The Prime Ordeal

B Sury

After a long stint (1981–1999) at TIFR, Bombay, B Sury moved to ISI, Bangalore.

Prime numbers have fascinated mankind through the ages. In fact, one may think that we know all about them. However, this is not so! One does not know the answers to many basic questions on primes. We shall concentrate here mainly on questions and discoveries whose statements are elementary and accessible. Right at the end, we mention a result whose statement is simple but whose proof uses rather sophisticated mathematics. Even here, we do not try to be exhaustive. The subject is too vast for that to be possible.

Numbers in their prime
for no reason or rhyme
show up at a rhythm
with probability 1/logarithm.
If this is a law they knew,
they also break quite a few
but that is not a crime!

Keywords
Primes, Carmichael numbers, Giuga's conjecture, Bell numbers, prime number theorem, AKS algorithm.

1. Introduction

We start with the first major discovery about primes, which is the proof by Euclid's school that there are infinitely many prime numbers. Euclid's proof of the infinitude of primes will eternally remain beautiful no matter what advances modern mathematics makes. In spite of its simplicity, it still retains quite a bit of mystery. For instance, it is unknown as yet whether the product of the first few primes added to 1 takes a prime value infinitely often. It is even unknown whether it takes a composite value infinitely often! Do you see the mystery? What is the first time we get some composite number? Does anyone know the answer already? Anyway, let me tell you that $2.3.5.7.11.13 + 1$ is not a prime.

Actually, it is often the case that for any sequence of natural numbers which does not obviously take only composite values, the question as to whether it does take infinitely many prime values remains unanswered. Here are some examples (the $p_1, p_2, \ldots$ are prime numbers):

(i) $\quad p_1 p_2 \cdots p_n + 1,$

(ii) $p_1 p_2 \cdots p_n - 1$,
(iii) $n! + 1$,
(iv) $n! - 1$,
(v) $2^n - 1$,
(vi) $2^n + 1$,
(vii) $n^2 + 1$,
(viii) $f(n)$ for any polynomial of degree ≥ 2 such that there is no k dividing all the values $f(r), r \in \mathbf{Z}$.

Of course, in (v), it is obviously necessary that n itself be prime, and in (vi), a necessary condition is that n is a power of 2. As for (vii), it was proved by a contemporary mathematician Henryk Iwaniec in 1978 using some advanced mathematics that infinitely many numbers of the form $n^2 + 1$ can be expressed as a product of at most 2 primes. Note that the condition in (viii) cannot be weakened; for instance, if we merely say that all the coefficients of f be not divisible by any k, it is not sufficient. Indeed, $f(x) = x(x + 1)$ is a counterexample. That the sequence in the last example takes infinitely many prime values was conjectured by Viktor Bouniakowsky in the 19th century. In contrast to the last example, the degree one case is known to take infinitely many prime values – this is the famous theorem of Lejeune Dirichlet on primes in arithmetic progressions. Incidentally, here is a little exercise : If we make the (apparently weaker) conjecture that under the hypothesis of example (viii), every such f takes ONE prime value, it is actually equivalent to asserting that each such f takes infinitely many prime values!

Here is another issue of importance – in cryptography, for example. Given a natural number n, how does one recognize whether it is prime or not ? This is of crucial importance in many modern cryptosystems where the belief is that it is comparatively much easier (computationally) to answer this question than to factorize a given number. Basically, the idea would be to unearth properties of prime numbers which terize them (that is,

It was proved by a contemporary mathematician Henryk Iwaniec in 1978 using some advanced mathematics that infinitely many numbers of the form $n^2 + 1$ can be expressed as a product of at most 2 primes.

Given a natural number n, how does one recognize whether it is prime or not? This is of crucial importance in many modern cryptosystems where the belief is that it is comparatively much easier (computationally) to answer this question than to factorize a given number.

One website in German translated 'the little theorem of Fermat' as 'the small sentence of Fermat'! It is even funnier when we recall that Fermat was a judge who did pass sentences at times!

would not hold for even a single composite number). One such fundamental property (which is an easy exercise) is that a natural number $n > 1$ is prime if, and only if, n divides $(n-1)!+1$. This is known as Wilson's congruence. Another such property is that any prime p divides the binomial coefficients $\binom{p}{r}$ for each r in the range $0 < r < p$. That this is untrue for every composite number is again a nice little exercise.

