$1 = 11\times86-15\times63$
$1 = 11\times86-15\times\{321-3\times86\}$
$1 = 11\times86-15\times321+45\times86$
$1 = -15\times321+56\times86$ x = -15 , y = 56

(3) Find gcd (420 , 531)

$531 = 1\times420+111 \rightarrow$ $531-1\times420 = 111$
$420 = 3\times111+87 \rightarrow$ $420-3\times111 = 87$
$111 = 1\times87+24 \rightarrow$ $111-1\times87 = 24$
$87 = 3\times24+15 \rightarrow$ $87-3\times24 = 15$
$24 = 1\times15+9 \rightarrow$ $24-1\times5 = 9$
$15 = 1\times9+6 \rightarrow$ $15-1\times9 = 6$
$9 = 1\times6+3 \rightarrow$ $9-1\times6 = 3$
$6 = 2\times3+0 \rightarrow$ $6-2\times3 = 0$ so
gcd (420 , 531) = 3 Now we write as a linear combination
$3 = 9-1\times6$
$3 = 9+(-1)\times6$
$3 = 9+(-1)\times\{15-1\times9\}$
$3 = 9-1\times15+1\times9$
$3 = -1\times15+2\times9$
$3 = -1\times15+2\times\{24-1\times15\}$
$3 = -1\times15+2\times24-2\times15$
$3 = 2\times24-3\times15$
$3 = 2\times24-3\times\{87-3\times24\}$
$3 = 2\times24-3\times87+9\times24$
$3 = -3\times87+11\times24$
$3 = -3\times87+11\times\{111-1\times87\}$
$3 = -3\times87+11\times111-11\times87$
$3 = 11\times111-14\times87$
$3 = 11\times111-14\times\{420-3\times111\}$
$3 = 11\times111-14\times420+42\times111$
$3 = -14\times420+53\times111$
$3 = -14\times420+53\times\{531-1\times420\}$
$3 = -14\times420+53\times531-53\times420$
$3 = 53\times531+(-67)\times420 \rightarrow x = -67 , y = 53$

Theorem: ***If gcd (a,b) = d then prove that:*** $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Proof :

Since gcd (a,b) = d → d|a , d|b So ∃ for some integer k_1 , k_2 repectivly s.t

$a = k_1 d$ $b = k_2 d$

$\frac{a}{d} = k_1$……..(1) $\frac{b}{d} = k_2$……..(2)

let 'c' be the common divisor of 'k_1' and 'k_2' i.e $c|k_1$ and $c|k_2$ then ∃ some integer r,s s.t

$k_1 = cr$ and $k_2 = cs$ using the values of k_1 and k_2 in eq (1) and (2)

$\frac{a}{d} = cr \rightarrow a = d(cr)$ cr is integer

$\frac{b}{d} = cs \rightarrow b = d(cs)$ cs is integer

→ dc |a and dc |b this shows that dc is common divisor of a,b , but gcd (a,b) = d

so dc|d which is only possible if c = ±1 but 'c' and 'd' both +ve. So c=1

→ $(k_1,k_2) = 1$ From (1) and (2) Hence prove $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Theorem: ***Let 'a' and 'b' integers , not both zero then 'a' and 'b' relatively prime if and only if there exist integers 'x' and 'y' s.t 1 = ax+by.***

Proof :

Since'a' and 'b' are relatively prime so gcd (a,b) = 1Then by using the result,

∃ for some integer 'x' and 'y' s.t 1 = ax+by ∵ gcd(a, b)=d=ax+by for some integers

Conversely ,

Let 1 = ax+by ……(1)

We have to prove that gcd (a,b) = 1.For this we suppose gcd (a,b) = d.We have to prove that d = 1

As gcd (a,b) = d → d|a and d|b

Then d|ax+by ∀ x,y ∈ Z

d|1 from (1) Which is only possible if d = 1 So gcd (a,b) = 1.

Question : ***if a|c and b|c with gcd (a,b) = 1 then ab|c.***

Proof :

Since a|c and b|c then ∃ some integer t, r s.t

c = ta …… (1) and c = sb …… (2)

Since gcd (a,b) =1

ax+by = 1 ……. (3) ∀ x,y ∈ Z × ing eq (3) by 'c'

c = acx + bcy

c = a(sb)x + b(ta)y from (1) and (2)

c = absx + abty

c = ab(sx + ty)……..(4) x,y,t,s are integers. so sx + ty is also integers,

let sx + ty = v ∈ Z put in (4) c = ab.v

→ ab|c

Euclid's Lemma: If a|bc with gcd (a,b) = 1 then a|c.

Proof:

Since a|bc so ∃ integer 'k' s.t bc = ka …….(1)

since gcd (a,b) = 1 so, there exist integers 'x' and 'y' s.t

ax+by = 1 …….. (2) × ing eq (2) by 'c'

acx +bcy = c

acx + aky = c fron eq (1)

c = a(cx+ky) since c,k,x,y ∈ Z so, cx + ky = t ∈ Z

c = at → a|c

Question : If gcd(a,b)=1 then gcd (a-b, a+b)= 1 or 2

Proof:

Let gcd(a-b, a+b)=d. We have to prove d=1 or 2

By the definition of gcd d|a-b and d|a+b

if a|b, a|c then a|a+b or a|b-c

⇨ d|a-b + a+b & d|a-b-a-b

d|2a & d|-2b or d|2b

∴ gcd(a,b)=1 ax+by=1…….(1) for some integers x, y ×ing eq (1) by 2

2ax+2by=2……(2)

As d|2a & d|2b so there exist some integers x, y such that

d|2ax+2by from (2) d|2 so which is true for d=1, or 2

Question : Let a,b and c be integers, then (ca, cb)=c(a, b), for any positive integers c.

Solution:

Let (a,b)=d, then ∃ some integers x,y s.t

ax+by=d..... (1) multiplying it by c

acx+bcy= dc → (ac,bc)=c(a,b)

Theorem : Let a,b an c be integers if (a,b)=1, (a,c)=1, then (a,bc)=1

Solution:

If (a,b)=1, ∃ some integers x, y s.t ax+by=1

If (a,c)=1, ∃ some integers u, v s.t au+cv=1

by=1-ax..... (1) cv=1-av..... (2) multiplying (1) and (2)

by cv = (1-ax)(1-au)

bc(yv)=1-au-ax+a^2xu

=1-a(u+x-axu) as y, v, u, x, a ∈ Z, so, y v = t ϵ Z, u+x – axu = s ∈ Z

bct=1-as → as+bct=1→ (a,bc)=1

Least Common Multiples(L.C.M)

Let a,b be two integers not both are zero. Then an integer m is called Least Common Multiple of a,b if

- a|m, b|m
- If there exist an integer c such that a|c, b|c then m ≤ c or m|c . L.C.M of a,b is denoted by <a, b>=m

Example:Take a= 8, b=12 , m =24, 48,72,96 then <8, 12>=24

Another way to find the greatest common divisor and least common factor of two positive integers is to use the prime factorizations of these integrs,Suppose that the prime factorizations of the positive integrs a and b are

$a = P_1^{a_1} . P_2^{a_2} \dots\dots\dots P_n^{a_n}$, $b = p_1^{b_1} . p_2^{b_2} \dots\dots\dots p_n^{b_n}$ Where each exponent is a non negative integers.Then gcd(a,b) is given by

gcd(a,b)=$P_1^{\min(a_1,b_{1,})} . P_2^{\min(a_2,b_{2,})} \dots\dots\dots P_n^{\min(a_n,b_{n,})}$

their Least Common Multiples is

lcm(a,b)= $P_1^{\max(a_1,b_{1,})} . P_2^{\max(a_2,b_{2,})} \dots\dots\dots P_n^{\max(a_n,b_{n,})}$

Question : Find the gcd and lcm of
$a = 2^3.3^2.11^4.37^3$, $b=2^2.3.5^2.7.11.29.37^4$

Theorem: Let take positive integers 'a' and 'b' then gcd (a,b).lcm (a,b)= ab.

Proof:

Let gcd(a,b)=d, lcm(a,b)=m. Now we have to prove d.m=a.b

Since gcd(a,b)=d then ∃ x,y ϵ Z such that (linear combination) ax+by=d …… (1)

Also d|a & d|b then ∃ r, s Such that

a= rd , b= sd

If m= $\frac{ab}{d}$ using Then m=as, m=br where r, s ϵ Z

⇨ a|m and b|m now we have to prove that m is the least common multiple.

For this supose 'c' is the multiple of a and b. Then a|c, b|c there exist integers k_1, k_2 we have

c= ak_1 , c= bk_2 …….(2)

Also $\frac{c}{m} = \frac{c}{ab/d}$ $\therefore m = \frac{ab}{d}$

$\frac{c}{m} = \frac{dc}{ab} = \frac{c(ax+by)}{ab} = \frac{cax+cby}{ab}$ $\therefore$ $d = ax + by$ from (1)

$\frac{c}{m} = \frac{ac}{ab}x + \frac{cb}{ab}y = \left(\frac{c}{b}\right)x + (\frac{c}{a})y$ where $k_1 = \frac{c}{a}$ and $k_2 = \frac{c}{b}$ from (2)

$\frac{c}{m} = k_2\, x + k_1 y$ $\therefore$ x, y, k_1, k_2 $\in$ Z $xk_2 + k_2y = t$

$\frac{c}{m}$ = t c = mt → m|c → m ≤ c

m = $\frac{ab}{d}$ → $md = ab$

Question : Show that ax+by=m iff gcd(a,b) |m.

