COMPUTERS IN NUMBER THEORY

R.F. Churchhouse
University College, Cardiff, United Kingdom

ABSTRACT

Computers have been used to assist research in several branches of mathematics and significant discoveries have been made but the majority of these can only be appreciated by those who have a deep knowledge of the subject. Number theory, however, is exceptional in that many of its problems are concerned with very familiar types of integers, such as squares or primes, and these can understood by almost anyone, though the proofs of the corresponding theorems are often of great subtlety and complexity. Computers provide a powerful tool for the search for new theorems and conjectures in number theory and they also pose a challenge to the programmer since brute-force attacks on problems might require enormous amounts of time on even the most powerful computers whereas by exploiting a range of number-theoretic properties a skilful programmer might reduce the running-time by factors of thousands or more.

In these lectures some examples of discoveries in number theory made by the use of computers are given which illustrate all these points. In addition some unsolved problems open to computer attack are described.

1. Number Theory

Number Theory is one of the oldest and richest branches of mathematics, it is also one of the most active and probably the one most suited to the use of computers, since it deals to a considerable extent, with discrete entities (integers, primes, squares, etc.). Number-theoretic problems exercised the minds of the Ancient Greeks, Egyptians and Chinese and some of the fundamental theorems, such as Euclid's beautifully simple proof that there are an infinity of primes, were discovered by them some 2500 years ago. Modern Number
Theory might be said to have begun in the 17th century with Fermat and Pascal, since which time enormous contributions have been made by some of the greatest mathematicians of all time: Euler, Jacobi, Gauss (above all), Cauchy, Hermite, the extraordinary Indian genius Ramanujan (1887-1920) and many outstanding mathematicians of this century. As a result of all these researches a vast armoury of theorems, many of which have an almost breath-taking power and beauty, has been discovered and it is my firm belief that anyone who takes the trouble to become acquainted with these results will not only enjoy an endless intellectual banquet but also open up the possibility of taking practical advantage of them by massively reducing the work required, by computer or by hand, to solve certain types of problems: the tools are there for us to use, the challenge is to our imagination to see how to use them.

2. Applications of Number Theory

Number theorists study their subject for its own sake, because it is fascinating and offers challenges at every level, from the elementary to the profound. Number Theory is, however, a fundamental branch of mathematics, as one of its alternative names 'Higher Arithmetic' implies. It is therefore not surprising that many of its concepts, results and techniques have proved to be of value, not only in other areas of mathematics but also in branches of science and engineering, including, of course, computing. Algorithms for the solution of problems in integers or rationals may seem an obvious area of application, less obvious are those of methods for the generation of pseudo-random numbers, the construction of error-correcting codes, systems of encipherment and methods of decipherment.

3. The computer as an aid to research

Even the most cursory glance at the Collected Works of mathematicians such as Euler, Jacobi, Gauss and Ramanujan reveals that they were not afraid of lengthy computations, on the results of which they would then base their conjectures most, but not all, of which they subsequently proved. It is clear that had computers been available these great men would have exploited them to the full; indeed we know that Jacobi visited Manchester to meet Babbage at a British Association meeting specifically to learn about his plans for the 'Analytical Engine' and Ramanujan based several of his conjectures on the results of the computations of McMahon. One can only conjecture what discoveries such people would have made had
computers been available.

In the past 20 years or so computers have been used to make some significant contributions to mathematical research including:

(1) Proof of the four-colour theorem;
(2) Disproof of Euler's Conjecture on the sums of fifth powers;
(3) Confirming that the first 250,000,000 zeros of the Riemann Zeta Function lie on the critical line;
(4) Unravelling the structure of large groups;
(5) Proof that there are no odd perfect numbers less than 10400;
(6) Finding the value of Π to 29,000,000 decimal places;
(7) Finding large Mersenne primes (eg 2216,091-1);
(8) Revealing the complex structure of Julia sets.

4. The Prime Number Theorem

To illustrate how a study of numerical evidence produced on a computer might lead one quite quickly to a correct conjecture consider the table of counts of the number of primes less than 10^n (3 ≤ n ≤ 10) shown below

<table>
<thead>
<tr>
<th>N</th>
<th>Number of primes &lt; N</th>
</tr>
</thead>
<tbody>
<tr>
<td>10^3</td>
<td>168</td>
</tr>
<tr>
<td>10^4</td>
<td>1,229</td>
</tr>
<tr>
<td>10^5</td>
<td>9,592</td>
</tr>
<tr>
<td>10^6</td>
<td>78,498</td>
</tr>
<tr>
<td>10^7</td>
<td>664,579</td>
</tr>
<tr>
<td>10^8</td>
<td>5,761,455</td>
</tr>
<tr>
<td>10^9</td>
<td>50,847,534</td>
</tr>
<tr>
<td>10^10</td>
<td>455,052,512</td>
</tr>
</tbody>
</table>

Such a table can be produced on a computer using the Sieve of Eratosthenes (which identifies the primes as well as counting them) or, if we only wish to count them, by a method such as that described by Chiu [1].