Using the above property of primes, one can prove by induction on n that $n^p - n$ is a multiple of p for every n. Equivalently, if p does not divide n, then p divides $n^{p-1} - 1$. This is known as the little theorem of Fermat.

Interestingly, I found that one website in German translated 'the little theorem of Fermat' as 'the small sentence of Fermat' ! It is even funnier when we recall that Fermat was a judge who did pass sentences at times!

At this point, it is better to stop and point out the answer to a question which would have crossed the minds of many people. *Is there a 'formula' for the n-th prime?* Indeed, there are many formulae for primes! However, they are all worthless in a practical sense; that is, one cannot hope to computationally produce primes by such formulae. However, later we do talk about a recent algorithm by three Indians which tells us in polynomial time whether a given number is prime or not. Here is a 'formula' for primes based on Wilson's congruence. Put $f(x,y) = \frac{1}{2}\{1 + \frac{x-y}{|x-y|}\}$ if $x \neq y$, and $f(x,x) = 0$. Note that $f(x,y)$ is simply 1 or 0 according as to whether $x > y$ or $x \leq y$. Put $\pi(n) = 1 + \sum_{i=3}^{n}\{(i-2)! - i[(i-2)!/i]\}$ for $n \geq 3$ and $\pi(1) = 0, \pi(2) = 1$. This counts the number of primes up to n. Then, the n-th prime p_n is given by the formula :

$$p_n = 1 + \sum_{i=1}^{2^n} f(n, \pi(i)).$$

After some thought, we see that the formula, although

perfectly valid, is of no practical use in finding the n-th prime. A somewhat better formula was given several years ago by an Indian named J M Gandhi.

2. Carmichael Numbers: 'Carm'posites in Prime Clothing

Some avatar of Fermat's little theorem is used in most primality tests even today. But, unfortunately Fermat's little theorem does not characterize primes ! It does happen for some composite n that n divides $a^{n-1}-1$ for some a co-prime to n. In the terminology of cryptography, one says that n is a pseudo-prime to the base a and that a is a strong liar for n. Worse happens – there are, indeed, infinitely many numbers (known as Carmichael numbers after Robert Carmichael) n such that n divides $a^{n-1}-1$ for every a co-prime to n. The smallest such number is 561. The proof of the infinitude of the Carmichael numbers (as recently as 1994) also showed that there are at least $n^{2/7}$ such numbers $\leq n$ provided n is sufficiently large. The proof used deep, modern-day mathematics. In this article, I will concentrate on two conjectures (one made in 1950 and the other made in 1990) which aim to characterize primes. Ironically, they have turned out to be equivalent! As the conjectures involve Carmichael numbers also, we first prove a elementary criterion due to Theodor Korselt which characterises Carmichael numbers.

The proof of the infinitude of the Carmichael numbers (as recently as 1994) also showed that there are at least $n^{2/7}$ such numbers $\leq n$ provided n is sufficiently large.

In what follows, we will be using the following notations. We will say $a \equiv b \bmod m$ when $a-b$ is a multiple of m. These congruences have a calculus quite similar to equality. Namely, if $a \equiv b \bmod m$ and $c \equiv d \bmod m$ (same m, of course), then $a+b \equiv c+d$ and $ab \equiv cd \bmod m$.

Theorem. *A composite number n is a Carmichael number if, and only if, n is square-free and, for each prime divisor p of n, the number $p-1$ divides $n-1$.*

Proof. We shall assume and use the following fact which was first proved by Gauss. For any prime number p, there exist positive integers $a < p$ and $b < p^2$ which have 'orders' $p-1$ and $p(p-1)$ in the following sense:

When $a^r \equiv 1 \bmod p$, then $p-1$ divides r, and

when $b^s \equiv 1 \bmod p^2$, then $p(p-1)$ divides s.

(It should be noted that neither of these statements is trivial to prove although they are about two hundred years old.)

