NUMBER THEORY

Q:1:-Given integers a and b, not both of which are zero, there exist integers

x and y such that gcd(a, b)= ax+ by

Proof. Consider the setS of all positive linear combinations of a and b:

S = {au+ bv I au+ bv> 0; u, v integers}

Notice first that Sis not empty. For example, if a =f:. 0, then the integer I a I = au + b · 0 lies inS, where we choose u = 1 or u = -1 according as a is positive or negative. By virtue of the Well-Ordering Principle, S must contain a smallest element d. Thus, from the very definition of S, there exist integers x andy for which d =ax+ by. We claim that d = gcd(a, b).

Taking stock of the Division Algorithm, we can obtain integers q and r such that

a= qd + r, where 0 ::S r <d. Then r can be written in the form

r =a - qd =a - q(ax +by)

= a(l - qx) + b(-qy)

If r were positive, then this representation would imply that r is a member of S, contradicting the fact that d is the least integer in S (recall that r < d). Therefore, r = 0, and so a = qd, or equivalently dIa. By similar reasoning, d I b, the effect of which is to make d a common divisor of a and b.

Q:2:- a and b are given integers, not both zero, then the set

T = {ax+ by I x, yare integers} is precisely the set of all multiples of d = gcd(a, b).

Proof. Because d I a and d I b, we know that d I (ax + by) for all integers x, y. Thus, every member ofT is a multiple of d. Conversely, d may be written as d = axo + byofor suitable integers x0 and y0 , so that any multiple nd of dis of the form

nd = n(axo + byo) = a(nxo) + b(nyo)

Hence, nd is a linear combination of a and b, and, by definition, lies in T.

Q:3:-Let us see how the Euclidean Algorithm works in a concrete case

by calculating, say, gcd(12378, 3054).

The appropriate applications of the Division Algorithm produce the equations

12378 = 4. 3054 + 162

3054 = 18 . 162 + 138

162 = 1 . 138 + 24

138 = 5. 24 + 18

24 = 1. 18 + 6

18 = 3. 6+0

Our previous discussion tells us that the last nonzero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

6 = gcd(12378, 3054)

To represent 6 as a linear combination of the integers 12378 and 3054, we start with the next-to-last of the displayed equations and successively eliminate the remainders 18, 24, 138, and 162:

Thus, we have

6 = 24-18

= 24- (138- 5 . 24)

= 6. 24- 138

= 6(162- 138)- 138

= 6 . 162 - 7 . 138

= 6. 162- 7(3054- 18. 162)

= 132. 162- 7. 3054

= 132(12378 - 4. 3054)- 7. 3054

= 132 . 12378 + (-535)3054

6 = gcd(12378, 3054) = 12378x + 3054y

where x = 132 andy = -535. Note that this is not the only way to express the integer 6 as a linear combination of 12378 and 3054; among other possibilities, we could add and subtract 3054 · 12378 to get 6 = (132 + 3054)12378 + (-535- 12378)3054

Q:4:-Consider the linear Diophantine equation

172x + 20y = 1000

Applying the Euclidean's Algorithm to the evaluation of gcd(172, 20),

We find that

172 = 8. 20 + 12

20 = 1. 12 + 8

12 = 1. 8 + 4

8 =2·4

whencegcd(172 , 20) = 4. Because 411000, a solution to this equation exists. To obtain the integer 4 as a linear combination of 172 and 20, we work backward through the previous calculations, as follows:

$4 = 12-8$

$= 12 - (20 - 12)$

$= 2 \cdot 12- 20$

$= 2(172 - 8 . 20) - 20$

$= 2. 172 + (-17)20$

Upon multiplying this relation by 250, we arrive at

$1000 = 250 . 4 = 250[2 . 172 + (-17)20]$

$= 500 . 172 + (-4250)20$

so that $x = 500$ and $y = -4250$ provide one solution to the Diophantine equation in question. All other solutions are expressed by

$X = 500 + (20/4)t = 500 + 5t$

$y = -4250- (172/4)t = -4250- 43t$

for some integer t.

A little further effort produces the solutions in the positive integers, if any happen to exist. For this, t must be chosen to satisfy simultaneously the inequalities

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

or, what amounts to the same thing,

$36 -98- > t > -100$

43

Because t must be an integer, we are forced to conclude that $t = -99$. Thus, our Diophantine equation has a unique positive solution $x = 5$, $y = 7$ corresponding to the value $t = -99$.