In the 18th century such an extensive count of the primes was not available but Gauss (in 1792, when he was 15) studied Lambert's table of the primes up to 10^5 and correctly conjectured the asymptotic formula for π(N), the number of primes less than N. With the evidence in the table above we can do likewise.

We observe that the fraction of integers which are primes falls steadily, from about one in 6 at the beginning of the table to about one in 22 at the end. Computing the ratio
possess the property of unique factorisation. For a more detailed account of this see [3];

(ii) If we compare the estimate for the number of primes less than $N$ obtained from the Prime Number Theorem, as given above, we find that for all $N < 10^{10}$

$$\pi(N) - \text{li}(N) < 0$$

and it was conjectured that this holds for all $N$, but in 1914 Littlewood [4] proved that not only does $\pi(N) - \text{li}(N)$ change sign, it does so infinitely often. It is, however, possible that we will never find even the first value, $N_0$, such that

$$\pi(N_0) - \text{li}(N_0) > 0$$

since all that we know at present is that

$$N_0 < 10^{1165}$$

6. Some elementary number theoretic concepts, techniques and theorems

One of the simplest but most powerful techniques in number theory is the use of modular arithmetic, associated with which is the concept of congruences.

In what follows, $a$, $b$, $m$ denote integers.

**Definition** We say that "$a$ is congruent to $b$ modulo $m$" and write

$$a \equiv b \pmod{m}$$

if $(a - b)$ is divisible by $m$.

Thus: $17 \equiv 2 \pmod{5}$, $90 \equiv -1 \pmod{13}$.

Congruences have the important property that congruences to the same modulus can be added, subtracted and multiplied in the usual way, i.e. if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$ then

$$a_1a_2 \equiv b_1b_2 \pmod{m}$$

and

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$$
Thus; \[ 27 \equiv 2 \pmod{5} \text{ and } 38 \equiv 3 \pmod{5} \]

imply that \[ 27 \times 38 \equiv 6 \equiv 1 \pmod{5} \]

Division however requires special treatment and is, in any case, less useful.

Congruences to different moduli can be combined, e.g.:

If \( a \equiv 1 \pmod{5} \) and \( \equiv 2 \pmod{7} \) and \( \equiv 3 \pmod{11} \) then

\[
a \equiv 366 \pmod{385} \quad \text{(so that 366 is the smallest positive solution, all other solutions differing from 366 by multiples of 385 = 5 \times 7 \times 11).}
\]

The standard method for combining congruences to different moduli is the Chinese Remainder Theorem, for a description of which see [5].

**Modular arithmetic**

If \( E_1 \) and \( E_2 \) are integer-valued arithmetic expressions and \( E_1 = E_2 \) then \( E_1 \equiv E_2 \pmod{m} \) for any integer \( m \). Conversely if we find for some integer \( m \) that \( E_1 \not\equiv E_2 \pmod{m} \) then \( E_1 \not\equiv E_2 \). This almost trivial observation can be a remarkably powerful weapon in some cases.

**Example**

(i) Any perfect square \( \equiv 0 \pmod{4} \) or \( \equiv 1 \pmod{4} \)

For if \( m \) is an integer, \( m \equiv 0 \pmod{2} \) or \( m \equiv 1 \pmod{2} \)

i.e. \( m = 2k \) or \( m = 2k + 1 \)

and then \( m^2 = 4k^2 \equiv 0 \pmod{4} \)

or \( m^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{4} \)

(ii) If \( n \geq 2 \) the number \( 2^n - 1 \) is not a perfect square.

For if \( n \geq 2 \), \( 2^n - 1 \equiv -1 \pmod{4} \equiv 3 \pmod{4} \)

but any square \( \equiv 0, 1 \pmod{4} \not\equiv 3 \pmod{4} \).

**Exercise**

(i) If \( m \equiv 3 \pmod{5} \) or \( \equiv 3 \pmod{7} \) then \( m \) is not a square.

(ii) No integer \( \equiv 3 \pmod{4} \) is the sum of two squares.

(iii) No integer \( \equiv 7 \pmod{8} \) is the sum of three squares.
6.1 Fermat's Theorem One of the most useful theorems in elementary number theory, which enables us to make massive short-cuts in certain computations, is due to Fermat. (The notation \( (a,b) = k \) denotes that the highest common factor of \( a \) and \( b \) is \( k \).) In its simplest form Fermat's Theorem is:

**Theorem** If \( p \) is a prime and \( (a,p) = 1 \) then \( a^{p-1} \equiv 1 \pmod{p} \).

Thus, since \( (2,7) = 1 \) the theorem tells us that \( 2^6 \equiv 1 \pmod{7} \) i.e. \( 64 \equiv 1 \pmod{7} \), which is true. Less obviously, for example, since \( (3,19) = 1 \) we must have \( 3^{18} \equiv 1 \pmod{19} \). (Verification: \( 3^3 = 27 \equiv 8 \pmod{19} \), so \( 3^6 = 8^2 = 64 \equiv 7 \pmod{19} \), so \( 3^{12} = 7^2 = 49 \equiv 11 \pmod{19} \), so \( 3^{18} = 7 \times 11 \pmod{19} = 77 \equiv 1 \pmod{19} \), as predicted.)