Proof:

$\therefore$ ax+by=m……(1)

Let gcd(a,b)=d so d|a & d|b. Then ∃ $k_1 k_2$ such that

$a = k_1 d$, $b = k_2 d$; $k_1 k_2 \in Z$

Put in (1) $k_1dx+k_2dy=m$ → $d(k_1x+k_2y)=m$

m=kd $k_1x+k_2y=k \in Z$

d|m but gcd(a, b)=d so gcd(a, b) |m

conversily

gcd(a, b) |m. Now we have to prove that ax+by=m……..(1)

Let gcd(a, b)=d, then d|m

$ax_o+by_o=d$……(2) where x_o, $y_o \in Z$

Also d|m then there exist integer t s.t m=dt

$atx_o+bty_o=dt$ multi eq (2) by t

m= $a(tx_o)+b(ty_o)$ Take $x_ot=x$, and $y_ot=y$

so m=ax+by proved.

Prime Numbers

- The numbers which are divisible by 1 and itself only is called prime numbers.
- The numbers which are greater than 1 and divisible by 1 and itself is called prime.
  The set of prime is denoted by 'P'. Example : 2,3,5,7,11 …….

Composite numbers:

The number which are not prime and greater than '1'.
OR The number which can be divide by other number .
Example : 4,6,8,9,10,12,15, ……..
Remarks :

- 2 is only even prime .
- 1 is neither even nor odd prime.

Theorem: if 'p' is prime and p|ab where a,b Є Z then either p|a or p|b.

Proof:

Since 'p' is prime and p|ab. We have to prove that p|a or p|b.
If p|a then we have done, and nothing to prove
If 'p' is not divides 'a' and also 'p' is prime so gcd (a,p) = 1
By Euclid's lemma If gcd (a,b) = 1 and a|bc then a|c.
Where gcd (a,p) = 1 and p|ab then p|b → p|b.
Similarly we can show p|a.

Corollary : If 'p' is prime and $p|a_1.a_2……a_n$, then $p|a_k$ for some a_k, Where $1 \le k \le n$.

Proof :

we prove it by M.I ,

Step 1:

If n = 1 then $p|a_1$. So the result is true for n = 1
If n = 2 then $p|a_1a_2 \rightarrow p|a_1$ or $p|a_2$ by above result

Step 2:

Now we suppose that the result is true for n = k
$\rightarrow p|a_1.a_2……a_k$ then $p|a_i$ for some i $(1 \le i \le k)$
Now we will prove for n = k+1
Take $p|a_1.a_2……a_k.a_{k+1} \rightarrow p|\ (a_1.a_2…..a_k)(a_{k+1})$
By using the statement, " if 'p' is prime and p|ab then p|a or p|b "
So $p|a_1.a_2……a_k$ or $p|a_{k+1}$
If $p|a_1.a_2…….a_k$ then by hypothesis $p|a_i$ for some i .
and If $p|a_{k+1}$ then obviously result is true for n=k+1.
Hence the result is true for all n by mathematical induction .

Corollary : If p ,$q_1,q_2,q_3,……..,q_n$ are all primes and $p|q_1.q_2.q_3……q_n$. Then $p = q_k$ for some k, where $1 \le k \le n$.

Proof:

Let p,q_1,q_2,q_3 ……. q_n are prime numbers and
If $p|q_1.q_2.q_3$ ……. q_n we have to show that $p = q_k$ for some k $(1 \le k \le n)$
we know a result,

If p is prime and $p|a_1.a_2.a_3 \ldots\ldots a_n$, then $p|a_k$ for some a_k where $1 \le k \le n$.
Where p is prime so $p > 1$.
Also $p|q_1.q_2.q_3 \ldots\ldots q_n$ then $p|q_k$ for some k ($1 \le k \le n$),
Since q_k is prime which is divisible by 1 or itself .
Where $p|q_k$ and $p \neq 1$ so it force to take $p = q_k$.

Question : If 'p' is a prime s.t $p|a^2 + b^2$ and $p|a$ then $p|b$.

Proof :

Since 'p' is prime,

Where if p|a then $p|a^2$ …….. (2) also $p|a^2 + b^2$

Let a,b,c are integers If a|b , a|c then a|b-c or a|b+c

where $p|a^2 + b^2$, $p|a^2$ then $p|a^2+b^2-a^2$

$\rightarrow p|b^2 \rightarrow p|b$.

Theorem: Every integer n>1 has prime divisors .

Proof : Let n>1 be the integer.

Case 1: If n is prime then 'n' divide itself so it has a prime divisor.

Case 2: If 'n' is not prime then 'n' will be composite . then ∃ integer 'd' s.t d|n. where $1 < d < n$.

Among all such integers 'd' we suppose 'p_1' is the smallest divisor of 'n' {By well ordering principle}

If p_1 is prime then we have a prime divisor. And if 'p_1' is not a prime then p_1 is composite, then there exist integer 'q' s.t $q|p_1$ where $1 < q < p_1 \rightarrow q|p_1$ and $p_1|n$ then q|n. Which is contradiction to the choice of the least element p_1.

Therefore we can write n such as $n = p_1n_1$ where p_1 is prime and $1 < n_1 < n$.

Fundamental theorem of arithematic

Statement : Every +ve integer n > 1 is either a prime or a product of prime and this representation is unique , apart from the order in which the factors occur.

Proof : Let n > 1 be the integer.

Case 1: If n is prime then 'n' divide itself so it has a prime divisor.

Case 2: If 'n' is not prime then 'n' will be composite. Then ∃ integer 'd' s.t d|n. where $1 < d < n$.

among all such integers 'd' we suppose 'p_1' is the smallest divisor of 'n' {By well ordering principle}

If p_1 is prime then we have a prime divisor. And if 'p_1' is not a prime then p_1 is composite, then there exist integer 'q' s.t $q|p_1$ where $1 < q < p_1 \rightarrow q|p_1$ and $p_1|n$ then q|n.

Which is contradiction to the choice of the least element p_1.

Therefore we can write n such as $n = p_1n_1$ where p_1 is prime and $1 < n_1 < n$.

Next if n_1 is prime , then we have our prime representation , in the contrary case , the argument is repeated to produce a second prime p_2 s.t $n_1 = p_2n_2$, where $1 < n_2 < n_1$ i.e $n = p_1p_2n_2$ if n_2 is prime , then we have done otherwise n_2 is composite, write as $n_2 = p_3n_3$, with p_3 is prime and $n = p_1p_2\, p_3n_3$, $1 < n_3 < n_2$ and we obtain a decreasing sequence s.t $n > n_1 > n_2 \ldots\ldots > 1$

Can't continue indefinitely , so that after a finite number of steps n_{k-1} is a prime , call it p_k this leads to the prime factorization $n = p_1.p_2.p_3 \ldots\ldots\ldots\ldots\ldots p_k$.

Uniqueness :

Let us suppose that the integer 'n' can be represented as a product of primes in two ways say,

$n = p_1.p_2.p_3 \ldots\ldots p_r$ …… (1)

$n = q_1.q_2.q_3 \ldots\ldots q_s$ ……..(2) with $r \le s$ compairing (1) and (2)

$p_1.p_2.p_3 \ldots\ldots p_r = q_1.q_2.q_3 \ldots\ldots q_s$ where p_i's and q_j's are all primes ,

written in increasing magnitude so that $p_1 \le p_2 \le p_3 \ldots\ldots\ldots\ldots \le p_r$, $q_1 \le q_2 \le q_3 \ldots\ldots\ldots\ldots q_s$
because $p_1 | q_1.q_2.q_3 \ldots\ldots\ldots q_s$ then $p_1 = q_k$ for some k as $q_k \ge q_1$.But then $p_1 \ge q_1$ ……(3)
similarly if $q_1 | p_1.p_2.p_3 \ldots\ldots\ldots p_r$, then $q_1 = p_m$ for some m as $p_m \ge p_1$ so $q_1 \ge p_1$ …… (4)
combine (3) and (4) $p_1 = q_1$
$p_1.p_2.p_3 \ldots\ldots\ldots p_r = q_1.q_2.q_3 \ldots\ldots\ldots q_s$ we may cancel this common factor and obtain ,
$p_2.p_3 \ldots\ldots\ldots p_r = q_2.q_3 \ldots\ldots\ldots q_s$ now repeat the procedure to get $p_2 = q_2$, then we have
$p_3 \ldots\ldots\ldots p_r = q_3 \ldots\ldots\ldots q_s$ continuing in this way , we have if $r < s$, then $1 = q_{r+1} . q_{r+2} \ldots\ldots\ldots\ldots q_s$
Which is wrong because each $q_i > 1$ hence r = s and $p_1 = q_1$, $p_2 = q_2$, …… , $q_r = p_r$
Hence our proof is complete.

