

Legendre, Grimm, Balanced Prime, Prime triplet, Polignac's conjecture, a problem and 17 tips with proof to solve problems on number theory

Shubhankar Paul

Abstract— In this paper we will prove five conjectures, one problem viz.

- 1) Legendre Conjecture.
- 2) Grimm's Conjecture.
- 3) Balanced Primes are infinite.
- 4) Prime triplets are infinite.
- 5) Polignac's conjecture.
- 6) Can a prime p satisfy $2^{p-1} \equiv 1 \pmod{p^2}$ and $3^{p-1} \equiv 1 \pmod{p^2}$ simultaneously?

And 17 tips with proof to solve problems on number theory.

Index Terms— Legendre Conjecture, Balanced Primes, Polignac's conjecture.

I. INTRODUCTION

A. Contents

- 1) What is Prime.
- 2) How Prime generates.
- 3) Legendre's Conjecture.
- 4) Solution.
- 5) Result.
- 6) Conclusion.
- 7) Grimm's Conjecture.
- 8) Solution.
- 9) Balanced Prime problem.
- 10) Solution.
- 11) Prime Triplet problem.
- 12) Solution.
- 13) Polignac's conjecture.
- 14) Solution.
- 15) A problem.
- 16) Solution.
- 17) 17 tips with proof to solve problems on number theory.

B. What is prime

A number which is divisible by 1 and that number only is called a prime number.

I suggest another definition of prime is : When we adorn odd numbers in increasing series in

Manuscript received December 01, 2013.

Shubhankar Paul, Passed BE in Electrical Engineering from Jadavpur University in 2007. Worked at IBM as Manual Tester with designation Application Consultant for 3 years 4 months.

natural number line starting with 1,2,3 there is gap of odd numbers. This gap numbers are filled with prime numbers. See the example below under "How primes generate"

All odd composite number can be written in the form : $3^i 5^j 7^k \dots$ all prime numbers where i, j, k, \dots runs from 0 to infinity.

C. How primes generate

Prime numbers are odd numbers (except 2). Let's say 1,2,3 only these 3 numbers are given and we are supposed to make natural numbers.

1 2 3 2^2 $2*3$ but 2^2 and $2*3$ both even number. But between two even numbers there must be an odd number. We call it 5 a prime number because no other integer can give birth to this number. Prime number series generates in this way.

II. LEGENDRE'S CONJECTURE

Between 132 (=169) and 142 (=196) there are five primes (173, 179, 181, 191, and 193); between 302 (=900) and 312 (=961) there are eight primes (907, 911, 919, 929, 937, 941, 947, and 953); between 352 (=1225) and 362 (=1296) there are ten primes (1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, and 1291).

The problem is to prove Legendre's Conjecture, which states that there is at least one prime number between every pair of consecutive squares, or find a counter-example.

Solution

Let's say n is even and $(n+1)$ is odd. Let's take $n^2 + 1 = 3m$ (i.e. $n^2 + 1$ is divisible by 3 and $(n+1)^2 - 2 = 3(m+r)$)

Now, between 2 consecutive odd multiple of 3 there are 2 odd numbers. (e.g. between 9 and 15 there 2 odd numbers 11 and 13)

So, there are r number of gaps between $3m$ and $3(m+r)$ So, in the gaps there are $2r$ odd numbers and $(r+1)$ numbers are divisible by 3.

\Rightarrow There are total $2r + (r+1) = 3r + 1$ number of odd numbers between n^2 and $(n+1)^2$

Now, $(n+1)^2 - n^2 = 2n+1$

\Rightarrow There are $(2n+1)-1 = 2n$ numbers between n^2 and $(n+1)^2$

⇒ There are n odd numbers between n^2 and $(n+1)^2$

Therefore, $n = 3r + 1$

So, there is no multiple of numbers after $(m+r)$ in between n^2 and $(n+1)^2$ because 3 is least odd number.

Now, there are $(m+r)/2 - 1$ number of odd numbers before $(m+r)$

Now, after 3 next odd number is 5.

Now, if s is multiplied by 3 gives the number $3(m+r)$ and $(s-2)$ multiplied by 5 gives the previous odd number of $3(m+r)$ and $(s-4)$ multiplied by 7 gives $3(m+r) - 4$ and so on.... then there are $\{5(s-2) - 3s\}$ numbers do not produce any multiple between n^2 and $(n+1)^2$ because after 3 next odd number is 5.

Similarly, there are $\{7(s-4) - 5(s-2)\}$ number of numbers do not produce any multiple between n^2 and $(n+1)^2$ because after 5 next odd number $s = 7$. And so on. This is worst possible scenario because if we take more difference then number of numbers which doesn't produce any odd multiple between n^2 and $(n+1)^2$ will be more. But we are considering less.

Now we will calculate the number of numbers which do not produce multiple between n^2 and $(n+1)^2$ and less than $(m+r)$.

The series is as follows :

$\{5(s-2) - 3(s-0)\} = 2s - 5*2 + 3*0$

$\{7(s-4) - 5(s-2)\} = 2s - 7*4 + 5*2$

$\{9(s-6) - 7(s-4)\} = 2s - 9*6 + 7*4$

...

...

...

$[(2n+3)(s-2n) - (2n+1)\{s-(2n-2)\}] = 2s - (2n+3)*2n + (2n+1)(2n-2)$

Adding we get, $2ns - 2n(2n+3)$ ($s = m+r$ here)

So, this is the number of numbers which doesn't produce any multiple between n^2 and $(n+1)^2$.

Now, when we multiply a number the quotient also a multiple of that number at the same time except the square numbers.

Because square numbers have odd number of multiples. But between two consecutive square number there cannot be any square number. So, we are fine to take number of odd multiples before $(m+r)$ as $(m+r)/2 - 1$.

So, number of numbers that produce multiple between n^2 and $(n+1)^2$ is :

$(m+r) - 1 - \{2n(m+r) - 2n(2n+3)\}$

$= (m+r) - 1 - 2n(m+r) + 2n(2n+3)$

Now, there are n numbers between n^2 and $(n+1)^2$

So, if we prove $n - [(m+r) - 1 - 2n(m+r) + 2n(2n+3)]$ is positive then it means there are odd numbers between n^2 and $(n+1)^2$ which is not born by multiplying any number. (Implying they are prime according to alternate definition).

Now putting $m = (n^2+1)/3$ and $r = (n-1)/3$ from above and simplifying we get,

$(4n^3 - 29n^2 - 17n + 3)/12$

Which is greater than 0 for $n > 7$.

Upto $n = 7$ we can check manually that there is at least one prime between n^2 and $(n+1)^2$

Between 2^2 and 1^2 there is 3

Between 3^2 and 2^2 there is 5, 7

Between 4^2 and 3^2 there is 11, 13

Between 5^2 and 4^2 there is 17, 19, 23

Between 6^2 and 5^2 there is 29, 31

Between 7^2 and 6^2 there is 37, 41, 43, 47.

Result

1) So, we have seen manually upto $n = 7$ that there is at least one prime between n^2 and $(n+1)^2$

2) We have proved that there is at least one prime between n^2 and $(n+1)^2$ for $n > 7$.

Conclusion

Legendre's Conjecture is true.

