

# Classroom

---



*In this section of Resonance, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.*

P H Talapadur  
C/o Secretary  
School of Mathematics  
TIFR, Homi Bhabha Road  
Mumbai 400 005, India.

## The Twin Prime Problem

### Introduction

If two consecutive odd numbers are prime numbers, then they are called twin primes. Whether there are infinitely many twin primes is an open question. There are several old and new results which give a necessary and/or sufficient condition for the existence of infinitely many twin primes. Many of them are interesting although not one of them is of enough practical value to answer the question either way. After recalling some of the prominent ones, we proceed to give another criterion.

### Clement's Criterion

In 1949, Clement proved the following criterion:

*Let  $n \geq 2$ . Then,  $n, n + 2$  are primes if, and only if,  $4((n - 1)! + 1) + n \equiv 0 \pmod{n + 2}$ .*

**Proof.** If the congruence holds, then  $n \neq 2, 4$  and so  $(n - 1)! + 1 \equiv 0 \pmod{n}$  which forces  $n$  to be a prime.

Also  $4(n - 1)! + 4 + n \equiv 4(n - 1)! + 2 \equiv 0 \pmod{n + 2}$ . Multiplying by  $n(n + 1)$  and rewriting, we get  $4((n - 1)! + 1) + (n + 2)(2n - 2) \equiv 0 \pmod{n + 2}$  which forces  $n + 2$  to be prime.

### Keywords

Probability model, binomial distribution, expected value, optimisation.



Conversely, if  $n, n + 2$  are primes, then  $n \neq 2$  and

$$(n - 1)! + 1 \equiv 0 \pmod{n}$$

$$(n + 1)! + 1 \equiv 0 \pmod{n + 2}$$

But  $n(n + 1) = (n + 2)(n - 1) + 2$ ; so the last congruence gives  $2(n - 1)! + 1 \equiv 0 \pmod{n + 2}$ . Let us write  $2(n - 1)! + 1 = k(n + 2)$ . Then, the congruence  $(n - 1)! \equiv -1 \pmod{n}$  would give  $2k + 1 \equiv 0 \pmod{n}$  i.e.,  $2k \equiv -1 \pmod{n}$ . Substituting this in  $4(n - 1)! + 2 = 2k(n + 2)$ , we get  $4(n - 1)! + 2 \equiv -(n + 2) \pmod{n(n + 2)}$ . In other words, we have  $4(n - 1)! + 4 + n \equiv 0 \pmod{n(n + 2)}$ , the congruence that we wanted to establish.

Another interesting result due to Sergusov (1971) and Leavitt & Mullin (1981) is :

$n = p(p + 2)$  with both  $p$  and  $p + 2$  primes if, and only if,  $\phi(n)\sigma(n) = (n - 3)(n + 1)$ .

Here,  $\phi(n)$  is Euler's totient function which counts the number of natural numbers until  $n$  which are coprime to  $n$  and,  $\sigma(n)$  is the sum of the divisors of  $n$ .

For a few other elementary criteria which address the twin prime conjecture, the reader may consult [1].

### Brun's Constant

The series  $\sum \frac{1}{p}$  over all primes diverges to infinity. See [2] for a proof of infinitude of primes based on this idea. We not only know that the reciprocal series of primes diverges but we also know how 'fast' it diverges. Indeed, the finite sum  $\sum_{p \leq x} \frac{1}{p}$  behaves asymptotically (i.e., as  $x \rightarrow \infty$ ) exactly like the function  $\log \log x$ . One of the cornerstones of (analytic) number theory is the so-called 'prime number theorem' which asserts that the number of primes  $\pi(x)$  until  $x$  grows asymptotically like  $\frac{x}{\log x}$ .

Having said this, it will come as a surprise that the series  $\sum (\frac{1}{p} + \frac{1}{p+2})$  over all the twin primes  $p, p + 2$  converges



to a number between 1.9 and 2. This was proved by V Brun in 1919 using the so-called Brun sieve and the sum is now known as Brun's constant. Brun showed that the corresponding function  $\pi_2(x)$  which counts the primes  $p$  until  $x$  for which  $p + 2$  is also prime, grows *at the most* as fast as  $\frac{x}{(\log x)^2}$ . However, as we notice, this is only an upper bound and does not say anything at all about the existence or nonexistence of infinitely many twin primes.

There are conjectures in analytic number theory which, if true, would imply that the above upper bound is indeed the correct asymptotic order of  $\pi_2(x)$ . The interested reader may consult the book [3] for a proof of Brun's theorem.

### Maria Suzuki's Criterion

Very recently (in [4]), Maria Suzuki has obtained the following elementary reformulation of the twin prime conjecture. This is the following:

*If all primes  $p$  which are congruent to 1 mod 6 are, from some stage onwards, of the form  $36ab + 6a - 6b + 1$  for some nonnegative integers  $a, b$ , then the number of twin primes is finite.*

Using this, she proves the criterion:

*There are infinitely many twin primes if, and only if, there are infinitely many  $n$  which 'cannot' be expressed as  $6|ab| + a + b$  for any integers  $a, b$ .*

This is also just an existential criterion and one does not know how to make practical use of it.