Corollary : Show that every odd prime number is either of the form 4n+1 or 4n-1 (4n+3)

Proof :

Suppose 'm' be an integer. By using division algorithm , there exist unique integers
'n' and 'r' s.t m = nd+r …….(1) where $0 \le r < d$, take d = 4, so r = 0, 1, 2, 3 put in (1),
m= 4n ……..(1) if r = 0
if r = 1,2,3 ,then ,
m = 4n + 1 ……(2)
m = 4n + 2 ……(3)
m = 4n + 3 ……(4)
now 4n can't be prime for any integer n.
4n+2 = 2(2n+1) is prime only for n = 0 , which is even prime ,
hence every odd prime is of the form 4n+1 or 4n+3.

Theorem: Prove that there are infinte many prime numbers.

Proof :

Suppose on contrary that prime numbers are finite. i.e $\{ p_1.p_2.p_3 \ldots\ldots p_n \}$ be the complete list of prime numbers .
Let $N = p_1.p_2.p_3 \ldots\ldots p_n + 1$…… (1)
Case 1: If N is prime then we obtain a prime number greater then all those prime numbers which are in list , which is contradiction .
Case 2 : If N is not a prime then N will be composite. Write 'N' in prime factorization form.
$N = p_1.p_2.p_3 \ldots\ldots p_n$. Let $p_i | p_1.p_2.p_3 \ldots\ldots p_n$ for some i. Let $p_i | N$ …… (2)
Where $p_i > 1 \rightarrow$ prime number.
$\rightarrow p_i | N - p_1.p_2.p_3 \ldots\ldots p_n$ If a|b and a|c then a|b - c
$p_i | p_1.p_2.p_3 \ldots\ldots p_n + 1 - p_1.p_2.p_3 \ldots\ldots p_n \rightarrow p_i | 1$ Which is only possible when $p_i = 1$,
Which is contradiction because to the choice that $p_i > 1$. so our supposition wrong .
Hence , prime numbers are infinite .

Diophantine Equation

Definition:

The simplest type of diophantine equation that we shall consider is the linear Diophantine equation in two unknown is ax + by = c , where a,b,c are constants .

Theorem: ***The linear Diophantine equation ax+by = c admits a solution iff d|c , where d = gcd (a,b).***

Proof :

Since gcd (a,b) = d , i.e d|a , d|b. So there exist integers 'r' and 's' s.t a = dr , b = ds
if a solution of ax+by = c exist. So that $ax_o+by_o = c$ for suitable 'x_o' and 'y_o'.Then $c = ax_o+by_o$
$c = drx_o+dsy_o = d(rx_o+sy_o)$, since r, x_o, s, $y_o \in Z$
then $c = d(rx_o+sy_o)$, $rx_o+sy_o = q \in Z$
c = dq , d|c

Conversely

Suppose that d|c , then ∃ integer 't' s.t c = dt using (given integers 'a' and 'b' no both of which are zero, then there exist integer 'x' and 'y' s.t d = ax+by. So we can find integer x_o and y_o s.t $ax_o+by_o = d$
multiply this eq by 't' , we get $atx_o + bty_o = t$
→ $a(tx_o) + b(ty_o) = c$,
Hence , the Diophantine eq, ax + by = c has a solution $x = tx_o$, $y = ty_o$.

Theorem: The linear Diophantine eq. ax+by = c has a solution iff d|c, Where gcd (a,b) = d if 'x_o' , 'y_o' is any particular solution of this equation , Then all other solutions are given by $x = x_o+(\frac{b}{d})t$, $y = y_o-(\frac{a}{d})t$.

Proof :

Write whole solution of the previous theorem same as it is: [The linear Diophantine equation ax+by = c admits a solution iff d|c , where d = gcd (a,b)]
Then next:
Now, It is given that x_o , y_o is the solution of given equation . suppose x_1,y_1 is any other solution of this equation , then since $ax_o + by_o = c = ax_1 + by_1$
$by_o – by_1 = ax_1 – ax_o$
$b (y_o – y_1) = a (x_1 – x_o)$
$a (x_1 – x_o) = b (y_o- y_1)$ …….. (1)
there exist relatively prime integers 'r' and 's' s.t
a = dr , b = ds , put in (1) d|a, d|b
we get $dr (x_1 – x_o) = ds (y_o – y_1)$
where 'd' is common factor , we get
$r(x_1 – x_o) = s(y_o – y_1)$
→ $r|s(y_o – y_1)$, with gcd (r,s) = 1 By using Euclid lemma ,
$r|y_o – y_1$ or in other words $y_o – y_1 = rt$ for some integers 't' ,we now get
$r(x_1 – x_o) = s(y_o – y_1)$
$r(x_1 – x_o) = srt$ $\rightarrow x_1 – x_o = st$
this leads to the formula $x_1 = x_o + st$, $y_1 = y_o - rt$
$x_1 = x_o + (\frac{b}{d})t$, $y_1 = y_o-(\frac{a}{d})t$

Example: **Consider the linear Diophantine eq. 172x + 20y = 1000**
gcd (172,20) = 4 So the solution of given Diophantine eq will be exist.

$172 = 8\times20+12 \rightarrow \quad 172 - 8\times20 = 12$
$20 = 1\times12+ 8 \rightarrow \quad 20-1\times12 = 8$
$12 = 1\times8 + 4 \rightarrow \quad 12-1\times8 = 4$
$8 = 2\times4 + 0 \rightarrow \quad 8-2\times4 = 0 \quad$ gcd (172 , 20) = 4
$4=12-1\times8$
$4=12-1\times \{20-1\times (12)\}$
$4=12-1\times20+1\times12$
$4=-1\times20+2\times12$
$4=-1\times20+2\times\{172-8\times20\}$
$4=-1\times20+2\times172-16\times20$
$4=2\times172+(-17)\times 20$ x = 2 , y = -17

Which of the following Diophantine eqs can't be solved.

I. 6x + 51y = 20
II. 33x+14y = 115
III. 14x+35y = 93

Solution: ***6x+51y = 22***
$51= 8\times6+3$
$6 = 2\times3+0$
gcd (6,51) = 3
3 can't divided by 22 so its solution does not exist.
other questions do yourself with same method.

Question: (a) 172x + 20y = 1000 , (b) 56x + 72y = 40
Solution: ***(a)***
$172 = 8\times20 + 12 \rightarrow \quad 172 - 8\times20 = 12$
$20 = 1\times12 + 8 \rightarrow \quad 20 - 1\times12 = 8$
$12 = 1\times8 + 4 \rightarrow \quad 12 - 1\times8 = 4$
$8 = 2\times4 + 0 \rightarrow \quad 8 - 2\times4 = 0 \quad$ gcd (172 , 20) = 4 , a=172, b=20, d=4
Also 4|1000 so its solution is possible
$4=12 - 1\times8$
$4=12 - 1\times\{20 - 12\}$
$4=12 - 20 + 12$
$4=-20 + 2\times12$
$4=2\times12 - 20$
$4=2\times\{172 - 8(20)\}-20$
$4=2\times172 - 16\times20 - 20$
$4=2\times172 +(- 17)\times 20 \quad x = 2 , y = -17, a = 172 , b = 20$
$1000 = 250 \times4$ since gcd (12,16) = 4
$= 250\times\{2\times172 - 17\times20\}$
$= 500\times172 - 4250\times20$
So that $x_o = 500$, $y_o = -4250$
Provide one solution to the Diophantine eq's. So all the other possible solutions of Diophantine equation

can be calculate by this formula $x = x_o + (\frac{b}{d})\, t$, $y = y_o - (\frac{a}{d})\, t$

$x = 500 + (\frac{20}{4})\, t$, $y = -4250 - (\frac{172}{4})\, t$

$x = 500 + 5t$, $y = -4250 - 43t$. Now we must have to choose 't' is inequality

$5t + 500 > 0$, $-4250 - 43t > 0$

$5t > -500$, $-4250 > 43t$

$t > -100$…… (1) , $-98.83 > t \rightarrow$ $t < -98.83$ ……(2)

Combine (1) and (2)

$-100 < t < -98.83 \rightarrow$ $t = -99$

$x = 500 + 5t$, $y = -4250 - 43t$

$x = 500 + 5(-99)$, $y = -4250 - 43(-99)$

$x = 500 - 495$, $y = -4250 + 4257$ $x = 5$, $y = 7$

(b) 56x + 72y = 40 (do yourself)

Question: Determine all solution in integers of the following Diophantine eq's:

A. 24x +138y=18

B. 221x + 35y=11

Solution: 24x + 138y = 18

$138 = 5\times24 + 18 \rightarrow$ $138 - 5\times24 = 18$

$24 = 1\times18 + 6 \rightarrow$ $24 - 1\times18 = 6$

$18 = 3\times6 + 0 \rightarrow$ $18 - 3\times6 = 0$ gcd (24 , 138) = 6

$6|18$

$24 - 1\times18 = 6$

$24 - 1\times [138-5(24)] = 6$

$24 - 138 + 5\times24 = 6$

$6\times24 - 1\times138 = 6$

$x = 6$, $y = -1$

$6|18$ so its solution is possible

$18 = 3\times6$

$= 3\times\{6\times24 - 1\times138\}$

$= 18\times24 - 3\times138$ $a = 24$, $b = 138$, $x_o = 18$, $y_o = -3$

Provide one solution to the Diophantine eq's. So all the other possible solutions of Diophantine equation can be calculate by this formula $x = x_o + (\frac{b}{d})\, t$, $y = y_o - (\frac{a}{d})\, t$

$x = 18 + (\frac{138}{6})\, t$, $y = -3 - (\frac{24}{6})\, t$

$x = 18 + 23t$, $y = -3 - 4t$ Now we must to choose 't' inequality .

