Which Positive Integers are Interesting?

B Sury

B Sury was in the School of Mathematics of TIFR Bombay from 1981 to 1999. Since 1999, he has been with the Indian Statistical Institute in Bangalore. His research interests are in algebra and number theory. He is the Karnataka co-ordinator for the Mathematical Olympiad Programme in India.

To Ramanujan, each number was a personal friend
in whose company, a lifetime he did spend.
Let us too begin this quest
to befriend numbers of interest.
A friend of a friend is a friend, may we not pretend ?!

Much has been written about the numbers π and e (which are themselves related by the beautiful identity $e^{i\pi} = -1$). However, if we are to think of only those interesting numbers which are positive integers, each of us comes with our own list. Indeed, the question "which positive integers are interesting?" is not well-defined. For, if n were the smallest uninteresting positive integer, it is interesting for that reason! Be that as it may, we identify some positive integers which have certain unique characteristics. In some of these examples, this number is unique with those characteristics and, in other cases, it is the smallest or the largest positive integer encountered where a pattern changes, although there may be other numbers with those characteristics. We also use our discussion as an excuse to unveil interesting mathematics behind some of these phenomena. The numbers are not necessarily arranged according to size.

30031

We are exposed to a beautiful thought process in school when we learn Euclid's proof of the infinitude of primes. Recall that the argument proceeds by observing that once we have gotten hold of the first few prime numbers, the number obtained by adding 1 to their product must have a prime factor which is necessarily larger than the previous ones. As this large number leaves remainder 1 on division by any of these primes, any of its prime

Keywords
Interesting positive integers, idoneal numbers, Carmichael numbers, Wieferich primes, Mersenne primes, Fermat primes, Bernoulli numbers, Kaprekar constant, Skewes constants, look-and-say sequence, Graham's constant.

factors is larger than the previous primes (and hence gives a new prime). The '*hope*' (if one may call it that) that this new number is itself a prime, leads quickly to disillusionment. The first example is $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$. I leave it to the reader to find the prime factors of this number. The intriguing question as to whether we do get primes infinitely often in this process is still open! The largest known prime P for which the product of all the primes until P is 1 less than a prime number is 42209.

In the above proof of infinitude of primes, we used the sequence of numbers of the form $2 \times 3 \times \cdots p_n + 1$. One could as well have used the sequence $2 \times 3 \times \cdots p_n - 1$ instead. In that case, $2 \times 3 \times 5 \times 7 - 1 = 11 \times 19$ is composite. Once again, it is unknown whether there are infinitely many primes of this form.

Let us pause for a moment to mull over an irony – *among all numbers of the form* $2 \times 3 \times \cdots p_n + 1$*, it is certain that either we have infinitely many primes or infinitely many composite numbers but, we do not know the answer to either of these at present!*

Among all numbers of the form $2 \times 3 \times \cdots p_n + 1$, it is certain that either we have infinitely many primes or infinitely many composite numbers but, we do not know the answer to either of these at present!

561

In cryptography, one of the recurring themes is the employment of the so-called Fermat little theorem – *If p is a prime number and a is an integer which is not a multiple of p, the number $a^{p-1} - 1$ is a multiple of p.*

The thought that this property might characterize all primes perishes soon. There are composite positive integers n such that every positive integer a co-prime to n possesses the property that $a^{n-1} - 1$ is a multiple of n. Such numbers – now known as Carmichael numbers – have a characterizing property. This is the property:

n is a Carmichael number if and only if it is square-free and each prime divisor p of n satisfies $p-1$ divides $n-1$.

Look at '*Prime ordeal*', *Resonance*, Vol.13, No.9, pp.866–881, 2008 for a proof.

The smallest Carmichael number is 561. Indeed, $561 = 3 \times 11 \times 17$ and $560 = 16 \times 5 \times 7$.

If a is relatively prime to 561, then $a^{560} - 1$ has factors $a^2 - 1, a^{10} - 1, a^{16} - 1$ which are multiples of $3, 11, 17$ respectively, by Fermat's little theorem.

15

For an integer $n > 1$, look at all its divisors including 1 and n. Let $s(n)$ denote the sum of all digits of all the divisors.

For example, $s(10) = 1 + 2 + 5 + (1 + 0) = 9$.

Let us iterate this process, that is, look at $s_2(n) = s(s(n)), s_3(n) = s(s_2(n))$ etc. In general, $s_{k+1}(n) = s(s_k(n))$.

