V19CS076

Krithikha Balamurugan

# Tutorial - 3
## Primes and their Distribution

[1] We will give an example to show that the following conjective is not true.
Every positive integer can be written in the form, p & $a^2$, where p is written either a prime or 1.

Take $x = 25$ hence $25 = 0 + 25$
$= 21 + 4$
$= 9 + 16$
$= 16 + 9$

But none of 0, 4, 9 and 16 is prime or 1

2) a) Let $p = 3n+1$ be a prime number, $n \in Z^+$
If n is odd
Then 3n is odd $\Rightarrow$ 3n+1 is even
And only 2 is only even prime
$\therefore$ $p = 3n+1$ cant be prime if n is odd
$\therefore$ n must be even
i.e $n = 2k$ for some $k \in Z^+$
now $p = 30+1 = 3(2k)+1 = 6k+1$
Thus we proved that any prime of form 3n+1 are also if form 6k+1

b) We prove that result by induction.
first +ve integer of form $3n+2 = 2$ is prime then 2 is prime divisor of 2 that is clearly of form:

- $3n+2$ :- Suppose that energy integer greater than

or equal to 2 but less than $k = 3n+2$ has a prime division of form $3l+2$.
Now we want to show that $k=3n+2$ has a prime divisor of form $3l+2$

Case 1 :- If $k = 3n+2$ is prime
$\Rightarrow k = 3n+2$ is itself a prime divisor of the form $3l+2$.

Case 2 :- If $k=3n+2$ is not prime
$\Rightarrow k = 3n+2$ is composite
$\Rightarrow k = 3n+2 = ab$ for some $a, b \in Z$
$1 \leq a, b \leq k = 3n+2$
Since the product ab is the form $3n+2$ therefore one of the a and b is of the form $3k_1+2$ and other is of form $3k_2+1$ we can write $k = 3n+2 = (3k_1+2)(3k_2+1)$
where $1 \leq a = 3k_1+2 < 3n+2$
By induction hypothesis $a = 3k_1+2$ has a prime divisor of the form $3k_1+2$ hence $3n+2$ has a prime divisor at form $3n+2$

(c) $n^3-1$ is given to us
$n^2-1$ can be written as product of $(n-1)$ and $(n^2-n+1)$
$n^3-1 = (n-1)(n^2-n+1)$
$> 0$ we can ryt
$n^3-1 = ab$ for integers a and b.
If ab is prime either a or b must be 1 (or else we can have more than 2 factors

U19CS076

Thus either

$n-1=1$ or $n^2-n+1=1$

$n=2$ $n^2-n=0$

(if it is true) $n=0,1$

(if it is true).

So we rest $n=0$, $n=1$ and $n=2$ in $n^3-1$ to see which one (1) are prime

$n=0$ $n^3-1=0-1=-1$ not prime

$n=1$ $n^3-1=1-1=0$ not prime

$n=2$ $n^3-1=8-1=7$ prime.

Thus 7 is the only prime in form of $n^3-1$.

(2). $3p+1$ is perfect square.

$3p+1=q^2$

$3p=q^2-1$

$3p=(q-1)(q+1)$

Left hand side is product of two primes 3 and p. Therefore 3 divides exactly one of $(q-1)$ and $(q+1)$ and p divides one of $(q-1)$ and $(q+1)$.

Because $q-1<q+1$, $q+1$ can't be 1. Therefore the only possibilities are:

a → $q-1=3$, $q+1=p$

b → $q-1=p$, $q+1=3$

c → $q-1=1$, $q+1=3p$

a → If $q-1=3$, then $p=5$, p is prime satisfy the condition of the problem

b → If $q+1=3$ then $p=1$. This can't be one case since p is supposed to be prime, this is not satisfy the condition of problem.

c → If $q-1=1$ then $3=3p$ that is $p=1$. This

U19CS076

Cant be true same case as (b).
So only solution is $p=5$

(2). $n^2-4$ is given
$n^2=4$ can be written as product of $(n-2)$ and $(n-2)$
$$n^2-4 = (n-2)(n+2)$$
So we can write
$n^2-4 = ab$ for integers $a, b$
If $n^2-4 = ab$ is prime, either a or b must be 1 (or else we should have more than two factors)
Thus either and $n+2$ cant be 1 $(n-2<0)$
$n-2=1$
$n=3$ --- only soln
when $n=3$; $n^2-4 = 3^2-4 = 5$
Thus 5 is only prime in term of $n^2-4$.