$18 + 23t > 0$, $-3 - 4t > 0$

$23t > -18$, $-3 > 4t$

$t > -0.7826$ ……. (1) , $-0.75 > t \rightarrow$ $t < -0.75$ …… (2)

Combine (1) and (2)

$-0.7826 < t < -0.75 \rightarrow$ so its other solution is not possible.

B. 221x + 35y = 11 (do yourself)

C. 23x - 49y= 179

Question : Find all solutions in integers of 15x+7y=210..... (1) also determine the number of solutions in positive integers.

Solution :

If we put x=0, then, we get y=30 so x=0, y=30 is one solution of eq (1). Also (15,7)=1, and 1|210 so all the other solutions can be determine by

$x= x_o +\left(\frac{b}{d}\right)t$, $y=y_o-\left(\frac{a}{d}\right)t$ Where $x_o=0$, $y_o=30$ then $x=0+7t$, $y=30-15t$

$x=7t$.....(2) $y=30-15t$..... (3) , where t ranges over the integers

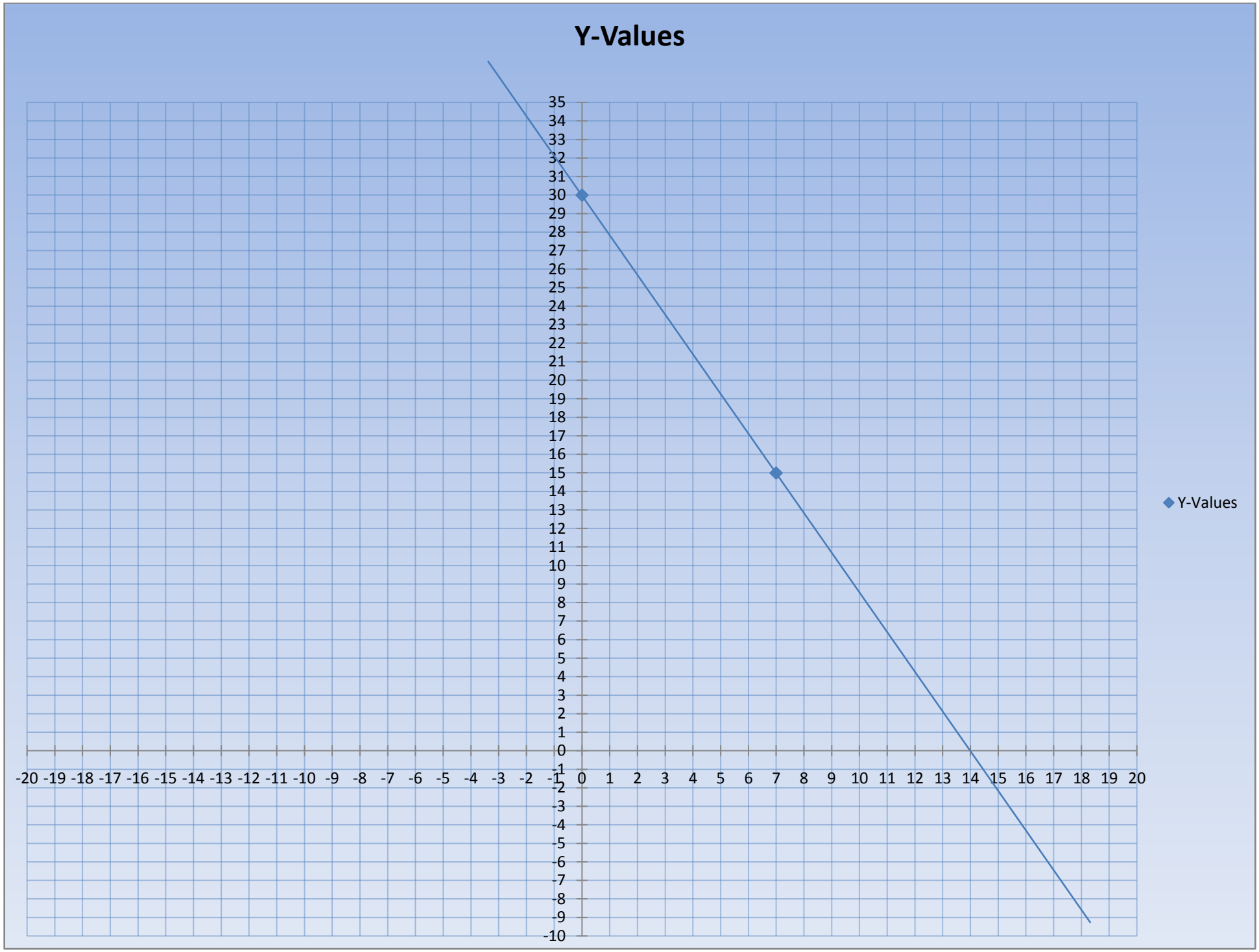
To find the number of solutions in positive integers. Take $x > 0$, $y > 0$ then (2) and (3) becomes

$7t > 0 \rightarrow t > 0$ ..... (4)

$30-15t > 0 \rightarrow 30 > 15t \rightarrow 2 > t$ ..... (5)

Combine (4) and (5) $0 < t < 2$

So $t=1 \rightarrow x = 7, y = 15$ is only one solution in positive integers.


Y-Values
35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0 -1 -2 -3 -4 -5 -6 -7 -8 -9 -10
-20 -19 -18 -17 -16 -15 -14 -13 -12 -11 -10 -9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
Y-Values

Question : Find the solution of 91x+ 221y=1053, are there solutions in positive integrs.

Solution :

As gcd(91,221)=13, So all divides by 13, the given equation is equivalent to 7x+17y=81..... (1)
By inspection, one solution is x=14, y= -1, also (7,17)=1, and 1| 81, so all the other solutions can be determine by $x= x_o +\left(\frac{b}{d}\right)t$, $y=y_o- \left(\frac{a}{d}\right)t$ Where $x_o=14$, $y_o = -1$ then
x=14+17t, y= -1-7t, Where t ranges over the integers.
To find the numbers of solution in positive integers. Take x > 0, y > 0
14+17t > 0 → 17t > -14 → t > -14/17 → t > - 0.82……..(2)
Now -1-7t > 0 → -1 > 7t → t < -1/7 → t < - 0.14……..(3)
- 0.82 < t < - 0.14 combine (2) and (3)
So now integral value exists for t. Hence there are no solutions in positive integers.

Question:Find all solutions in positive integers of 11x+7y=200..... (1)

Solution:

As a=11, b=7 First we will calculate gcd of (11, 7)
11=1 × 7+ 4 → 11-1× 7=4
7=1 × 4 +3 → 7- 1× 4 =3
4=1 × 3 +1 → 4- 1 × 3=1
3=1 × 3 +0
1= 4-1 × 3= 4-1 × [7-1 x 4]
1= 4-1 ×7+1×4 = 2×4 -1×7 = 2× [11-1×7] -1×7
1= 2×11-2×7-1×7 → 1= 2 ×11-3×7 x-ing by 200
200= 400 ×11 – 600×7 where one solution is $x_o=400$, $y_o=600$
also (11,7)=1, and 1|200, so all the other solutions are given by
$x= x_o +\left(\frac{b}{d}\right)t$, $y=y_o- \left(\frac{a}{d}\right)t$ use the values of x_o, and y_o
x=400+7t, y= - 600 -11t, where t ranges over the integers.
To find the number of solutions in positive integers x > 0, y > 0, gives
- 400/7 < t < - 600/11→ - 57.14 < - 54.54
And hence positive solutions occurs only for t= -55,-56,-57, therefore the only positive solutions are (x=15, y= 5), (x=8, y=16) (x=1, y=27)

Question : Do there exist infinitly many positive integer solutions of 10x-7y= -17. Explain.

