NUMBER THEORY

UNIT 4 SOME SPECIAL NUMBERS

1. Introduction

In the previous units we have come across various properties of the integers. The theory is so rich that many variations are possible and many questions can be asked. One of the most famous problems in contemporary mathematics is the fascinating **Fermat's Last Theorem**, which we introduced in the previous unit.

As we remarked in the introduction, there are many different ways to classify integers, into primes and composites, according to divisibility, etc. In this unit we shall briefly look at some special types of numbers. We will also state some unsolved problems and conjectures.

2. Triangular Numbers

Definition 2.1. (Triangular number)

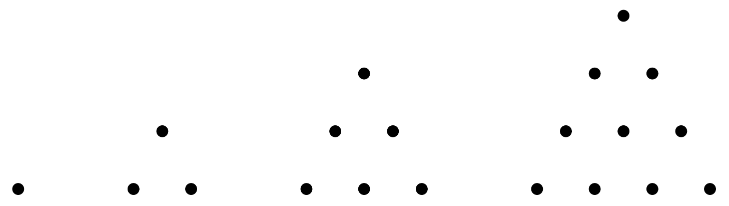
A **triangular number** is a number of the form

$$1+2+3+\cdots+n$$

where n is a positive integer.

Illustrations. The first three triangular numbers are 1, $1+2=3$ and $1+2+3=6$.

The triangular numbers are so called because of the following arrangement of dots which forms triangular arrays:



Using the formula for the sum of the terms of an arithmetic sequence, we see that the *n*-th triangular number is equal to

$$\frac{n(n+1)}{2}.$$

Example 2.1.

Prove that the sum of two consecutive triangular numbers is a perfect square.

Solution.

Consider the *n*-th and $(n+1)$ st triangular numbers. They are equal to

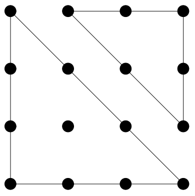
$$\frac{n(n+1)}{2} \text{ and } \frac{(n+1)(n+2)}{2}$$

respectively. Their sum is equal to

$$\frac{n(n+1)}{2}+\frac{(n+1)(n+2)}{2}=\frac{n+1}{2}\left[n+(n+2)\right]=(n+1)^2$$

which is a perfect square.

The fact that the sum of two consecutive triangular numbers is a perfect square can be illustrated geometrically as follows:



Example 2.2.

Prove that infinitely many triangular numbers are perfect squares.

Solution.

We want to find positive integers *n* for which

$$\frac{n(n+1)}{2}=k^2$$

for some positive integer *k*. Suppose such *n* exists, then replacing *n* by $4n^2+4n$, we have

$$\frac{(4n^2+4n)(4n^2+4n+1)}{2} = 4\times\frac{n(n+1)}{2}\times(4n^2+4n+1) = \left[2k(2n+1)\right]^2$$

which is also a perfect square. Now when $n=1$, we get the triangular number 1 which is a perfect square. Replacing n by $4n^2+4n$ successively, we get infinitely many triangular numbers which are perfect squares, with n = 1, 8, 288, 332928, …

3. Twin Primes

Definition 3.1. (Twin primes)

Two prime numbers which differ by 2 are said to be **twin primes**.

Illustrations. 5 and 7 are twin primes. 101 and 103 are twin primes.

The question of whether there are infinitely many twin primes remains an open problem. The largest twin primes known to date are

$$665551035\times 2^{80025}\pm 1,$$

which was discovered in 2000. Both numbers have 24099 digits.

Example 3.1.

The number 5 appears in two pairs of twin primes, since 3, 5 are twin primes, and 5, 7 are twin primes. Is there another number with the same property?

Solution.

The answer is no.

Suppose there is such a number p.

Then $p-2$ and p are twin primes, and p and $p+2$ are twin primes.

In other words, $p-2$, p and $p+2$ are all primes.

Note, however, that one of these numbers must be divisible by 3.

So if all of them are primes, then one of them must be equal to 3.

This is not possible unless $p = 5$.

4. Fermat Primes

Suppose $2^m + 1$ is a prime number for some positive integer *m*. What can we say about *m*? For example, can *m* be divisible by 3? Well, if $m = 3k$, then we have

$$2^m + 1 = 2^{3k} + 1 = \left(2^k + 1\right)\left(2^{2k} - 2^k + 1\right)$$

and so $2^m + 1$ is not prime. We leave it as an exercise to show that $2^m + 1$ is prime only if *m* is a power of 2.