If \( p \) is not a prime the theorem has to be modified, since it may not be true (for example 4 is not a prime and although \( (3,4) = 1 \), \( 3^3 = 27 \not\equiv 1 \pmod{4} \)). The appropriate modification involves the use of a fundamental number theoretic function, \( \phi(n) \), which is known as Euler's Function and is defined by:

**Definition** When \( n \) is a positive integer we denote by \( \phi(n) \) the number of positive integers which are less than \( n \) and relatively prime to it (i.e. the number of positive integers \( m \) such that \( (m,n) = 1 \) and \( m < n \). Thus if \( n = 6 \), \( \phi(6) = 2 \) since \( (1,6) = (5,6) = 1 \) but \( (2,6) = (4,6) = 2 \) and \( (3,6) = 3 \).

Note that if \( n \) is a prime \( \phi(n) = n-1 \) since no integer less than \( n \) has a factor in common with it.

The general form of Fermat's Theorem is given by:

**Theorem** If \( (a,n) = 1 \) then \( a^{\phi(n)} \equiv 1 \pmod{n} \).

[For a proof, see 5].

This is a very powerful theorem enabling us to carry out apparently extraordinary calculations mentally, e.g.
Problem  What is the remainder when $2^{730}$ is divided by $1001$?

Solution  1001 is not a prime, but is equal to $7 	imes 11 	imes 3$. We shall see shortly that it follows that

$$\phi(1001) = (7-1)(11-1)(13-1) = 6 	imes 10 	imes 12 = 720.$$  

Since $(2, 1001) = 1$ we have, from Fermat's (general) theorem

$$2^{720} \equiv 1 \pmod{1001}$$

Hence

$$2^{730} = 2^{720} \times 2^{10} \equiv 1 \times 2^{10} \pmod{1001}$$

$$= 1024 \pmod{1001} \equiv 23 \pmod{1001}$$

Hence $2^{730}$ leaves remainder 23 when divided by 1001.

Without the aid of Fermat's Theorem this would be a very tedious calculation rather than a simple mental exercise. To make use of the theorem however we need a convenient method for calculating $\phi(n)$; this is provided by:

**Theorem**  If $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ where the $p_i$ are distinct primes then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$$

For a proof see [5].

**Example**  If $n = 45 = 3^2 \times 5$, then

$$\phi(45) = 45 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 24$$

It follows from Fermat's general theorem that since $(7, 45) = 1$

$$7^{24} \equiv 1 \pmod{45}$$

(Check: $7^2 = 49 \equiv 4 \pmod{45}$, so $7^6 \equiv 4^3 = 64 \equiv 19 \pmod{45}$

so $7^{12} \equiv 19^2 = 361 \equiv 1 \pmod{45}$, so $7^{24} \equiv 1^2 \equiv 1 \pmod{45}$).

The converse of Fermat's Theorem is not true: i.e. if $p$ is a prime and $(a, p) = 1$ then if $a^m \equiv 1 \pmod{p}$ it is not necessarily true that $m = p-1$. For example: 7 is a prime and $(2, 7) = (3, 7) = 1$ so that $2^6 \equiv 1 \pmod{7}$ and $3^6 \equiv 1 \pmod{7}$ but it is also true that $2^3 \equiv 1 \pmod{7}$ whereas $3^3 \equiv -1 \pmod{7}$. If however $(p-1)$ is the smallest positive exponent $m$ for which $a^m \equiv 1 \pmod{p}$ we say that $a$ is a **primitive root** $(\pmod{p})$; this means that the $(p-1)$ powers of $a$, $a^2$, $a^3$, …, $a^{p-1}$ leave a complete set of residues $(\pmod{p})$ i.e. the numbers $(1, 2, …,$

365
p-1), in some order, e.g.

\[ 3, 3^2, 3^3, 3^4, 3^5, 3^6 \equiv 3, 2, 6, 4, 5, 1 \pmod{7}. \]

In the early days of computers primitive roots were sometimes used to generate data to test sort programs, for if \( p \) is a prime and \( a \) is a primitive root \( \pmod{p} \) then \( a, a^2, \ldots, a^{p-1} \) generates a complete set of residues \( \pmod{p} \) and these when sorted should produce \( (1, 2, \ldots, p-1) \). This enabled us to avoid having to provide \( (p-1) \) items of data; of course the sort program would also need to be tested in the case where some items of data were equal but this is also easily dealt with because if \( a \) is such that \( (a, p) = 1 \) and \( a^{n(p-1)} \equiv 1 \pmod{p} \) then \( (a, a^2, a^3, \ldots, a^{(p-1)}) \) generates half of the elements of the set \( (1, 2, \ldots, p-1) \) twice over. Thus since \( 2^3 \equiv 1 \pmod{7} \) we have \( (2, 2^2, 2^3, 2^4, 2^5, 2^6) \equiv (2, 4, 1, 2, 4, 1) \pmod{7} \).