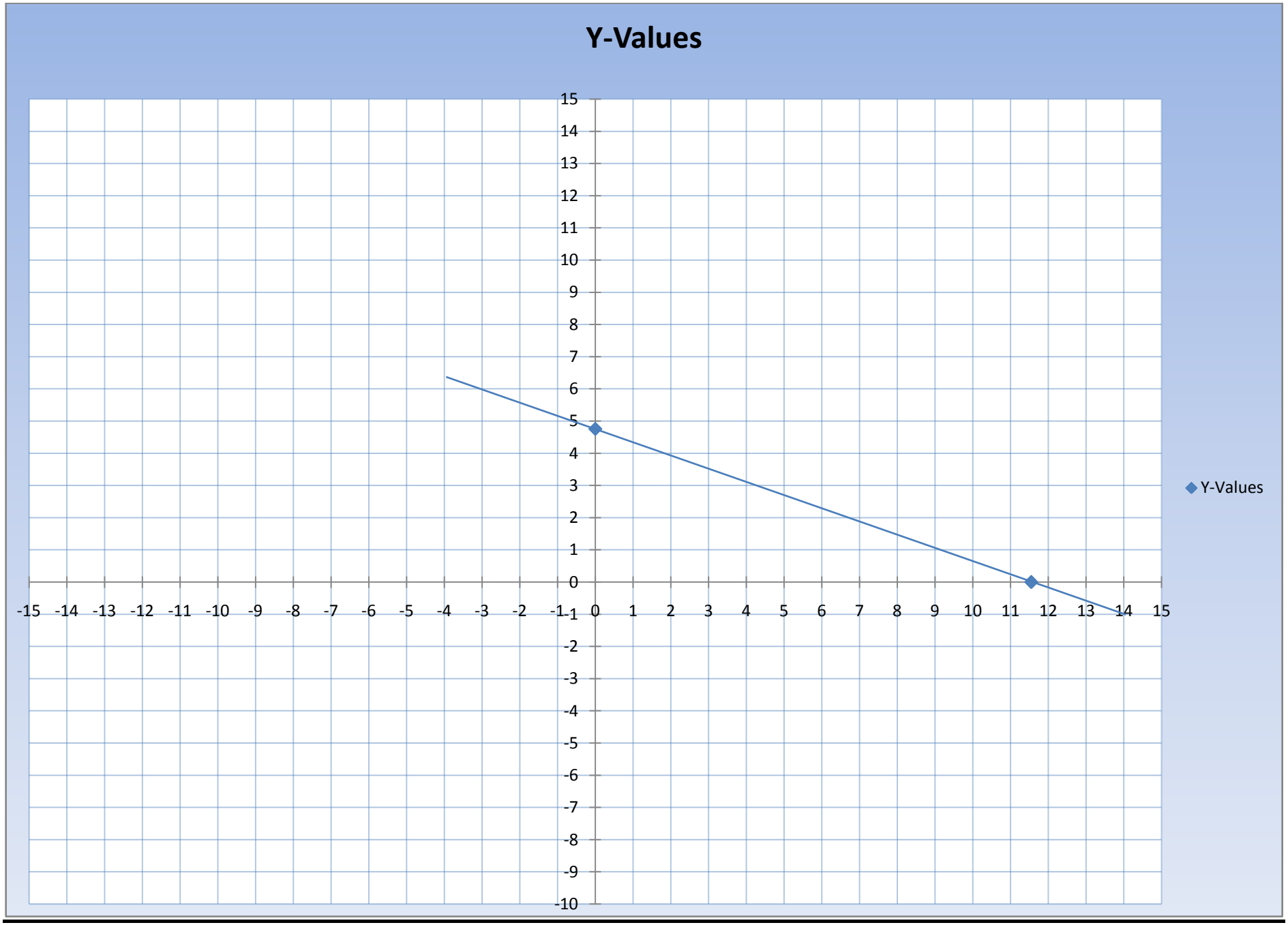
Solution :

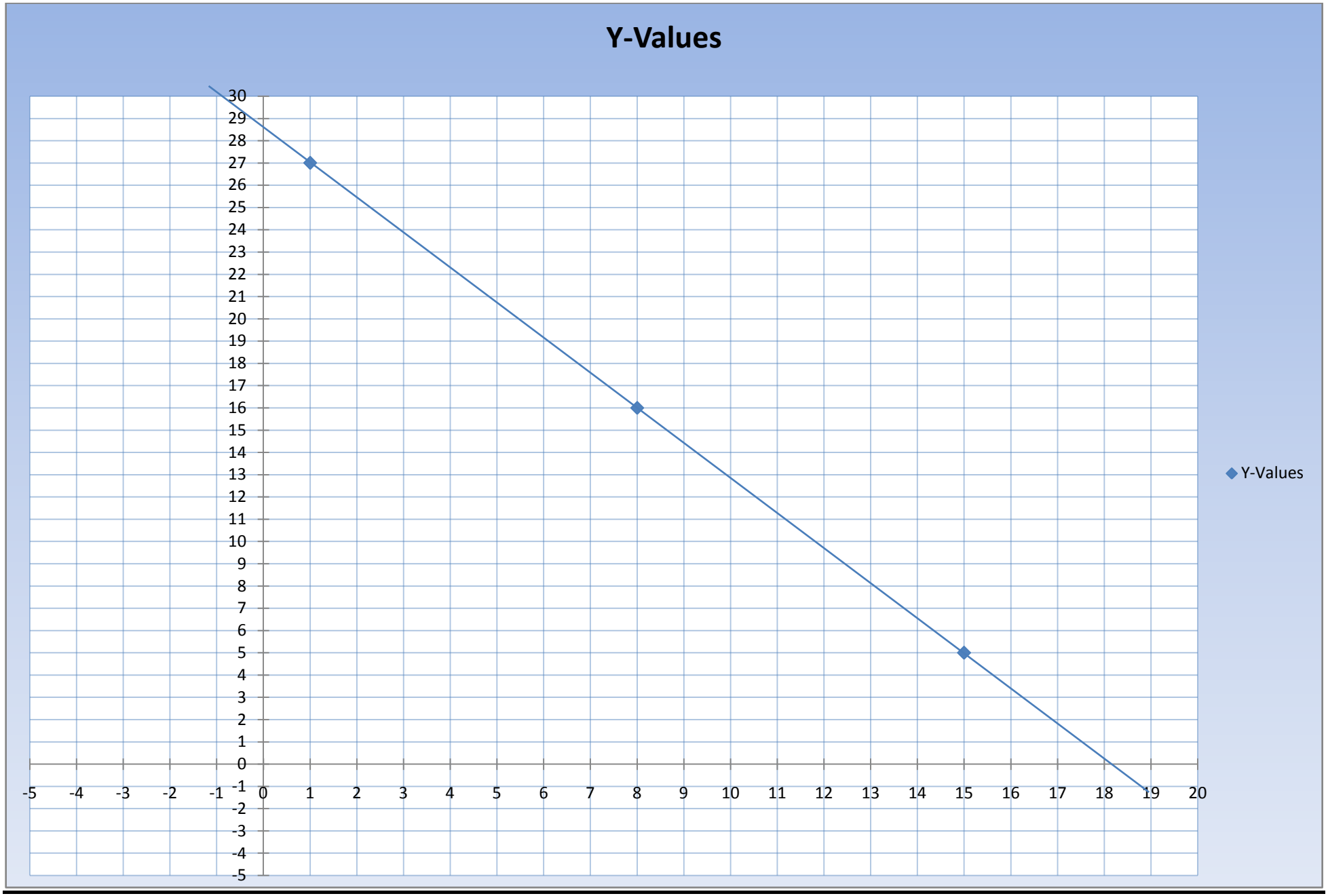
Yes, by inspection 10(-1) -7.1= -17, so x= -1, y =1 is one solution of the equation. Hence all solutions are given by x= -1-7t , y =1-10t, if t < -1/7 , then, x > 0 if t < 1/10, then y > 0, and therefore any integer $t \leq -1$ yes a positive solutions.

Question : Find the smallest positive integer b, s.t the linear diophantine equation 1111x+704y=15000+b has a solution.

Solution :

Since (1111,704)=11, so the solutions exist iff 11 divides 15000+b, the smallest positive value of b is thus 4.


Y-Values
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
-1
-2
-3
-4
-5
-6
-7
-8
-9
-10
-15 -14 -13 -12 -11 -10 -9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Y-Values


Y-Values
30
29
28
27
26
25
24
23
22
21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
-1
-2
-3
-4
-5
-5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
Y-Values

Remainder Theorem

Remainder of $\frac{a\times b\times c}{n}$ [i.e a×b×c when divided by 'n'] is equal to the remainder of expression.

$\frac{a_r\times b_r\times c_r}{n}$ [i.e $a_r\times b_r\times c_r$ when divided by 'n']

Where 'a_r' is remainder when 'a' is divided by 'n'.

Where 'b_r' is remainder when 'b' is divided by 'n'.

Where 'c_r' is remainder when 'c' is divided by 'n'.

Example :Find the remainder of 15×17×19 , when divided by 7.

Solution:

Remainder of $\frac{15\times17\times19}{7}$ will be equal to $\frac{1\times3\times5}{7}=\frac{15}{7}=2\frac{1}{7}=1$

So we obtain remainder '1'.

Example: Find the remainder of* 19×20×21*, when divided by 9.

Solution:

Remainder of $\frac{19\times20\times21}{9}$ will be equal to $\frac{1\times2\times3}{9}=\frac{6}{9}$

So we obtain remainder '6'.

Polynomial Theorem

This is very powerfull theorem to find the remainder according to polynomial theorem,

$(x+a)^n = x^n + c_1{}^n x^{n-1}a + c_2{}^n x^{n-2}a^2 + \ldots\ldots + c_n{}^n x^0 a^n$ ……. (1)

Dividing by 'x'

$\frac{(x+a)^n}{x} = \frac{x^n + c^n{}_1 x^{n-1}a + c^n{}_2 x^{n-2}a^2 + \cdots\ldots + c^n{}_n x^0 a^n}{x}$ …….(2)

Remainder of expression (2) will be equal to remainder of '$\frac{a^n}{x}$' because rest of the term contains 'x' are completely divides by 'x'.