Now, first let $n = p_1 p_2 \cdots p_r$ be a square-free number such that for each $i \leq r$, the number $p_i - 1$ divides $n-1$. Evidently, for every a co-prime to n, a is co-prime to each p_i. Thus, one has by Fermat's little theorem that $a^{p_i - 1} \equiv 1 \bmod p_i$. So, $a^{n-1} = (a^{p_i-1})^* \equiv 1 \bmod p_i$. In other words, p_i divides $a^{n-1} - 1$ for each $i \leq r$. Thus, $n = p_1 p_2 \cdots p_r$ itself divides $a^{n-1} - 1$. This shows that n is a Carmichael number.

Conversely, let n be a Carmichael number. If p is a prime dividing n, consider a natural number a of 'order' $p-1 \bmod p$. We claim that we can always choose such an a which is co-prime to n.

First, if a is co-prime to n, then by hypothesis, $a^{n-1} \equiv 1 \bmod n$, which implies $a^{n-1} \equiv 1 \bmod p$, and thus $p-1$ divides $n-1$. If $(a, n) > 1$, then look at the set of primes $p = p_1, \cdots, p_k$ which divide n but not a. Consider $a + p_1 \cdots p_k$ in place of a. Evidently, $a + p_1 \cdots p_k$ is co-prime to n. Moreover, it is of the form $a + pd$, and so, its 'order' mod p is the same as that of a.

Now, let p^2 divide n for some prime p, if possible. Let b be of order $p(p-1) \bmod p^2$. If b is co-prime to n, then $b^{n-1} \equiv 1 \bmod n$ which gives $b^{n-1} \equiv 1 \bmod p^2$ which again implies that $p(p-1)$ divides $n-1$. Thus p divides $(n-1)$, an impossibility because p divides n. So, n must be square-free if b can be chosen co-prime

to n. But, if $(b, n) > 1$, then once again we look at the set of primes $p = p_1, p_2, \cdots, p_k$ which divide n but not b. Then $b + p_1^2 p_2 \cdots p_k$ is co-prime to n and has the same order mod p^2 as b has, namely, $p(p-1)$.

The proof is complete.

We end with an easy exercise:

Suppose $n = p_1 \cdots p_r$ is a Carmichael number and $m \equiv 1$ mod L where $L = LCM$ of $p_1 - 1, \cdots, p_r - 1$. If $q_i = 1 + m(p_i - 1)$ are all primes, then $N = q_1 \cdots q_r$ is also a Carmichael number.

3. 'Nava' Giuga and Long 'Agoh'

Let us start with the first of the 2 conjectures we wish to discuss. If p is a prime, then clearly

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \mod p.$$

Giuseppe Giuga conjectured in 1950 that this characterises primes; that is,

Conjecture (Giuga 1950):

$\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \mod n \Rightarrow n$ *is prime.*

As he showed, the conjecture can be reformulated as follows:

Theorem. $\sum_{k=1}^{n-1} k^{n-1} \equiv -1$ *mod n if, and only if, for each prime divisor p of n, both p and $p-1$ divide $\frac{n}{p} - 1$.*

Equivalently, a composite number n satisfies $\sum_{k=1}^{n-1} k^{n-1} \equiv -1$ mod n if, and only if, it is a Carmichael number such that $\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p}$ is a natural number.

In the above statement, the sum and the product run over primes and $p|n$ denotes 'p divides n'.

Proof. Note that for any prime p, we have $\sum_{k=1}^{p-1} k^r \equiv -1$ or 0 mod p according as whether $p-1$ divides r or not.

Therefore, for a prime p dividing n, we have

$$\sum_{k=1}^{n-1} k^{n-1} \equiv \sum_{k=1}^{p-1} k^{n-1} + \sum_{k=p+1}^{2p-1} k^{n-1} + \cdots + \sum_{k=n-p+1}^{n-1} k^{n-1}$$

$\equiv -n/p$ or $0 \bmod p$ according as to whether $p-1$ divides $n-1$ or not.

