NOTES ON FERMAT'S LAST THEOREM VI

ceNTRe
Macquarie University
NSW 2109 Australia

A. J. van der Poorten

Centre for Number Theory Research, Macquarie University

Our only certain knowledge of Diophantus rests upon the fact that he quotes Hypsicles [~ -150] *and that he is quoted by Theon Alexandrinus* [whose date is fixed by the solar eclipse of June 16, 364].

O. Neugebauer, *The Exact Sciences in Antiquity*.

Number theory was strong in antiquity. But the books of Diophantus were lost after the burning of the library of Alexandria and had little influence on mathematics until the 17th century when Fermat was inspired by Bachet's recent translation.* The ideas underlying the solutions to the problems in the *Arithmetica* were substantially in advance of those then current in the West.

Diophantus is largely concerned with the problem of finding a rational solution to various equations; we recognise the methods are geometrical. Thus, dealing with Pythagorean triples, he considers the equation $x^2 + y^2 = 1$ in rationals x and y; we know this to be a circle. An obvious, albeit trivial, point on this locus is $(-1, 0)$ and a typical line through that point is parametrised by $x = u - 1$, $y = tu$. It intersects the circle when $u^2 - 2u + 1 + t^2u^2 = 1$ and, happily, we can cancel the known solution $u = 0$ and obtain $u = 2/(1 + t^2)$ yielding a new point $x = (1 - t^2)/(1 + t^2)$, $y = 2t/(1 + t^2)$. This is of course essentially the solution of Notes I, now illustrating that the circle may be parametrised by rational functions.

In this case we get infinitely many solutions, given by a simple formula. Different problems might have infinitely many solutions not given by a rational formula, or just finitely many solutions, or none at all.

Problem 24 of Book IV of Diophantus suggests we split a given number, say 6, into two parts so that their product is a cube minus its cube root. That is, $y(6 - y) = x^3 - x$. Once again, $(-1, 0)$ provides a trivial solution but now when we try $x = u - 1$, $y = tu$ we get, after cancelling the known solution $u = 0$,

$$t(6 - tu) = (u - 1)(u - 2) \quad \text{or} \quad u^2 - (3 - t^2)u + (2 - 6t) = 0\,.$$

In general this leads to irrational values for u. However, on selecting the slope $t = \frac{1}{3}$, we may cancel once more to obtain $u = \frac{26}{9}$ whence $x = \frac{17}{9}$, $y = \frac{26}{27}$ is a

1991 *Mathematics Subject Classification.* 11D41, 11-01.
Work supported in part by grants from the Australian Research Council and a research agreement with Digital Equipment Corporation.

* Six of the 13 books came into the hands of the Astronomer Johannes Müller (*Regiomantus*) in 1570; quite recently four additional books came to light; see J. Sesiano, *Books IV to VII of Diophantus' Arithmetica*, Springer-Verlag, 1982.

new solution. The fun thing is that we can now construct the tangent at this new solution to find a further solution, and so on. In general given two solutions, the secant yields a third solution. Of course the complexity of the solutions threatens to increase dramatically.

For example, writing to Mersenne in 1643, Fermat asks for right-angled triangles so that both the hypotenuse and the sum of the two sides are squares. Taking the sides as $\frac{1}{2}(1 \pm y)$ and the hypotenuse as x^2, we of course have $y^2 = 2x^4 - 1$ by Pythagoras. Fermat can guess the basic solution $P(13, 239)$. But the geometrical problem requires $-1 < y < 1$. The tangent at P provides a further solution $2P(\frac{1525}{1343}, \frac{2750257}{1803649})$. This still won't do. Finally, we get $3P(\frac{2165017}{2372159}, \frac{3503833734241}{5627138321281})$ from the secant through the two solutions, corresponding to a triangle with sides

$$a = 1061652293520 \qquad b = 4565486027761 \qquad c = 4687298610289\,.$$

Not only is this *a* solution but the method guarantees that this is the *smallest* solution!

With yet higher degree equations these methods fail in general. The upshot is that given a polynomial equation $f(x, y) = 0$ with integer coefficients we have three cases essentially depending on the (total) degree of f. Namely if f is of degree at most two we have none or infinitely many solutions — these cases are parametrised by rational functions. This is the case of *rational curves* or curves of genus 0. If f is of degree 3 or 4 we may have finitely many — the method of *infinite ascent* of the last examples may cycle, or infinitely many solutions. This is the case of *elliptic curves* or curves of genus 1. These curves do not, of course have anything to do with ellipses — those are conics and may be parametrised by rational functions. Rather, the point is that these curves are parametrised by elliptic functions*. Finally, curves of *general type*, of genus $g \geq 2$, seem only to have sporadic rational points.