For instance,

$$s_2(10) = s(9) = 1 + 3 + 9 = 13,$$

$$s_3(10) = s(13) = 1 + 1 + 3 = 5,$$

$$s_4(10) = s(5) = 1 + 5 = 6,$$

$$s_5(10) = s(6) = 1 + 2 + 3 + 6 = 12,$$

$$s_6(10) = s(12) = 1 + 2 + 3 + 4 + 6 + (1 + 2) = 19,$$

$$s_7(10) = s(19) = 1 + (1 + 9) = 11,$$

$$s_8(10) = s(11) = 1 + (1 + 1) = 3,$$

$$s_9(10) = 1 + 3 = 4,$$

$$s_{10}(10) = s(4) = 1 + 2 + 4 = 7,$$

$$s_{11}(10) = 1 + 7 = 8,$$

$$s_{12}(10) = 1 + 2 + 4 + 8 = 15,$$

$$s_{13}(10) = 1 + 3 + 5 + (1 + 5) = 15.$$

Therefore, after 12 iterations, 10 leads to 15; note that 15 is a fixed point for the function s. The beautiful thing that happens is that *every* positive integer $n > 1$ leads to 15 (so, 15 is like a black hole!).

15 is like a black hole – the 'sum of digits of all divisors' function iterated multiple times leads to 15 always.

The proof is very simple. The integer n has less than $2\sqrt{n}$ divisors (for each divisor $d < \sqrt{n}$, the divisor n/d is a divisor $> \sqrt{n}$). Any positive integer m has $[\log_{10}(m)]+1$ digits (if it has d digits, then $10^{d-1} \leq m < 10^d$ which gives, on taking logs to the base 10 what is asserted). As each digit is at most 9, the sum of the digits of m is at most $9([\log_{10}(m)] + 1)$. Therefore, n is a positive integer, for any divisor m of n, the sum of digits of m is at most $9([\log_{10}(n)] + 1)$ which gives

$$s(n) < 18\sqrt{n}([\log_{10}(n)] + 1).$$

Using this, we get $s(n) < n$ if $n \geq 10^4$.

For $n < 10^4$, we can use a better upper bound for the number of divisors of n to again deduce $s(n) < n$, if $n > 15$. We leave it to the ingenuity of the reader to complete by herself the argument for proving $s(n) < n$ when $n > 15$. In fact, it turns out that $s(n) < n$ excepting the six values $16, 18, 24, 28, 36, 48$. For these six values, we have $s_2(n) < n$ excepting 18 for which $s_4(18) < 18$. Thus, by descending, it follows that one needs to check only the numbers 2 to 15. This can be done by hand. In fact, for large n, the argument shows that $s_k(n) = 15$ where k is of the order of $\log \log n$.

15 again!

The number 15 has a claim to fame for another reason too. To motivate it, we recall a few things. Lagrange proved that every positive integer is expressible as a sum of four squares of integers. On the other hand, Gauss proved that a natural number n is expressible as a sum of three squares of integers if and only if it is NOT of the form $4^k(8r+7)$. Indeed, Gauss was so excited about

Ramanujan wrote down a list of 55 such 'positive forms' $ax^2+by^2+cz^2+dw^2$ for positive integers a, b, c, d which he claimed were the only ones of this form which take ANY positive integer value as the variables take integer values. His list was almost perfect – the one exception, $x^2 + 2y^2 + 5z^2 + 5w^2$, takes all values excepting the value 15(!).

this discovery which he noted in his mathematical diary as:

"EYPHKA! $\Delta + \Delta + \Delta = n$."

It is said that this was the single discovery that turned Gauss's mind into taking up mathematics as a career although he was a great philologist as well. Fermat stated the result that a positive integer > 1 is a sum of two squares of integers if and only if, in its prime decomposition, every prime of the form $4k + 3$ appears with an even power. Ramanujan wrote down a list of 55 such 'positive forms' $ax^2 + by^2 + cz^2 + dw^2$ for positive integers a, b, c, d which he claimed were the only ones of this form which take ANY positive integer value as the variables take integer values. His list was almost perfect – the one exception $x^2 + 2y^2 + 5z^2 + 5w^2$ takes all values excepting the value 15(!)

