ceNTRe
Macquarie University
NSW 2109 Australia

NOTES ON FERMAT'S LAST THEOREM V

A. J. van der Poorten

Centre for Number Theory Research, Macquarie University

By the powers conferred on us, by Dr. Paul Wolfskehl, deceased of Darmstadt, hereby we fund a prize of one hundred thousand Marks, to be given to the person who will be first to prove the great theorem of Fermat.

Göttingen, June 27, 1908
Die Königliche Gesellschaft der Wissenschaften.

In the first year of the Wolfskehl Prize, 621 'solutions' were submitted. That surely raises the question of how, and why, do mathematicians make mistakes? I don't want to philosophise that man is born to sin and error (though the trigonometric allusion deserves remark). Nor, really, do I want to comment on blunders, slips of the pen or misprints. Moreover, no doubt the 621 'solutions', and the thousands that followed, contained a great deal of outright nonsense. By that I intend to include pure principle, say that of maintaining that it is god's will that indeed a square splits into two squares, but therefore 'of course' that a cube split into at least three cubes, a fourth power into at least four fourth powers, and so on. Euler is sometimes blamed for a conjecture to that effect, but whatever, it's outright wrong. One of the few times that I've been able to send an amateur scurrying away was by pointing out that, sadly, $144^5 = 27^5 + 84^5 + 110^5 + 133^5$.

Of course, slips of the pen can be followed by an entire coherent chain of correct reasoning and may be astonishingly hard to pick. If one has a great deal invested in an argument one may be emotionally incapable of being sufficiently critical. It helps to be aware of the principle, once nicely put to me by Kurt Mahler, according to which one cannot expect to get *gehaktes Rindfleisch* from a meatgrinder unless one has put meat into that meatgrinder. In other words, if I prove some surprising fact I had better have had some pretty clever idea, or have used some wondrous secret. On those occasions that I have looked at questions that the great ones couldn't handle I have always asked myself what new knowledge, or new combination of old knowledge I had available; in other words, what meat did I have.

The best way to find absurd errors or unjustified assumptions is to have a student read your manuscript. The impact of an innocent question like 'I couldn't quite understand why it's right to write $1 = 2$' can be shattering. It is also bad for one's self-confidence to be asked to explain why it is correct to neglect a blatant counterexample. I recall a report on a survey which asked mathematicians how

---

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.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

many papers they had read in complete detail the previous year. It appears that the average paper is read by some 0.76 mathematicians, and that includes author, referee and reviewers. It is little wonder that actually having one's paper read can be revealing.

We also make mistakes by our use of 'obviously', 'evidently' 'clearly', and the like. Now it is the case that no argument tries to dot every 't' and cross every 'i'. Even correct arguments will contain such 'gaps'. But, the trouble is that we may have conquered the apparent difficulty without realising that we have now brought a real difficulty to light. It's that kind of thing that causes such admissions as 'my proof developed a gap, and that gap became a chasm that swallowed the proof'. Such situations can have lead to premature announcements. Nonetheless, in that the real problem may have been revealed, success may follow after all. One conquers and then, slowly and reluctantly, realises that all that has been done thus far is to expose a true obstruction to a proof. Sometimes, however, the sheer excitement of it all seems to allow one to leap the new abyss, doing something far more clever than one is normally capable of, and suddenly one has proved Theorem 3 (van der Poorten), or better yet, Theorem B. 'Amateurs' don't know the principle of the meatgrinder. They believe that jumping a crack will suffice.

But I began this tirade in an attempt to explain why we believe that Andrew Wiles does have a proof of the FLT. Wiles presented his work at the June, 1993 workshop on 'Iwasawa theory, automorphic forms, and p-adic representations' at the Isaac Newton Institute for Mathematical Sciences in Cambridge, England in a sequence of three lectures with title 'Elliptic curves, modular forms, and Galois representations'. Rumors had circulated for some days that something interesting was about to be said and excitement mounted as it became apparent that Wiles might be able to claim a fundamental advance in the matter of Taniyama's conjecture. His expert audience saw quality meat. They saw new combinations of ideas that might allow chasms to be jumped. And, the subject is understood well enough for it to be very surprising indeed if the real problems after all reside in the technicalities necessarily slurred in the course of Wiles' presentation. Thus there is real confidence in Wiles' corollary: *Suppose that p, u, v and w are integers, with $p > 1$. If $u^p + v^p + w^p = 0$, then $uvw = 0$.* We will not be needing to use the fine remark of Allan Adler

... thus, the entire proof of Fermat's Last Theorem collapses like a house of cards. The great problem is still unsolved and they are right in the Star Trek episodes when they say that in the 23rd century the problem is still open!

