40
Twentieth-Century Number Theory

Much of what went under the name 'number theory' in the twentieth century had little to do with the natural numbers. There was an obsession with results concerning abstract structures used to prove results concerning abstract structures. It was as if carpenters were using their tools to make new tools to make new tools — without ever using any of these tools to build a house. Happily, there were exceptions. A few number theorists escaped the obsession with abstraction and produced the meaningful concrete results listed below.

The Bachet Equation

The *Bachet equation* is the Diophantine equation $x^2 + k = y^3$, where k is a given nonzero integer. It is named after Claude-Gaspar Bachet (1581–1638), who studied it in the seventeenth century, but it goes back to Diophantus himself (see Problem 17 of Book VI of the *Arithmetica*). Many special cases of the Bachet equation had been solved before, but it was only in 1968 that Alan Baker, a Cambridge mathematician, found a completely general solution, working for any given k. At first, Baker's solution was merely an enormous bound $M(k)$ on the sizes of x and y. However, soon after, Baker and other mathematicians, such as H. Davenport, transformed Baker's insights into a practical method for actually obtaining a solution set for any given k. W. J. Ellison used Baker's ideas to show, for the first time, that when $k = 28$, the Bachet equation has only three solutions in

W. S. Anglin, *Mathematics: A Concise History and Philosophy*

positive integers (with $x = 6$, 22, and 225). Ray P. Steiner used a version of Baker's result, due to M. Waldschmidt, to show, again for the first time, that when $k = 999$, the Bachet equation has only 6 solutions in positive integers (with $x = 1$, 27, 251, 1782, 2295, and 3,370,501). In his *Algebraic Numbers and Diophantine Approximation,* K. B. Stolarsky had claimed that $x^2 + 999 = y^3$ could not be solved by 'a thousand wise men'. Alan Baker was wise man a thousand and one.

Hilbert's Tenth Problem

At the second International Congress of Mathematicians (in Paris, 1900), David Hilbert (1862–1943) presented a list of problems he hoped would be settled in the twentieth century. Some of these problems were the following:
(1) prove or disprove the continuum hypothesis;
(2) show that arithmetic is consistent;
(8) show that all the nontrivial zeros of the Riemann zeta function lie on the line $x = \frac{1}{2}$;
(10) find an algorithm (computer program) that will tell you whether or not a given polynomial Diophantine equation (with known integer coefficients and known exponents) has a solution.

Today we know that several of Hilbert's problems cannot be solved in the way he intended. It was proved, for example, that, from the usual axioms of set theory (assuming they are consistent), there is no proof of the continuum hypothesis, and no proof of its negation. Hilbert's tenth problem falls into this category. In 1970, Yuri V. Matijasevich showed that the desired computer program cannot exist. This is because, as Matijasevich proved, almost any mathematical problem can be translated into a problem about solving a Diophantine equation. The procedure Hilbert was looking for would have been so powerful that it could have solved problems that cannot be settled in any way whatsoever, using only our present axioms (assuming they are consistent). Matijasevich based his proof on work done by a woman mathematician, Julia Robinson. In a 1992 *Mathematical Intelligencer* article, Matijasevich reveals some of the personal history behind his solution of Hilbert's tenth problem.

Incidentally, Hilbert's eighth problem is still unresolved and is considered to be the most important outstanding problem in contemporary number theory.

Computational Advances

Thanks to the computer, twentieth-century number theorists succeeded in finding twenty new perfect numbers and hundreds of new amicable pairs. They also produced programs capable of factoring 100 digit integers in just a few hours.

Particularly noteworthy was the computer solution of Archimedes's cattle problem (200 B.C.), which is equivalent to the Diophantine equation

$$x^2 - (8 \times 2471 \times 957 \times 4657^2)y^2 = 1$$

This was achieved, for the first time, in 1965, by H. C. Williams, R. A. German, and C. R. Zarnke.

Congruent Numbers

In 1983, using the 'theory of modular forms of weight 3/2', J. B. Tunnell advanced the knowledge of congruent numbers by showing that if n is a square-free odd congruent number then the number of ways of writing n in the form

$$2x^2 + y^2 + 8z^2$$

with x, y, and z integers and z odd, equals the number of ways of writing n in the same form, but with z even. For example, with z odd, 11 has exactly 8 decompositions into the above form, namely,

$$2(\pm 1)^2 + (\pm 1)^2 + 8(\pm 1)^2$$

If z is even, 11 has exactly 4 such decompositions:

$$2(\pm 1)^2 + (\pm 3)^2 + 8(0)^2$$

Since $8 \neq 4$, it follows that 11 is not congruent.