The mathematician and puzzlist John Conway came up with the following general observation which he proved along with his student William Alan Schneeberger. Consider

$$q(x_1, x_2, \cdots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

in n variables which takes only strictly positive values for all real values of the variables other than $x_i = 0$ for all i (one calls it *positive-definite*), where all a_{ij}'s are integers and $a_{ij} = a_{ji}$ for $i \neq j$. They proved the remarkable theorem that if this function takes all the integer values from 1 to 15 when we consider integer values for the variables x_i, then it takes ALL integer values! Conway–Schneeberger's proof was very involved and the mathematician Manjul Bhargava who received a Fields medal in 2014 (not for this work though) came up with a much simpler proof of this result and, what is more, vastly generalized the result. Thus, 15 is special for the reason that:

If $\sum_{i,j=1}^{n} a_{ij}x_ix_j$ is positive-definite, and a_{ij} are integers such that $a_{ij} = a_{ji}$, and if all integer values from 1 to 15 occur as values of the form when evaluated at suitable integers $x_1, x_2, \cdots, x_n$ then ALL poisitive integers occur as values. Moreover, 15 is the smallest such number.

1729

Any list of interesting positive integers is likely to include the taxicab number 1729. The story of Ramanujan coming up with the observation that 1729 is the smallest positive integer which is the sum of two perfect cubes in two different ways

$$10^3 + 9^3 = 1729 = 12^3 + 1^3,$$

is too well-documented to repeat here. However, what may not be so well-known is that 1729 is also a Carmichael number! Indeed, $1729 = 7 \times 13 \times 19$ and $1728 = 2^6 \times 3^3$. If a is coprime to 1729, then $a^{1728} - 1$ has factors $a^6 - 1, a^{12} - 1, a^{18} - 1$ which are multiples of $7, 13, 19$ respectively. So, by the criterion for Carmichael numbers mentioned during the discussion on 561 tells us that 1729 is a Carmichael number as well.

1806

This number has a very curious origin. It turns out to be the unique solution to the following problem.

Find all the even numbers n which satisfy

$$n = \prod_{p \text{ prime}, (p-1)|n} p.$$

Note that this means n includes ALL possible primes p for which $p - 1$ divides n. Thus, numbers like $n = 2, 6$ are ruled out.

1806 is the unique number *n* for which the numerator of the Bernoulli number B_n equals *n*.

Note that n must be square-free. One easily sees that $2, 3, 6, 7, 43$ divide n. Moreover, any such n must be divisible by these numbers (and perhaps others). Because of the hypothesis that a prime $p|n$ if, and only if,

495 has as much claim to fame as 6174, as it is the unique 3-digit Kaprekar number.

$(p-1)|n$, if a new prime factor of n arises, it must be one more than a product of smaller prime factors of n. However, the above numbers cannot give a new prime because the numbers

$$2\times 43+1, 2\times 3\times 43+1, 2\times 7\times 43+1, 2\times 3\times 7\times 43+1$$

are all composite. Therefore, the unique answer to the problem is the number $2.\times 3\times 7\times 43 = 1806$.

The discovery/appearance of this number is due to Kellner and is in the context of Bernoulli numbers – the numerator of the n-th Bernoulli number is the above product. Thus, 1806 is the unique number n for which the numerator of B_n equals n.

6174

This was a discovery by D Kaprekar in the 1940's. Starting with any 4-digit number (other than those with identical digits), apply the following transformation. Arrange the digits in the descending order, say $a > b > c > d$. Subtract the number with the digits $dcba$ from $abcd$ to obtain a 4-digit number (even if it is a 3-digit number, it should be regarded as a 4-digit number with 0 in the beginning). This transformation produces after finitely many iterations (at the most 7), the number 6174 which has come to be known as the Kaprekar constant. Note that 6174 is invariant under this transformation.

Before proving that every 4-digit number leads to 6174, we should first look for such constants among 2-digit and 3-digit numbers.

It is immediately seen that any 2-digit number (other than those with identical digits) leads to the cycle

$$09 \to 81 \to 63 \to 27 \to 45 \to 09.$$

The unique 3-digit Kaprekar constant is 495. So, 495 has at least as much claim to fame as 6174 (!)

Indeed, if abc is a 3-digit number with $a \geq b \geq c$ and $a > c$, and if we write

$$abc - cba = pqr,$$

then

$$10 + c - a = r, 10 - 1 + b - b = q, a - 1 - c = p.$$

Thus, $q = 9$ and $p + r = 9$. Hence, we need to check only the numbers

$$990, 891, 792, 695, 594,$$

each of which is seen to lead to 495 which is fixed by the iteration.