III. GRIMM'S CONJECTURE

Grimm's conjecture states that to each element of a set of consecutive composite numbers one can assign a distinct prime that divides it.

For example, for the range 242 to 250, one can assign distinct primes as follows:

242: 11 243: 3 244: 61 245: 7 246: 41 247: 13 248: 31 249: 83 250: 5

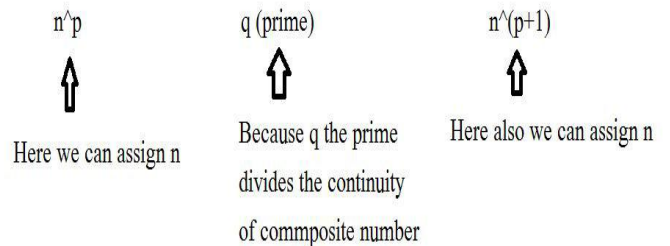
The problem is to prove the conjecture, or find a counter-example.

Solution

Case 1 :

If we can prove there is at least one prime between n^p and $n^{(p+1)}$ then we can assign n ,

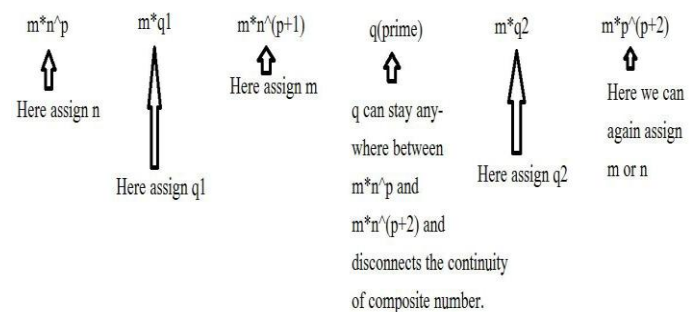
both n^p and $n^{(p+1)}$ as the image below says :



Case 2 :

If we can prove there is at least one prime between $m*n^p$ and $m*n^{(p+2)}$ then we can assign

n to $m*n^p$, m to $m*n^{(p+1)}$ and again n or m to $n^{(p+2)}$ as the below picture says :



Now,

- 1) Between 2 and 2^2 there is a prime 3
- 2) Between 2^2 and 2^3 there is prime 5, 7.
- 3) Between 3 and 3^2 there is prime 5, 7.
- 4) Onwards i.e. between 2^3 and 2^4 or 3^2 and 3^3 ... there are consecutive square numbers. According to Legendre's conjecture (which have been proved above) there is at least one prime.
- 5) Now Case 2 is trivial from Case 1.

So, Grimm's conjecture is true.

IV. BALANCED PRIME PROBLEM

A **balanced prime** is a prime number that is equal to the arithmetic mean of the nearest primes above and below. Or to put it algebraically, given a prime number P_n , where n is its index in the ordered set of prime numbers,

$$p_n = \frac{p_{n-1} + p_{n+1}}{2}.$$

The first few balanced primes are

5, 53, 157, 173, 211, 257, 263, 373, 563, 593, 607, 653, 733, 947, 977, 1103 (sequence A006562 in OEIS).

For example, 53 is the sixteenth prime. The fifteenth and seventeenth primes, 47 and 59, add up to 106, half of which is 53, thus 53 is a balanced prime.

When 1 was considered a prime number, 2 would have correspondingly been considered the first balanced prime since

$$2 = \frac{1 + 3}{2}.$$

It is conjectured that there are infinitely many balanced primes.

Problem source :

http://en.wikipedia.org/wiki/Balanced_prime

Solution

Let there are finite number of balanced primes.

We are considering primes of the form $p-12, p-6, p$.

Now let's $p_n - 6$ be the last balanced prime.

Now we form odd number table as below :

Any one column is divisible by 3. Let the left most column is divisible by 3. *Italic* numbers are divisible by 5 and Underlined numbers are divisible by 7.

$p_n - 10$	$p_n - 8$	$p_n - 6$
$p_n - 4$	<u>$p_n - 2$</u>	p_n
$p_n + 2$	$p_n + 4$	$p_n + 6$
$p_n + 8$	$p_n + 10$	$p_n + 12$
$p_n + 14$	$p_n + 16$	$p_n + 18$
$p_n + 20$	$p_n + 22$	$p_n + 24$
$p_n + 26$	$p_n + 28$	$p_n + 30$
$p_n + 32$	$p_n + 34$	$p_n + 36$
$p_n + 38$	<u>$p_n + 40$</u>	$p_n + 42$
$p_n + 44$	$p_n + 46$	$p_n + 48$
$p_n + 50$	$p_n + 52$	<u>$p_n + 54$</u>
$p_n + 56$	$p_n + 58$	$p_n + 60$
$p_n + 62$	$p_n + 64$	$p_n + 66$
$p_n + 68$	$p_n + 70$	$p_n + 72$
$p_n + 74$	$p_n + 76$	$p_n + 78$
$p_n + 80$	<u>$p_n + 82$</u>	$p_n + 84$
$p_n + 86$	$p_n + 88$	$p_n + 90$
$p_n + 92$	$p_n + 94$	<u>$p_n + 96$</u>
$p_n + 98$	$p_n + 100$	$p_n + 102$
$p_n + 104$	$p_n + 106$	$p_n + 108$

We see that $p_n + 96$ and $p_n + 102$ are composite and forming a balanced prime sets viz. $p_n + 94, p_n + 100$ and $p_n + 106$.

Now according to our assumption one of this must be divisible by any prime before it i.e. one of them have to be composite.

Now, we will find infinite number of balanced prime sets only by 5 and 7 and it will occur in a regular frequency i.e. after every 70 numbers and in a particular column it will occur after every 210 numbers.

There are only finite number of primes before p_n .

⇒ They cannot make every balanced prime set unbalanced by dividing any of three primes forming the balanced prime set.

So, there needs to be born primes after p_n so that every regular occurrence of balanced prime set by 5,7 can be made unbalanced by dividing with those primes at least one of the prime forming balanced set.

But there is no regular occurrence of prime whereas 5,7 will be forming balanced set of primes in a regular manner.

⇒ There will be a shortcoming somewhere of primes to make each and every balanced pair formed by 5,7 in a regular manner.

⇒ There will be balanced prime after p_n .

Here is the contradiction.

⇒ Balanced primes are infinite.

Proved.

V. PRIME TRIPLET PROBLEM

In mathematics, a **prime triplet** is a set of three prime numbers of the form $(p, p + 2, p + 6)$ or $(p, p + 4, p + 6)$. With the exceptions of $(2, 3, 5)$ and $(3, 5, 7)$, this is the closest possible grouping of three prime numbers, since every third odd number greater than 3 is divisible by 3, and hence not prime.

The first prime triplets (sequence A098420 in OEIS) are

$(5, 7, 11), (7, 11, 13), (11, 13, 17), (13, 17, 19), (17, 19, 23), (37, 41, 43), (41, 43, 47), (67, 71, 73), (97, 101, 103), (101, 103, 107), (103, 107, 109), (107, 109, 113), (191, 193, 197), (193, 197, 199), (223, 227, 229), (227, 229, 233), (277, 281, 283), (307, 311, 313), (311, 313, 317), (347, 349, 353), (457, 461, 463), (461, 463, 467), (613, 617, 619), (641, 643, 647), (821, 823, 827), (823, 827, 829), (853, 857, 859), (857, 859, 863), (877, 881, 883), (881, 883, 887)$

A prime triplet contains a pair of twin primes (p and $p + 2$, or $p + 4$ and $p + 6$), a pair of cousin primes (p and $p + 4$, or $p + 2$ and $p + 6$), and a pair of sexy primes (p and $p + 6$).

