ceNTRe
Macquarie University
NSW 2109 Australia

# NOTES ON FERMAT'S LAST THEOREM III

A. J. van der Poorten

Centre for Number Theory Research, Macquarie University

*Sophie Germain was a French mathematician, a contemporary of Cauchy and Legendre, with whom she corresponded. Her theorem, brought by Legendre to the attention of the illustrious members of the Institut de France, was greeted with great admiration.*

P. Ribenboim

**Abel's formulæ.** Suppose $x^p+y^p+z^p=0$. Then

$$\gcd(x+y,\frac{x^p+y^p}{x+y})=1 \quad \text{or} \quad p,$$

and if $p \mid x^p+y^p$, then $p \mid x+y$ and $p \parallel \dfrac{x^p+y^p}{x+y}$.

To see this, just notice that

$$\frac{x^p+y^p}{x+y}=\frac{(x+y-y)^p+y^p}{x+y}\equiv py^{p-1}-\tfrac12 p(p-1)y^{p-2}(x+y) \mod (x+y)^2$$

$$\text{and} \qquad \equiv (x+y)^{p-1} \mod p.$$

The basic underlying fact is that for any $a$, $b$

$$(a+b)^p=a^p+b^p \mod p;$$

indeed, this characterises primes $p$. But more than that, there is Fermat's Theorem (often referred to as his *little* theorem) according to which $a^p\equiv a \mod p$ for any rational integer $a$, so for integers $a_1, a_2, \dots, a_n$ we have the congenial result that

$$(a_1+a_2+\cdots+a_n)^p\equiv a_1+a_2+\cdots+a_n \mod p.$$

In any case, by the factorisations $-z^p=(x+y)\dfrac{x^p+y^p}{x+y}, \dots,$ we have

$$\begin{array}{lll} x+y=c^p & \dfrac{x^p+y^p}{x+y}=\gamma^p \quad \text{if} & p\nmid z \\ y+z=a^p & \dfrac{y^p+z^p}{y+z}=\alpha^p & p\nmid x \\ z+x=b^p & \dfrac{z^p+x^p}{z+x}=\beta^p & p\nmid y \end{array}$$

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

So, in the *first case* of Fermat's Last Theorem, when $p \nmid xyz$, we have, say, $2x = -a^p + b^p + c^p$.

Incidentally, if $p \mid z$, then $x + y = p^{p-1}c^p$ and $\dfrac{x^p + y^p}{x + y} = \gamma^p$ with $p \nmid \gamma$.

Now Sophie Germain argues as follows: If $x^p + y^p + z^p = 0$ then $x^p + y^p + z^p \equiv 0 \mod q$, for every $q$. Suppose now that $q = 2p + 1$ happens to be prime. Then $q \nmid y$, say, entails $y^p \equiv \pm 1 \mod q$, so necessarily $q \mid xyz$, say $q \mid x$. Hence $-a^p + b^p + c^p \equiv 0 \mod q$, so $q \mid abc$; in fact one sees that $q \mid a$. Thus $y \equiv -z$, so $\alpha^p \equiv py^{p-1} \mod q$. Also, of course, $\gamma^p \equiv y^{p-1} \mod q$. Thus $p$ is a $p$-th power mod $q$, which entails $p \equiv \pm 1 \mod q$, whence we have a contradiction.

Using these ideas Legendre generalised the result to $q = 2kp + 1$ prime for several further values of $k$, enabling all cases $p < 100$ to be dealt with. In 1823 this was a remarkable advance.

No-one doubts that there are infinitely many primes $p$ so that also $2kp + 1$ is prime for some suitable small $k$, but such results remain inaccessible. Nonetheless, fairly recently Adleman and Heath-Brown *inter alia* used a generalisation of Sophie Germain's result, and work of Fouvry, to prove that the first case of the FLT held for infinitely many prime exponents.

Sophie Germain employed her own version of the formulas I mention. Suppose $0 < x < y < z$. Abel considered the case of Fermat's equation $x^n + y^n = z^n$ when one of $x$, $y$ or $z$ is prime. Abel showed that $x$ must be the prime, that $z = y + 1$, that the exponent $n$ must be a prime $p$, and that $p \mid y(y + 1)$. However, his proof that the equation

$$x^p + y^p = (y + 1)^p$$

has no nontrivial solutions was shown to be faulty by Markoff some seventy years later. Thus that Abel's equation has no solutions remained unproved until several weeks ago. For all we knew, $z - y = 1$ was possible in the FLT. On the other hand, some 20 years ago, Kustaa Inkeri and I used Baker's method to prove that $y - x$ must be large relative to the exponent if Fermat's equation was to have a solution. Related methods had been used in preceding years by Inkeri *et al* to show that in any putative solution to Fermat's equation each of $x$, $y$ and $z$ would have to be very large indeed.