For a 4-digit number $abcd$ with $a \geq b \geq c \geq d$ and $a > d$, write the first iteration as $abcd - dcba = pqrs$.

Then, $10 + d - a = s$.

Now, if $b = c$, we have $r = 9+c-b = 9, q = 9+b-c = 9$ and $a - 1 - d = p$.

Thus, if $b = c$, we get $q = r = 9$ and $p + s = 9$ which leaves us to check only the five numbers

$$9990, 8991, 7992, 6993, 5994.$$

Each of these is easily seen to lead to 6174 which is fixed by the Kaprekar iteration.

Finally, in case $b > c$, we have

$$10+d-a = s, 10-1+c-b = r, b-1-c = q, a-d = p.$$

These imply $q + r = 8$ and $p + s = 10$. This means that one needs to check only the 25 numbers

$$p80s, p71s, p62s, p53s, p44s$$

for

$$(p, q) = (9, 1), (8, 2), (7, 3), (6, 4), (5, 5).$$

Each of these leads to 6174.

After this, we could go in two different directions – look at a general number d of digits or/and a general base b in place of 10. We mention a few results and leave it to the interested reader to investigate further.

For instance, if the base $b = 2r$, then the only 3-digit Kaprekar constant in base b has the digits $r-1, 2r-1$ and r – the proof of this generalization is the same as that of 495 in base 10.

It can be proved that there are no odd bases b admitting a 3-digit Kaprekar constant.

As for 4-digit Kaprekar constants, there is one in base 5 which is 3032 – so, once again this has as much claim to be of interest as 6174 has!

The other bases where 4-digit Kaprekar constants exist are of the form $b = 4^k \times 10$. In this base, the 4-digit Kaprekar constant has digits $6 \times 4^k, 2(4^k-1)+1, 8(4^k-1)+7$ and 4×4^k.

This can be proved similarly to the case of base 10.

There is no 5-digit Kaprekar constant in base 10. On the other hand, base 15 has the Kaprekar constant with the 5 digits

$$10, 4, 14, 9, 5.$$

There exist 5-digit Kaprekar constants in each base of the form $b = 6k + 3 \geq 15$; this is left to the interested reader to determine.

3435

This is sometimes known as the Ramachandra number. An eminent number theorist K Ramachandra observed when he was in college that his professor's car's registration number 3435 has the property

$$3435 = 3^3 + 4^4 + 3^3 + 5^5.$$

This is the only number > 1 with this property. However, this remains just a curiosity and does not seem to unveil any serious mathematics.

1848

We will see that 1848 is the largest of 65 numbers written down by Euler with a certain property. It is known that there could be at the most two larger numbers with that property. It is easy to show that if an odd number has a unique expression as a sum of two squares of positive integers $n = x^2 + y^2$ and, if x, y are coprime, then n must be a prime number. Euler generalized this property in order to obtain a primality criterion. He defined a positive integer m to be '*Idoneal*' or '*convenient*' ('Idoneus Numerus' in Latin) if it satisfies the property:

If an odd positive integer n admits a unique expression $n = x^2 + my^2$ with $x, y > 0$ and if, in addition, the GCD $(x, my) = 1$, then n must be prime.

Euler wrote down a list of 65 convenient numbers (the smallest 'inconvenient' number is 11) based on a criterion he obtained. The largest in his list is 1848. Until date, no bigger convenient number has been found. S Chowla was the first to prove in 1934 that there are only finitely many convenient numbers. This is based on deep methods (coming under the umbrella of class field theory) outside the scope of our discussion. Later, in 1973, it was shown by Weinberger that Euler could have missed at most two other convenient numbers. Indeed, assuming the truth of a deep unsolved problem known as the generalized Riemann hypothesis, it follows that there could be at the most one number missing in Euler's list.

Using the fact that 1848 is idonean, Euler observed that $18518809 = 197^2 + 1848(100)^2$ is a prime.

Using the fact that 1848 is idonean, Euler observed that $18518809 = 197^2 + 1848(100)^2$ is a prime.

An interesting question is, 'which numbers have all digits to be equal to 1 with respect to two different bases > 1'.

8191

We know that every positive integer can be represented in binary form (that is, in base 2) in terms of 0's and 1's. There is nothing sacrosanct (mathematically) about base 2 and, one may represent numbers in any base one wants to use. Notice that the number 31 has the base 2 expansion

$$(11111)_2$$

and the base 5 expansion

$$(111)_5.$$

So, it is natural to ask which natural numbers have all their digits to be equal to 1 with respect to *two different* bases > 1.