A prime can be a member of up to three prime triplets - for example, 103 is a member of $(97, 101, 103), (101, 103, 107)$ and $(103, 107, 109)$. When this happens, the five involved primes form a prime quintuplet.

A prime quadruplet $(p, p + 2, p + 6, p + 8)$ contains two overlapping prime triplets, $(p, p + 2, p + 6)$ and $(p + 2, p + 6, p + 8)$.

Similarly to the twin prime conjecture, it is conjectured that there are infinitely many prime triplets. The first known gigantic prime triplet was found in 2008 by Norman Luhn and François Morain. The primes are $(p, p + 2, p + 6)$ with $p = 2072644824759 \times 2^{33333} - 1$. As of May 2013 the largest known prime triplet contains primes with 16737 digits and was found by Peter Kaiser. The primes are $(p, p + 4, p + 6)$ with $p = 6521953289619 \times 2^{55555} - 5$.

Problem source : http://en.wikipedia.org/wiki/Prime_triplet

Solution

One of the column is divisible by 3. Let the left most column is divisible by 3. We will mark other composite numbers by underline.

Let's say $p_n - 6, p_n - 2$ and p_n form the last triplet prime set. We assume there is finite number of prime triplet set.

After p_n one of every triplet set should get divided by prime before it.

$p_n - 10$	$p_n - 8$	$p_n - 6$
$p_n - 4$	$p_n - 2$	p_n
$p_n + 2$	<u>$p_n + 4$</u>	<u>$p_n + 6$</u>
$p_n + 8$	$p_n + 10$	$p_n + 12$
$p_n + 14$	<u>$p_n + 16$</u>	<u>$p_n + 18$</u>
$p_n + 20$	$p_n + 22$	$p_n + 24$
$p_n + 26$	<u>$p_n + 28$</u>	<u>$p_n + 30$</u>
$p_n + 32$	$p_n + 34$	$p_n + 36$
$p_n + 38$	<u>$p_n + 40$</u>	<u>$p_n + 42$</u>
$p_n + 44$	$p_n + 46$	$p_n + 48$
$p_n + 50$	<u>$p_n + 52$</u>	<u>$p_n + 54$</u>
$p_n + 56$	$p_n + 58$	$p_n + 60$
$p_n + 62$	<u>$p_n + 64$</u>	<u>$p_n + 66$</u>
$p_n + 68$	$p_n + 70$	$p_n + 72$
$p_n + 74$	<u>$p_n + 76$</u>	<u>$p_n + 78$</u>
$p_n + 80$	$p_n + 82$	$p_n + 84$
$p_n + 86$	<u>$p_n + 88$</u>	<u>$p_n + 90$</u>
$p_n + 92$	$p_n + 94$	$p_n + 96$
$p_n + 98$	<u>$p_n + 100$</u>	<u>$p_n + 102$</u>
$p_n + 104$	$p_n + 106$	$p_n + 108$

As we can see the primes occur in a regular manner if we mark the composite number as above. But primes don't have any regular pattern to generate.

Here is the contradiction. So this case cannot happen.

Again we form the table as below :

$p_n - 10$	$p_n - 8$	$p_n - 6$
$p_n - 4$	$p_n - 2$	p_n
$p_n + 2$	<u>$p_n + 4$</u>	$p_n + 6$
$p_n + 8$	$p_n + 10$	<u>$p_n + 12$</u>
$p_n + 14$	<u>$p_n + 16$</u>	$p_n + 18$
$p_n + 20$	$p_n + 22$	<u>$p_n + 24$</u>
$p_n + 26$	<u>$p_n + 28$</u>	$p_n + 30$
$p_n + 32$	$p_n + 34$	<u>$p_n + 36$</u>
$p_n + 38$	<u>$p_n + 40$</u>	$p_n + 42$
$p_n + 44$	$p_n + 46$	<u>$p_n + 48$</u>
$p_n + 50$	<u>$p_n + 52$</u>	$p_n + 54$
$p_n + 56$	$p_n + 58$	<u>$p_n + 60$</u>
$p_n + 62$	<u>$p_n + 64$</u>	$p_n + 66$
$p_n + 68$	$p_n + 70$	<u>$p_n + 72$</u>
$p_n + 74$	<u>$p_n + 76$</u>	$p_n + 78$
$p_n + 80$	$p_n + 82$	<u>$p_n + 84$</u>
$p_n + 86$	<u>$p_n + 88$</u>	$p_n + 90$

$p_n + 92$	$p_n + 94$	<u>$p_n + 96$</u>
$p_n + 98$	<u>$p_n + 100$</u>	$p_n + 102$
$p_n + 104$	$p_n + 106$	<u>$p_n + 108$</u>

As we can see the primes occur in a regular manner if we mark the composite number as above. But primes don't have any regular pattern to generate.

Here is the contradiction. So this case cannot happen.

- ⇒ The composite number should occur in an awkward pattern
- ⇒ More primes are necessary to make them composite as for each prime occurrence of the multiples of the primes are regular but primes don't occur in regular pattern.

Again we form the table as below :

$p_n - 10$	$p_n - 8$	$p_n - 6$
$p_n - 4$	$p_n - 2$	p_n
$p_n + 2$	<u>$p_n + 4$</u>	$p_n + 6$
$p_n + 8$	<u>$p_n + 10$</u>	$p_n + 12$
$p_n + 14$	$p_n + 16$	<u>$p_n + 18$</u>
$p_n + 20$	<u>$p_n + 22$</u>	$p_n + 24$
$p_n + 26$	$p_n + 28$	<u>$p_n + 30$</u>
$p_n + 32$	$p_n + 34$	<u>$p_n + 36$</u>
$p_n + 38$	<u>$p_n + 40$</u>	$p_n + 42$
$p_n + 44$	$p_n + 46$	<u>$p_n + 48$</u>
$p_n + 50$	<u>$p_n + 52$</u>	$p_n + 54$
$p_n + 56$	$p_n + 58$	<u>$p_n + 60$</u>
$p_n + 62$	<u>$p_n + 64$</u>	$p_n + 66$
$p_n + 68$	<u>$p_n + 70$</u>	$p_n + 72$
$p_n + 74$	<u>$p_n + 76$</u>	$p_n + 78$
$p_n + 80$	$p_n + 82$	<u>$p_n + 84$</u>
$p_n + 86$	<u>$p_n + 88$</u>	$p_n + 90$
$p_n + 92$	$p_n + 94$	<u>$p_n + 96$</u>
$p_n + 98$	$p_n + 100$	<u>$p_n + 102$</u>
$p_n + 104$	$p_n + 106$	<u>$p_n + 108$</u>

Not to form any prime triplet after $p_n \Rightarrow$ there must be a composite number in each row.

Now, before p_n the number of primes is less than p_n .

Now, after p_n next multiple of p_n will occur in the same column is $6p_n$.