Q:5:-A customer bought a dozen pieces of fruit, apples and oranges, for $1.32. If an apple costs 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

To set up this problem as a Diophantine equation, let x be the number of apples and y be the number of oranges purchased; in addition, let z represent the cost (in cents) of an orange. Then the conditions of the problem lead to

$(z + 3)x + zy = 132$

or equivalently

$3x + (x + y)z = 132$

Because $x + y = 12$, the previous equation may be replaced by

$3x + 12z = 132$

which, in tum, simplifies to $x + 4z = 44$.

Stripped of inessentials, the object is to find integers x and z satisfying the

Diophantine equation

$x + 4z = 44$ (1)

Inasmuch as gcd (1, 4) = 1 is a divisor of 44, there is a solution to this equation. Upon

multiplying the relation $1 = 1(-3) + 4 \cdot 1$ by 44 to get

$44 = 1(-132) + 4. 44$

it follows that $x_0 = -132$, $z_0 = 44$ serves as one solution. All other solutions of

Eq. (1) are of the form

$X= -132 +4t$ $z=44-t$

wheret is an integer.

Not all of the choices fort furnish solutions to the original problem. Only values

oft that ensure 12 :::: x > 6 should be considered. This requires obtaining those values

of t such that

12 :::: -132 + 4t > 6

Now, 12:::: -132 + 4t implies that t ::S 36, whereas -132 + 4t > 6 gives t > 34!.

The only integral values oft to satisfy both inequalities are t = 35 and t = 36. Thus,

there are two possible purchases: a dozen apples costing 11 cents apiece (the case

where t = 36), or 8 apples at 12 cents each and 4 oranges at 9 cents each (the case

where t = 35).

Q:6:-The number $\sqrt{2}$ is irrational.

Proof. Suppose, to the contrary, that $\sqrt{2}$ is a rational number, say, $\sqrt{2}$ = ajb, where a

and bare both integers with gcd(a, b)= 1. Squaring, we get a 2 = 2b2 , so that b I a 2 .

If b > 1, then the Fundamental Theorem of Arithmetic guarantees the existence of a

prime p such that pI b. It follows that pI a 2 and, by Theorem 3.1, that pI a; hence,

gcd(a, b) :::: p. We therefore arrive at a contradiction, unless b = 1. But if this happens, then a 2 = 2, which is impossible (we assume that the reader is willing to grant that

no integer can be multiplied by itself to give 2). Our supposition that $\sqrt{2}$ is a rational

number is untenable, and so $\sqrt{2}$ must be irrational.

There is an interesting variation on the proof of Theorem 3.3. If .../2 = ajb with

gcd(a, b) = 1, there must exist integers rands satisfying ar + bs = 1. As a result,

$\sqrt{2}=\sqrt{2}(ar+bs)=(\sqrt{2}a)r+(\sqrt{2}b)s=2br+as$

This representation of $\sqrt{2}$ leads us to conclude that $\sqrt{2}$ is an integer, an obvious

impossibility.

Q:7:-If all the n > 2 terms of the arithmetic progression

p, p + d, p + 2d, ... , p + (n- l)d

are prime numbers, then the common differenced is divisible by every prime q < n.

Proof. Consider a prime number q < n and assume to the contrary that q l d. We

claim that the first q terms of the progression

p, p + d, p + 2d, ... ' p + (q- l)d (1)

will leave different remainders when divided by q. Otherwise there exist integers j and k, with 0 ~ j < k ~ q - 1, such that the numbers p + jd and p + kd yield the same remainder upon division by q. Then q divides their difference (k- j)d. But gcd(q , d) = 1, and so Euclid's lemma leads to q I k - j, which is nonsense in light of

the inequality k - j ~ q - 1.

Because the q different remainders produced from Eq. (1) are drawn from the q integers 0, 1, ... , q-1, one of these remainders must be zero. This means that q I p + td for some t satisfying 0 ~ t ~ q- 1. Because of the inequality q < n ~ p ~ p + td, we are forced to conclude that p + td is composite. (If p were less than n, one of the terms of the progression would be p + pd = p(l +d).) With this contradiction, the proof that q I d is complete.