To prove the theorem, first suppose $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \bmod n$. Then, for every prime $p|n$, we have $(p-1)|(n-1)$ and $\frac{n}{p} \equiv 1 \bmod p$. Note that $(p-1)|(n-1)$ implies $p-1$ divides $p(\frac{n}{p}-1) = n-p = (n-1)-(p-1)$ and so $(p-1)$ also divides $\frac{n}{p}-1$.

Conversely, suppose $p(p-1)$ divides $\frac{n}{p}-1$ for each prime divisor p of n. First of all, this forces n to be square-free. Now, for any prime $p|n$, we also have $\sum_{k=1}^{n-1} k^{n-1} \equiv -\frac{n}{p} \equiv -1 \bmod p$. This proves the first statement. The second assertion is easy. If $p(p-1)|(\frac{n}{p}-1)$ for each prime $p|n$, we have that n is a Carmichael number (in particular, it is square-free). Then,

$$\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} = \sum_{p|n} \frac{1}{p} - \frac{1}{n}.$$

So, multiplying by n, we must show that n divides $\sum_{p|n} \frac{n}{p} - 1$. Thus, we need to show that each prime divisor of n divides $\sum_{p|n} \frac{n}{p} - 1$. This follows because each prime divisor p of n satisfies $p|(\frac{n}{p}-1)$ and $p|\frac{n}{q}$ for $p \neq q$.

Giuga's conjecture amounts to the assertion that there is no Giuga number which is also a Carmichael number.

Remarks. A composite number n such that $p|(\frac{n}{p}-1)$ for each prime $p|n$, is called a *Giuga number*. Equivalently, $\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \in \mathbf{N}$. Then, Giuga's conjecture amounts to the assertion that there is no Giuga number which is also a Carmichael number. As of today, only 12 Giuga numbers are known and all of them have sum minus product (of reciprocals of prime divisors) equal to 1. The numbers $30, 858, 1722$ are Giuga numbers. Until now, no odd Giuga numbers have been found. Any possible

odd Giuga number must have at least 10 prime factors because the sum $\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{23}+\frac{1}{29}+\frac{1}{31} < 1$.

The smallest Giuga sequence where the sum minus product is >1, has 59 bfactors!

In an article in Volume 103 of the *American Mathematical Monthly* of 1996, David Borwein, Jonathan Borwein, Peter Borwein and Roland Girgensohn propose that a good way to approach Giuga's conjecture is to study Giuga numbers in general. More generally, they define a *Giuga sequence* to be a finite sequence $n_1 < n_2 < \cdots < n_r$ of natural numbers such that $\sum_{i=1}^{r} \frac{1}{n_i} - \prod_{i=1}^{r} \frac{1}{n_i}$ is a natural number. Thus, a Giuga sequence consisting of primes gives rise to a Giuga number, viz., to the product of those primes. The smallest Giuga sequence where the sum minus product is > 1, has 59 factors! Here is an easy method to produce arbitrarily long Giuga sequences.

Theorem. *Suppose $n_1 < n_2 < \cdots < n_r$ is a Giuga sequence satisfying $n_r = \prod_{i=1}^{r-1} n_i - 1$. Then, the sequence $n_1 < n_2 < \cdots < \tilde{n}_r, \tilde{n}_{r+1}$ is a Giuga sequence whose sum minus product is the same, where $\tilde{n}_r = \prod_{i=1}^{r-1} n_i + 1, \tilde{n}_{r+1} = \tilde{n}_r \prod_{i=1}^{r-1} n_i - 1$.*

Starting with a sequence like $2, 3, 5$ say, this gives Giuga sequences of arbitrary lengths whose sum minus product is 1. The proof is a simple exercise of manipulation. In fact, one has the following nice result:

Proposition.

Look at a sequence $n_1 < n_2 < \cdots < n_r$ which satisfies $\sum_{i=1}^{r} \frac{1}{n_i} + \prod_{i=1}^{r} \frac{1}{n_i} = 1$. For example, the sequence $n_1 = 2, n_k = \prod_{i<k} n_i + 1$ is such a sequence. Then, $n_1 < n_2 < \cdots < n_k < n_{k+1} := \prod_{i=1}^{k} n_i - 1$ is a Giuga sequence.