The notion of *genus* arises by considering the set of complex points (z, w) so that $f(z, w) = 0$. One now has a *surface* of solutions, whose closure is topologically a sphere in the rational case, a torus in the elliptic case ('a sphere with one hole'), and a surface with more than one hole in the general case. These notions go back to Riemann — hence, *Riemann surface*, and were studied by Poincaré at the turn of the century.

In any event, the elliptic case provides the interesting collection of diophantine problems. Siegel did prove in 1929 that there are only finitely many *integer* points on curves of genus one or more, but in 1983 — one of the major results of this century — Faltings settled Mordell's Conjecture to the effect that curves with genus greater than one have only finitely many *rational* points. Thus, since then we have known that any one Fermat equation $x^n + y^n = z^n$ with $n \geq 5$ can have at most finitely many solutions.

In the elliptic case the solutions have a structure revealed by the method sketched above. One can always *model* elliptic curves by an equation $y^2 = x^3 + ax + b$ with $4a^3 + 27b^2 \neq 0$ — this may involve strategically locating points at infinity to reduce the degree from 4 to 3. For example Fermat's equation $a^3 + b^3 = c^3$ corresponds

* which I'll talk about in my next lecture.

to $y^2 = x^3 - 432$ by the transformation $x = 12c/(a+b)$ and $y = 36(a-b)/(a+b)$; the elliptic curve $y^2 = 2x^4 - 1$ requires more work than I am prepared to invest at this moment. Then, if a straight line cuts the curve at points P, Q and R we write $P + Q + R = 0$, with 0 being the point with $y = \infty$. If $P = (x, y)$ then $-P = (x, -y)$. A tangent at P, which 'cuts' the curve twice at P, also cuts the curve at $-Q$, that is, so that $2P + Q = 0$. Obviously all this defines a commutative operation, but, remarkably this 'addition' is also associative — as one may show using the fact that two cubic curves with 8 points in common also have a 9-th common point. Thus the rational points on an elliptic curve form an abelian group. More than that, in 1922 Mordell confirmed a suggestion of Poincaré that the group is *finitely generated*, here meaning that one need start with just finitely many points to generate all the rational points by the construction described above. Finitely generated abelian groups are all of the shape $\mathbb{Z}^r \oplus T$, that is, they have a finite *torsion* part T consisting of points of *finite* order — those points P for which $mP = 0$ for some m — and an infinite part $\mathbb{Z}^r$. So, deciding whether there are infinitely many rational points on an elliptic curve reduces to determining whether its *rank* r is or is not 0. We now know the possibilities for the torsion subgroup. In 1977, Barry Mazur established that if the cubic $4x^3 + ax + b$ is irreducible then $T \simeq C_{2n+1}$, a cyclic group of order $2n+1$, with $n \leq 4$; if the cubic has just one rational linear factor then $T \simeq C_{2n}$ with $n \leq 6$; and if the cubic splits completely then $T \simeq C_2 \times C_{2n}$ with $n \leq 4$. Whatever, it is not too difficult to find all the torsion points in any particular example. To be precise, presuming that the parameters a and b are integers, a fairly elementary theorem of Nagell and Lutz entails that a torsion point has integral co-ordinates and that the y co-ordinate is 0 (in which case $2P = 0$) or is a divisor of $4a^3 + 27b^2$. Moreover, it is also elementary to argue that $E(\mathbb{Q})$ is a subgroup of the group $E(\mathbb{R})$ of real points on the curve, and that $E(\mathbb{R})$ is isomorphic to the circle $\mathbb{R}/\mathbb{Z}$ or the product $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ according as $4a^3 + 27b^2$ is positive or negative. In this way one sees that the content of Mazur's very deep result is the various bounds on n yielding just 15 possibilities for the rational torsion group.

In 1928 André Weil generalised Mordell's theorem to elliptic curves over number fields (and in 1940 to the case of abelian varieties). Thereby, we now speak of the group $E(\mathbb{Q})$ of rational points (excluding ∞) on an elliptic curve E as the *Mordell-Weil* group of the curve.