Kummer's results dealt with both the first and second cases, but were incongenial for extended computation. To the contrary, the results of Mirimanoff and Wieferich at the turn of the century, and a little later, of Fürtwangler, seemed almost to dispose of the first case. They showed that if there is a first case solution for exponent $p$ then

$$p^2 \mid 2^{p-1} - 1 \quad \text{and} \quad p^2 \mid 3^{p-1} - 1\,.$$

These results relied on a complicated analysis of the conditions first proved by Kummer. At first no examples of $p$ satisfying the first condition were known. Then in 1913 Meissner noticed $2^{1092} \equiv 1 \mod 1093^2$ and in 1922 Beeger found that $3511^2 \mid 2^{3510} - 1$. Computer checks of some twenty years ago showed that there are no other cases for the base 2 with exponent less than $3 \times 10^9$. For the base 3 one has $11^2 \mid 3^{10} - 1$; the next case is $3^{1006002} - 1 \equiv 0 \mod 1006003^2$.

Further such criteria for additional bases were derived subsequently. It is surely most improbable that the two criteria mentioned are ever satisfied simultaneously. Whatever, we have no understanding of the *Fermat quotients* $q_p(a) = (a^p - a)/p$ at all. Their divisibility by $p$ appears to us as no more than a statistical accident.*

## Appendices.

**Fermat's Theorem.** Since the object of these notes is to chat about Fermat's Last Theorem, the least I can do is to say a few words about a result that properly bears his name. Throughout $p$ is a rational prime.

The claim $n^p \equiv n \pmod{p}$ is obvious by induction since $(n+1)^p \equiv n^p + 1 \pmod{p}$.

A rather more to the point proof is to notice that $1, 2, \ldots, p-1$ are all the different remainders mod $p$ that are relatively prime to $p$. But if $a$ is not zero mod $p$ then the numbers $a, 2a, \ldots, (p-1)a$ are different and nonzero mod $p$. Hence mod $p$ they must be just a permutation of $1, 2, \ldots, p-1$. Thus $(p-1)! \equiv (p-1)!a^{p-1}$ and Fermat's Theorem is evident.

It follows, incidentally, that there is an $a' \in \{1, 2, \ldots, p-1\}$ so that $aa' \equiv 1 \pmod{p}$. Of course one writes $a' = a^{-1}$, and notes that $a^{-1} = a^{p-2} \pmod{p}$.

It is also fun to remark that the polynomial $X^p - X$ has distinct zeros mod $p$ since it and its derivative $pX^{p-1} - 1 \equiv -1 \mod p$ are trivially relatively prime. Hence, plainly,

$$X^p - X \equiv X(X-1)(X-2)\cdots\big(X-(p-1)\big) \mod p$$

and *inter alia* — amongst other things, we have Wilson's Theorem

$$(p-1)! \equiv -1 \pmod{p}.$$

It is of course a corollary to Fermat's Theorem that if a prime $p$ divides the $n$-th Fermat number $F_n = 2^{2^n} + 1$ then $p = k.2^{n+1} + 1$ for some integer $k$. Thus, as did Euler, but unlike Fermat — who must have made an arithmetical blunder, we can readily find a divisor of $F_5$.

**Bernoulli numbers.** Even engineers know about the power series

$$\sin z = z - \frac{1}{3!}z^3 + \frac{1}{5!}z^5 - \cdots \qquad \text{and} \qquad \cos z = 1 - \frac{1}{2!}z^2 + \frac{1}{4!}z^4 - \cdots,$$

but what is the series expansion for $\tan z$?

---

* Apropos Meissner, Landau's *Zahlentheorie* points out that with $p = 1093$ and all congruences mod $1093^2$, clearly $3^7 = 2187 = 2p + 1$ so $3^{14} \equiv 4p + 1$. Just so, $2^{14} = 16384 = 15p - 11$, whence $2^{28} \equiv -330p + 121$. Thus

$$3^2 \cdot 2^{28} \equiv -2970p + 1089 \equiv -2969p - 4 \equiv 310p - 4\,; \quad 3^2 \cdot 2^{28} \cdot 7 \equiv 2170p - 28 \equiv -16p - 28\,.$$