It was observed by Goormaghtigh nearly a century ago that 8191 has this property;

$$(111)_{90} = (1111111111111)_2.$$

In usual decimal (base 10) notation, this number is 8191.

The question can be posed in another form as follows. If $b_1 \neq b_2$ are two positive integers > 1, then the number with m ones in base b_1 is $1 + b_1 + b_1^2 + \cdots + b_1^{m-1} = \frac{b_1^m - 1}{b_1 - 1}$.

Therefore, we are asking if this number can consist of n one's in another base b_2.

This is equivalent to solving

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}$$

in natural numbers $x, y > 1$ for some $m, n > 2$.

The largest known solution is 8191 mentioned above. It is still unknown whether there are only finitely many solutions in all variables x, y, m, n. In fact, no other solutions is known.

1093

Fermat's last 'theorem' – asserting that the equation $x^n + y^n = z^n$ has no solutions in positive integers x, y, z when $n > 2$ – took 350 years to be justifiably called a theorem. However, there were several subjective results from the old times. One of them due to Wieferich showed that the first case of Fermat's last theorem holds good for a prime p for which $2^{p-1} - 1$ is not a multiple of p^2. That is, for such a prime p, the equation $x^p + y^p = z^p$ has no solutions in positive integers x, y, z coprime to p. If there were no such 'Wieferich primes', we would have a relatively elementary proof of (the first case of) Fermat's last theorem. However, there are Wieferich primes and 1093 is the smallest. The next is 3511. To this day, no others are known although on probabilistic grounds one expects asymptotically $\log\log(x)$ Wieferich primes until x as $x \to \infty$.

The relation of congruence modulo a positive integer is a very convenient way to express many divisibility statements. If m is a fixed positive integer, one calls two integers a and b to be congruent modulo m, if $a - b$ is a multiple of m (meaning $a - b = mc$ for some integer c). The notation $a \equiv b \bmod m$ is due to the great mathematician C-F Gauss who also discussed the notion in the first place. Congruence relation generalizes equality and, it is an easy exercise to check that it satisfies natural properties like:
$a \equiv b \bmod m$; $c \equiv d \bmod m$ implies

$$a + c \equiv b + d \; mod \; m \; , \; ac \equiv bd \; mod \; m.$$

Fermat's little theorem can be re-stated as the assertion: $a^{p-1} \equiv 1 \bmod p$ if p is a prime $a \not\equiv 0 \bmod p$.

Then, Wieferich's congruences are $2^{p-1} \equiv 1 \bmod p^2$ for $p = 1093, 3511$.

If 2 is replaced by some other positive integers, there are

1093 and 3511 are the only known Wieferich primes although on probabilistic grounds, one expects asymptotically log log (x) Wieferich primes not exceeding x as x goes to infinity.

Neither Mersenne primes nor Fermat primes can be Wieferich primes.

other examples when analogous congruences hold; viz.,

$$3^{10} \equiv \ 1 \ \ mod \ \ 11^2$$

$$7^4 \equiv \ 1 \ \ mod \ \ 5^2$$

$$31^6 \equiv \ 1 \ \ mod \ \ 7^2$$

To see that $2^{1092} - 1$ is a multiple of 1093^2, we proceed as follows.
Now $3^7 = 2187 = (2 \times 1093) + 1 = 2p + 1$, say.
Then $3^{14} \equiv 4p + 1 \bmod p^2$.
Also, $2^{14} = 16384 = 15p - 11$ which gives $2^{28} \equiv -330p + 121 \bmod p^2$.
So, $3^2 \times 2^{28} \equiv -1876p - 4 \bmod p^2$.
On dividing by 4, we have

$$3^2 \times 2^{26} \equiv -469p - 1 \ \ mod \ \ p^2.$$

Raising to the 7-th power, we have:
$3^{14} \times 2^{26\times 7} \equiv -(1 + 469p)^7 \equiv -(1 + 7 \times 469p) \bmod p^2$
$\equiv -(1+3283p) \equiv -(1+4p) \equiv -3^{14} \bmod p^2$ as observed above.
Hence $2^{26\times 7} \equiv -1 \bmod p^2$ which gives $2^{1092} = 2^{26\times 7\times 6} \equiv (-1)^6 \equiv 1 \bmod p^2$.