7. **Representation by sums of powers**

Some of the nicest theorems and a few of the most long standing conjectures in number theory are concerned with the representation of integers as the sum of particular types of integers, such as squares or higher powers, triangular numbers, primes, etc. Among the theorems are the following classics:

(I) Every prime of the form \( 4n+1 \) can be represented as the sum of two squares;

(II) Every positive integer can be represented as the sum of three triangular numbers; (triangular numbers are those integers of the form \( \frac{1}{2}n(n+1) \))

(III) Every positive integer can be represented as the sum of four squares.

These can all be generalised in various ways, for example one might ask:

Given two relatively prime integers, \( a, b \) what primes are representable in the form \( am^2 + bn^2 \)? For specific values of \( a \) and \( b \) this makes a nice exercise for anyone with a little knowledge of programming and access to even a very small computer. From the numerical evidence it should be possible to formulate a conjecture, proving the conjecture however would require some knowledge of number-theory.

To illustrate the usefulness of the computer in attacking questions of these types here are a few cases which I investigated fairly recently, first in the form of a question then the theorem (where I discovered and proved it) or the conjecture which I believe to be true, but cannot prove.
Question 1 Every positive integer is the sum of 4 squares, but there are an infinity of positive integers which are not the sum of 3 squares. For what values of k is it true that every positive integer, N, is representable in the form

\[ N = n_1^2 + n_2^2 + n_3^2 + n_4^k \]

[We assume that \( n_4 \geq 0 \), since k may be odd].

Evidence from the computer led very quickly to the solution, which is given by:

**Theorem 1**

(i) If \( k \leq 6 \) every positive integer, \( N \), can be represented in the form

\[ N = n_1^2 + n_2^2 + n_3^2 + n_4^k \quad \text{, \( n_4 \geq 0 \)} \quad (7.1) \]

(ii) If \( k \geq 7 \) and is odd every sufficiently large positive integer \( N \) can be represented in the form (7.1);

(iii) If \( k \geq 8 \) and is even there are an infinity of positive integers \( N \), which cannot be represented in the form (7.1) and furthermore the set of these integers has density at least \( \frac{1}{96} \).

For the proof of this see [6].

**Question 2** What is the smallest value of \( k \) such that the statement:

Every positive integer \( N \) is representable in the form

\[ N = n_1^2 + n_2^3 + n_3^4 + \ldots + n_k^{k+1} \quad \text{(} n_i \geq 0 \text{)} \]

is true?

The computer run indicates that \( k = 5 \) (\( k = 2, 3, 4 \) fail at \( N = 3, 7, 15 \) respectively) so we have:

**Conjecture 2** Every positive integer \( N \) is representable in the form

\[ N = n_1^2 + n_2^3 + n_3^4 + n_4^5 + n_5^6 \quad \text{(} n_i \geq 0 \text{)} \]

(The computer evidence further indicates that there is always a representation with \( n_5 = 0 \) or with \( n_5 = 1 \)).

This conjecture is likely to be very difficult to prove: sums involving mixed powers have weak congruence properties compared to sums of the same power. The best that has been proved in relation to Question 2 is that "for all sufficiently large \( N, k \leq 17\)." [7]

**Question 3** What is the smallest value of \( k \) such that the statement:

Every positive integer \( N \) is representable in the form:

\[ N = p_1^2 + p_2^2 + p_3^2 + \ldots + p_k^2 \]

where the \( p_i \) are primes is true.

367
(For the purpose of this question 1 is considered to be a prime, otherwise 1, 2 and 3 cannot be so represented.)

Clearly k=4 and since primes are relatively common (compared to squares for example) it might have been expected that k=5 or k=6 would be the answer; but this is not so. In this case the computer led me to both a conjecture and a theorem viz:

**Conjecture 3** Every positive integer, N, is representable in the form

\[ N = p_1^2 + p_2^2 + p_3^2 + ... + p_8^2 \]

where the \( p_i \) are primes (1 is regarded as a prime in this case).

This is likely to be very hard to prove. However, to my surprise, the evidence from the computer indicated certain regularly spaced sets of integers that are \textbf{not} representable as the sum of the squares of 7 primes. Having identified two particular sets of these integers I was able to prove:

**Theorem 3** If \( N \) is congruent to any of

\[ 795, 803, 811, 812, 816 \text{ or } 817 \]

\((\text{mod } 720)\) or \((\text{mod } 1320)\) then \( N \) is not representable as the sum of the squares of 7 primes.

For the proof of this see [8].