Between p_n and $6p_n$ there are p_n number of rows.

But before p_n there are less than p_n number of primes which can make composite one number of each row.

- ⇒ There will be primes left in a row.
- ⇒ Triplet prime set is there after p_n .
- ⇒ Triplet prime set is infinite.

Proved.

VI. COROLLARY

Twin primes are infinite as in the case of twin prime also each row should have at least one composite number.

Polignac's conjecture :

In number theory, **Polignac's conjecture** was made by Alphonse de Polignac in 1849 and states:

For any positive even number n , there are infinitely many prime gaps of size n . In other words: There are infinitely many cases of two consecutive prime numbers with difference n .

The conjecture has not yet been proven or disproven for a given value of n . In 2013 an important breakthrough was made by Zhang Yitang who proved that there are infinitely many prime gaps of size n for some value of $n < 70,000,000$. [2]

For $n = 2$, it is the twin prime conjecture. For $n = 4$, it says there are infinitely many cousin primes $(p, p + 4)$. For $n = 6$, it says there are infinitely many sexy primes $(p, p + 6)$ with no prime between p and $p + 6$.

Problem source : http://en.wikipedia.org/wiki/Polignac%27s_conjecture

Solution

For twin prime see the corollary of **Triplet Prime** problem. (End of Solution of **Triplet Prime**)

Now, we will prove there are infinitely many cousin primes. Let, the series of cousin primes is finite.

Let, $p_n - 6$ and $p_n - 2$ form the last cousin prime pair.

Any one column is divisible by 3. Let the left most column is divisible by 3. We will mark other composite numbers by underline.

Now we form the table as below :

$p_n - 4$	$p_n - 2$	<u>p_n</u>
$p_n + 2$	$p_n + 4$	<u>$p_n + 6$</u>
$p_n + 8$	$p_n + 10$	<u>$p_n + 12$</u>
$p_n + 14$	$p_n + 16$	<u>$p_n + 18$</u>
$p_n + 20$	$p_n + 22$	<u>$p_n + 24$</u>
$p_n + 26$	$p_n + 28$	<u>$p_n + 30$</u>
$p_n + 32$	$p_n + 34$	<u>$p_n + 36$</u>
$p_n + 38$	$p_n + 40$	<u>$p_n + 42$</u>
$p_n + 44$	$p_n + 46$	<u>$p_n + 48$</u>
$p_n + 50$	$p_n + 52$	<u>$p_n + 54$</u>
$p_n + 56$	$p_n + 58$	<u>$p_n + 60$</u>
$p_n + 62$	$p_n + 64$	<u>$p_n + 66$</u>
$p_n + 68$	$p_n + 70$	<u>$p_n + 72$</u>
$p_n + 74$	$p_n + 76$	<u>$p_n + 78$</u>
$p_n + 80$	$p_n + 82$	<u>$p_n + 84$</u>
$p_n + 86$	$p_n + 88$	<u>$p_n + 90$</u>
$p_n + 92$	$p_n + 94$	<u>$p_n + 96$</u>
$p_n + 98$	$p_n + 100$	<u>$p_n + 102$</u>
$p_n + 104$	$p_n + 106$	<u>$p_n + 108$</u>

The condition to satisfy that there is no cousin prime pair after $p_n - 2$ is one of the two columns should be composite (except the column divisible by 3).

- ⇒ The primes occur in a regular fashion.
- ⇒ Here is the contradiction.

Now, to deny the case there needs to be composite number in the middle column in an irregular fashion.

Now, next $p_n - 2$ occurs in the middle column after $p_n - 2$ rows.

- ⇒ There are more than $p_n - 2$ composite numbers before next $p_n - 2$ occurs in the table.
- ⇒ But before $p_n - 2$ there are less than $p_n - 2$ number of primes.
- ⇒ This case cannot happen.
- ⇒ There are infinite number of Cousin primes.

Proved.

The conclusion can be done in other way also : All the number of third column is composite. But there is at least difference of 2 between any consecutive prime.

- ⇒ There will be numbers left between the series of multiples of prime before $p_n - 2$.
- ⇒ There will be Cousin prime generated after $p_n - 2$.

Here is the contradiction.

- ⇒ There are infinite number of Cousin primes.

Proved.

Now we will prove there are infinite number of sexy primes.

Let, the series of sexy primes is finite.

Let, $p_n - 8$ and $p_n - 2$ form the last sexy prime pair.

One of the column is divisible by 3. Let the left most column is divisible by 3. We will mark other composite numbers by underline.

Now we form the table as below :

$p_n - 4$	$p_n - 2$	<u>p_n</u>
$p_n + 2$	<u>$p_n + 4$</u>	$p_n + 6$
$p_n + 8$	$p_n + 10$	<u>$p_n + 12$</u>
$p_n + 14$	<u>$p_n + 16$</u>	$p_n + 18$
$p_n + 20$	$p_n + 22$	<u>$p_n + 24$</u>
$p_n + 26$	<u>$p_n + 28$</u>	$p_n + 30$
$p_n + 32$	$p_n + 34$	<u>$p_n + 36$</u>
$p_n + 38$	<u>$p_n + 40$</u>	$p_n + 42$
$p_n + 44$	$p_n + 46$	<u>$p_n + 48$</u>
$p_n + 50$	<u>$p_n + 52$</u>	$p_n + 54$
$p_n + 56$	$p_n + 58$	<u>$p_n + 60$</u>
$p_n + 62$	<u>$p_n + 64$</u>	$p_n + 66$
$p_n + 68$	$p_n + 70$	<u>$p_n + 72$</u>
$p_n + 74$	<u>$p_n + 76$</u>	$p_n + 78$
$p_n + 80$	$p_n + 82$	<u>$p_n + 84$</u>
$p_n + 86$	<u>$p_n + 88$</u>	$p_n + 90$
$p_n + 92$	$p_n + 94$	<u>$p_n + 96$</u>
$p_n + 98$	<u>$p_n + 100$</u>	$p_n + 102$
$p_n + 104$	$p_n + 106$	<u>$p_n + 108$</u>

The condition to satisfy that there is no sexy prime pair after $p_n - 2$ is alternate number in each column should be composite (except the column divisible by 3).

- ⇒ The primes occur in a regular fashion.
- ⇒ Here is the contradiction.

Now, to deny the case there needs to be more composite numbers.

Now, next $p_n - 2$ occurs in the middle column after $p_n - 2$ rows.

- ⇒ There are more than $p_n - 2$ composite numbers before next $p_n - 2$ occurs in the table.
- ⇒ But before $p_n - 2$ there are less than $p_n - 2$ number of primes.
- ⇒ This case cannot happen.
- ⇒ There are infinite number of Sexy primes.

Proved.

Problem

Can a prime p satisfy $2^{p-1} \equiv 1 \pmod{p^2}$ and $3^{p-1} \equiv 1 \pmod{p^2}$ simultaneously?

Solution

Let p be the prime which simultaneously satisfy both the equation.

