TUTORIAL - 3

U19CS012

PRIMES AND THEIR DISTRIBUTION

[BHAGVA RANA]

U19CS012

(1) Give an example to show that the following conjecture is not true:
Every positive integer can be written in form $p+a^2$, where p is either prime or 1, and $a \geq 0$.

(1) dot's represent $25 = p + a^2$

For $a = 1$, $p = 25-(1)^2 = 24$ ≠ Not prime

$a = 2$, $p = 25-(2)^2 = 21$ ≠ Not prime

$a = 3$, $p = 25-(3)^2 = 16$ ≠ Not prime

$a = 4$, $p = 25-(4)^2 = 9$ ≠ Not Prime

$a = 5$, $p = 25-(5)^2 = 0$ ≠ Not Prime

∵ There is no prime 'p' for ∀ all values of 'a'.

∴ The above mentioned conjecture is not true.

(2) Prove the following Assertions

(a) Any prime of the form $3n+1$ is also of form $6m+1$.

Proof: $3n+1$ is prime ⇒ $3n+1$ is odd

dot $p = 3n+1$, then $p-1 = 3n$ is even

∴ n is even, ∴ $n = 2m$, for some m

∴ $p = 3(2m)+1 = 6m+1$, Hence Proved.

(b) Each integer of form $3n+2$ has a prime factor of this form.

Proof: dot p be any prime factor of $3n+2$

∴ $p = 3k+1$ or $3k+2$, for some k [By Division Algorithm]

∴ $3n+2 = (3k_1+1)(3k_2+1) \dots (3k_r+1)$

[By Fundamental Theorem of Arithmetic]

But this latter product is of form $[3^{\gamma} k_1 \cdots k_{\gamma} + \cdots + 1]$, where every term except 1, is a factor of 3.

∴ Product is of form $3(q)+1$, which is contradiction.

(c) The only prime of the form n^3-1 is 7.

(c) Proof:

$$n^3-1 = (n-1)(n^2+n+1)$$

For 'n^3-1' to be prime, $n > 1$

For $n=2$, $n^3-1 = (2)^3-1 = (7) = (1)(2^2+2+1)$

For any $n>2$, $p = n^3-1$ will be factor of two integers $[(n-1)$ & (n^2+n+1) $\forall\, n>2]$ neither of which is 1.

∴ for $n \neq 2$, p can't be prime.

∴ Only prime of n^3-1 form is '7'.

(d) The only prime p for which $3p+1$ is a perfect square is $p=5$.

(d) Proof:

$$3(5)+1 = 16 = 4^2$$

Suppose, $3p+1 = n^2$, for some integer n, $n \neq 4$

$$3p = n^2-1 = (n+1)(n-1)$$

If $(n+1) = p$, then $n-1 = 3 \Rightarrow n=4$

Assume $n+1 \neq p$, ∴ $\gcd(n+1, p) = 1$

∴ $(n+1) \mid 3$ [By Euclid Lemma]

∴ $(n+1) = 1$ or 3 ∴ $n=2$

∴ $3p+1 = 4$ $[p=1]$

{A contradiction}

Similar reasoning for $n-1$.

If $n-1 = p$, then $n+1 = 3$, $\Rightarrow n = 2$.

Leading to contradiction of $3p+1 = 4 \quad p = 1$

$\therefore n-1 \neq p$, then $\gcd(n-1, p) = 1$

$\therefore (n-1) \mid 3$ [By Euclid's Lemma]

$\therefore (n-1) = 1$ or 3

$\therefore [n = 4]$

From both reasing, we get only one answer $n = 4$

$\therefore$ Thus only prime for which $3p+1$ is perfect square (4^2) is for $p = 5$. , Hence Proved

(e) The only prime of form n^2-4 is 5.

Proof:

Let $p = n^2-4 = (n+2)(n-2)$

$\because p$ is prime, one of the factor must be '1' & the other factor has to be 'p'.

Suppose, $n+2 = p \quad \therefore n-2 = 1 \quad n = 3$

$\therefore p = 5$

Suppose, $n+2 = 1 \quad \therefore n = -1$

$\therefore p = n-2 = -3 \quad \therefore n+2 \neq 1$

[$\because$ only possibility is $n = 3$, $\therefore p = 5$]

[The only prime of form n^2-4 is 5.], Hence proved.