In view of this, we have the following definition.

Definition 4.1. (Fermat number, Fermat prime)

A **Fermat number** is a number of the form

$$2^{2^n} + 1$$

for some non-negative integer *n*. If a Fermat number is prime, then it is called a **Fermat prime**.

Illustrations. $2^{2^0} + 1 = 2$, $2^{2^1} + 1 = 3$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$ and $2^{2^4} + 1 = 65537$ are all Fermat primes.

The Fermat numbers are so-called because Fermat once conjectured that all numbers of the form $2^{2^n} + 1$ are prime numbers, and this is illustrated above for the cases *n* = 0, 1, 2, 3, 4.

Unfortunately, these are the only known Fermat primes so far. In fact, we have

$$2^{2^5} + 1 = 641 \times 6700417,$$

so that $2^{2^5} + 1$ is not prime.

Example 4.1.

Let F_n denote the Fermat number $2^{2^n}+1$. Show that there are infinitely many *n* such that F_n+2 is not prime.

Solution.

We will show that $7 \mid F_n+2$ whenever *n* is odd.

Note that $2^3 \equiv 1$ (mod 7). When *n* is odd, $2^n \equiv (-1)^n = -1 \equiv 2$ (mod 3), so $2^{2^n} \equiv 2^2 = 4$ (mod 7).

It follows that $F_n+2=(2^{2^n}+1)+2 \equiv 0$ (mod 7).

Example 4.2.

Let F_n denote the Fermat number $2^{2^n}+1$. Show that for $n>1$, the unit digit of F_n is 7.

Solution.

When $n>1$, $2^n = 4k$ for some integer *k*.

Thus $2^{2^n}+1=2^{4k}+1=16^k+1\equiv 1^k+1=2$ (mod 5).

Since F_n is odd when $n>1$, its unit digit must be 7.

5. Perfect Numbers

Definition 5.1. (Perfect number)

A **perfect number** is a positive integer *n* whose sum of positive factors other than itself is equal to itself, i.e. the sum of the positive factors of *n* is equal to 2*n*.

Illustrations. 6 is a perfect number since $1+2+3=6$. 28 is also a perfect number since $1+2+4+7+14=28$.

Things are rarely perfect, and perfect numbers are rare. In fact, the next four perfect numbers already get enormously large: 496, 8128, 33550336, 8589869056. Whether there are infinitely many perfect numbers remains an open problem, but it can be shown (which we leave as an exercise) that if

$$1+2+2^2+\cdots+2^{k-1}=2^k-1$$

is prime, then $2^{k-1}(2^k-1)$ is a perfect number. Moreover, it has been proved that every *even* perfect number can be expressed in this form.

So far no odd perfect number is known, nor has it been proved that no odd perfect numbers exist.

Example 5.1.

(IMO 1998 HK Team Selection Test 2) Recall that *n* is perfect if the sum of the divisors of *n* is 2*n*. Suppose now *n* is an odd perfect number, show that *n* has at least 3 distinct prime factors.

Solution.

For positive integer *k*, let $\sigma(k)$ denote the sum of the positive factors of *k*.

Suppose *n* only has one prime factor, say $n=p^a$. Then we have

$$2=\frac{\sigma(n)}{n}=\frac{\sigma(p^a)}{p^a}=\frac{1+p+\cdots+p^a}{p^a}=1+\frac{1}{p}+\cdots+\frac{1}{p^a}<\frac{1}{1-\frac{1}{p}}=\frac{p}{p-1}<2,$$

which is a contradiction. Similarly, if *n* has only two prime factors, say $n=p^aq^b$, then

$$2=\frac{\sigma(n)}{n}=\frac{\sigma(p^a)\sigma(q^b)}{p^aq^b}=\frac{1+p+\cdots+p^a}{p^a}\cdot\frac{1+q+\cdots+q^b}{q^b}<\frac{1}{1-\frac{1}{p}}\cdot\frac{1}{1-\frac{1}{q}}\le\frac{1}{1-\frac{1}{3}}\cdot\frac{1}{1-\frac{1}{5}}=\frac{15}{8}<2,$$

which is again a contradiction. It follows that *n* must have at least three distinct prime factors.