The sequence 2,3,7, 43, ... where each term is 1 more than the product of all the previous terms also proves the inifinitude of primes.

The proof is straightforward verification.

Incidentally, note that the sequence given as an example above proves the infinitude of primes because the pairwise GCD $(n_i, n_j) = 1$ for all $i \neq j$.

Fermat's last theorem can be proved for a prime p (in an easy, natural manner) provided p does not divide the numerators of B_2, B_4, ..., B_{p-3}.

The Giuga conjecture involved the sums $\sum_{k=1}^{n-1} k^{n-1}$. In general, a sum of the form $\sum_{k=1}^{r-1} k^n$ can be 'easily' evaluated in terms of certain rational numbers called the Bernoulli numbers. These ubiquitous numbers turn up in such diverse situations that it is impossible to mention most of them here. Suffice it to say that Fermat's last theorem can be proved for a prime p (in an easy, natural manner) provided p does not divide the numerators of $B_2, B_4, \cdots, B_{p-3}$. How are the B_n's defined? Often, they are defined by means of the generating series $\sum_{n=0}^{\infty} B_n \frac{z^n}{n!} = \frac{z}{e^z-1}$. The equality can be simplified to give the recursion $\sum_{r=0}^{n} \binom{n+1}{r} B_r = 0$ and using $B_0 = 1$, one can determine them. It turns out that $B_1 = -\frac{1}{2}$ and $B_r = 0$ for all odd $r > 1$. More generally, the Bernoulli polynomials are defined as $B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$; it is of degree n. Note that $B_n(0) = B_n$.

It is an elementary exercise to show that

$$\sum_{k=1}^{r-1} k^n = \frac{1}{n+1}(B_{n+1}(r) - B_{n+1}).$$

In this manner, the sums of powers can be expressed in terms of Bernoulli numbers.

The von Staudt–Clausen theorem says that the denominator of B_{2k} is precisely $\prod_{(p-1)|2k} p$; note this is square-free. In particular, it makes sense to talk about $(2k+1)B_{2k} \bmod 2k+1$; note that for $(a,b) = 1$, one talks of $\frac{1}{a} \bmod b$ – it is the unique $c \bmod b$ for which $ac \equiv 1 \bmod b$.

The von Staudt–Clausen theorem says that the denominator of B_{2k} is precisely $\prod_{(p-1)|2k} p$;

For example, $15B_{14} = 15 \times \frac{7}{6} = \frac{35}{2} \equiv 35 \times 8 \equiv -5 \bmod 15$.

$13B_{12} = 13 \times \frac{-691}{2.3.5.7.13} \equiv -1 \bmod 13$.

Looking at such data, Takashi Agoh conjectured in 1990 (conjectured by 'Agoh' not long 'ago'!):

$nB_{n-1} \equiv -1$ mod n if, and only if, n is prime.

A few years later (in 1994) he used the von Staudt–Clausen theorem and showed that his conjecture is actually equivalent to Giuga's conjecture. Then, in September 2004, Bernd Kellner gave a new proof of the equivalence of the two conjectures (which gives another proof of the von Staudt–Clausen theorem) based on the following result :

Theorem (Kellner). *If $m > 1$, and n is even, then*

$$\sum_{k=1}^{m-1} k^n \equiv -\sum_{p|m,(p-1)|n} \frac{m}{p} \equiv mB_n \mod m.$$

The proof is elementary but rather involved and we do not discuss it here. This theorem allows for a further reformulation of the Giuga and Agoh conjectures, and may now be called:

Conjecture (Agoh–Giuga–Kellner):

An integer $n \geq 2$ is prime if, and only if,

$$\sum_{p|n,(p-1)|(n-1)} \frac{1}{p} - \frac{1}{n} \in \mathbf{Z}.$$

4. All's Bell

In this section, we discuss a conjecture due to Djuro Kurepa which can be stated in elementary language but the proof which appeared in 2004 involves some sophisticated mathematics. Those who have learnt Galois theory would be able to appreciate it but others can also get a flow of the argument. Of course, the fact that an elementary statement may require very sophisticated methods should not come as a surprise. A case in point is Fermat's Last Theorem (FLT) which says that for an odd prime p, there do not exist nonzero integers x, y, z such that $x^p + y^p + z^p = 0$. The question of Kurepa doesn't quite require the kind of sophisticated mathematics required in FLT though. Kurepa conjectured in

The n-th Bell number P_n is the number of ways of writing an n-element set as unions of non-empty subsets. We see that $P_1 = 1$, $P_2 = 2$, $P_3 = 5$, $P_4 = 15$, $P_5 = 52$, etc.