- ⇒ $2^{(p-1)} - 1 = mp^2$ (1)
- ⇒ $3^{(p-1)} - 1 = np^2$ (2)

Now dividing both sides of equation (1) by 8 we get, $2^{(p-1)} - 1 = (8m-1)p^2$ (as $LHS \equiv -1$ and $p^2 \equiv 1 \pmod{8}$ and putting $m = 8m-1$) (3)

Legendre, Grimm, Balanced Prime, Prime triplet, Polignac's conjecture, a problem and 17 tips with proof to solve problems on number theory

Now dividing both sides of equation (2) by 8 we get,
 $3^{(p-1)} - 1 = 8np^2$ (as $LHS \equiv 0$ and $p^2 \equiv 1 \pmod{8}$) and putting $n = 8n$ (4)

Now, dividing both sides of equation (3) by 3 we get,
 $2^{(p-1)} - 1 = (24m+15)p^2$ (as $LHS \equiv 0$ and $p^2 \equiv 1 \pmod{3}$) so $8m-1$ must be $\equiv 0 \pmod{3}$, so putting $m = 3m+2$ (5)

Now dividing both sides of equation (4) by 3 we get,
 $3^{(p-1)} - 1 = 8(3n+1)p^2$ (as $LHS \equiv -1$ and $p^2 \equiv 1 \pmod{3}$), $8n$ must be $\equiv -1 \pmod{3}$, so putting $8n = 8(3n+1)$)(6)

Now, dividing both sides of equation (6) by 16 we get,
 $LHS \equiv 0$ or $8 \pmod{16}$

Case 1 : $LHS \equiv 8 \pmod{16}$

- $\Rightarrow p - 1 = 2k$ where k is odd.
- $\Rightarrow p - 1 = 2(2k+1)$ (putting $2k+1$ in place of k as k is odd)
- $\Rightarrow p = 4k+3$
- $\Rightarrow p^2 = 16k^2 + 24k + 9$
- $\Rightarrow 8p^2 = 128k^2 + 192k + 72$
- $\Rightarrow 8p^2 \equiv 8 \pmod{16}$
- $\Rightarrow 3n+1$ must be $\equiv 1 \pmod{16}$
- $\Rightarrow n$ must be of the form $16n$

Equation (6) becomes, $3^{(p-1)} - 1 = 8(48n+1)p^2$ (7)

Now, dividing both sides of equation (5) by 16 we get,
 $LHS \equiv -1 \pmod{16}$

$p^2 \equiv 1$ or $9 \pmod{16}$

Case 1a : $p^2 \equiv 1 \pmod{16}$

- Now, $p^2 = 16k^2 + 24k + 9$
- $\Rightarrow k$ is odd as $p^2 \equiv 1 \pmod{16}$
- $\Rightarrow p^2 = 16(2k+1)^2 + 24(2k+1) + 9$ (putting $k = 2k+1$ as k is odd)
- $\Rightarrow p^2 = 64k^2 + 112k + 49$
- $\Rightarrow p = 8k + 7$

Now, $24m+15$ must be $\equiv -1 \pmod{16}$
 $\Rightarrow m$ is even.

Equation (5) becomes, $2^{(p-1)} - 1 = (48m+15)p^2$ (putting $2m$ in place of m as m is even)(8)

Now, dividing both sides of equation (7) by 32,
 $3^{(p-1)} - 1 = 3^{(8k+7-1)} - 1 = 3^{(8k+6)} - 1 = (3^{(8k)})(3^6) - 1$

Now, $3^{(8k)} \equiv 1 \pmod{32}$ (as (any odd number)⁸ $\equiv 1 \pmod{32}$)

$3^6 \equiv 25 \pmod{32}$
 $\Rightarrow LHS = (3^{(8k)})(3^6) - 1 \equiv 1 \cdot 25 - 1 \equiv 24 \pmod{32}$

Now, we have, $p^2 = 64k^2 + 112k + 49$
 $\Rightarrow 8p^2 = 512k^2 + 896k + 392$
 $\Rightarrow 8p^2 \equiv 8 \pmod{32}$

Now, $48n+1 \equiv 1 \pmod{32}$ if n is even & $48n+1 \equiv 17 \pmod{32}$ if n is odd.

When n is even, $RHS \equiv 8 \cdot 1 \equiv 8 \pmod{32}$

When n is odd, $RHS \equiv 17 \cdot 8 \equiv 8 \pmod{32}$

But $LHS \equiv 24 \pmod{32}$

Here is the contradiction.

Case 1b : $p^2 \equiv 9 \pmod{16}$

- Now, $p^2 = 16k^2 + 24k + 9$
- $\Rightarrow k$ is even.
- $\Rightarrow p^2 = 16(2k)^2 + 24(2k) + 9$ (putting $2k$ in place of k as k is even)

- $\Rightarrow p^2 = 64k^2 + 48k + 9$
- $\Rightarrow p = 8k + 3$

Now, dividing both sides of equation (5) by 16 we get,
 $LHS \equiv -1 \pmod{16}$

Now, $24m+15 \equiv 15 \pmod{16}$ if m is even & $24m+15 \equiv 7 \pmod{16}$ if m is odd

When m is even, $RHS = (24m+15)p^2 \equiv 15 \cdot 9 \equiv 7 \pmod{16}$

When m is odd, $RHS = (24m+15)p^2 \equiv 7 \cdot 9 \equiv -1 \pmod{16}$
 $\Rightarrow m$ is odd.

Equation (5) becomes, $2^{(p-1)} - 1 = (48m+39)p^2$ (putting $2m+1$ in place of m as m is odd).....(9)

Now, dividing both sides of equation (7) by 32 we get,
 $LHS = 3^{(p-1)} - 1 = 3^{(8k+3-1)} - 1 = (3^{(8k)})(3^2) - 1 \equiv 1 \cdot 9 - 1 \equiv 8 \pmod{32}$

Now, we have, $p^2 = 64k^2 + 48k + 9$

- $\Rightarrow 8p^2 = 512k^2 + 384k + 72$
- $\Rightarrow 8p^2 \equiv 8 \pmod{32}$
- $\Rightarrow 48n+1$ must be $\equiv 1 \pmod{32}$
- $\Rightarrow n$ is even.

Equation (7) becomes, $3^{(p-1)} - 1 = 8(96n+1)p^2$ (putting $2n$ in place of n as n is even)(10)

Now, dividing both sides of equation (9) by 32 we get,
 $LHS \equiv -1 \pmod{32}$

$p^2 \equiv 9$ or $25 \pmod{32}$

Case 1b(i) : $p^2 \equiv 9 \pmod{32}$

- $\Rightarrow k$ is even.
- $\Rightarrow p^2 = 64(2k)^2 + 48(2k) + 9$ (putting $2k$ in place of k as k is even)
- $\Rightarrow p^2 = 256k^2 + 96k + 9$
- $\Rightarrow p = 16k+3$

Now, $48m + 39 \equiv 7 \pmod{32}$ if m is even and $\equiv 23 \pmod{32}$ if m is odd.
 $\Rightarrow m$ must be even.

Equation (9) becomes, $2^{(p-1)} - 1 = (96m+39)p^2$ (putting $2m$ in place of m as m is even).....(11)

Now, dividing both sides of equation (10) by 64 we get,
 $LHS = 3^{(p-1)} - 1 = 3^{(16k+3-1)} - 1 = (3^{(16k)})(3^2) - 1 \equiv 1 \cdot 9 - 1 \equiv 8 \pmod{32}$ (as (any odd power)¹⁶ $\equiv 1 \pmod{64}$)

We have, $p^2 = 256k^2 + 96k + 9$

- $\Rightarrow 8p^2 = 2048k^2 + 768p + 72$
- $\Rightarrow 8p^2 \equiv 8 \pmod{64}$

Now, $96n+1$ must be $\equiv 1 \pmod{64} \Rightarrow n$ is even.