6. Mersenne Primes

In the previous section, we remarked that if

$$1+2+2^2+\cdots+2^{k-1}=2^k-1$$

is prime, then $2^{k-1}(2^k-1)$ is a perfect number. Moreover, every even perfect number is of this form. Hence, searching for even perfect numbers is equivalent to searching for primes of the form 2^n-1.

We also remarked that whether there are infinitely many perfect numbers remains unknown. This essentially means that whether there are infinitely many primes of the form $2^n - 1$ is also unknown.

Definition 6.1. (Mersenne number, Mersenne prime)

A **Mersenne number** is a number of the form

$$2^n - 1$$

where *n* is a positive integer. If a Mersenne number is prime then it is called a **Mersenne prime**.

Illustrations. $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ and $2^7 - 1 = 127$ are all Mersenne primes.

Hence, if we can find a Mersenne prime, we can find a perfect number. In Section 4, we studied primes of the form $2^m + 1$, and remarked that it is prime only if *m* is a power of 2. By a similar reasoning, we can deduce that if $2^n - 1$ is prime, then *n* itself must be prime. The details are left as an exercise.

In the above illustrations we showed that $2^n - 1$ is prime for *n* = 2, 3, 5, 7. Some early mathematicians conjectured that $2^n - 1$ is prime whenever *n* is prime. This, unfortunately, is not true, for

$$2^{11} - 1 = 2047 = 23 \times 89$$

already provides a counterexample.

Till February 2003 only 39 Mersenne primes are known. The largest Mersenne prime known to date is $2^{13466917} - 1$, discovered in November 2001, and this corresponds to the perfect number

$$2^{13466916}(2^{13466917} - 1)$$

which is the largest perfect number known to date.

It might be interesting to note that the majority of known large primes are Mersenne primes. This is because there exists an efficient algorithm, known as the **Lucas-Lehmer test**, to test whether a Mersenne number is prime. This is given below.

Theorem 6.1. (Lucas-Lehmer test)

Let M_p denote the *p*-th Mersenne number, i.e. $M_p = 2^p - 1$, and consider the sequence

$$a_1 = 4,\ a_{n+1} = a_n{}^2 - 2 \text{ for } n \geq 1.$$

Then M_p is prime if and only if $a_{p-1} \equiv 0 \pmod{M_p}$.

The simplicity of the test lies in the fact that we need only compute the sequence $\{a_n\}$ (mod M_p). For instance, when $p = 7$, we have $M_p = 2^7 - 1 = 127$, and we check that

$$\begin{aligned}
a_1 &\equiv 4 && \pmod{127} \\
a_2 &\equiv 4^2 - 2 = 14 && \pmod{127} \\
a_3 &\equiv 14^2 - 2 \equiv 67 && \pmod{127} \\
a_4 &\equiv 67^2 - 2 \equiv 42 && \pmod{127} \\
a_5 &\equiv 42^2 - 2 \equiv -16 && \pmod{127} \\
a_6 &\equiv (-16)^2 - 2 \equiv 0 && \pmod{127}
\end{aligned}$$

It follows that M_7 is prime.

7. Pythagorean Triples

In the exercises of Unit 3, we came across the **Pythagorean triples** and studied some of their properties. Here we give more details and we will look at some more examples.

Definition 7.1. (Pythagorean triple)

A triple (*a*, *b*, *c*) of positive integers is said to be a **Pythagorean triple** if

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

If *a*, *b*, *c* are relatively prime, then the triple is called a **primitive solution**.

The origin of the name ‘Pythagorean triples’ should be clear, for if (*a*, *b*, *c*) is a Pythagorean triple, then we can form a right-angled triangle of sides *a*, *b* and *c*, and the relation $a^2 + b^2 = c^2$ follows from the Pythagoras’ Theorem. Having a right-angled triangle is nothing special, but it would be more fascinating if all its sides have integer length. Conversely, if we have a right-angled triangle of integer side lengths *a*, *b*, *c*, where *c* is the hypotenuse, then (*a*, *b*, *c*) is a Pythagorean triple.

Clearly, if we have one Pythagorean triple, or equivalently, a right-angled triangle with integral side lengths, then we can enlarge the triangle by an integral factor to get another Pythagorean triple. So we are only interested in the primitive solutions.

It would be desirable if we can find a way of generating Pythagorean triples. The steps below show one of these ways.

(1) Start with an odd positive integer greater than 1, say 3.

(2) Square the chosen integer, i.e. $3^2 = 9$.

(3) Split the square into two parts which differ by 1, i.e. $9 \to 4, 5$.

