ceNTRe
Macquarie University
NSW 2109 Australia

NOTES ON FERMAT'S LAST THEOREM II

A. J. van der Poorten

Centre for Number Theory Research, Macquarie University

Der Fermatsche Satz ist zwar mehr ein Curiosum
als ein Hauptpunkt der Wissenschaft.
E. E. Kummer

Lamé's argument produced a flurry of investigation in Paris on the matter of unique factorisation of cyclotomic integers. To understand the underlying ideas we had better recall just why the usual integers $\mathbb{Z}$ are known to have unique factorisation. The argument goes back to Euclid and relies on observing that given integers a and b, with $b \neq 0$, there is some multiple, say kb, of b so that

$$|a-kb| < |b|\,.$$

Of course one picks k as the integer part of the quotient of a/b; then $a-kb$ is the *remainder*. The point is that a common divisor of a and b is also a common divisor of b and of $r=|a-kb|$. Now iterating the argument reveals the greatest common divisor $d=(a,b)$ of a and b — without one having to factorise a or b. In fact the process is the same thing as expanding a/b as a *continued fraction*:

$$k_0+\cfrac{1}{k_1+\cfrac{1}{k_2+\cfrac{1}{\ddots\;\cfrac{1}{k_{n-1}+\cfrac{1}{k_n}}}}}$$

usually abbreviated by writing $a/b=[k_0\,,\,k_1\,,\,\ldots\,,\,k_{n-1}\,,\,k_n]$. Its truncations

$$[k_0\,,\,k_1\,,\,\ldots\,,\,k_{h-1}\,,\,k_h]=p_h/q_h$$

yield rational numbers (called *convergents* because they converge rapidly to a/b, each approximating it surprisingly well) where p_h and q_h are relatively prime, and are given by the recursive formulæ

$$\begin{pmatrix} p_h & p_{h-1}\\ q_h & q_{h-1}\end{pmatrix}\begin{pmatrix} k_{h+1} & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix} p_{h+1} & p_h\\ q_{h+1} & q_h\end{pmatrix},\quad\text{where}\quad \begin{pmatrix} p_{-1} & p_{-2}\\ q_{-1} & q_{-2}\end{pmatrix}=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}.$$

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

It follows that $p_h q_{h-1} - p_{h-1} q_h = (-1)^{h+1}$, and since by definition $p_n/q_n = a/b$, we must have $a = dp_n$ and $b = dq_n$, where $d = \gcd(a,b)$. Hence

$$dp_n q_{n-1} - p_{n-1} dq_n = (-1)^{n+1} d = q_{n-1} a - p_{n-1} b$$

displays the gcd as a $\mathbb{Z}-$ *linear* combination $d = sa + tb$ of a and b.

Since the Euclidean Algorithm itself relies on the *Well Ordering Principle*:

A non-empty set of positive integers contains a smallest element,

we might have appealed directly to that principle — which is of course equivalent to the Principle of Induction, to remark that the set

$$I = (a,b) = \{sa + tb : s, t \in \mathbb{Z}\}$$

of all $\mathbb{Z}$-linear combinations of a and b has a least positive element d, and that d is fairly readily seen to be a greatest common divisor, usually also denoted by (a,b), of a and b.

It is easy to see, say by induction, that every positive integer is a product of positive irreducible integers (one views 1 as being an empty such product). To see that the decompositions are unique, up to the order of the factors, suppose to the contrary that n has two essentially distinct decompositions. Of course then n is neither irreducible nor 1, so we may set $n = ab$ with positive a and b both less than n. Our hypothesis now becomes that there is some irreducible q which divides $n = ab$ — one writes $q \mid ab$ — but neither $q \mid a$ nor $q \mid b$.