1971 that for any odd prime p, the sum $K_p := \sum_{n=0}^{p-1} n!$ is not a multiple of p. Of course $K_2 = 2$. This is, of course, not a characterisation of primes; for example, $K_4 = 10$. The proof (only in 2004) of Kurepa's conjecture due to D Barsky and B Benzaghou involves the so-called Bell numbers. One way of defining the Bell numbers is as follows. The n-th Bell number P_n is the number of ways of writing an n-element set as unions of non-empty subsets. We see that $P_1 = 1, P_2 = 2, P_3 = 5, P_4 = 15, P_5 = 52$ etc. (There is a lot of combinatorics involving the Bell numbers.) From combinatorial considerations, one can prove that $P_{n+1} = \sum_{k=0}^{n} \binom{n}{k} P_k$, where we have written P_0 to stand for 1. From this, it is easy to prove (analogously to the proof for Bernoulli numbers) that the generating function for P_n's is given by

$$F(x) = \sum_{n=0}^{\infty} P_n x^n =$$

$$\sum_{n=0}^{\infty} \frac{x^n}{(1-x)(1-2x)\cdots(1-nx)} \qquad (1)$$

The Kurepa question can be formulated in terms of the Bell numbers easily. It turns out using some elementary combinatorics that $P_{p-1} \equiv \sum_{n=0}^{p-2} n!$ modulo p. Thus, since K_p is the sum of $(p-1)!$ with the right hand side above, Kurepa's conjecture amounts to the statement that $P_{p-1} \not\equiv 1$ modulo p because $(p-1)! \equiv -1$ modulo p. The idea of the proof of Kurepa's conjecture is to consider what is known as the Artin–Schreier extension $\mathbf{F}_p[\theta]$ of the field $\mathbf{F}_p$ of p elements, where θ is a root (in the algebraic closure of $\mathbf{F}_p$) of the polynomial $x^p - x - 1$. This is a cyclic Galois extension of degree p over $\mathbf{F}_p$. Note that the other roots of $x^p - x - 1$ are $\theta + i$ for $i = 1, 2, \cdots, p-1$. The reason that this field extension comes up naturally is as follows. The generating series $F(x)$ of the Bell numbers can be evaluated modulo p; this means one computes a 'simpler' series $F_p(x)$ such that $F(x) - F_p(x)$ has all coefficients multiples of p. Since Kurepa's

It turns out using some elementary combinatorics that $P_{p-1} \equiv \sum_{n=0}^{p-2} n!$ modulo p.

conjecture is about the Bell numbers P_{p-1} considered modulo p, it makes sense to consider $F_p(x)$ rather than $F(x)$. Reading the equality (1) modulo p, one gets

$$F_p(x) = \sum_{n=0}^{p-1} \sum_{i\geq 0} \frac{x^{ip+n}}{(1-x)\cdots(1-(ip+n)x)}$$

$$= \sum_{n=0}^{p-1} \sum_{i\geq 0} \frac{x^n}{(1-(ip+1)x)\cdots(1-(ip+n)x)} \frac{x^{ip}}{(1-x)\cdots(1-ipx)}$$

$$\equiv \sum_{n=0}^{p-1} \sum_{i\geq 0} \frac{x^n}{(1-(ip+1)x)\cdots(1-(ip+n)x)} \left(\frac{x^p}{(1-x)\cdots(1-px)}\right)^i$$

modulo p. Therefore,

$$F_p(x) = \frac{\sum_{n=0}^{p-1} x^n(1-(n+1)x)\cdots(1-(p-1)x)}{1-x^{p-1}-x^p}$$