On the other hand, we show that a prime p which is either of the form $b^N + 1$ or of the form $1+b+b^2+\cdots+b^n$ for some b, *cannot* satisfy $b^{p-1} \not\equiv 1 \bmod p^2$.

In particular, we have the observation:

Neither Mersenne primes (that is, primes of the form $1 + 2 + 2^2 + \cdots + 2^{n-1}$), nor Fermat primes (that is, primes of the form $2^n + 1$) can be Wieferich primes.

More generally, we prove:

Let p be a prime whose expression in a base $b > 1$ is of the form

$$1 + b^k + b^{2k} + \cdots + b^{nk}$$

for some $n, k \geq 1$. Then,

$$b^{p-1} \equiv 1 + \frac{p-1}{(n+1)k}(b^k - 1)p \not\equiv 1 \mod p^2.$$

Here is the proof.

Now $p = 1 + b^k + \cdots + b^{nk} = \frac{b^{(n+1)k}-1}{b^k-1}$.
Now, p and $b^k - 1$ are relatively prime because p is a prime and

$$p \geq b^k + 1 > b^k - 1.$$

Since p divides $b^{(n+1)k} - 1$, the order of b mod p is a divisor of $(n+1)k$. If it were smaller, say mr, with $m|(n+1)$ and $r|k$, then either $m < n+1$ or $r < k$.
If $r < k$, then the assertion $b^{(n+1)r} \equiv 1 \mod p$ means p divides

$$(1 + b^r + \cdots + b^{nr})(b^r - 1).$$

Now, p and $b^r - 1$ are relatively prime because p is a prime and $p \geq b^k + 1 > b^r - 1$.
Hence $p = 1 + b^k + \cdots + b^{nk}$ divides $1 + b^r + \cdots + b^{nr}$, which is impossible as p is the bigger number.
Now, if $m < n+1$, then the condition $b^{mk} \equiv 1$ means p divides $1 + b^k + \cdots + b^{(m-1)k} = \frac{b^{(mk}-1}{b^k-1}$ as p and $b^k - 1$ are relatively prime because p is a prime and $p \geq b^k + 1 > b^k - 1$.
This is impossible, as $p = 1 + b^k + \cdots + b^{nk}$ is larger than $1 + b^k + \cdots + b^{(m-1)k}$.
We have shown that the order of b mod p is $(n+1)k$; hence, this order $(n+1)k$ divides $p-1$.
Now, raise $b^{(n+1)k} = 1 + p(b^k - 1)$ to the $\frac{p-1}{(n+1)k}$-th power. We have

$$b^{p-1} \equiv 1 + p(b^k - 1)\frac{p-1}{(n+1)k} \mod p^2.$$

Now, again the observation that p is relatively prime to $b^k - 1$ implies that p does not divide $(b^k - 1)\frac{p-1}{(n+1)k}$.

This completes the proof.

Let p be an odd prime and let x, y, z be integers such that $(p, xyz) = 1$ and $x^p + y^p \equiv z^p \bmod p^2$. Then, there exists a positive integer $a \leq (p-1)/2$ such that $(a+1)^p - a^p - 1 \equiv 0 \bmod p^2$. In particular, if none of the $(p-1)/2$ congruences hold, the first case of Fermat's last theorem holds.

In view of the observation above, *an elementary proof of the first case of Fermat's last theorem exists (thanks to Wieferich's criterion) for Mersenne primes and Fermat primes.*

Wieferich's criterion can be proved with a bit of knowledge of the Eisenstein reciprocity law which generalizes the so-called quadratic reciprocity law of Gauss (again!). This is somewhat outside the scope of our discussion. However, we can fortunately give an elementary result which is in the spirit of (but weaker than) Wieferich's criterion and gives a sufficient criterion for Fermat's last theorem to hold good.

Let p be an odd prime and let x, y, z be integers such that $(p, xyz) = 1$ and $x^p + y^p \equiv z^p \bmod p^2$. Then, there exists a positive integer $a \leq (p-1)/2$ such that $(a+1)^p - a^p - 1 \equiv 0 \bmod p^2$. In particular, if none of the $(p-1)/2$ congruences hold, the first case of Fermat's last theorem holds.