None of these theorems and conjectures involved the use of more than a minute or two, at most, of computer time and the programming was essentially trivial; nevertheless two theorems and three conjectures emerged. There is a lot of scope for further experimentation using computers along these lines and it is quite likely that some interesting theorems and conjectures will result.

8. \textbf{Squares in the Fibonacci Sequence}

A very nice example of how a knowledge of elementary number theory can be used to avoid massive multi-length computations is provided by Wunderlich's test for squares in the Fibonacci Sequence [9].

The Fibonacci Sequence (F.S.) is generated by the three-term linear recurrence

\[ u_{n+1} = u_n + u_{n-1} \]

\((n \geq 1, u_0=0, u_1=1)\)

so that the sequence begins:

\[ 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ... \]

The sequence, which was known to mathematicians of the early 13th century, has a remarkable number of properties e.g

(i) every 4th term of the F.S. is divisible by 3;
(ii) every 8th term of the F.S. is divisible by 7;
(iii) every 10th term of the F.S. is divisible by 11; etc., etc.
and (iv) every 5th term of the F.S. is divisible by 5 (5 is the only prime which divides exactly its fair share of the sequence, so to speak).

The terms of the F.S. grow exponentially since

$$u_{n+1} = \frac{u_n + \sqrt{5}}{2} = u_n (1.618\ldots)$$

so that $$u_n \approx A(1.618)^n$$ (where $$A^{-1} = \sqrt{5}$$, in fact) and, for example, the millionth term of the sequence contains nearly 200,000 digits when written in decimal. It might seem therefore that a study of the first million terms of the F.S. would require extensive multi-length computations.

The question Wunderlich investigated was:

The terms 0, 1, 2, and 144 which occur in the F.S. are squares; are there any more?

The 'obvious' method of investigation: computing the terms of the F.S. and testing them to see if they are squares, is decidedly unattractive and very inefficient. Wunderlich had access to an IBM 7090 computer (this was in 1963) with a 32K-bit memory, i.e. rather more than $$10^6$$ bits, but not much more. In theory, with multi-length facilities, the memory was big enough to hold the value of the millionth term of the F.S., but Wunderlich in fact represented each term of the F.S. by a single bit, irrespective of whether the term was the first or the millionth. His method was essentially as follows:

With about $$10^6$$ bits available for data, we set-up a Boolean array of $$10^6$$ elements; the n-th element represents the n-th term of the F.S. All the elements of the array are initially set to 'True'; when we know for certain that the n-th term of the F.S. is not a square we set the n-th element of the array to 'False'. Now we make two observations based on elementary number theory.

(i) the defining relation of the F.S. remains true if all the values are interpreted (mod M) i.e. since

$$u_{n+1} = u_n + u_{n-1}$$

then

$$u_{n+1} \ (\text{mod} \ M) \equiv u_n \ (\text{mod} \ M) + u_{n-1} \ (\text{mod} \ M),$$

where M is any integer.

(ii) If $$u_n$$ is a square then $$u_n \equiv 0, 1 \ (\text{mod} \ 4)$$.

We now write down the terms of the F.S. (mod 4):

0, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, ........

and we see that the sequence of values repeats in a cycle of length 6. A cycle of length at most 15 could have been predicted since
(mod 4) the pair of consecutive terms \( u_{n-1}, u_n \) can only have at most 16 possible values and so the pair of values must repeat after at most 16 steps. Since \( u_{n+1} \) depends only on \( u_{n-1} \) and \( u_n \) the values of \( u_{n+1} \) (mod 4) must also repeat in a cycle of length at most 16; the pair \((0,0)\) however cannot occur so the cycle length cannot exceed 15. Thus (mod 4) the F.S. reduces to repetitions of the 6-long sequence:

\[
0, 1, 1, 2, 3, 1
\]

and since integers \( \equiv 2, 3 \) (mod 4) cannot be squares we can eliminate all terms of the F.S. in positions 4 and 5 in each block of 6, i.e. we have already eliminated one-third of the entire (infinite) sequence. In the array the appropriate bits are set to 'False'.

What we have just done (mod 4) we can do to other moduli; (mod 5), for example, the F.S. reduces to

\[
0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, \ldots
\]

- a cycle of length 20 (by the type of argument used above we know that the cycle couldn't exceed 24 in length). Now any integer \( \equiv 2, 3 \) (mod 5) cannot be a square, which eliminates 8 terms in every block of 20. We set the appropriate bits of the array to 'False', some of them will be 'False' already but the majority will not. The fraction still surviving (i.e. still set to 'True') should be about

\[
(1 - \frac{1}{3}) (1 - \frac{2}{5}) = \frac{2}{5}
\]

We continue this process, (mod 7), (mod 11).... At each stage we eliminate slightly less than half of the terms remaining at the previous stage. With \( 10^6 \) bits in the array we'd expect to have to make rather more than 20 such tests (since \( 2^{20} \div 10^6 \)) before most of the non-squares were eliminated. If any elements of the array survive a few more tests they are probably squares. In fact only

\[
0, 1, 1, 1, 144
\]

of the first million terms of the F.S. survived so Wunderlich had proved that there are no more squares in the first million terms of the F.S.