on simplification. Notice that θ^{-1} is a root of the polynomial $1-x^{p-1}-x^p$ above. Thereafter, doing some algebra in the field extension $\mathbf{F}_p[\theta]$ of $\mathbf{F}_p$ expresses the various Bell numbers P_n modulo p as

$$P_n \equiv -\mathrm{Tr}(\theta^{c_p})\mathrm{Tr}(\theta^{n-c_p-1}),$$

where Tr denotes the trace to $\mathbf{F}_p$ from the Artin–Schreier extension $\mathbf{F}_p[\theta]$ and $c_p = \frac{p^p-t_p}{p-1}$ and $t_p = \frac{p^p-1}{p-1}$. Thereafter, the analysis of the properties of the trace functions implies that if $P_{p-1}-1$ were to be zero modulo p, then θ^{c_p} would be zero, which is absurd since θ is not zero, as it generates a degree p extension. This was one instance of proving an elementary statement on primes which needs some sophisticated mathematics.

The n-th Bell number P_n modulo a prime p can be expressed in terms of the trace function on a certain field containing F_p.

Recently, three Indians stunned the world with the discovery of a polynomial-time deterministic primality testing algorithm.

5. AKS – A Case of Indian Expertise

Having said that there are no (practically) 'nice' formulae for primes, and having also said that producing large primes is a basic requirement in fields like cryptography, how does one reconcile one with the other? The fact is that there are many probabilistic algorithms to certify primes with very high probability. We shall not discuss them but we raise the mathematical question as to whether there are deterministic algorithms to decide in reasonable computational time whether a given number is prime or not. Until very recently, no deterministic algorithm was known which was polynomial-time and which could detect every prime. Recently, three Indians (Manindra Agrawal, a professor of computer science at IIT Kanpur and his BTech students Neeraj Kayal and Nitin Saxena) stunned the world with the discovery of a polynomial-time deterministic primality testing algorithm. We mention very briefly the Agrawal–Kayal–Saxena algorithm. Most algorithms start with Fermat's little theorem and apart from other shortcomings, are also infeasible at first glance because of having to compute p coefficients in order to check the validity of the congruence $(x-a)^p \equiv x^p - a \bmod p$. The basic idea of the AKS algorithm is to make it feasible by evaluating both sides modulo a polynomial of the form $x^r - 1$. Their algorithm would take $O(r^2 log^3 p)$ time to verify $(x-a)^p \equiv x^p - a \bmod x^r - 1$ in $F_p[x]$. As there are composites also which satisfy this congruence, one has to choose r and a suitably. One general comment to note is that it is far easier to test a polynomial over F_p for irreducibility than to test primality of a natural number. In a nutshell, here is the AKS algorithm:

AKS algorithm to check primality of n

Step I

Check if n is a perfect power; if not go to the next step.

Step II

Find a prime number $r = O(log^6 n)$ such that $r-1$ has a prime divisor $q > 4\sqrt{r}\log n$, where q divides the order of n mod r.

Step III

With r as above, check for each $a \leq 2\sqrt{r}\log n$, if

$$(x-a)^n \equiv x^n - a \mod x^r - 1 \quad in \quad (Z/nZ)[x].$$

If the congruence is not satisfied for some a, declare that n is composite. If it is satisfied for all a, declare n prime.

6. Sundries

We will finish with a few more remarks about primes. We mentioned Bouniakowsky's conjecture which asserts the infinitude of prime values. Can a polynomial take only prime values? It is again an easy, elementary exercise to prove that there is no nonconstant polynomial in some variables $x_1, \cdots, x_r$ which takes only prime values at all integers. However, it is a deep consequence of the solution of Hilbert's 10th problem by Hilary Putnam, Martin Davis, Julia Robinson and Yuri Matiyashevich that there exist polynomials $f(x_1, \cdots, x_r)$ over integers such that the set of positive values taken by f equals the set of prime numbers! Of course, the polynomials do take negative values as well as certain prime values more than once. Indeed, one can take f to be of degree 25 and r to be of 26. This expresses the fact that the set of prime numbers is a Diophantine set.