(3). For $p \geq 5$ is a prime number then by the quotient, remainder theorem, p can be expressed as $6k$ or $6k+1$ or $6k+2$ or $6k+3$ or $6k+4$ or $6k+5$ for some integer k.
If it is given p is prime number so it cant be expressed in $6k$, $6k+2$, $6k+3$ because it is multiple of 2 and 3.

The only numbers which can expressed p are $6k+1$ or $6k+5$.
If $p = 6k+1$ when by squaring p and adding 2
$$p^2+2 = (6k+1)^2 + 2$$
$$= 36k^2 + 12k + 1 + 2$$
$$= 36k^2 + 12 + 3$$

$= 3(12k^2 + 4k + 1)$

So it can be observe that $p^2+2$ is composite

Now it $p = 6k+5$

$p^2 + 2 = (6k+5)^2 + 2$

$= 36k^2 + 25 + 60k + 2$

$= 36k^2 + 60k + 27$

$= 3(12k^2 + 20k + 9)$

and if it also composite.

Thus if $p \geq 5$ is a prime number, then $p^2+2$ is composite.

(4) a) We have to prove than $p^n | a^n$,

Given that p is prime number and $p | a^n$.

We know that if p is prime and $p | ab$ then $p|a$ or $p|b$ — (1)

Let assume $p|a^n = p|(a^{n-1} a)$

Then by (1) either $p|a^{n-1}$ or $p|a$ as p is prime

if $p|a$ then $p^n|a^n$

if $p|a^{n-1}$ then again by (1) either $p|a^{n-2}$ or $p|a$

if $p|a$ then again $p^n|a^n$

So if $p|a^{n-2}$ then again by (1) either $p|a^{n-3}$ or $p|a$

If $p|a$, then again $p^n|a^n$

in this process, ultimately $p|a$ which gives $p^n|a^n$.

Hence proved.

(B) It is given that $\gcd(a,b) = p$ and p is a prime number.

U19CS076

Case - 1 $a = pm$ & $b = pn$ can be written when p & na & p & n and m, n doesn't have common factor

Then gcd of :-

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

$$gcd(a^2, b) = gcd(p^2m^3, pn)$$
$$= p^2 \, gcd(m^3, n)$$
$$= p^2$$

$$gcd(a^3, b^2) = gcd(p^3m^3, p^2n^2)$$
$$= p^2 \, gcd(pm^3, n^2)$$
$$= p^2$$

Case - 2 $a = pm$ & $b = p^k m$ where $k \geq 2$.

Where p & m & p & n and m, n doesn't have common factor.

then gcd of $gcd(a^2, b^2) = gcd(p^2m^2, p^{2k}n^2)$
$$= p^2 \, gcd(m^2, p^{2k-2}n^2)$$
$$= p^2 \quad , k \geq 2$$

$$gcd(a^2, b) = gcd(p^2m^2, p^k n)$$
$$= p^2 \, gcd(m^2, p^{k-2} n)$$
$$= p^2$$

$$gcd(a^3, b^2) = gcd(p^3m^3, p^{2k}n^2)$$
$$= p^3 \, gcd(m^3, p^{2k-3} n^2)$$
$$= p^3$$

Case 3 : when $a = p^k m$, $b = pn$ $k \geq 2$

$$gcd(a^2, b^2) = p^2$$
$$gcd(a^2, b) = p$$
$$gcd(a^3, b^2) = p^2$$

possible values of $gcd(a^2, b^2) = p^2$
$$gcd(a^2, b) = p \text{ or } p^2$$

U19CS076

$gcd(a^3, b^2) = p^2$ or $p^3$

② a) We have to show that every integer of the form $n^4+4$ with $n>1$ is composite

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

$n^4+4$ can be written ~~as~~ product of $(n^2+2n+2)$ $(n^2-2n+2)$ and for $n \geq 1$ both the numbers are +ve and greater than 1,

so $n^4+4$ is composite.

b) Any integer of form $8^n+1$ where $n \geq 1$ is composite

$$8^n+1 = (2^3)^n+1$$
$$= (2^n)^3+1 \qquad \because a^3+b^3$$
$$= (2^n+1)(2^{2n}-2^n+1)$$

For $n \geq 1$ both the numbers $2^n+1$ and $2^{2n}-2^n+1$ are +ve and greater than 1.

so $8^n+1$ is composite.

c. Each integers $n \geq 11$ can be written as sum of ~~to~~ two composite numbers.