So $3^2 \cdot 2^{26} \cdot 7 \equiv -4p - 7$ and $3^{14} \cdot 2^{182} \cdot 7^7 \equiv -(4p+7)^7 \equiv -7 \cdot 4p \cdot 7^6 - 7^7$. Thus $3^{14} \cdot 2^{182}$ is just $-4p - 1 \equiv -3^{14}$. Hence $2^{182} \equiv -1$ and Meissner's observation follows.
But, is $3^{1092} \equiv 1$ as well? Clearly no, because for any $p$, both $x^{p-1} \equiv y^{p-1} \equiv 1 \pmod{p^2}$ as well as $x + y = mp$ with $p \nmid m$, is impossible.
Now take $x = 3^7$, $y = -1$ to see that $3^{1092} \not\equiv 1 \pmod{1093^2}$.

The trick is first to notice that $f(z)=z/(e^z-1)+\frac{1}{2}z$ is an even function, that is, $f(-z)=f(z)$, and then to write — noting $B_3=B_5=B_7=\cdots=0$,

$$\frac{z}{e^z-1}=\sum_{k=0}^{\infty}\frac{1}{k!}B_kz^k=1-\tfrac{1}{2}z+\frac{1}{2!}B_2z^2+\frac{1}{4!}B_4z^4+\frac{1}{6!}B_6z^6+\cdots.$$

Clearly the Bernoulli numbers $B_k$ can be computed by the inductive definition

$$\binom{k+1}{1}B_k+\binom{k+1}{2}B_{k-1}+\cdots+\binom{k+1}{k}B_1+B_0=0$$

with $B_0=1$. So $B_1=\frac{1}{2}$, $B_2=\frac{1}{6}$, $B_4=-\frac{1}{30}$, .... Obviously the $B_k$ all are rational numbers. However, their numerators soon grow at a furious rate: indeed, because the cited series evidently has radius of convergence $2\pi$, we must have $|B_{2k}|\sim(2k)!/(2\pi)^{2k}$.

What this is all about is the calculus of finite differences, now unsung, but still taught in applied maths courses when I was littler. Here the difference operator $\Delta: f(x)\mapsto f(x+1)-f(x)$ and its inverse $\Delta^{-1}$, the indefinite sum, replace the derivative $D: f(x)\mapsto f'(x)$ and its inverse $D^{-1}$, the indefinite integral. In this context one defines the Bernoulli polynomials $B_n(x)$ by

$$D(\Delta^{-1}x^n)=B_n(x),\quad n=0,1,2,\ldots.$$

But on expanding $f(x+1)$ as a Taylor series about $x$, we see that

$$\Delta f(x)=\sum_{n=1}^{\infty}\frac{f^{(n)}(x)}{n!}=\sum_{n=1}^{\infty}\frac{D^n}{n!}f(x)=(e^D-1)f(x),$$

so

$$D\Delta^{-1}=\frac{D}{e^D-1}\quad\text{and}\quad D\Delta^{-1}x^n=\sum_{m=0}^{\infty}\frac{B_m}{m!}D^mx^n=\sum_{m=0}^{\infty}\binom{n}{m}B^mx^{n-m},$$

and in particular $B_n=B_n(0)$. Of course $\Delta^{-1}x^n$ 'means' $1^n+2^n+\cdots+(x-1)^n$ because

$$\Delta\Big(\sum_{m=1}^{x-1}m^n\Big)=x^n\quad\text{whence}\quad\Delta^{-1}x^n=\sum_{m=1}^{x-1}m^n=\frac{1}{n+1}\big(B_{n+1}(x)-B_{n+1}(1)\big).$$

Shorn of its error term and other frills, the now fairly evident formula

$$f(x)=\int_x^{x+1}f(t)\,dt+\sum_{n=1}^{\infty}\frac{B_n}{n!}\Delta D^{n-1}f(x),$$

is the useful Euler-Maclaurin formula, allowing one to compare sums with integrals.

I'm going to religiously confine each of the Notes to just four pages so there's just no room for $\tan z$; but surely $iz\coth iz=z\cot z$ and $\tan z=\cot z-2\cot 2z$ gives enough hint. Worse though, there is then no space to discuss Euler's evaluation of the special values of the Riemann $\zeta$-function, that is, of the sums

$$\zeta(2k)=\sum_{n=1}^{\infty}\frac{1}{n^{2k}}=1+\frac{1}{2^{2k}}+\frac{1}{3^{2k}}+\frac{1}{4^{2k}}+\cdots=(-1)^{k-1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k}.$$

---

Most of this section is just things I knew, but in the late-seventies I was helped by access to a draft of Paulo Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag 1980.