However, since q is irreducible, $q \nmid a$ entails that the gcd $(a,q) = 1$. Thus there are integers s and t, say, so that $1 = sa + tq$, whence $b = sab + tqb$, and evidently $q \mid b$. Thus every irreducible integer is *prime*, a prime being an element p, which is *not* a *unit* — that is, $p \nmid 1$ — with the property that $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Once every irreducible is prime, it follows immediately that decomposition into irreducibles is unique.

Now consider, for example, the Eisenstein integers $\{a + \rho b : a, b \in \mathbb{Z}\}$, where $\rho = \frac{1}{2}(-1 + \sqrt{-3})$ so $\rho^3 = 1$. We associate with each such number its *norm*

$$\mathrm{N}(a + \rho b) = (a + \rho b)(a + \rho^2 b) = a^2 - ab + b^2 .$$

One then shows, following the idea of division with remainder, that given integers $a + \rho b$ and $c + \rho d$, there are integers $u + \rho v$ and $r + \rho s$ so that

$$a + \rho b = (u + \rho v)(c + \rho d) + (r + \rho s) \text{ with } \mathrm{N}(r + \rho s) \le \tfrac{3}{4}\mathrm{N}(c + \rho d) .$$

Thus the Eisenstein integers form a Euclidean ring with respect to the norm, and, just as for $\mathbb{Z}$, it follows that they constitute a unique factorisation domain.

In similar spirit one sees that the Gaussian integers $\{a + ib : a, b \in \mathbb{Z}\}$ have the Euclidean property with respect to their norm $N(a + ib) = a^2 + b^2$.

With rather more effort, Cauchy succeeded in guessing correctly that the domains $\mathbb{Z}[\zeta_m]$ of cyclotomic integers are Euclidean for

$$m = 5, 6, 7, 8, 9, 10, 12, 14, 15$$

as well; here $\zeta_m^m = 1$, and the ζ_m are *primitive* m-th roots — no smaller power of ζ_m is 1. Mind you, this was a less comprehensive achievement than may appear. Cauchy appears to miss the fact that, when n is odd, $\zeta_n = -\zeta_{2n}$, so $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{2n}]$. In addition to these results, Cauchy also claimed to have analytic arguments suggesting that $\mathbb{Z}[\zeta_m]$ is Euclidean for all large m, say bigger than 10, but he was unable to find a decisive proof.

The explanation for this failure came from Germany, in a letter from Kummer to Liouville. At this time German mathematics was far more sophisticated than that in France, inspired by stars like Gauss, Jacobi and Dirichlet. On April 28, 1847 Kummer explained that it is not the case in general that the domains $\mathbb{Z}[\zeta_m]$ have unique factorisation, though he had succeeded in retrieving unique factorisation by introducing *ideal* numbers.

Suitably chastened, Cauchy showed in the next *Comptes Rendus de l'Académie des Sciences* that, indeed, the numbers $\mathbb{Z}[\zeta_{23}]$ do not have the property of unique factorisation into irreducibles.

Once forewarned, it is easy to see that unique factorisation is in fact rather unusual. Take for example the domain $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b : a, b \in \mathbb{Z}\}$. We see that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Plainly the irreducibles 2 and 3 are not prime; nor are the irreducibles $1 \pm \sqrt{-5}$. Kummer deals with this by introducing *ideal* numbers — the word 'imaginary' is already in use — and shows that he may write, say, $2 = \mathfrak{a}\bar{\mathfrak{a}}$, $3 = \mathfrak{b}\bar{\mathfrak{b}}$, whereby the preceding decompositions become

$$6 = \mathfrak{a}\bar{\mathfrak{a}} \cdot \mathfrak{b}\bar{\mathfrak{b}} = \mathfrak{a}\bar{\mathfrak{b}} \cdot \bar{\mathfrak{a}}\mathfrak{b}.$$

The new ideal irreducibles are prime. At little more than the cost of writing a few gothic letters, unique factorisation is restored.