Let me now return to a classical problem to illustrate the difficulties in guessing whether the rank r is or is not 0. The problem of determining those integers n which are the area of a right-angled triangle with rational sides goes back to Arabic manuscripts of more than a thousand years ago and is the basis of the *Liber Quadratorum* (1225) of Leonardo of Pisa (*Fibonacci*). We are to find Pythagorean triples (a, b, c) so that $\frac{1}{2}ab = n$, or — this is the same thing after setting $x = c^2/4$, $x \pm n = (a \pm b)^2/4$ — a rational square x so that both $x + n$ and $x - n$ are such squares; that is n is the common difference of a three-term arithmetic progression of squares[†]. Traditionally, the successful n are called *congruent* numbers. For example (Fibonacci), 5 is congruent by virtue of the Pythagorean triple $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$,

[†] Fermat could show by descent that one cannot have four squares in AP; that is: 1, 25, 49 is an extreme case. The beauty of the group structure of the rational points on elliptic curves is that it both allows one to find all solutions *and* to show that there are no nontrivial solutions.

or, equivalently, because of the square $x = 11\frac{97}{144} = \left(\frac{41}{12}\right)^2$. Much more painfully, $n = 157$ is congruent because of an x with denominator of some 100 digits!

The elliptic curve reporting that all of $x-n$, x and $x+n$ are squares of course is $y^2 = x^3 - n^2x$. Here it is known that when n is prime and $\equiv 3 \pmod 8$ then the rank is 0; the rank is at most 1 if n is prime and $\equiv 5$ or $7 \pmod 8$; and is at most 2 if n is prime and $\equiv 1 \pmod 8$. Finding the solution $(-4,6)$ for $y^2 = x^3 - 5^2x$ proves its rank is at least 1, and therefore 1. But Fermat could not have decided whether the rank is 0 or 1 in the case $n = 157$ since the smallest solution lies well outside any region in which he — or we — could hope to search for solutions. To decide in general even whether the rank is nonzero one needs some new principle.

The idea turns out to be to consider the equation modulo p; that is, to ask, for each prime p, for the number a_p of pairs $(x,y) \pmod p$ with $y^2 \equiv x^3 + ax + b$. On crude statistical grounds — for each pair the probability that the congruence holds is $1/p$ — one guesses that $a_p \sim p$ and, indeed, in 1933 Hasse established that $|a_p - p| < 2\sqrt{p}$ — the 'Riemann hypothesis for elliptic curves'.

On collecting all this *local* data one hopes to obtain *global* information; that is information on the rational solutions. I will talk about 'local and global' in a later lecture, but let me just say here that the interrelationships turn out to be extremely striking, both actually and conjecturally.

But what does this all mean for Fermat's Last Theorem? We have learned that Faltings' proof of the Mordell Conjecture confirms that each equation $x^n + y^n = z^n$ with $n > 4$ has at most finitely many solutions, and that those solutions — if any, are probably just sporadic accidents. That does make it a little remarkable that there never is a nontrivial solution for $n > 2$. So it might make sense to look for additional structure. Indeed, let's contemplate the very simple equation $A+B=C$ in integers and then the elliptic curve $y^2 = x(x-A)(x+B)$, observing that its discriminant is essentially $(ABC)^2$. There is reason to guess that the discriminant should not be more than a small power (6 or so) of the product $\prod_{p|ABC} p$ of the different primes dividing A, B and C. The truth of this conjecture immediately entails Fermat's Last Theorem as well as conquering a host of other inaccessible problems, such as that an equation $x^u - y^v = k$, with k composed from a nominated set of primes, has only small solutions in the integer exponents u, v and in relatively prime integers x and y. The ABC-conjecture is still just that, a conjecture. However, Ribet was able to show in 1987, by proving a conjecture of Serre, that in the very special case $A = x^p$, $B = y^p$, $C = z^p$ the truth of the FLT followed from yet more fundamental remarks of Taniyama, Weil and Shimura, and those for just the special case of *semi-stable* elliptic curves. At that time, I heard Tate lecture on these matters at an AMS meeting at Arcata. It was exciting to see that our general views on elliptic curves entailed the FLT, but in so far as the various conjectures did not appear to be particularly accessible we seemed little nearer to actually dealing with Fermat's Last Theorem.

I've been chatting with Don Zagier, the Australian Mathematical Society's 1993 Mahler Lecturer, and a visitor to ceNTRe. Other than for the concluding thoughts, virtually all this material is my vulgarisation of ideas pirated from his remarks and from his articles 'Lösungen von Gleichungen in ganzen Zahlen', *Miscellanea Math.* (1991), 311–326 and 'Elliptische Kurven: Fortschritt und Anwendungen', *Jber. d. Deutschen Math.-Verein* **92** (1990), 58–76.