Q:8:-For arbitrary integers a and b, a= b (mod n) if and only if a and b leave the same nonnegative remainder when divided by n.

Proof. First take a = b (mod n), so that a = b + kn for some integer k. Upon division

by n, b leaves a certain remainder r; that is, b = qn + r, where 0 ::": r < n. Therefore,

a= b + kn = (qn + r) + kn = (q + k)n + r

which indicates that a has the same remainder as b.

On the other hand, suppose we can write a = q1 n + r and b = q2n + r, with the

same remainder r (0 ::": r < n). Then

a- b = (q,n + r)- (q2n + r) = (q, - q2)n

whence n I a- b. In the language of congruences, we have a= b (mod n).

If a and bare relatively prime positive integers, then the

arithmetic progression

a, a+ b, a + 2b, a+ 3b, ...

contains infinitely many primes.

Dirichlet's theorem tells us, for instance, that there are infinitely many prime

numbers ending in 999, such as 1999, 100999, 1000999, ... for these appear in the

arithmetic progression determined by 1000n + 999, where gcd(lOOO, 999) = 1.

There is no arithmetic progression a, a+ b, a+ 2b, ... that consists solely of

prime numbers. To see this, suppose that a + nb = p, where p is a prime. If we put

nk = n + kp fork= 1, 2, 3, ... then the nkth term in the progression is

a+ nkb =a+ (n + kp)b =(a+ nb) + kpb = p + kpb

Because each term on the right-hand side is divisible by p, so is a+ nkb. In other

words, the progression must contain infinitely many composite numbers.

It is an old, but still unsolved question of whether there exist arbitrarily long

but finite arithmetic progressions consisting only of prime numbers (not necessarily

consecutive primes). The longest progression found to date is composed of the 22

primes:

11410337850553+4609098694200n 0 ~ n ~ 21

The prime factorization of the common difference between the terms is

23 . 3. 52 .7. 11. 13. 17. 19.23. 1033

which is divisible by 9699690, the product of the primes less than 22.

Q:9:-let us solve the linear congruence

17x = 9 (mod 276)

Because 276 = 3 · 4 · 23, this is equivalent to finding a solution for the system of

congruences

17x = 9 (mod 3)

17x = 9 (mod 4)

17x = 9 (mod 23)

or x = 0 (mod 3)

$x=1 (mod4)$

$17x = 9 \pmod{23}$

Note that if $x = 0 \pmod 3$, then $x = 3k$ for any integer k. We substitute into the second congruence of the system and obtain

$3k = 1 (mod4)$

Multiplication of both sides of this congruence by 3 gives us

$k = 9k = 3 \pmod 4$

so that $k = 3 + 4j$, where j is an integer. Then

$X= 3(3 + 4j) = 9 + 12j$

For x to satisfy the last congruence, we must have

$17(9 + 12j) = 9 \pmod{23}$

or$204j = -144 \pmod{23}$, which reduces to $3j = 6 \pmod{23}$; in consequence, $j = 2 \pmod{23}$. This yields $j = 2 + 23t$, with t an integer, whence

$X = 9 + 12(2 + 23t) = 33 + 276t$

All in all, $x = 33 \pmod{276}$ provides a solution to the system of congruences and, in tum, a solution to $17x = 9 \pmod{276}$

The system of linear congruences

$ax +by = r \pmod n$

$ex + dy = s \pmod n$

has a unique solution modulo n whenever gcd(ad- be, n) = 1.

Proof. Let us multiply the first congruence of the system by d, the second congruence by b, and subtract the lower result from the upper. These calculations yield

$(ad- bc)x = dr- bs \pmod n$ (1)

The assumption gcd(ad- be, n) = 1 ensures that the congruence

$(ad- bc)z = 1 \pmod n$

posseses a unique solution; denote the solution by t. When congruence (1) is multiplied by t, we obtain

$x = t(dr - bs) \pmod n$

A value for y is found by a similar elimination process. That is, multiply the first congruenceofthe system by c, the second one by a, and subtract to end up with

$(ad- bc)y =as- cr \pmod n$

Multiplication of this congruence by t leads to

$y = t(as- cr) \pmod{n}$

A solution of the system is now established.