If $n$ is even then $n = 2k$

$$n-6 = 2k-6$$
$$= 2(k-3)$$
$$n = 2(k-3)+6$$

both are composite

If $n$ is odd $n = 2k+1$

$$n-9 = 2k+1-9$$
$$= 2k-8$$
$$n-9 = 2(k-4)$$
$$n = 2(k-4)+9$$

both are composites.

U19CS076

⑥ All primes $\leq 50$ will divide $50!$ since each is a term of 50
By the fundamental theorem of arithmetic each term $k$ of $50!$ that is not prime has a unique prime factorization and each term of unique factorization of $k$ is smaller than $k$. and so is a prime that is $<50$.

$\therefore$ There is no prime $>50$

$\therefore$ all prime $<50$ are all primes that divide $50!$

which are : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 and 47.

⑦ $x^7-1$ is given to us.
$x^7-1$ can be written of product of $(x-1)$ and $(x^6+x^5+x^4+x^3+x^2+x+1)$

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

So we can write,

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

If $ab$ is prime either $a$ or $b$ must be 1 (or else we would have more than two factors)

Thus either

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

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

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

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

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

$(x+1)(x^2-x+1)=0$ NOT possible

Scanned with CamScanner

$x = -1 \rightarrow$ No real solution

So we rest $x = 0$, $x = -1$, $x = 2$ in $x^7 - 1$ to see which ones are prime

$x = 0 \quad x^7 - 1 = 0 - 1 = -1$ not prime

$x = -1 \quad x^7 - 1 = (-1)^7 - 1 = -2$ not prime

$x = 2 \quad x^7 + 1 = 2^7 - 1 = 127$ prime

127 is prime expressed as $x^7 - 1$ when $x = 2$.

(8) a) Primes that are 1 more than a power of 2

$17 = 2^4 + 1$, $257 = 2^8 + 1$

b). Primes of form $n^2 + 1$

$1^2 + 1 = 2$

$2^2 + 1 = 5$

$4^2 + 1 = 17$

$6^2 + 1 = 37$

$10^2 + 1 = 101$

(9) Using division algorithm its $p$ is an integer then

$p = 10k, 10k+1, 10k+2, 10k+3, 10k+4, 10k+5,$
$10k+6, 10k+7, 10k+8, 10k+9.$

and $p$ is odd prime

so $\rightarrow 10k+1, 10k+3, 10k+7, 10k+9$ only these term follow that a prime $p$ will be of form

$p = 10k + 1$

$$p^2 - 1 = (10k+1)^2 - 1$$
$$= 100k^2 + 20k + 1 - 1$$
$$= 10(10k^2 + 2k) \text{ divisible by } 10$$

Scanned with CamScanner

U19CS076

$$p^2+1 = (10k+1)^2+1$$
$$= 100k^2+20k+1+1$$
$$= 10(10k^2+2k)+2$$
$\rightarrow$ Not divisible by 10

For $p = 10k+1$ term either $p^2-1$ or $p^2+1$
$\rightarrow p^2-1$ is divisibly by 10

$p = 10k+3$
$$p^2-1 = (10k+3)^2-1$$
$$= 100k^2+9+60k-1$$
$$= 100k^2+60k+8$$
$$= 10(10k^2+6k)+8$$
$\rightarrow$ Not divisible by 10
$$p^2+1 = (10k+3)^2+1$$
$$= 100k^2+60k+10$$
$$= 10(10k^2+6+1)$$ divisibly by 10

For $p = 10k+3 \rightarrow p^2+1$ is divisible by 10

$p = 10k+7$

$$p^2-1 = (10k+7)^2-1$$
$$= 100k^2+140k+48$$
$$= 10(10k^2+14k)+48$$
Not divisible by 10.
$$p^2+1 = (10k+7)^2+1$$
$$= 100k^2+140k+50$$
$$= 10(10k^2+14k+5)$$
divisible by 10

For $p = 10k+7 \rightarrow p^2+1$ is divisible by 10

U19CS076

For $p = 10k + 9$

$$p^2 - 1 = (10k+9)^2 - 1$$
$$= 100k^2 + 180k + 80$$
$$= 10(10k^2 + 18k + 8)$$

divisible by 10

$$p^2 + 1 = (10k+9)^2 + 1$$
$$= 100k^2 + 180k + 82$$

Not divisible by 10

For $p = 10k+9 \rightarrow p^2 - 1$ is divisible by 10

10. We want to find the prime factors of these numbers

$$1234 = 2 \cdot 617$$
$$10140 = 2^2 \cdot 5 \cdot 3 \cdot 13^2$$
$$36000 = 2^5 \cdot 5^3 \cdot 3^2$$