Proof. By Fermat's little theorem, $z \equiv z^p = x^p + y^p \equiv x + y \bmod p$.
As $(p, x) = 1$, there is an integer x' such that $xx' \equiv 1 \bmod p$ (viz., write $1 = pu + xx'$ for some x').
Note that since $z \equiv x + y \bmod p$, we have $zx' \equiv 1 + yx' \bmod p$.
Consider the integer $a \equiv yx' \bmod p$ with $1 \leq a \leq (p-1)/2$. Writing $a = yx' + pt$ and applying the binomial expansion, we have

$$a^p \equiv y^p (x')^p \ \ mod \ \ p^2.$$

Also, $a + 1 \equiv yx' + 1 \bmod p$ which gives, on raising to the p-th power and applying binomial theorem as before, that

$$(a+1)^p \equiv (yx')^p + 1 \equiv a^p + 1 \ \ mod \ \ p^2.$$

This proves the assertion.

Note that if the $(p-1)/2$ congruences in the statement above are replaced by the single congruence corresponding to $a = 1$, we have Wieferich criterion.

71

John Conway discovered an amazing fact. Start with any positive integer other than 22. Let us start with 1 say. Define the sequence which just reads out the number of times each chain of digits is repeated in turn. That is, after 1, we have 11 (meaning one 1) and after that we have 21 (to mean two 1's) and 1211 (to mean one 2, one 1) and 111221 (meaning one 1, one 2, two 1's) etc. In general, if $a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r}$ with $a_i \neq a_{i+1}$, then the next term of the sequence is defined to be

$$k_1 a_1 k_2 a_2 \cdots k_r a_r.$$

For example, the sequence starting from 1 is:

$$1, 11, 21, 1211, 111221, 312211,$$

$$13112221, 1113213211, 31131211131221, \cdots$$

If d_n is the number of digits in the n-th term, then Conway discovered the remarkable fact that the ratio d_{n+1}/d_n approaches a constant λ (called Conway's constant) which is the unique real root of the polynomial $x^{71} - x^{69} - 2x^{68} - x^{67} + 2x^{66} + 2x^{65} + x^{64} - x^{63} - x^{62} - x^{61} - x^{60} - x^{59} + 2x^{58} + 5x^{57} + 3x^{56} - 2x^{55} - 10x^{54} - 3x^{53} - 2x^{52} + 6x^{51} + 6x^{50} + x^{49} + 9x^{48} - 3x^{47} + 7x^{46} - 8x^{45} - 8x^{44} + 10x^{43} + 6x^{42} + 8x^{41} - 5x^{40} - 12x^{39} + 7x^{38} - 7x^{37} + 7x^{36} + x^{35} - 3x^{34} + 10x^{33} + x^{32} - 6x^{31} - 2x^{30} - 10x^{29} - 3x^{28} + 2x^{27} + 9x^{26} - 3x^{25} + 14x^{24} - 8x^{23} - 7x^{22} - 7x^{21} + 9x^{20} - 3x^{19} - 4x^{18} - 10x^{17} - 7x^{16} + 12x^{15} + 7x^{14} + 2x^{13} - 12x^{12} - 4x^{11} - 2x^{10} - 5x^9 + x^7 - 7x^6 + 7x^5 - 4x^4 + 12x^3 - 6x^2 + 3x - 6$ of degree 71. If this is remarkable, it is even more remarkable that every starting number (other than 22) leads to this same constant λ of degree 71. The proof is very involved and comes under the umbrella of what is now known as the cosmological theorem.

All numbers in the look-and-say sequence from the 8th one onwards arise from certain 92 basic strings.

I give a very rough explanation of this phenomenon for the sake of the more mathematically precocious reader among high school students. Some experimentation will tell us that all the numbers in this sequence from the 8th one onwards arise from certain basic strings of elements – 92 of them. In effect, these 92 'atoms' can be written down explicitly and all elements of the Conway sequence can be described in a sense through these 92 elements. Thus, each element of the sequence is a word in the 92 basic elements and *the number of digits* can be described recursively. This amounts to having a 92×92 matrix which describes the recursion. A well-known technique on recursion shows that the n-th term is expressible in terms of 'eigenvalues' of the matrix. These eigenvalues are solutions of a polynomial equation which is obtained from the matrix. In the case above, the polynomial has degree 71 and the ratios d_{n+1}/d_n approach the only positive real root of this polynomial – this is the λ mentioned above!