U19CS012

③ If $p \geq 5$, is a prime number, show that p^2+2 is composite.

③ By Division Algorithm,

$$p = 6k + r \qquad 0 \leq r < 6$$

$r \neq 0$ as $p = 6k \Rightarrow 6 \mid p$

$r \neq 2$ as $p = 6k+2 \Rightarrow 2 \mid p$

$r \neq 3$ as $p = 6k+3 \Rightarrow 3 \mid p$

$r \neq 4$ as $p = 6k+4 \Rightarrow 2 \mid p$

$\therefore$ $p = 6k+1$ or $6k+5$

$\therefore$ $p^2+2 = (6k+1)^2 + 2 = 36k^2 + 12k + 3$

OR

$p^2+2 = (6k+5)^2 + 2 = 36k^2 + 12k + 27$

In Either case, $3 \mid p^2+2$, So p^2+2 is composite.

, Hence proved.

---

④ (a) Given that p is prime and $p \mid a^n$, prove that $p^n \mid a^n$

We know that, if p is prime and $p \mid ab$

then $p \mid a$ or $p \mid b$. —①

Let us assume, $p \mid a^n = p \mid a^{n-1}$ (a)

Then by ①, either $p \mid a^{n-1}$ or $p \mid a$ as p is prime

if $p \mid a$ then $p^n \mid a^n$

if $p \mid a^{n-1}$ then again by either $p \mid a^{n-2}$ or $p \mid a$

if $p \mid a$ then again, $p^n \mid a^n$

So, if $p \mid a^{n-2}$ then again by (2) either $p \mid a^{n-3}$ or $p \mid a$

if $p \mid a$, then again $p^n \mid a^n$

in this process, Ultimately $p \mid a$ which gives $p^n \mid a^n$

, Hence proved.

(b) If $\gcd(a,b) = p$, a prime, what are the possible values of $\gcd(a^2, b^2)$, $\gcd(a^2, b)$ and $\gcd(a^3, b^2)$?

Using 4(a) if $\gcd(a,b) = p$

then ① $p \mid a$

② $p \mid b$

③ $p^2 \mid a^2$ } ∴ [$\gcd(a^2, b^2) = p^2$]

④ $p^2 \mid b^2$ ⑤ [$p^3 \mid a^3$ & $p^3 \mid b^3$]

(a) $\gcd(a^2, b^2) = p^2$

(b) $\gcd(a^2, b) = \gcd(p^2(k_1), p(k_2)) = p$

(c) $\gcd(a^3, b^2) = \gcd(p^3(k_1), p^2(k_2)) = p^2$

5.) Establish the following statement:

(a) Every integer of the form n^4+4, with $n > 1$, is composite.

$n^4+4 = n^4 - 4n^2 + 4 + 4n^2$ [add & subtract $(4n)$]

$= (n^4 + 4n^2 + 4) - 4n^2$

$= (n^2+2)^2 - (2n)^2$

$= (n^2 + 2 - 2n)(n^2 + 2 + 2n)$

∵ $n > 1$, $n \geq 2$, $n^2 \geq 2n$ and $n^2 - 2n \geq 0$

$n^2 - 2n + 2 \geq 2 > 0$

∴ Both the factors are positive

Since n^4+4 has two integer positive factors, ∴ it is composite

Hence proved!

(b) An integer of form 8^n+1, where $n \geq 1$ is composite.

(b) Proof: $a^3 + 1 = (a+1)(a^2 - a + 1)$

∴ $(2^n)^3 + 1 = (2^n+1)(2^{2n} - 2^n + 1)$

∴ $(2^n+1) \mid (2^{3n}+1)$ and $2^{3n} = 8^n$

∴ $(2^n+1) \mid 8^n+1$

∴ integer of form 8^n+1 is composite.

U19CS012

(c) Each integer $n \geq 11$ can be written as the sum of two composite numbers.

Proof: Suppose n is even

Then $\exists k$ s.t. $n = 2k$

$n = 2k = 6 + 2(k-3)$ [Add & Sub 6]

$\therefore n$ is sum of 6 $(= 2.3)$ and $2(k-3)$

If $k \geq 5$, (So $(k-3) > 1$, So $2(k-3)$ is product of two numbers > 1)

Then $2k \geq 10$, $n > 11$

and n is the sum of two composites.