These ideas had not arisen in the context of Fermat's Last Theorem, but rather from a desire to generalise the *law of quadratic reciprocity* of Gauss (1801). The law states that if p and q are distinct odd primes then the two congruences

$$x^2 \equiv p \mod q \quad \text{and} \quad y^2 \equiv q \mod p$$

either both have a solution in integers x and y, or are both insoluble, except when both p and q are 3 modulo 4, in which case one is solvable and the other is not. The question was to generalise this rule to powers higher than the second.

By the way, at first glance such a reciprocity law doesn't seem a big deal. But imagine that it is important to describe all primes q such that $x^2 \equiv p \mod q$ has a solution. In principle, one must test each q, trying $\lfloor \frac{1}{2}q \rfloor$ different potential $x \mod q$. On the other hand, given quadratic reciprocity, it is immediately clear that the good q are those of certain congruence classes $\mod 4p$. This turns an apparently infinite problem into a finite one.

Gauss himself had shown in 1832 that in order to formulate a reciprocity law for fourth powers one needed the Gaussian integers $\mathbb{Z}[i]$ and he had established a cubic reciprocity law using the number $\mathbb{Z}[\rho]$. His results suggested that for higher powers n one must first deal with the following question:

Can every prime p congruent to 1 modulo n be written as the norm of a cyclotomic integer in $\mathbb{Z}[\zeta_n]$?

Incidentally, the norm of $a(\zeta_n) = a_0 + a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1}$ is the product of the different $a(\zeta_n^r)$ as ζ_n^r runs through the primitive n-th roots of unity. [It is not too hard to see that ζ_n^r is a primitive n-th root exactly when r and n are relatively prime. The number of such r is denoted by $\phi(n)$, where ϕ is the so-called Euler totient function.]

It seems clear that Jacobi, and later Eisenstein, realised that the question just posed has an affirmative answer if and only if the domain $\mathbb{Z}[\zeta_n]$ has unique factorisation. A beautiful proof of this is given by Kummer (*Collected Papers*, Springer 1975, Vol I, 241–243). Apparently Kummer had suggested in 1844, in a paper withdrawn before publication, that the answer is yes for all n, but had made the timely discovery that this is false for $n = 23$.

The mythology of Fermat's Last Theorem claims that Kummer perpetrated Lamé's error, and that battered, but not defeated, he retrieved matters by his introduction of ideal numbers. Whatever, it was in 1847, just when the Parisian mathematicians were beating their heads against the wall of unique factorisation, that Kummer got the idea of applying his ideal theory to Fermat's Last Theorem.

As regards unique factorisation into irreducibles, it turns out that there are just 30 different cyclotomic fields $\mathbb{Q}[\zeta_n]$ with unique factorisation:

$$n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28,\\ 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$$

The notion 'Euclidean' plays no role in the eventual argument [J. H. Masley and H. L. Montgomery, 'Cyclotomic fields with unique factorisation', *J. für Math.* **286/87** (1976), 248–256.]. Showing that these fields have unique factorisation is routine; excluding all other cases is not quite. In 1979, only 13 of the fields were known to be Euclidean.

Kummer eventually established the higher reciprocity laws. It was a task he valued far more highly than his researches on Fermat's Last Theorem to which owes his fame.

Bei meinen Untersuchungen über die Theorie der complexen Zahlen und den Anwendungen derselben auf den Beweis des Fermatschen Lehrsatzes, welchen ich der Akademie der Wissenschaften vor drei jahre mitzutheilen die Ehre gehabt habe, ist es mir gelungen die allgemeinen Reciprocitätsgesetze für beliebig hohe Potenzreste zu entdecken, welche nach dem gegenwärtigen Stande der Zahlentheorie als die Hauptaufgabe und die Spitze dieser Wissenschaft anzusehen sind.

E. E. Kummer (1850)

This section is substantially plagiarised from the introduction to the thesis of Hendrik Lenstra Jr., which I translated from the Dutch for *Math. Intelligencer* **2** (1980), 6–15; 73–77; 99–103.