Skewes's Constants

The great mathematician C F Gauss conjectured at the age of 15, what is now called the prime number theorem. He conjectured that the number $\pi(x)$ of primes not exceeding a number x is asymptotically given by the logarithmic integral function $li(x) = \int_2^x \frac{dt}{\log\ t}$. Here, by 'asymptotically', we mean that the ratio $\pi(x)/li(x)$ approaches 1 as x grows unboundedly large. However, the inequality $\pi(x) < li(x)$ was seen to hold for values of x when these functions could be calculated. J E Littlewood proved in 1914 that the difference actually changes signs infinitely often. Hence, there is indeed a smallest natural number n for which $\pi(n) \geq li(n)$. But, this was an existential proof. Littlewood had a doctoral student named Skewes who, one day in 1933, presumably said "(Ex)Skewes me! Assuming the Riemann Hypothesis, I can show that there is a number N no larger than $10^{10^{10^{34}}}$ such that $\pi(N) \geq li(N)$".

Twenty years later, Skewes himself showed without assuming the Riemann Hypothesis, that there is a number M no larger than $10^{10^{10^{964}}}$ such that $\pi(M) \geq li(M)$. These two numbers have come to be known as Skewes's constants. The latest developments have brought the constants down to e^{728} although no explicit value of n is known for which $\pi(n) \geq li(n)$. In the above, we have used the phrase Riemann Hypothesis for an (perhaps the most important) open problem in mathematics.

Littlewood showed that the sign of $\pi(x) - li(x)$ changes infinitely often.

Graham's Constant G

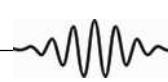
The number is so gigantic that additional notation is needed to write it down. This number arose as follows.

Consider a hypercube in n dimensions. This is the generalization of a square in 2 dimensions and a cube in 3 dimensions; it has 2^n vertices. If we join every vertex to every other one, we get what is known as a complete graph. R L Graham and B L Rothschild considered the following problem. If we colour each edge with one of two available colours, is it always true that there must exist a complete subgraph containing four coplanar vertices such that all its six edges are of the same colour?

This is not necessarily true for 3-dimensional cubes – we leave it to the reader to construct an example. On the other hand, Graham and Rothschild proved the existence of a complete, monochromatic subgraph containing four coplanar vertices in any colouring, if the dimension n is large enough. Until now, one does not know the minimal possible value of n with this property but the proof of Graham and Rothschild showed the existence of an n which is at the most a constant G known as Graham's constant. To define what G is, we introduce Knuth's up-arrow notation.

Graham's constant is the largest number that has appeared in a mathematical proof; it is so gigantic that additional notation is needed to write it down.

For positive integers a, b we already know the usual exponentiation a^b as a shorthand notation for multiplying a to itself b times. Knuth introduces the up-arrow no-



tation as: $a \uparrow b$ for a^b. Next, define

$$a \uparrow\uparrow b = \underbrace{a \uparrow (a \uparrow (a \uparrow (\cdots)))}_{b \text{ times}}.$$

For example, $4 \uparrow\uparrow 3 = 4^{(4^4)}$ while $3 \uparrow\uparrow 4 = 3^{(3^{(3^3)})} = 3^{(3^{27})}$ a much larger number. In fact, the former has about 154 digits whereas the latter has more than 10^{12} digits.

Now, the next stage is easy to define.

For positive integers a, b define

$$a \uparrow\uparrow\uparrow b = \underbrace{a \uparrow\uparrow (a \uparrow\uparrow (a \uparrow\uparrow (\cdots)))}_{b \text{ times}}.$$

More generally,

$$a \uparrow^n b = \underbrace{a \uparrow^{n-1} (a \uparrow^{n-1} (a \uparrow^{n-1} (\cdots)))}_{b \text{ times}},$$

where $\uparrow^k$ stands for $\underbrace{\uparrow\uparrow \cdots \uparrow}_{k \text{ times}}$.

In terms of these notations, Graham's constant $G = g_{64}$ where

$$g_1 = 3 \uparrow^4 3, g_2 = 3 \uparrow^{g_1} 3, \cdots, g_n = 3 \uparrow^{g_{n-1}} 3.$$

We cannot even have a reasonable comprehension of how big this number is but it has appeared in a mathematical proof; such is the *power* of the human mind!

Suggested Reading

[1] A video summary of the article created by the author can be accessed at https://www.youtube.com/watch?v=DRMkhsTD3Zc&authuser=0

Address for Correspondence
B Sury
Stat-Math Unit
Indian Statistical Institute
8th Mile Road
Bengaluru 560 059, India.
Email: sury@isibang.ac.in