### A Criterion involving Binomial Coefficients

Now, we give another elementary criterion for the existence of infinitely many twin primes. Our criterion is founded on the following simple idea:

**Lemma.**  $n > 1$  is prime  $\Leftrightarrow n \mid \binom{n}{r}$  for all  $1 \leq r < n$ .



**Proof.** It is obvious for prime  $p$  that  $p \mid \binom{p}{r}$  for all  $1 \leq r < p$ . Thus, we assume that  $n$  is composite and show that for a prime divisor  $p$  of  $n$ ,  $n$  does not divide  $\binom{n}{p}$ .

Write  $n = p^r m$  with  $r \geq 1$  and  $(p, m) = 1$ . Now  $\frac{\binom{n}{p}}{n} = \frac{(n-1)\cdots(n-p+1)}{p(p-1)\cdots 1}$  cannot be an integer as  $p$  does not divide the numerator. This proves the lemma.

Therefore, we have:

**Theorem.** *Let  $m > 3$  and  $m + 2$  be two consecutive odd numbers. Then, both are primes if, and only if,  $m(m + 2)$  divides each of the binomial coefficients  $\binom{m+2}{r}$ ;  $3 \leq r \leq m - 1$ .*

**Proof.** Suppose first that  $m, m + 2$  are primes. Since  $m + 2$  is prime, it divides each of the binomial coefficients occurring in the statement. Further, for the same reason,  $m$  divides each of  $\binom{m}{r}$ ;  $1 \leq r \leq m - 1$ . Using the binomial identity  $\binom{n}{r} + \binom{n}{r+1} = \binom{n+1}{r+1}$ , we find that  $m$  divides each of  $\binom{m+1}{r}$ ;  $2 \leq r \leq m - 1$ . Using the identity once more, we have that  $m$  divides each of the binomial coefficients  $\binom{m+2}{r}$ ;  $3 \leq r \leq m - 1$ . Therefore, since  $m$  and  $m + 2$  are coprime,  $m(m + 2)$  itself divides all these binomial coefficients.

Conversely, suppose that  $m(m + 2)$  divides  $\binom{m+2}{r}$ ;  $3 \leq r \leq m - 1$ . Now, as  $m + 2$  is odd, it divides  $\binom{m+2}{2}$  also. Hence, the lemma shows that  $m + 2$  must be prime. Moreover, since  $m$  is odd, both  $\binom{m+1}{2}$  and  $\binom{m}{2}$  are multiples of  $m$ . Using the above basic binomial identity (now we view it as the expression  $\binom{n}{r+1} = \binom{n+1}{r+1} - \binom{n}{r}$ ), we find that  $m$  divides  $\binom{m+1}{r}$ ;  $3 \leq r \leq m - 1$ . Using it once more, we obtain the fact that  $m$  divides  $\binom{m}{r}$ ;  $3 \leq r \leq m - 1$ . Once again, the lemma implies that  $m$  has to be a prime. This proves the theorem.

**Remark.** We notice that the set of binomial coefficients occurring in the statement of the theorem can be



replaced by the smaller set  $\binom{m+2}{r}$ ;  $3 \leq r \leq (m+1)/2$ . This is in view of the evident relation  $\binom{n}{r} = \binom{n}{n-r}$ .

We can use the Pascal triangle to obtain the following variant of the theorem.

**Theorem'** *Let  $m > 3$  be an odd number. Then, both  $m$  and  $m + 2$  are primes if, and only if,  $m(m + 2)$  divides each of the binomial coefficients*

$$\binom{m+2}{3}, \binom{m+3}{4}, \binom{m+4}{5}, \dots, \binom{2m-2}{m-1}.$$

**Proof.** We recall (see the figure) that the basic binomial identity simply means in Pascal's triangle that in any horizontal row, the sum of two adjacent terms equals the term below (and in between) them. Now, if  $m(m + 2)$  divides the binomial coefficients

$$\binom{m+2}{3}, \binom{m+3}{4}, \binom{m+4}{5}, \dots, \binom{2m-2}{m-1}.$$

These are the terms appearing diagonally on the left corner of the triangle. Considering the difference between two consecutive terms on this diagonal gives us the fact that  $m(m + 2)$  divides all the terms of the next diagonal just above it. Proceeding in this manner, the whole triangle can be exhausted. Thus, by the theorem that we just proved,  $m, m + 2$  must be primes.

Conversely, if  $m, m + 2$  are primes, then  $m(m + 2)$  divides the top row from which once again it is clear that it divides each term of this triangle. In particular, it divides the left corner terms.

### Suggested Reading

- [1] P Ribenboim, **A new book of prime number records.**
- [2] S Shirali, *Resonance*,
- [3] E Landau, **Analytic number theory.**
- [4] M Suzuki, **American Mathematical Monthly, Vol.107, 2000.**



$$\begin{array}{cccccccc}
 \binom{m+2}{3} & & \binom{m+2}{4} & & \binom{m+2}{5} & \dots & \binom{m+2}{m-3} & & \binom{m+2}{m-2} & & \binom{m+2}{m-1} \\
 & \binom{m+3}{4} & & \binom{m+3}{5} & & \dots & & \binom{m+3}{m-2} & & \binom{m+3}{4} & \\
 & & \ddots & & & & & & \ddots & & \\
 & & & \binom{2m-4}{m-3} & & \binom{2m-4}{m-2} & & \binom{2m-4}{m-1} & & & \\
 & & & & \binom{2m-3}{m-2} & & \binom{2m-3}{m-1} & & & & \\
 & & & & & \binom{2m-2}{m-1} & & & & & 
 \end{array}$$