The result itself was not important, there might, after all be squares in positions beyond the millionth; (in fact there are none at all; this was proved by purely number-theoretic methods by Cohn [10] in 1966). What is important is the method, which is a fine example of how a knowledge of number theory and elegant programming can be exploited to great advantage. The running time on the 7090 was only about 3 minutes, and at no stage was an integer as big as 300 generated.

Questions (1) If \( a, b \) are relatively prime integers,

\[
u_0 = 0, u_1 = 1 \text{ and } u_{n+1} = au_n + bu_{n-1} \quad (n \geq 1)
\]

does the sequence contain an infinity of squares?
The answer is not known in general; some special cases show that there is no simple answer:
e.g. (i) \(a = 2, b = -1\) gives 0, 1, 2, 3, 4, 5, ...
so that \(u_n = n\) and the sequence contains an infinity of squares (and cubes, and primes...);
(ii) \(a = 3, b = -2\) gives 0, 1, 3, 7, 15, ...
so that \(u_n = 2^n - 1\) and only 0, 1 are squares;
(iii) \(a = 3, b = -1\) gives 0, 1, 2, 3, 21, 55, 144, ...
- the alternate terms of the F.S. so we can say that there are no more squares after 144.

(2) The F.S. contains at least 4 cubes
0, 1, 1 and 8
are there any more?
We don't know; cubes are much harder to deal with than squares
so a theoretical attack presents more formidable problems.

9. Diophantine Equations
A Diophantine Equation is an equation involving one or more variables to which we seek a solution in integers. They are named after Diophantus of Alexandria who wrote about some equations of this type c. 250 A.D. A well-known example is the Pythagorean Equation
\[ x^2 + y^2 = z^2 \]
(so-called because every non-trivial solution corresponds to a right-angled triangle the three sides of which are integers) which has an infinity of solutions the first of which is \(3^2 + 4^2 = 5^2\).
All the solutions of the Pythagorean equation are covered by the parametric solution
\[ x = a^2 - b^2, \ y = 2ab, \ z = a^2 + b^2 \]
where \(a, b\) are arbitrary integers.

Diophantine Equations may have no solutions, or a finite number or an infinity. When there are an infinity of solutions there may be a parametric solution (which transforms the equation into an algebraic identity) and in such a case the parametric solution may generate all the numerical solutions of the equation, as in the case above, or only some of them as is the case of the equation
\[ x^4 + y^4 = u^4 + v^4 \]
a parametric solution of which is given by
\[ x = a^7 + a^5b^2 - 2a^3b^4 + 3a^2b^5 + ab^6 \]
\[ y = a^6b - 3a^5b^2 - 2a^4b^3 + a^2b^5 + b^7 \]
\[ u = a^7 + a^5b^2 - 2a^3b^4 - 3ab^2 + ab^6 \]
\[ v = a^6b + 3a^5b^2 - 2a^4b^3 + a^2b^5 + b^7 \]

When \( a=1, b=2 \) this gives
\[ 133^4 + 134^4 = 158^4 + 59^4. \]

The smallest solution, but there are other solutions which are not given by the parametric formula above.

The generalised form of the Pythagorean Equation
\[ x^n + y^n = z^n \]
is the most notorious Diophantine Equation of all ('Fermat's Last Theorem'). Fermat wrote in his copy of Diophantus's book that he had a proof that there are no non-trivial solutions when \( n \geq 3 \) but that the margin of the book was too small to contain the proof. Unfortunately no trace of the alleged proof has been found. The theorem has not yet been proved, despite attempts by thousands of people over the past 350 years. It is very likely that Fermat's proof had a flaw; hundreds of incorrect 'proofs' have been produced.

It has been proved that there are no non-trivial solutions for all \( n < 25,000 \).

Euler (c.1780) generalised Fermat's Last Theorem to:

**Conjecture:** The equation
\[ x_1^n + x_2^n + \ldots + x_{n-1}^n = x_n^n \]
has no non-trivial solution in integers for \( n \geq 3 \).

In the case \( n=3 \), Euler's Conjecture is true. For nearly 200 years no progress was made for \( n \geq 4 \) but in 1966 Lander and Parkin [11] using a CDC6600 found that
\[ 27^5 + 84^5 + 110^5 + 133^5 = 144^5 \]
so disproving Euler's Conjecture when \( n=5 \) and, very recently, Elkies found a counter-example in the case \( n=4 \) viz:
\[ (2682440)^4 + (15365639)^4 + (18796760)^4 = (20615673)^4 \]
(this was, in fact, announced whilst the CERN School of Computing was taking place, but I only heard of it on my return to the U.K.).

Euler's Conjecture is therefore thoroughly discredited; on purely theoretical grounds there seemed to be no good reason why it should be true, but it took knowledgable programmers using computers to disprove it.