Equation (10) becomes, $3^{(p-1)} - 1 = 8(192n+1)p^2$ (putting $2n$ in place of n as n is even).....(12)

Now, dividing both sides of equation (11) by 64 we get,
 $LHS \equiv -1 \pmod{64}$

$p^2 \equiv 9$ or $41 \pmod{64}$

Case 1b(i)/(a) : $p^2 \equiv 9 \pmod{64}$

- $\Rightarrow k$ is even.
- $\Rightarrow p^2 = 256(2k)^2 + 96(2k) + 9$ (putting $2k$ in place of k as k is even)
- $\Rightarrow p^2 = 1024k^2 + 192k + 9$
- $\Rightarrow p = 32k + 3$

$96m+39 \equiv 7$ if m is odd and $\equiv 39$ if m is even $\pmod{64}$

According to our case, $96m+39$ must be $\equiv 7 \pmod{64}$

Because then, $RHS \equiv 9 \cdot 7 \equiv -1 \pmod{64}$

Equation (11) becomes, $2^{p-1} - 1 = (192m+135)p^2$ (putting $2m+1$ in place of m as m is odd).....(13)

Now, dividing both sides of equation (12) by 128 we get,
LHS = $3^{p-1} - 1 = 3^{(32k+3)-1} - 1 = (3^{32k})(3^2) - 1 \equiv 1 * 9 - 1 \equiv 8 \pmod{128}$ (as (any odd number)³² $\equiv 1 \pmod{128}$)

We have, $p^2 = 1024k^2 + 192k + 9$
 $\Rightarrow 8p^2 = 8192k^2 + 1536k + 72$
 $\Rightarrow 8p^2 \equiv 72 \pmod{128}$

Now, $192n+1 \equiv 1$ if n is even and $\equiv 65$ if n is odd (mod 32)
We see that in both the cases, RHS $\equiv 72 \pmod{128}$

Here is the contradiction.

Case 1b(i)/(b) : $p^2 \equiv 41 \pmod{64}$
 $\Rightarrow p^2 = 256(2k+1)^2 + 96(2k+1) + 9$
 $\Rightarrow p^2 = 1024k^2 + 1216k + 361$
 $\Rightarrow p = 32k+19$

Now, dividing both sides of equation (11) by 64 we get,
LHS $\equiv -1 \pmod{64}$
 $p^2 \equiv 41 \pmod{64}$
 $\Rightarrow 96m+39$ must be $\equiv 39 \pmod{64}$ (as $41 * 39 \equiv -1 \pmod{32}$)
 $\Rightarrow m$ is even.

Equation (11) becomes, $2^{p-1} - 1 = (192m+39)p^2$ (putting $2m$ in place of m as m is even) (14)

Now, dividing both sides of equation (12) by 128 we get,
LHS = $3^{p-1} - 1 = 3^{(32k+19)-1} - 1 = (3^{32k})(3^{18}) - 1 \equiv 1 * 73 - 1 \equiv 72 \pmod{128}$

We have, $p^2 = 1024k^2 + 1216k + 361$
 $\Rightarrow 8p^2 = 8192k^2 + 9728k + 2888$
 $\Rightarrow 8p^2 \equiv 72 \pmod{128}$
 $\Rightarrow 192n+1$ must be $\equiv 1 \pmod{128}$
 $\Rightarrow n$ is even.

Equation (12) becomes, $3^{p-1} - 1 = 8(384n+1)p^2$ (putting $2n$ in place of n as n is even)(15)

Now, dividing both sides of equation (14) by 256 we get,
LHS $\equiv -1 \pmod{256}$

We have $p^2 = 1024k^2 + 1216k + 361$
 $\Rightarrow p^2 \equiv 169$ or 233 or $297 \pmod{256}$

Now, $192m+39 \equiv 231$ or 167 or $103 \pmod{256}$
We see that in this way the cases will go on increasing the problem giving ultimately no solution. So we can conclude that there is no prime p which satisfy $2^{p-1} \equiv 1 \pmod{p^2}$ and $3^{p-1} \equiv 1 \pmod{p^2}$ simultaneously.

17 tips with proof to solve problems on number theory :

1. (Any odd number)² $\equiv 1 \pmod{4}$

Proof : Let a be any odd number.

$\Rightarrow a = 2n+1$
 $\Rightarrow a^2 = (2n+1)^2$
 $\Rightarrow a^2 = 4n^2 + 4n + 1$
 $\Rightarrow a^2 = 4n(n+1) + 1$
 $\Rightarrow a^2 \equiv 1 \pmod{4}$

Proved.

2. (Any odd number)² $\equiv 1 \pmod{8}$

Proof : Let a be any odd number.

$\Rightarrow a = 2n+1$
 $\Rightarrow a^2 = (2n+1)^2$
 $\Rightarrow a^2 = 4n^2 + 4n + 1$

$$\Rightarrow a^2 = 4n(n+1) + 1$$

Now if n is odd then $(n+1)$ is even; if n is even then $(n+1)$ is odd.

$\Rightarrow n(n+1)$ is divisible by 2.
 $\Rightarrow 4n(n+1)$ is divisible by 8
 $\Rightarrow a^2 = 4n(n+1) + 1 \equiv 1 \pmod{8}$

Proved.

3. (Any odd number)² $\equiv 1$ or $9 \pmod{16}$

We have already proved (any odd number)² $\equiv 1 \pmod{8}$

Let a be any odd number.

Then $a^2 = 8n+1$

If n is even then $8n$ is divisible by 16.

$$\Rightarrow a^2 = 8n + 1 \equiv 1 \pmod{16}$$

If n is odd then $8n = 8(2n+1) = 16n + 8$ (putting $2n + 1$ in place of n as n is odd)

$\Rightarrow 8(2n+1) = 16n+8 \equiv 8 \pmod{16}$
 $\Rightarrow a^2 \equiv 8(2n+1) + 1 \equiv 8 + 1 = 9 \pmod{16}$
 $\Rightarrow a^2 \equiv 1$ or $9 \pmod{16}$

Proved.

4. (Any odd number)⁴ $\equiv 1 \pmod{16}$

We have already proved, (any odd number)² $\equiv 1 \pmod{8}$

Let a be any odd number.

$\Rightarrow a^2 = 8n+1$
 $\Rightarrow a^4 = (8n+1)^2$
 $\Rightarrow a^4 = 64n^2 + 16n + 1$
 $\Rightarrow a^4 = 16(4n^2+1) + 1$
 $\Rightarrow a^4 \equiv 1 \pmod{16}$

Proved.

5. (Any odd number)² $\equiv 1$ or 9 or -7 or $-15 \pmod{32}$

We have already proved, (any odd number)² $\equiv 1$ or $9 \pmod{16}$

Let a be any odd number.

$$\Rightarrow a^2 = 16n+1 \text{ or } 16m+9$$

Taking $a^2 = 16n+1$.