Tunnell conjectured that the converse of this theorem is also true, but that remains to be proved.

Fermat's Last Theorem

About 1637, Fermat had conjectured that the equation

$$x^{p+2} + y^{p+2} = z^{p+2}$$

has no solution in positive integers. This conjecture, known as 'Fermat's last theorem', was studied by G. Frey, K. Ribet, and J.-P. Serre. Finally, in 1994, it was proved by A. Wiles, with help from R. Taylor.

Angles in Pythagorean Triangles

Elementary, recreational number theory was still going strong. In his 1988 *American Mathematical Monthly* article, W. S. Anglin proved the following. Let B be any angle in degrees, with $0 < B < 90$. Let ϵ be any real number such that $0 < \epsilon < 1$, and $\epsilon < B$, and $\epsilon < 90 - B$. Let

$$\begin{aligned} X &= \tan(B-\epsilon) + \sec(B-\epsilon) \\ Y &= \tan(B+\epsilon) + \sec(B+\epsilon) \end{aligned}$$

Suppose u and v are relatively prime positive integers such that

$$X < \frac{u}{v} < Y$$

Then the Pythagorean triangle with sides $2uv$, $u^2 - v^2$, and $u^2 + v^2$ has an angle of A degrees (the one opposite the side $u^2 - v^2$) such that $|A - B| < \epsilon$.

Partitions

A 'partition' of a positive integer is a way of writing it as a sum of nonincreasing positive integers. For example, 5 has 7 partitions, namely,

$$5,\ \ 4+1,\ \ 3+2,\ \ 3+1+1,\ \ 2+2+1,\ \ 2+1+1+1,\ \ 1+1+1+1+1$$

The number $p(n)$ is the number of partitions n has. For example, $p(5) = 7$. In 1918, Ramanujan (1887-1920) and Godfrey Harold Hardy (1877–1947) gave the first known fast way of calculating $p(n)$ for any n, and in 1937, Hans Rademacher refined their work into the first known formula for $p(n)$. It is

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\, \sqrt{k}\, \frac{d}{dn} \left(\frac{\sinh\left(\frac{\pi}{k}\sqrt{(2/3)(n-1/24)}\right)}{\sqrt{n-1/24}} \right)$$

where

$$A_k(n) = \sum_{0 \le h \le [k/2],\ \gcd(h,k)=1} 2\cos\left(\pi\ s(h,k) - \frac{2\pi n h}{k}\right)$$

with the 'Dedekind sum' $s(h,k)$ defined as

$$s(h,k) = \sum_{r=1}^{k-1} (r/k)(hr/k - [hr/k] - 1/2)$$

(Note that $s(0,1)$ is taken to equal 0.)

Hardy and Rademacher made substantial contributions to the discovery of this formula, but the spark of insight came from Ramanujan, an extraordinary genius born near Madras, India. Perhaps the greatest number theorist of the twentieth century, Ramanujan sometimes credited his discoveries to providence. He once said:

> An equation for me has no meaning unless it expresses a thought of God. [1]

Exercises 40

1. Show that 3,370,501 is one of the values of x solving $x^2 + 999 = y^3$.

2. It is a corollary of Matijasevich's work that if x and y are positive integers and
$$z = y(2 - (x^2 + xy - y^2)^2)$$
then $z > 0$ iff z is a Fibonacci number. Find a Fibonacci number > 1 expressed in the above form.

3. Use Tunnell's theorem to show that 417 is not congruent.

4. Find a Pythagorean triangle that has an angle within 0.001 of 12°.

5. In 1971, R. Finkelstein and H. London published a paper showing that $x^3 + 5 = 117y^3$ has no integer solutions. Prove this using the fact that 9 divides 117.

Essay Question

1. Because they must 'publish or perish', second-rate mathematicians fill the journals with useless abstractions, calling their work 'number theory' when it is merely jejune generalisation. Can you suggest some replacement for the 'publish or perish' system that is currently cluttering our libraries with junk?

[1] R. Kanigel, *The Man who Knew Infinity* (New York: Charles Scribner's Sons, 1990), pages 7 and 282.