Suppose n is odd. Then $\exists k$ s.t. $[n = 2k+1]$

$\therefore n = 2k+1$

$= 2(k-1) + 3$ [3 is prime]

$= 2(k-2) + 5$ [5 is prime]

$= 2(k-3) + 7$ [7 is prime]

$= 2(k-4) + 9$

So, if $k \geq 6$, then $2(k-4)$ is product of two numbers > 1, So

$n = (2k+1) \geq 13$ and n is sum of two composites.

6.) Find all prime numbers that divide 50!

6.) All primes < 50 will divide 50! since each is a term of 50!.

By Fundamental theorem of Arithmetic, each term k of 50! that is non-prime has a unique prime factorization and each term of the unique factorization of k is smaller than k. and so is a prime that is < 50.

$\therefore$ There is no prime > 50 represented in this factorization of k.

$\therefore$ All primes < 50 are all the primes that divide 50!.

(2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47)

U19CS012

7.) Find a prime which can be expressed as x^7-1 where x is an integer

7.)

$$x^7-1 = (x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$$

So, we can write,

$x^7-1 = a*b$ for integers a and b.

If ab is prime either $a=1$ or $b=1$

Either $x-1=1$ OR $x^6+x^5+x^4+x^3+x^2+x^1+1=1$

$x=2$ $x(x^5+x^4+x^3+x^2+1)=0$

$x=0$ $x^5+x^4+x^3+x^2+1=0$

$x^3(x^2+x+1)+1(x^2+x+1)=0$

$x^3+1=0$ $x^2+x+1=0$

$(x+1)(x^2-x+1)$ No real sol^n

$[x=-1]$ No real sol^n

So, we get $x=0$, $x=-1$, $x=2$

in x^7-1 to see which one(s) are prime.

$x=0$ $(0)^7-1=-1$ Not prime

$x=-1$ $(-1)^7-1=-2$ Not prime

$x=2$ $x^7-1=(2)^7-1=$ 127 PRIME $[x=2]$.

ANS: '127' is a prime which can be expressed as x^7-1 where

6.) (a) An unanswered question is whether there are infinitely many primes that are 1 more than a power of 2, such as $5=2^2+1$

Find two more of these primes.

$2^4+1=17$, $2^8+1=257$ examples of two more similar type primes

(b) There exist infinitely many primes of form n^2+1. Eg: $257=16^2+1$

Exhibit Five more primes of this form.

$1^2+1=2$ $4^2+1=17$ $10^2+1=101$

$2^2+1=5$ $6^2+1=37$

vision

U19CS012

9.) If $p \neq 5$ is an odd prime, prove that p^2-1 or p^2+1 is divisible by 10.

9.) Proof: p is of form $10k+1$, $10k+9$
$10k+3$, $10k+7$

$10k+$ even ; can have factor of 2, so Not prime.

$(10k+1)^2 = 100k^2 + 20k + 1 \quad \therefore \quad 10 \mid p^2-1$

$(10k+3)^2 = 100k^2 + 60k + 9 \quad \therefore \quad 10 \mid p^2+1$

$(10k+7)^2 = 100k^2 + 140k + 49 \quad \therefore \quad 10 \mid p^2+1$

$(10k+9)^2 = 100k^2 + 180k + 81 \quad \therefore \quad 10 \mid p^2-1$

Hence, p^2-1 / p^2+1 is divisible by 10, $\forall$ $p \in$ odd prime ($\neq 5$)

10.) Find the prime factorization of the integers 1234, 10140, & 36000.

10.) $1234 = 2 \times 617$ (617 prime)

$10140 = 10 \times 1014 = 2.5.(2.507) = 2^2.5.(3.13^2)$
$= [2^2.3.5.13^2]$

$36000 = 36\,1000 = 2^2.3^2.10.25.4$
$= 2^2.3^2.2.5.5^2.2^2$
$= [2^5.3^2.5^3]$

SUBMITTED BY:
BHAGYA VINOD RANA
U19CS012
IInd Yr (CSE)