If n is even then $16n$ is divisible by 32.

$$\Rightarrow a^2 = 16n+1 \equiv 1 \pmod{32}$$

If n is odd then $a^2 = 16(2n+1) + 1$ (putting $2n+1$ in place of n as n is odd)

$\Rightarrow a^2 = 32n + 17$
 $\Rightarrow a^2 \equiv 17 \pmod{32}$
 $\Rightarrow a^2 \equiv 32 - 15 \pmod{32}$
 $\Rightarrow a^2 \equiv -15 \pmod{32}$

Taking $a^2 = 16m+9$

If m is even, then $16m$ is divisible by 32.

$$\Rightarrow a^2 = 16m+9 \equiv 9 \pmod{32}$$

If m is odd then $a^2 = 16(2m+1) + 9$ (putting $2m+1$ in place of m as m is odd)

$\Rightarrow a^2 = 32m + 25$
 $\Rightarrow a^2 \equiv 25 \pmod{32}$
 $\Rightarrow a^2 \equiv 32 - 7 \pmod{32}$
 $\Rightarrow a^2 \equiv -7 \pmod{32}$

So, $a^2 \equiv 1$ or 9 or -7 or -15

Proved.

$$6. \text{ (Any odd number)}^4 \equiv 1 \text{ or } -15 \pmod{32}$$

We have already proved, $(\text{any odd number})^4 \equiv 1 \pmod{16}$

Let a be any odd number.

$$\text{Then } a^4 = 16n+1$$

If n is even then $16n+1$ is divisible by 32.

$$\Rightarrow a^4 = 16n+1 \equiv 1 \pmod{32}$$

If n is odd then $a^4 = 16(2n+1)+1$ (putting $2n+1$ in place of n as n is odd)

$$\Rightarrow a^4 = 32n+17$$

$$\Rightarrow a^4 \equiv 17 \pmod{32}$$

$$\Rightarrow a^4 \equiv 32 - 15 \pmod{32}$$

$$\Rightarrow a^4 \equiv -15 \pmod{32}$$

So, $a^4 \equiv 1 \text{ or } -15 \pmod{32}$

Proved.

$$7. \text{ (Any odd number)}^8 \equiv 1 \pmod{32}$$

We have already proved $(\text{any odd number})^4 \equiv 1 \pmod{16}$

Let a be any odd number.

$$\Rightarrow a^4 = 16n+1$$

$$\Rightarrow a^8 = (16n+1)^2$$

$$\Rightarrow a^8 = 256n^2 + 32n + 1$$

$$\Rightarrow a^8 = 32n(8n+1) + 1$$

$$\Rightarrow a^8 \equiv 1 \pmod{32}$$

Proved.

$$8. \text{ (Any odd number)}^2 \equiv 1 \text{ or } 9 \text{ or } 25 \text{ or } -15 \text{ or } 17 \text{ or } -7 \text{ or } -23 \text{ or } -31 \pmod{64}$$

We have already proved, $(\text{any odd number})^2 \equiv 1 \text{ or } 9 \text{ or } -7 \text{ or } -15 \pmod{32}$

$$\Rightarrow a^2 = 32n+1 \text{ or } 32m+9 \text{ or } 32p-7 \text{ or } 32q-15.$$

Taking $a^2 = 32n+1$

If n is even then $a^2 = 32(2n) + 1$ (putting $2n$ in place of n as n is even)

$$\Rightarrow a^2 = 64n + 1$$

$$\Rightarrow a^2 \equiv 1 \pmod{32}$$

If n is odd then $a^2 = 32(2n+1) + 1$ (putting $2n+1$ in place of n as n is odd)

$$\Rightarrow a^2 = 64n + 33 \pmod{64}$$

$$\Rightarrow a^2 \equiv 33 \pmod{64}$$

$$\Rightarrow a^2 \equiv 64 - 31 \pmod{64}$$

$$\Rightarrow a^2 \equiv -31 \pmod{64}$$

Taking $a^2 = 32m+9$

If m is even then $a^2 = 32(2m)+9$ (putting $2m$ in place of m as m is even)

$$\Rightarrow a^2 = 64m + 9$$

$$\Rightarrow a^2 \equiv 9 \pmod{64}$$

If m is odd then $a^2 = 32(2m+1) + 9$ (putting $2m+1$ in place of m as m is odd)

$$\Rightarrow a^2 = 64m + 41$$

$$\Rightarrow a^2 \equiv 41 \pmod{64}$$

$$\Rightarrow a^2 \equiv 64 - 23 \pmod{64}$$

$$\Rightarrow a^2 \equiv -23 \pmod{64}$$

Taking $a^2 = 32p-7$

If p is even then $a^2 = 32(2p) - 7$ (putting $2p$ in place of p as p is even)

$$\Rightarrow a^2 = 64p - 7$$

$$\Rightarrow a^2 \equiv -7 \pmod{64}$$

If p is odd then $a^2 = 32(2p+1) - 7$ (putting $2p+1$ in place of p as p is odd)

$$\Rightarrow a^2 = 64p + 25$$

$$\Rightarrow a^2 \equiv 25 \pmod{64}$$

Taking $a^2 = 32q - 15$

If q is even then $a^2 = 32(2q) - 15$

$$\Rightarrow a^2 = 64q - 15$$

$$\Rightarrow a^2 \equiv -15 \pmod{64}$$

If q is odd then $a^2 = 32(2q+1) - 15$ (putting $2q+1$ in place of q as q is odd)

$$\Rightarrow a^2 = 64q + 17$$

$$\Rightarrow a^2 \equiv 17 \pmod{64}$$

So, $a^2 \equiv 1 \text{ or } 9 \text{ or } 25 \text{ or } -15 \text{ or } 17 \text{ or } -7 \text{ or } -23 \text{ or } -31 \pmod{64}$

Proved.

$$9. \text{ (Any odd number)}^4 \equiv 1 \text{ or } 17 \text{ or } -31 \text{ or } -15 \pmod{64}$$

We have already proved $(\text{any odd number})^4 \equiv 1 \text{ or } -15 \pmod{32}$

Let a be any odd number.

$$\Rightarrow a^4 = 32n+1 \text{ or } 32m-15.$$

Taking, $a^4 = 32n+1$

If n is even then $a^4 = 32(2n)+1$ (putting $2n$ in place of n as n is even)

$$\Rightarrow a^4 = 64n+1$$

$$\Rightarrow a^4 \equiv 1 \pmod{64}$$

If n is odd then $a^4 = 32(2n+1)+1$ (putting $2n+1$ in place of n as n is odd)

$$\Rightarrow a^4 = 64n + 33 \pmod{64}$$

$$\Rightarrow a^4 \equiv 33 \pmod{64}$$

$$\Rightarrow a^4 \equiv 64 - 31 \pmod{64}$$

$$\Rightarrow a^4 \equiv -31 \pmod{64}$$

Taking, $a^4 = 32m - 15$

If m is even then $a^4 = 32(2m) - 15$ (putting $2m$ in place of m as m is even)

$$\Rightarrow a^4 = 64m - 15$$

$$\Rightarrow a^4 \equiv -15 \pmod{64}$$

If m is odd then $a^4 \equiv 32(2m+1) - 15$ (putting $2m+1$ in place of m as m is odd)

$$\Rightarrow a^4 \equiv 64m + 17$$

$$\Rightarrow a^4 \equiv 17 \pmod{64}$$

So, $a^4 \equiv 1 \text{ or } 17 \text{ or } -31 \text{ or } -15 \pmod{64}$

Proved.