Bertrand stated that there is a prime among $n+1, n+2, \cdots, 2n$. This is known as Bertrand's postulate and it was proved first by Chebychev and there are many simpler proofs. Incidentally, a generalisation of Bertrand's postulate is a theorem of Sylvester which asserts that in any sequence $n+1, n+2, \cdots, n+r$ with $n \geq r$, there is a number which is divisible by a prime $> r$.

There is no nonconstant polynomial in some variables x_1, ..., x_r which takes only prime values at all integers. However, it is a deep consequence of the solution of Hilbert's 10th problem by Putnam, Davis, Julia Robinson and Matiyashevich that there exist polynomials $f(x_1, ..., x_r)$ over integers such that the set of positive values taken by f equals the set of prime numbers!

The twin prime problem (whether there are infinitely many primes p with $p+2$ also prime) is still open. Brun proved that the series of reciprocals of twin primes converges.

Of course, the twin prime problem (whether there are infinitely many primes p with $p + 2$ also prime) is still open. Brun proved that the series of reciprocals of twin primes converges. Note that the series of reciprocals of all primes is divergent, as proved by Euler. Indeed, $\sum_{p \leq x} \frac{1}{p}$ behaves asymptotically like the function log log x for x tending to infinity.

Then, the Goldbach conjecture (asserting that every even number > 2 is a sum of two primes) is also open; Vinogradov proved using the Hardy–Ramanujan circle method that every sufficiently large odd number is a sum of three primes. The prime number theorem proved in the beginning of the 20th century shows that the 'prime counting function' $\pi(x)$ which counts the number of primes up to x, behaves asymptotically like the function $\frac{x}{\log\ x}$ as x tends to infinity. An equivalent formulation is to say that the product of all the primes up to some x is asymptotically like e^x. Here, and elsewhere, one means by the statement $f(x)$ is asymptotically like $g(x)$ that the ratio $f(x)/g(x)$ approaches 1 as x tends to infinity. One can deduce from the prime number theorem that the n-th prime is approximately of size n log$n$ for large n. That is, very roughly speaking, the probability that a given n is prime is $\frac{1}{\log\ n}$.

Vinogradov proved using the Hardy-Ramanujan circle method that every sufficiently large odd number is a sum of three primes.

In connection with the fact we mentioned about Gauss showing that for each prime p, there is an integer a whose order mod p is $p - 1$, here is a famous conjecture due to E Artin. He conjectured that each natural number a which is not a square is the order mod p for infinitely many primes p. It is also open.

Shortly before his death, Paul Erdos, in collaboration with Takashi Agoh and Andrew Granville, showed that any large composite n ($n \geq 400$ would do) satisfies

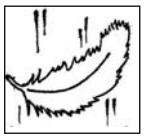
$$n \leq (\sum_{p \leq \sqrt{n}} \frac{1}{p})(\prod_{p \leq \sqrt{n}} p).$$

Using this, and nothing more than the Chinese remainder theorem, they showed that any prime n can be proved to be prime by expressing it as $n = N_1 + N_2 + \cdots + N_k$, where $p_1, \cdots, p_k$ are the first k primes and n is not divisible by any of them while each N_i is divisible by all the p_j with $j \neq i$ and not by p_i.

Address for Correspondence
B Sury
Statistics & Mathematics Unit
Indian Statistical Institute
Bangalore 560 059, India.
Email:surybang@gmail.com

Suggested Reading

[1] **P Ribenboim,** ***The new book of prime number records,*** **Springer-Verlag,** ***New York,*** **1996.**



"One of my favourite Baconian dreams is the possible connection between the theory of one-dimensional quasi-crystals and the theory of the Riemann zeta function. A 1-dimensional quasi-crystal is simply a nonperiodic arrangement of mass-points on a line whose Fourier transform is also an arrangement of mass-points on a line. We know that if the Riemann hypothesis is true, then the zeta function zeroes on the critical line are a quasi-crystal. This suggests a possible approach to the proof of the Riemann hypothesis."

– Freeman Dyson
(From Foreword of 'The Mathematical Century' by P Odifreddi published by Universities Press)