***Example : Find the remainder* $\frac{9^{99}}{8}$.**

Solution:

$\frac{9^{99}}{8}=\frac{(8+1)^{99}}{8}$ According to polynomial theorem will be equal to

$\frac{(1)^{99}}{8}=\frac{1}{8}\rightarrow$ Remainder = 1

***Example : Find the remainder* $\frac{8^{89}}{7}$.**

Solution:

$\frac{8^{89}}{7}=\frac{(7+1)^{89}}{7}$ According to polynomial theorem will be equal to

$\frac{(1)^{89}}{7}=\frac{1}{7}\rightarrow$ Remainder = 1

***Example : Find the remainder of* $\frac{9^{100}}{7}$**

Solution:

$\frac{9^{100}}{7}=\frac{(7+2)^{100}}{7}=\frac{2^{100}}{7}=\frac{2^{99}.2}{7}=\frac{2^{3\times33}.2}{7}=\frac{8^{33}.2}{7}=\frac{(7+1)^{33}.2}{7}=\frac{(1)^{33}.2}{7}=\frac{2}{7}$

Remainder = 2

Example : Find the remainder of $\frac{7^{23}}{8}$

Solution:

$\frac{7^{23}}{8} = \frac{7^{22}.7}{8} = \frac{(7^2)^{11}.7}{8} = \frac{49^{11}.7}{8} = \frac{(48+1)^{11}.7}{8} = \frac{(6\times8+1)^{11}.7}{8} = \frac{(1)^{11}.7}{8} = \frac{7}{8}$

→ Remainder = 7

Congruences

Congruences:

Let n be a positive integer. Two integers a and b are congruent modulo n. If n|a-b. If this is so then we can write a ≡ b (mod n). Such a statement is called a congruence

For example, 19 and 12 are congruent modulo 7; that is, 19 ≡ 12 (mod 7), because 7|19-12

Also, −8 and 10 are congruent modulo 6; that is, −8 ≡ 10 (mod 6).

Example: 8 ≡ 2(mod 3) because 3| 8 – 2

Activity: Checking congruences. Which of the following congruences are true?

(a) 11 ≡ 26 (mod 5) (b) 9 ≡ −9 (mod 5)
(c) 28 ≡ 0 (mod 7) (d) −4 ≡ −18 (mod 7)
(e) −8 ≡ 5 (mod 13) (f) 38 ≡ 0 (mod 13)

Writing a congruence as an equation

The congruence a ≡ b (mod n) is equivalent to the statement that there is an integer k such that a = b + nk.

Properties of congruences:

- a ≡ a (mod n)
- if a ≡ b (mod n) then b ≡ a (mod n)
- if a ≡ b (mod n) and b ≡ c (mod n), then a ≡ c (mod n)

Question : Using congruence find the remainder of " 5^{48} " is divided by "24".

Solution:

$5^1 \equiv 5$ mod(24)
$5^2 \equiv 5^2$ mod(24)
$5^2 \equiv 1$ mod(24)
$5^2 \equiv 1$ mod(24)
$(5^2)^{24} \equiv (1)^{24}$ mod(24)
$5^{48} \equiv (1)$ mod(24)
" 1 " is remainder

Question : Using congruence find the remainder of " 3^{21} " divided by "8".

Solution:

$3 \equiv 3$ mod(8)
$3^2 \equiv 9$ mod(8)

$3^2 \equiv 1 \bmod(8)$
$(3^2)^{10} \equiv (1)^{10} \bmod(8)$
$3^{20} \equiv (1) \bmod(8)$
$3.3^{20} \equiv (3)(1) \bmod(8)$
$3^{21} \equiv 3 \bmod(8)$
So ''3'' is the remainder.

Question : Find the remainder when " 11^{35} " is divided by "13" .

Solution:
$11 \equiv 11 \bmod(13)$
$11 \equiv -2 \bmod(13)$
$11^2 \equiv (-2)^2 \bmod(13)$
$11^2 \equiv 4 \bmod(13)$
$11^4 \equiv 16 \bmod(13)$
$11^4 \equiv 3 \bmod(13)$
$11^8 \equiv 9 \bmod(13)$
$11^{16} \equiv (-4)^2 \bmod(13)$
$11^{16} \equiv 16 \bmod(13)$
$11^{16} \equiv 3 \bmod(13)$
$11^{32} \equiv 9 \bmod(13)$
$11^{32} \equiv -4 \bmod(13)$
$11^{35} = (11)^{32} \times (11)^2 \times (11)^1$
$11^{35} = (-4) \times (4) \times (-2) \bmod(13)$
$11^{35} = 6 \bmod(13)$
So " 6 " is remainder .

Question : Find the remainder when " 3^{287} " is divided by "23" .

Solution:
$3^1 \equiv 3 \bmod(23)$
$3^2 \equiv 9 \bmod(23)$
$3^4 \equiv 81 \bmod(23)$ $\quad 3^4 \equiv 12 \bmod(23)$
$3^8 \equiv 144 \bmod(23)$
$3^8 \equiv 6 \bmod(23)$
$3^{16} \equiv 36 \bmod(23)$
$3^{16} \equiv 13 \bmod(23)$
$3^{16} \equiv 169 \bmod(23)$
$3^{32} \equiv 8 \bmod(23)$
$3^{64} \equiv 64 \bmod(23)$
$3^{64} \equiv 18 \bmod(23)$
$3^{64} \equiv -5 \bmod(23)$
$3^{128} \equiv 25 \bmod(23)$
$3^{128} \equiv 2 \bmod(23)$
$3^{256} \equiv 4 \bmod(23)$
$3^{287} = 3^{256} \times 3^{16} \times 3^8 \times 3^4 \times 3^2 \times 3^1$
$\equiv 4 \times 13 \times 6 \times 12 \times 9 \times 3 \bmod(23)$
$\equiv 6 \times 6 \times 12 \times 9 \times 3 \bmod(23)$
$\equiv 13 \times 12 \times 9 \times 3 \bmod(23)$

$\equiv 18\times9\times3 \mod(23)$
$\equiv 1\times3 \mod(23)$
$\equiv 3 \mod(23)$
Hence "3" is the remainder.

Question : Find the remainder of "2^{340}" when divided by 341.

Solution:
$341 = 11\times31$
$340 = 68\times5$
$2^5 \equiv 32 \mod(11)$
$2^5 \equiv 10 \mod(11)$
$2^5 \equiv -1 \mod(11)$
$(2^5)^{68} \equiv (-1)^{68} \mod(11)$
$2^{340} \equiv 1 \mod(11)$ ……. (1)
$2^5 \equiv 32 \mod(31)$
$2^5 \equiv 1 \mod(31)$
$(2^5)^{68} \equiv (1)^{68} \mod(31)$
$2^{340} \equiv 1 \mod(31)$ …….(2)
$2^{340} \equiv (1)(1) \mod(11\times31)$
$2^{340} \equiv 1 \mod(341)$
Hence "1" is remainder.

Question : Find the remainder,when 17^{17} is divided by 7.
Solution :
$17\equiv 3(\mod7)$, so $17^{17} \equiv 3^{17}(\mod7)$ aslo
$3^2=9\equiv 2 \pmod7$
$(3^2)^4\equiv 2^4 \pmod7$
$3^8\equiv 2 \pmod7$
$(3^8)^2\equiv 4 \mod7)$
$3.3^{16}\equiv 3.4 \pmod7$
$3^{17}\equiv 12 \pmod7$
$3^{17}\equiv 5 \pmod7$
$17^{17}\equiv5 \pmod7$ so 5 is the remainder.

Question : Find the remainder,when 4^{30} is divided by 23.
Solution:
$4^3= 64 \equiv -5 \pmod{23}$
$(4^3)^2\equiv (-5)^2 \pmod{23}$
$4^6\equiv 2 \pmod{23}$
$(4^6)^5\equiv (2)^5 \pmod{23}$
$4^{30}\equiv 9 \pmod{23}$, thus the remainder is 9.

Question : Show that 2^{37}-1 is a multiple of 223.
Solution :
Since $2^8\equiv 33 \pmod{223}$
$(2^8)^2\equiv (33)^2 \pmod{223}$
$2^{16}\equiv -26 \pmod{223}$; thus $2^{32}\equiv (-26)^2 \pmod{223}$
$2^{32}\equiv 7 \pmod{223}$

$2^{37} = 2^{32}.2^5 \equiv 7.32 \equiv 1 \pmod{223}$

Question : Find the least positive residue of
(a) 3^{500} modulo 13, (b) 12! modulo 13 ,
(c) 5^{16} modulo 17, (d) 5^{500} modulo 17.

Solution :

(a) : Since $3^3 \equiv 1 \pmod{13}$, we have
$(3^3)^{166} \equiv (1)^{166} \pmod{13}$, thus
$3^{500} \equiv 3^{498}.3^2 \equiv 1.9 \equiv 9 \pmod{13}$

(b) : $12! = (2.3.4)(5.6)(7.8)(9.10)(11.12) \equiv (-2)(4)(4)(-1)(2) \equiv 12 \pmod{13}$

(c) : $5^2 \equiv 8 \pmod{17}$

$5^4 \equiv 64 \equiv (-4) \pmod{17}$
$5^8 \equiv 16 \pmod{17}$
$5^8 \equiv -1 \pmod{17}$
$5^{16} \equiv 1 \pmod{17}$

(d) : $5^8 \equiv 1 \pmod{17}$ from c part
$(5^8)^2 \equiv 1 \pmod{17}$
$5^{16} \equiv 1 \pmod{17}$
$5^{496} = (5^{16})^{31} \equiv (1)^{31} \pmod{17}$
Hence $5^{500} = 5^{496}.5^4 \equiv 1.5^4 \equiv 13 \pmod{17}$

Question : Show that $2^{48}-1$ is divisible by 97.