$$10. \text{ (Any odd number)}^8 \equiv 1 \text{ or } -31 \pmod{64}$$

We have already proved $(\text{any odd number})^8 \equiv 1 \pmod{32}$

Let a be any odd number.

$$\Rightarrow a^8 = 32n+1$$

If n is even then $a^8 = 32(2n)+1$ (putting $2n$ in place of n as n is even)

$$\Rightarrow a^8 = 64n+1$$

$$\Rightarrow a^8 \equiv 1 \pmod{64}$$

If n is odd then $a^8 = 32(2n+1)+1$ (putting $2n+1$ in place of n as n is odd)

$$\Rightarrow a^8 = 64n+33$$

$$\Rightarrow a^8 \equiv 33 \pmod{64}$$

$$\Rightarrow a^8 \equiv 64 - 31 \pmod{64}$$

$$\Rightarrow a^8 \equiv -31 \pmod{64}$$

So, $a^8 \equiv 1$ or $-31 \pmod{64}$

Proved.

11. (Any odd number)⁸ $\equiv 1 \pmod{64}$

We have already proved, (any odd number)⁸ $\equiv 1 \pmod{32}$

Let a be any odd number.

$$\text{Then } a^8 = 32n+1$$

$$\Rightarrow a^{16} = (32n+1)^2$$

$$\Rightarrow a^{16} = 1024n^2+64n+1$$

$$\Rightarrow a^{16} = 64n(16n+1)+1$$

$$\Rightarrow a^{16} \equiv 1 \pmod{64}$$

Proved.

12. The square of any odd integer can be written as difference of square of two consecutive integers. The consecutive integers are of the form $2n(n-1)$ and $2n(n-1)+1$ where n is nth odd integer.

For example, 11 is 6th odd integer.

$$\text{Now, } 2n(n-1) = 2*6*(6-1) = 60$$

$$\text{Therefore, } 11^2 = 61^2 - 60^2$$

$$\text{or, } 11^2 + 60^2 = 61^2.$$

13. The square of any even integer can be written as either difference of two consecutive odd integers or two consecutive even integers. The consecutive odd/even integers are of the form n^2-1 and n^2+1 where n is n-th even integer considering 2 as first even integer.

For example, 8 is 4th even integer.

$$\text{Now } n^2-1 = 4^2-1 = 15 \text{ and } n^2+1 = 17$$

$$\text{Therefore, } 8^2 = 17^2 - 15^2$$

$$\text{or, } 8^2 + 15^2 = 17^2.$$

14. How to find Pythagorean triplet ?

1. Choose a composite number.
2. Now square it.
3. Now factorize it.
4. Now divide it in two factors such that both factors are either even or both are odd.
5. Now, find the middle number between the two.
6. Now find the difference between the two factors and divide it by 2.
7. Now, (original number)² + (number found in step 6)² = (middle number found in step 5)²

For example :

1. Lets take 14.
2. 196
3. $2*2*7*7$
4. $98*2$

$$5. 50$$

$$6. (98-2)/2 = 48$$

$$7. 14^2 + 48^2 = 50^2$$

15. Generalization of Pythagorean triplet finding method for equation : $A_1^2 + A_2^2 + \dots + A_n^2 = B^2$.

We have, $14^2 + 48^2 = 50^2$ from previous example.

$$\Rightarrow 14^2 + 48^2 + 120^2 = 50^2 + 120^2 = 130^2$$

So, we have, $14^2 + 48^2 + 120^2 = 130^2$

With this process continuing I am sure one can find the solution of

$$a^2 + b^2 + c^2 = d^2$$

And hence...

..

..

..

$$A_1^2 + A_2^2 + \dots + A_n^2 = B^2.$$

16. Only square numbers have odd number of factors.

Proof : Whenever a number divides a number a quotient appears.

\Rightarrow There is always an even number of factor for any number.

What if the quotient is same as the divider.

This case appears only in case of square numbers.

Let a be any number.

Now if we divide a^2 by a then the quotient is also a.

\Rightarrow In case of divider is a the number of factor is 1.

Rest all appears as two numbers : one is divider and another is quotient.

\Rightarrow There is even number of factors + 1 (for a)

\Rightarrow There is always odd number of factors of any square number.

Proved.

17. The odd number table to handle problems on prime number.

Let p be any odd number.

We will form a table of column 3 and infinite rows of odd numbers as below :

p	p+2	p+4
p+6	p+8	p+10
p+12	p+14	p+16
p+18	p+20	p+22
p+24	p+26	p+28
p+30	p+32	p+34
p+36	p+38	p+40
p+42	p+44	p+46
p+48	p+50	p+52
p+54	p+56	p+58
p+60	p+62	p+64
p+66	p+68	p+70
p+72	p+74	p+76
p+78	p+80	p+82
p+84	p+86	p+88
p+90	p+92	p+94
p+96	p+98	p+100
.....		

.....

Properties of this table :

- 1) All the numbers of any one column is divisible by 3.
- 2) The numbers which are divisible by q (q is prime) occurs in any column after q numbers in that column. For example if q is 5. Then the numbers which are divisible by 5 occurs after 5 rows in the same column. For example, if $p+50$ is divisible by 5 then $p+80$ will be the next number, in the same column, which is divisible by 5.

Conjecture

If a problem can be understood with knowledge set A then it can be solved with knowledge set A , where A is any subset of a given subject.

REFERENCES

- [1] Halberstam, H.; Richert, H.-E. Sieve methods. London Mathematical Society Monographs, No. 4. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974.
- [2] Havil, Julian, Gamma, Exploring Euler's constant. With a foreword by Freeman Dyson. Reprint of the 2003 edition [MR1968276]. Princeton Science Library. Princeton University Press, Princeton, NJ, 2009.
- [3] H. Iwaniec, Almost-primes represented by quadratic polynomials. *Invent.Math.* 47 (1978), no. 2, 171-188.
- [4] Dominic Klyve, Explicit Bounds on Twin Primes and Brun's Constant, A Thesis Submitted to the Faculty in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics
- [5] Edmund Landau, Elementary number theory. Translated by J. E. Goodman. Chelsea Publishing Co., New York, N.Y., 1958.
- [6] E. Landau, Collected works, Thales Verlag, Essen, 1987.
- [7] Leveque, Fundamentals of Number Theory
- [8] Thomas R. Nicely, Enumeration to 1014 of the Twin Primes and Brun's Constant, *Virginia Journal of Science*, Volume 46, Number 3, Fall 1996
- [9] Niven, Ivan; Zuckerman, Herbert S.; Montgomery, Hugh L. An introduction to the theory of numbers. Fifth edition. John Wiley & Sons, Inc., New York, 1991.

Shubhankar Paul, Passed BE in Electrical Engineering from Jadavpur University in 2007. Worked at IBM as Manual Tester with designation Application Consultant for 3 years 4 months. Worked at IIT Bombay for 3 months as JRF. Published 2 papers at International Journal.