Searching for solutions of Diophantine Equations on computers can be very time-consuming, particularly if the equation involves several variables. However congruence considerations can often cut the work factor dramatically as we now illustrate.
The equation
\[ x_1^4 + x_2^4 + x_3^4 + x_4^4 = x_5^4 \quad (9.1) \]
has a number of known solutions, the first being
\[ 30^4 + 120^4 + 272^4 + 315^4 = 353^4 . \]
If we wish to search for solutions of (9.1) using a computer we must
first of all set some upper bound on the value of \( x_5 \). Suppose that
we are prepared to search for \( x_5 < N \). Since the values of \( x_1, x_2, \)
\( x_3, x_4 \) lie in the interval \(<0,N>\) a brute-force search would involve
of the order of \( N^4 \) computations of the left hand side of (9.1)
followed by a test to see if result was a 4th power. Even for \( N=1000 \)
this gives us something like \( 10^{12} \) cases (we can reduce the total
somewhat by assuming that
\[ x_1 \leq x_2 \leq x_3 \leq x_4 \). 
If we exploit the strong congruence properties of fourth powers
however we can reduce the work-factor considerably.
We first observe that if \( x \) is prime to 5 then
\[ x^4 \equiv 1 \pmod{5} \]
by Fermat's Theorem. Hence in all cases we have
\[ x^4 \equiv 0, 1 \pmod{5} \]
If we now consider (9.1) \( \pmod{5} \) we have
\[ (0,1) + (0,1) + (0,1) + (0,1) \equiv (0,1) \pmod{5} \quad (9.2) \]
If \( x_5 \equiv 0 \pmod{5} \) then \( x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod{5} \) and we can remove
a factor of 5 throughout, so we may assume that \( x_5^4 \equiv 1 \pmod{5} \) and
so, from (9.2) three of \( x_1, x_2, x_3, x_4 \) must be divisible by 5 and the
other one is not. We may therefore take \( x_1 \equiv x_2 \equiv x_3 \equiv 0 \pmod{5}, x_4 \not\equiv 0 \pmod{5} \) (we are not assuming that \( x_1 \leq x_2 \leq x_3 \leq x_4 \) however). We
have, by this simple observation, cut the work by a factor of
\[ 5^3 \]
Furthermore \( x^4 \equiv 0,1 \pmod{16} \) and we deduce that we may assume that
\( x_5 \) is odd and three of \( x_1, x_2, x_3, x_4 \) are even and the other odd;
this reduces the work by a further factor of 8 (not 16 since we can't
assume that it is \( x_1, x_2 \) and \( x_3 \) that are even). So far then the work
has been cut by a factor of \( 2(5^4) = 1250 \). This is not the end of the
story, by rather deeper reasoning further reductions can be obtained,
for details see [12], but hopefully the benefits obtainable by the
use of quite elementary number theoretic properties are already
apparent. In problems involving solutions in integers such
possibilities are well worth considering.

Exercise For given integers \( k \) the Diophantine Equation
\[ x^3 + y^3 + z^3 = k \]
has been extensively studied \((x,y,z\) may be positive or negative)

(i) Prove that there are no solutions if \(k \equiv 4, 5 \pmod{9}\).

(ii) When \(k=3\) there are two known solutions \((x,y,z) = (1,1,1)\) or \((4,4,-5)\); are there any more? (We don't know of any, but there may be.)

(iii) The case \(k=30\) is of interest as the smallest for which no solution is known and for which there is no known theoretical reason why a solution should not exist. Prove that if

\[ x^3 + y^3 + z^3 = 30 \]

then just one of \(x,y,z\) is divisible by 7.

10. **Odd Perfect Numbers**

An integer \(N\) is said to be perfect if it is equal to the sum of its divisors (excluding itself), thus \(6 = 1+2+3\) and \(28 = 1+2+4+7+14\), are perfect. The ancient Greeks regarded perfect numbers as worthy of special interest and Euclid proved

**Theorem**  If \(p\) and \((2^p-1)\) are both prime the number

\[ 2^{p-1}(2^p-1) \]

is perfect.

The proof is very simple; write down all the divisors and add them up. Thus 6 and 28 are the particular cases \(p=2\) and \(p=3\); \(p=5\) also produces a perfect number, 496, since \(2^5-1 = 31\) is prime. Perfect numbers are, however, quite rare since \(2^p - 1\) is rarely prime. Primes of the form \(2^p-1\) are known as Mersenne Primes and at present 30 are known, the 30-th being

\[ 2^{216,091} - 1 \]

All the recent large Mersenne Primes have been found by Slowinski using a Cray.

Note that all the perfect numbers given by Euclid's theorem are even; the theorem does not tell us however either that all even perfect numbers are of this form (they are : this was proved by Euler in the 18th century) or that there are an infinity of them (which is still unproved since we do not know if there are infinity of Mersenne Primes).