Solution:

$2^8 \equiv 62 \equiv -35 \pmod{97}$
$2^{16} \equiv (-35)^2 \equiv 61 \equiv -36 \pmod{97}$
$2^{32} \equiv (-36)^2 \equiv 35 \pmod{97}$
$2^{48} = 2^{32}.2^{16} \equiv 35(-36) = -1260 \equiv -96 \equiv 1 \pmod{97}$
Therefore 97 divides $2^{48}-1$.

Question : Show that 47 divides $5^{23}+1$.

Solution:

$5^4 \equiv 14 \pmod{47}$
$5^8 \equiv 8 \pmod{47}$
$5^{16} \equiv 17 \pmod{47}$
$5^{24} = 5^{16}.5^8 \equiv 17.\ 8 \equiv -5 \pmod{47}$
So 47 divides $5^{24}+5$.
$5^{24}+5 = 5\,(5^{23}+1)$ $47 \mid 5(5^{23}+1)$ and $(5, 47)=1$
We conclude that 47 divides $5^{23}+1$.

Residue class

Given any integer a, the collection of all integers congruent to a modulo n is known as the residue class, or congruence class, of a modulo n.

Multiplicative inverses modulo n

A multiplicative inverse of a modulo n is an integer v such that $av \equiv 1 \pmod{n}$.

Existence of multiplicative inverses modulo n

• If the integers a and n are coprime, then there is a multiplicative inverse of a modulo n.
• If a and n are not coprime, then there is not a multiplicative inverse of a modulo n.

Example: Finding multiplicative inverses modulo n

For each of the following values of a and n, determine whether a multiplicative inverse of a modulo n exists and, if it does, find one.

(a) a = 5, n = 13 (b) a = 30, n = 73

Solution:

(a) To determine whether there is a multiplicative inverse, check whether 5 and 13 are coprime. They must be coprime, as they are both prime numbers.The integers 5 and 13 are coprime, so there is a multiplicative inverse of 5 modulo 13. Since $n \leq 13$, try the values 1, 2, 3, . . . one by one until you find the multiplicative inverse modulo 13. You needn't necessarily check the integer 1, as clearly $5 \times 1 \not\equiv 1 \pmod{13}$.

$5 \times 1 \equiv 5 \pmod{13}$ $5 \times 2 \equiv 10 \pmod{13}$
$5 \times 3 \equiv 15 \equiv 2 \pmod{13}$ $5 \times 4 \equiv 20 \equiv 7 \pmod{13}$
$5 \times 5 \equiv 25 \equiv 12 \pmod{13}$ $5 \times 6 \equiv 30 \equiv 4 \pmod{13}$
$5 \times 7 \equiv 35 \equiv 9 \pmod{13}$ $5 \times 8 \equiv 40 \equiv 1 \pmod{13}$

Stop, as you have found an integer v such that $5v \equiv 1 \pmod{13}$. So 8 is a multiplicative inverse of 5 modulo 13. You may have noticed a short cut that saves some calculations. You saw that
$5 \times 5 \equiv 12 \equiv -1 \pmod{13}$, so
$(-5) \times 5 \equiv -12 \equiv 1 \pmod{13}$. Since $-5 \equiv 8 \pmod{13}$, it follows that a multiplicative inverse of 5 modulo 13 is 8.

(b) To determine whether there is a multiplicative inverse, check whether 30 and 73 are coprime. The numbers are quite large so use Euclid's algorithm to find the highest common factor.
Euclid's algorithm gives
$73 = 2 \times 30 + 13$
$30 = 2 \times 13 + 4$
$13 = 3 \times 4 + 1$
$4 = 4 \times 1 + 0$.
As gcd(30, 73)=1, so there is a multiplicative inverse of 30 modulo 73.
Rearrange all but the last equation and then apply backwards substitution to find integers v and w with $30v + 73w = 1$. The integer v will be a multiplicative inverse of 30 modulo 73 since $30v = 1 - 73w$.
Rearranging the equations gives
$13 = 73 - 2 \times 30$
$4 = 30 - 2 \times 13$
$1 = 13 - 3 \times 4$.
Backwards substitution gives
$1 = 13 - 3 \times \{30 - 2 \times 13\}$
$= 7 \times 13 - 3 \times 30$
$= 7 \times \{73 - 2 \times 30\} - 3 \times 30$
$= 7 \times 73 - 17 \times 30$. (Check: $7 \times 73 - 17 \times 30 = 511 - 510 = 1$.)
Write the equation $7 \times 73 - 17 \times 30 = 1$ as a congruence modulo 73 to give the multiplicative inverse.
Since $(-17) \times 30 = 1 - 7 \times 73$, we obtain
$(-17) \times 30 \equiv 1 \pmod{73}$.
So -17 is a multiplicative inverse of 30 modulo 73.

find a multiplicative inverse that is a least residue modulo 73.
Since $-17 \equiv 56 \pmod{73}$,
56 is also a multiplicative inverse of 30 modulo 73.

Linear congruences:

A linear congruence is a congruence of the form $ax \equiv b \pmod{n}$,
where a and b are known, and x is unknown.

Solving the linear congruence $ax \equiv b \pmod{n}$
Let d be the highest common factor of a and n.

- If d = 1, then the linear congruence has solutions. The solutions are given by $x \equiv vb \pmod{n}$, where v is any multiplicative inverse of a modulo n.
- If b is not divisible by d, then the linear congruence has no solutions.
- If b is divisible by d, then the linear congruence has solutions and the solutions are given by the solutions of the equivalent linear congruence $\frac{a}{d}x \equiv \frac{b}{d} (mod\ \frac{n}{d})$.

Example: Solving a linear congruence when a and n are coprime and n ≤ 13
Solve the linear congruence $11x \equiv 7 \pmod{8}$.

Solution:

Simplify the linear congruence by replacing 11 with the least residue of 11 modulo 8.
Since $11 \equiv 3 \pmod{8}$, an equivalent linear congruence is $3x \equiv 7 \pmod{8}$.
Check that this linear congruence has solutions.
As 3 and 8 are coprime, this linear congruence has solutions.
Try the values 1, 2, 3, . . . one by one until you find a solution.
Trying the values 1, 2, 3, . . . one by one, we find that
$3 \times 1 \equiv 3 \pmod{8}$ $3 \times 2 \equiv 6 \pmod{8}$
$3 \times 3 \equiv 9 \equiv 1 \pmod{8}$ $3 \times 4 \equiv 12 \equiv 4 \pmod{8}$
$3 \times 5 \equiv 15 \equiv 7 \pmod{8}$.
So the solutions are given by
$x \equiv 5 \pmod{8}$.

Activity: Solving linear congruences when a and n are coprime and n ≤ 13
Solve the following linear congruences.
(a) $2x \equiv 5 \pmod{7}$ (b) $7x \equiv 8 \pmod{10}$ (c) $15x \equiv -13 \pmod{11}$

Example: **Solving a linear congruence when a and n are coprime and n > 13**
Solve the linear congruence $7x \equiv 13 \pmod{24}$.

Solution:

Check that the linear congruence has solutions. As 7 and 24 are coprime, the linear congruence has solutions. Since 24 is a large integer, use a multiplicative inverse of 7 modulo 24 to find the solutions. The solutions are given by
$x \equiv 13v \pmod{24}$,
where v is a multiplicative inverse of 7 modulo 24.
Use Euclid's algorithm and backwards substitution to find v.
Euclid's algorithm gives
$24 = 3 \times 7 + 3$
$7 = 2 \times 3 + 1$.

Backwards substitution gives
$1 = 7 - 2 \times 3$
$= 7 - 2\times(24 - 3 \times 7)$
$= 7 \times 7 - 2 \times 24$. So $7 \times 7 \equiv 1 \pmod{24}$,
and hence 7 is a multiplicative inverse of 7 modulo 24. So the solutions are given by
$x \equiv 13 \times 7 \equiv 91 \equiv 19 \pmod{24}$.
Remember to check your answer. That is, check that if
$x \equiv 19 \pmod{24}$ then $7x \equiv 13 \pmod{24}$. To do this, it helps to use the congruence $19 \equiv -5 \pmod{24}$.
(Check: $7 \times 19 \equiv 7 \times (-5) \equiv -35 \equiv 13 \pmod{24}$.)

Showing that some linear congruences have no solutions
Show that the following linear congruences have no solutions.
(a) $4x \equiv 5 \pmod{10}$ (b) $-12x \equiv 8 \pmod{42}$
(c) $48x \equiv 70 \pmod{111}$

Example: Solving a linear congruence when a and n are not coprime. Solve the linear congruence $12x \equiv 16 \pmod{20}$.
Solution:
Check that the linear congruence has solutions.
The highest common factor of 12 and 20 is 4. Since 16 is divisible by 4, the linear congruence has solutions.
Divide each of the integers 12, 16 and 20 in the linear congruence $12x \equiv 16 \pmod{20}$ by 4 to obtain an equivalent linear congruence.
and is equivalent to
$3x \equiv 4 \pmod{5}$.
Since the numbers involved are small, try the values 1, 2, 3, . . .
one by one until you find a solution.
Trying the values 1, 2, 3, . . . one by one, we find that
$3 \times 1 \equiv 3 \pmod{5}$ $3 \times 2 \equiv 6 \equiv 1 \pmod{5}$
$3 \times 3 \equiv 9 \equiv 4 \pmod{5}$.
So the solutions are given by
$x \equiv 3 \pmod{5}$.