(4) The original number in (1) together with the two 'parts' in (3) form a Pythagorean triple and is a primitive solution, i.e. (3, 4, 5) is a Pythagorean triple and is a primitive solution.

We leave it to the readers to verify that such a procedure indeed generates what we want. Since we can start with any odd positive integer greater than 1, we can have as many Pythagorean triples as we want.

Unfortunately, the above procedure does not give us all the primitive solutions. For instance, (8, 15, 17) is a primitive solution, but it cannot be generated from the above procedure. (Why not?)

In the exercises of Unit 3, we proved that a triple of the form

$$(u^2 - v^2, 2uv, u^2 + v^2),$$

where *u*, *v* are relatively prime integers of opposite parity and $u > v$, is a primitive solution. Conversely, every primitive solution is of this form. Readers who did not attempt this problem should try it at this point. Indeed, the primitive solution (8, 15, 17) corresponds to $u = 4$ and $v = 1$.

Finally, we illustrate the power of Pythagorean triples by one famous example of Diophantine equations.

Example 7.1.

Find all positive integers (*x*, *y*, *z*) for which $3^x + 4^y = 5^z$.

Solution.

Clearly, $x = y = z = 2$ is one solution. We will show that no other solution exists.

First, note that $5^z = 3^x + 4^y \equiv 0^x + 1^y = 1$ (mod 3), so z must be even.

Similarly, $3^x = 5^z - 4^y \equiv 1^z - 0^y = 1$ (mod 4), so x must also be even.

Write $x = 2a$ and $z = 2b$. The equation can then be rewritten as $(3^a)^2 + (2^y)^2 = (5^b)^2$.

It follows that $(3^a, 2^y, 5^b)$ is a Pythagorean triple and it is a primitive solution.

Consequently, we must have $3^a = u^2 - v^2$, $2^y = 2uv$ and $5^b = u^2 + v^2$, where $u > v$ and u, v are positive integers of different parity.

Since $2^y = 2uv$, we must have $v = 1$. Consequently, $u = 2^{y-1}$ and

$$3^a = (u - v)(u + v) = (2^{y-1} - 1)(2^{y-1} + 1).$$

As the two factors on the right differ by 2 and are both powers of 3, they must be 1 and 3.

Hence we must have $2^{y-1} = 2$, and thus the only solution is $x = y = z = 2$.

8. Exercises

1. Let n be a triangular number.

   (a) Prove that $8n+1$ is a perfect square. Is the converse true? (That is, if $8n+1$ is a perfect square, must n be a triangular number?)

   (b) Prove that $9n+1$ is also a triangular number. Can you find other linear polynomials in n with integer coefficients which must be a triangular number whenever n is a triangular number?

2. Let t_n denote the n-th triangular number. Prove that

   (a) $t_1 + t_2 + \cdots + t_n = \dfrac{n(n+1)(n+2)}{6}$

   (b) $9(2n+1)^2 = t_{9n+4} - t_{3n+1}$

   for all positive integers n.

3. Let p and q be twin primes other than 3 and 5. Prove that $pq+1$ is a perfect square and is divisible by 36.

4. Show that 2^m+1 is prime only if m is a power of 2.

5. Using the fact that $5\times 2^7 \equiv -1$ (mod 641), or otherwise, show that $2^{2^5}+1$ is divisible by 641.

6. Let F_n denote the Fermat number $2^{2^n}+1$.
   (a) Show that $F_{n+1} = F_0F_1F_2\cdots F_n + 2$ for all non-negative integer n.
   (b) Show that F_m and F_n are relatively prime whenever $m \neq n$.

7. Show that if

$$1+2+2^2+\cdots+2^{k-1} = 2^k - 1$$

is prime, then $2^{k-1}(2^k-1)$ is a perfect number.

8. (a) Show that an even perfect number must have unit digit 6 or 8.
   (b) We have seen that the first two perfect numbers are 6 and 28. Show that any other even perfect number must either end with 6 or 28.

9. Show that 2^n-1 is prime only if n is prime.

10. Show that $2^{12}(2^{13}-1)$ is a perfect number.

11. Using the Lucas-Lehmer test, verify that M_{11} is not prime.

12. In Section 7 we gave a four-step procedure of generating primitive solutions of Pythagorean triples. Verify that such a procedure indeed generates what we want.

13. Find a right-angled triangle whose side lengths are relatively prime integers between 1000 and 2000.