With that off my chest let me say a few additional things about the work on the FLT following Kummer. I became seriously interested in Fermat's Last Theorem in the seventies, partly because of some related work I had done[1]. Curiously, I also did some calculations on the Weil-Taniyama conjecture at much that time[2],

[1] 'Some remarks on Fermat's conjecture' (with K. Inkeri), *Acta Arith.* **XXXVI** (1980), 107–111.
[2] 'The polynomial $X^3 + X^2 + X - 1$ and elliptic curves of conductor 11', *Séminaire Delange--Pisot-Poitou (Théorie des nombres)* (18^e année: 1976/1977), Fasc.1, exp. n° 17, 7pp (Secrétariat Mathématique, Paris, 1977) and 'Elliptic curves of conductor 11' (with M. K. Agrawal, J. H. Coates and D. C. Hunt), *Math. Comp.* **34** (1980), 991–1002.
The dates now surprise me and remind me of the extraordinary delays then current in publication. Some years later John Loxton and I accidentally dedicated an article to the 80th birthday of Paul

of course with no idea that it might be related. I was surprised to find how little of great substance had been achieved on the FLT in the previous fifty years. Sure, there was the very extensive work of Vandiver filling minor gaps in Kummer's work and simplifying his criteria, and substantial generalisations of Mirimanoff's congruence conditions in the first case. Sadly, some of those generalisations were disputed, as much as anything else, I suspect, because barely anyone was prepared to plough through the details of the papers. But perhaps I should not deride this century's work. You can make your own judgment after reading Paulo Ribenboim's 13 *Lectures on Fermat's Last Theorem.*

Of course, the arrival of the computer made it feasible to carry out very extended calculations. In that way, the first case was verified up to the bit length, 3×10^9 or so (J. Brillhart, J. Tonascia and P. Weinberger, 'On the Fermat quotient', in Atkin and Birch, *Computers in Number Theory*, Academic Press, 1971, 213–222), and the general case up to 125 000 (S. S. Wagstaff, 'The irregular primes up to 125,000', *Math. Comp.* **32** (1978), 583–591).

However, a curious exception, to what I saw as a desert, was an observation of Terjanian who showed that *if the equation $x^{2p} + y^{2p} = z^{2p}$, has a solution then $2p$ divides one of x or y* (G. Terjanian, 'Sur l'équation $x^{2p} + y^{2p} = z^{2p}$', *C. R. Acad. Sc. Paris*, **285** (1977), 973–975.); here p is an odd prime. This settled the first case for even exponents. The argument is entirely elementary. We already know that one of x and y, say x, must be even and, by Abel's formulæ, that $\gcd\big(z^2 - y^2, (z^{2p} - y^{2p})/(z^2 - y^2)\big)$ is 1 or p. So it suffices to show that the gcd cannot be 1. But if the two factors are relatively prime, both must be squares. However, by playing with quadratic reciprocity, Terjanian shows by induction on the integers m, n, when y and z are odd, that $(z^{2m} - y^{2m})/(z^2 - y^2)$ is a square modulo $(z^{2n} - y^{2n})/(z^2 - y^2)$ if and only if m is a square modulo n. That suffices. The fact that Terjanian's result was not known until then, and the elementary argument, provided a great surprise.

In 1974 Rob Tijdeman demonstrated the power of Baker's method by dealing with Catalan's conjecture. The equation $x^u - y^v = 1$ in four integer variables, all at least 2, might seem more complicated than Fermat's Last Theorem but a refinement of Baker's method allowed Tijdeman to show that all four variables are bounded by effectively computable constants. However, it still remains computationally infeasible to show that indeed $3^2 - 2^3 = 1$ displays the only solution. Nor have we any handle at all, as yet, on the conjecture that for any $z \neq 1$, fixed, or varying with just given prime factors, the equation $x^u - y^v = z$ also has essentially only a few small solutions. It was this problem that led to my interest in the FLT.