Theorem: The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$, where $d=\gcd(a,n)$. If $d|b$, then it has d mutually incongruent solutions modulo n.
Proof.
We already have observed that the given congruence is equivalent to the linear Diophantine equation ax-ny=b. It is known that the latter equation can be solved if and only if d|b; moreover, if it is solvable and x_o, y_o is one specific solution, then any other solution has the form

$$x = x_\circ + \left(\frac{n}{d}\right)t \qquad y = y_\circ + \left(\frac{a}{d}\right)t. \qquad \text{for some choice of t.}$$

Among the various integers satisfying the first of these formulas, consider those that occur when t takes on the succesive values t= 0,1,2, ..., d-1:

$$x_\circ,\ x_\circ + \frac{n}{d}, x_\circ + \frac{2n}{d} \ldots\ldots\ x_\circ + \frac{(d-1)n}{d}$$

We claim that these integers are incongruent modulo n, and all other such intgers x are congruent to some one of them. If it happend that

$$x_\circ + \frac{n}{d}t_1 \equiv x_\circ + \frac{n}{d}t_2 \ (mod\ n)$$

Where $0 \le t_1 < t_2 \le d-1$, then we would have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \ (mod\ n)$$

Now gcd(n/d,n)= n/d, and therefore the factor n/d could be canceled to arrive at the congruence

$$t_1 \equiv t_2 \ (mod\ d)$$

Which is to say that $d|t_2-t_1$. But this is impossible in view of the inequality $0 < t_2 - t_1 < d$.

It remains to argue that any other solution $x_\circ + (n/d)t$ is congruent modulo n to one of the d integes listed above. The Division Algorithm permits us to write t as t = qd + r, where $0 \le r \le d-1$. Hence

$$\begin{aligned} x_\circ + \frac{n}{d}t &= x_\circ + \frac{n}{d}(qd + r) \\ &= x_\circ + nq + \frac{n}{d}r \\ &\equiv x_\circ + \frac{n}{d}r \ (mod\ n) \end{aligned}$$

With $x_\circ + (n/d)r$ being one of our d selected solutions. This ends the proof.

The argument that we gave in above theorem brings out a point worth station explicity: if $x_\circ$ is any solution of ax ≡ b(mod n), then the d = gcd(a, n) incongruent solutions are given by

$$x_\circ, x_\circ + \frac{n}{d}, x_\circ + 2(\frac{n}{d}) \ldots\ldots\ x_\circ + (d-1)(\frac{n}{d})$$

Corollary: If gcd(a,n)=1,then the linear congruence ax ≡ b(mod n) has a unique solution modulo n.

Given relatively prime intgers a and n, the congruence ax≡b(mod n) has a unique solution. This solution is sometimes called the (multiplicative) inverse of a modulo n.

Example: Consider the linear congruence 18x ≡30(mod 42).

Solution:

Because gcd(18, 42) = 6 and 6 surely divides 30, above theorem guarantees the existence of exactly six solution, which are incongruent modulo 42. By inspection one solution is found to be x = 4. Our analysis tells us that six solutions are as follows:

$$x \equiv 4 + \left(\frac{42}{6}\right)t \equiv 4 + 7t(\text{mod } 2) \quad t=0, 1,.....5$$

Or x ≡ 4, 11, 18, 25, 32, 39 (mod42)

Example : Solve the the linear congruence 9x ≡21 (mod 30).

Solution :

Because gcd(9,30)= 3 and 3|21, we know that there must be three incongruent solutions.One way to find these solutions is to divide the given congruence through by 3, threby replacing it by the equivalent congruence 3x ≡ 7 (mod 10). The relative primeness of 3 and 10 implies that the latter congruence admits a unique solution modulo 10. Although it is not the most efficient method, we could test the integers 0,1,2, ..., 9 in turn untill these solution is obtained. A better way is this: multiply both sides of the congruence 3x ≡ 7 (mod 10) by 7 to get

$$21x \equiv 49 \ (\text{mod } 10)$$

Which reduces to x ≡ 9 (mod 10). (This simplification is no accident, for the multiples 0 . 3, 1 . 3, 2 . 3, ... , 9 . 3 form a complete set of residues modulo 10; hence, one of them is necessarily congruent to 1 modulo 10.) but the original congruence was given modulo 30, so that its incongruent solutions are sought among the integers 0, 1, 2, ... , 29. Taking t = 0, 1, 2 in the formula

$$x = 9 + 10\,t$$

We obtain 9, 19, 29, whence

$$x \equiv 9 \ (\text{mod } 30) \qquad x \equiv 19 \ (\text{mod } 30) \quad x \equiv 29 \ (\text{mod } 30)$$

Are the required three solutions of 9x ≡ 21 (mod 30).

2nd Method

A different approach to the problem is to use the method that is suggested in the proof of above theorem. Because the congruence 9x ≡ 21 (mod 30) is equivalent to the linear Diophantine equation

$$9x - 30y = 21$$

We begin by expressing 3=gcd(9,30) as a linear combinationof 9 and 30. It is found, either by inspection or by using the Euclidean Algorithm, that 3= 9(-3) + 30 . 1, so that

$$21 = 7 .3 = 9(-21) - 30\,(-7)$$

Thus x= - 21, y = -7 satisfy the Diophantine and, in consequence, all solutions of the congruence in question are to be found from the formula

$$x = -21 + \left(\frac{30}{3}\right)t = -21 + 10t$$

The integers x= -21 + 10t, where t = 0,1, 2, are incongruent modulo 30 (but all are congruent modulo 10); thus, we end up with the incongruent solutions

$$x \equiv -21 \pmod{30} \qquad x \equiv -11 \pmod{30} \quad x \equiv -1 \pmod{30}$$

Or, if one prefers positive numbers, x ≡ 9, 19, 29 (mod 30).

Chinese Remainder Theorem

Let $n_1, n_2, \ldots\ldots, n_r$ be positive integers such that gcd(n_i, n_j) = 1 for $i \neq j$. Then the system of linear congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{r}$$

has a simultaneous solution, which is unique modulo the integer $n_1\ n_2, \ldots\ldots, n_r$.

Proof. We start by forming the product $n = n_1\, n_2, \ldots\ldots, n_r$. For each k =1, 2, ... , r, let

$$N_k = \frac{n}{n_k} = n_1. \ldots n_{k-1} n_{k+1} \ldots . n_r$$

In other words, N_k is the product of all the integers n_i with the factor n_k omitted. By hypothesis, the n_i are relatively prime in pairs, so that $gcd(N_k\,,\ n_k) = 1$. According to the theory of single linear congruence. It is therefore possible to solve the congruence $N_k x \equiv 1\ (mod\ n_k)$; call the unique solution x_k . our aim is to prove that the integer

$$\tilde{x} = a_1 N_1 x_1 + \ldots\ldots a_r N_r x_r$$

is a simultaneous solution of a given system.

First observe that $N_i \equiv 0\ (mod\ n_k\ )$ for $i \neq k$, because $n_k | N_i$ in this case. The result is

$$\tilde{x} = a_1 N_1 x_1 + \ldots\ldots a_r N_r x_r \equiv a_k N_k x_k\ (mod\ n_k)$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1(mod\ n_k)$, which forces

$$\tilde{x} \equiv a_k .1 \equiv a_k\ (mod\ n_k\ )$$

This shows that a solution to the given system of congruence exists.

As for the uniqueness assertion, suppose that x' is any other integer that satisfies these congruences. Then

$$\tilde{x} \equiv a_k \equiv x'(mod\ n_k\ ) \quad k = 1, 2, \ldots\ldots r$$

And so $n_k | \tilde{x} - x'$ for each value of k. Because $gcd(n_i\,,\ n_j) = 1$,

Now we have $n_1 n_2 \ldots\ldots n_r | \tilde{x} - x'$; hence $\tilde{x} \equiv x'(mod\ n\ )$. with this, the chinese remainder theorem is proven.

Example: The problem posed by Sun-Tsu corresponds to the system of three congruences

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

In the notation of above theorem , we have n= 3 . 5 . 7 = 105 and

$$N_1 = \frac{n}{3} = 35 \qquad N_2 = \frac{n}{5} = 21 \qquad N_3 = \frac{n}{7} = 15$$

Now the linear congruences

$$35x \equiv 1 \pmod 3 \qquad 21\,x \equiv 1 \pmod 5 \qquad 15\,x \equiv 1 \pmod 7$$

are satisfied by $x_1 = 2,\ x_2 = 1, x_3 = 1$, respectively. Thus a solution of the system is given by

$$x = 2\,.\,35\,.\,2 + 3\,.\,21\,.1 + 2\,.\,15\,.1 = 233$$

Modulo 105, we get the unique solution $x = 233 \equiv 23$ (mod 105).

References:

i. Burton, D.M. Elementary Number Theory Mcgraw Hill, 2000.

ii. Adler,Andrew, Coury,John E. The Theory of Number, Jones and Barttlet publishers, Boston, 1995.

The End

Prof: Asghar Ali
Al-Farooq Academy Din Colony Pattoki.
Cell:0345-6350976
0332-4080492