The Greeks also looked for odd perfect numbers, but didn't find any; nor have any been found to this day. Many theorems have been proved which collectively tell us that if an odd perfect number exists then it has at least 8 different prime factors, that all these
prime factors except one occur to an even power, and that the one exceptional prime is of the form \((4n+1)\) and occurs to an odd power of the form \((4k+1)\). Imposition of all these conditions immediately implies that any odd perfect number must be at least as big as:

\[
5(3.7.11.13.17.19.23)^2 > 10^{15}
\]

but it is possible to improve on this, even by hand. Computer attacks are clearly possible but brute force methods are quite infeasible and it is essential that every number-theoretic aspect should be exploited to cut down the possibilities by many orders of magnitude, and even so some sophisticated programming will be required.

In 1965 Tuckermann [13] published an account of how he was able to prove that there is no odd perfect number less than \(10^{36}\). Since then the same method has been used, on more powerful machines, to push this lower bound up to \(10^{400}\). The essentials of Tuckermann's method will now be described, but we first of all need to state a very important theorem.

**Theorem** If \(N = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k}\)

where the \(p_i\) are distinct primes then \(\sigma(N)\), the sum of the divisors of \(N\), including \(N\) itself is given by

\[
\sigma(N) = \left\{ \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right\}_{i=1}^{k}
\]

(The proof is simple: expand each factor in the product as

\((1+p_1^2 + p_1^4 + \ldots + p_1^{\alpha_1})\)

and note that the product now generates every divisor of \(N\) just once).

Note that if \(N\) is perfect \(\sigma(N) = 2N\).

Thus: \(\sigma(28) = \sigma(2^2.7) = \left(\frac{2^3-1}{2-1}\right) \left(\frac{7^2-1}{7-1}\right) = 56 = 2\times28\)

and \(\sigma(45) = \sigma(3^2.5) = \left(\frac{3^3-1}{3-1}\right) \left(\frac{5^2-1}{5-1}\right) = 78.\)

**Observation** If \(N\) is perfect, \(\sigma(N) = 2N\), therefore any odd prime
divisor of \( \sigma(N) \) is also a prime divisor of \( N \).

Thus if \( 3^2 \mid |N \) (i.e. \( N \) is divisible by \( 3^2 \) but not by any higher power of 3) then \( \sigma(N) \) is divisible by

\[
\frac{3^3 - 1}{3 - 1} = 13
\]

hence \( N \) itself is divisible by 13.

We can now describe Tuckermann's method.

Suppose that \( N \) is odd and perfect. Then \( N \) has the form

\[
N = p_1^{(4n_1+1)} p_2^{2\beta_2} p_3^{2\beta_3} \cdots p_k^{2\beta_k}
\]

where \( p_1 \equiv 1 \pmod{4} \). Thus \( p_1 \) is at least 5 and \( p_2 \) is at least 3.

Suppose that \( p_2 = 3 \); then \( N \) is divisible by at least \( 3^2 \).

There are now an infinity of cases \( 3^2 \mid |N \) or \( 3^4 \mid |N \) or \( 3^6 \mid |N \) or .... Suppose that \( 3^2 \mid |N \). Then, as we have just seen \( 13 \mid \sigma(N) \) and so \( 13 \mid |N \).

Now \( 13 \equiv 1 \pmod{4} \) so 13 might be \( p_1 \), if so it is possible that \( 13 \mid |N \), which implies that \( 14 \mid \sigma(N) \) which implies that \( 7 \mid |N \), and so on. The consequences of any hypothesis are best shown by a tree, viz. the beginning of which is:

```
3^2 || N
  /  \
13 || N
   / \ \
13 || N  13^2 || N
  / \   / \ 
7^2 || N 7^4 || N 61 || N 61^2 || N
```

Each branch of the tree is followed until any one of three conditions is met:

(i) the product of all the factors on the branches of the tree \( N_1 \) exceeds some threshold (e.g. \( 10^{400} \)); or

(ii) \( \sigma(N_1) > 2N_1 \), (for the introduction of further factors causes the ratio \( \sigma(N) / N \) to increase); or

(iii) a contradiction has occurred, e.g. we have assumed that \( 3^2 \mid |N \) and have deduced that \( 3^3 \mid |N \).
When any one of these three conditions is met the branch is terminated and the program backtracks to the previous node.

If an odd perfect number less than $10^{400}$ existed this program would have found it, but there are none. It is of course possible that odd perfect numbers do exist but are so large that we can never find them. The question of their existence is of purely academic interest; the lesson to be learned from the work of Tuckermann and others is how clever programmers can utilise elementary number theory to achieve in hours what would otherwise take centuries.

**Exercise** Show that if $N$ is an odd perfect number then $N$ cannot be divisible by 105.

* * *

**REFERENCES**


8. Churchhouse, R.F; Representation of integers as the sum of squares of primes, Caribbean Jour of Maths (to appear, 1988).


377