For some months in 1978 I had the pleasure of having used Baker's method to prove, subject to Vandiver's conjecture that p does not divide h^+, that Fermat's Last Theorem was true for all sufficiently large exponents. My argument survived the one week and one month tests, but my suspicions became certainty when I found that my arguments were so powerful that they handled the FLT without

Erdős (rather than the 75th), leading Andrzej Schinzel to say that he accepted the paper subject to one change, unless we wanted it kept for five years. I was able to retort that my error was understandable given the way that Erdős carries on about his age — smile from Schinzel, and that anyhow given *Acta Arith.* delays, it was probably spot on — laughter from everyone else.

hypothesis and could even prove some false 'facts'. To find my blunder I ultimately had to resort to the well-tried method of throwing the manuscript into the air and studying the page at which it opened. So it goes. My interest in the FLT faded, and I have been forced to a study of *Math. Reviews* — fortunately now available on CD — to check on the years until now.

For example, in 1989 Andrew Granville showed that 'The first case of Fermat's last theorem is true for all prime exponents up to $714,591,416,091,389$' (*Trans. Amer. Math. Soc.* **306** (1988), 329–359), *inter alia* by checking and extending the consequences of the Kummer-Mirimanoff congruences and proving that a first case solution with exponent p entails that $p^2 \mid r^p - r$ for all primes $r \leq 89$. In 1992 Buhler, Crandall and Sompolski used fast Fourier transforms and more efficient Bernoulli number identities to determine the 'Irregular primes to one million' (*Math. Comp.* **59** (1992), 717–722) and verified Vandiver's conjecture and Fermat's Last Theorem for those primes.

Yet more dramatic results appeared variously as 'cheap' and 'expensive' corollaries of Faltings' 1983 proof of Mordell's Conjecture. Faltings' work entails, as a very particular case, that for each exponent $n > 4$ the equation $x^n + y^n = z^n$ has at most finitely many solutions. Amongst others, Granville and Heath-Brown remarked that it promptly follows that the FLT holds for almost all exponents n, notwithstanding our still not knowing that it holds for infinitely many *prime* exponents.

Relying on a result of Etienne Fouvry ('Théorème de Brun-Titchmarsh: application au théorème de Fermat', *Invent. Math.* **79** (1985), 383–407), Len Adleman and 'Roger' Heath-Brown (*Invent. Math.* **79** (1985), 409–416) showed that the first case of the FLT holds for infinitely many prime exponents, the first result of that breadth. I quote a review of the late Emil Grosswald (MR: 87d:11020) in saying that 'the tools used, or quoted, in the proof are rather formidable and comprise, among others, a (very particular case of a recent) theorem of Faltings; old theorems of Sophie Germain and of Wieferich and Mirimanoff and a generalization of Sophie Germain's theorem; the Siegel-Valfish-Page theorem on primes in arithmetic progressions; the Bombieri-Vinogradov prime number theorem; Linnik's theorem (smallest prime in an arithmetic progression); the Brun-Titchmarsh theorem; Chebyshev's lower bounds estimates obtained from upper bounds; sieve methods, especially Rosser's sieve; Kloosterman sums and their evaluations by Weil, Iwaniec, and Kuznetsov; modular functions and the non-Euclidean Laplacian operator, etc.'.

The array of notions that will need mention to detail Wiles' eventual proof of Fermat's Last Theorem is yet more impressive — or depressing, for those who retained the dream of an elementary proof. For the rest, in *Mathematical Reviews* one finds mostly minor comments. There is also a note of Francisco Thaine, 'On the first case of Fermat's last theorem', (*J. Number Theory* **20** (1985), 128–142) whose useful remarks on the Kummer-Mirimanoff congruences eventually impacts on our understanding of elliptic curves.

According to Granville, by 1992 the FLT was known for all exponents to 4 million or so. Yet, had it not been for the recent Frey-Ribet observations showing that the truth of the FLT followed from the Weil-Taniyama conjecture, one could well have repeated Harry Edwards' remark in the introduction to his book (*Fermat's Last Theorem*, GTM **50**, Springer-Verlag 1977) that '*there is as yet little reason to believe the Theorem*'.