6

Euclidean Number Fields 1

Hendrik W. Lenstra, Jr.

Preface

The papers that formed part of my doctoral thesis on euclidean number fields (Amsterdam, 1977) were preceded by an introduction, written in Dutch, which was aimed at giving the general mathematical public an impression of the subject, of the historic background against which one should view it, and of the methods of proof employed. The article below is a translation of the first part of that introduction; the two remaining sections will appear in subsequent issues of this journal. Some minor adaptations have been made to take account of the effluxion of time and the consequent forward march of science. I am greatly indebted to Alf van der Poorten, of Macquarie University, who was kind enough to volunteer to transform my Dutch into English.

H. W. Lenstra, Jr.

The story of "Fermat's Last Theorem" has been told so often that it hardly bears retelling.

H. M. Edwards

N'y a-t-il pas là une lacune à remplir?

J. Liouville

Dramatis personae

Euclid of Alexandria	~300 B.C.
Diophantus of Alexandria	~250
Pierre de Fermat	1601–1665
Leonhard Euler	1707–1783
Joseph Louis Lagrange	1736–1813
Carl Friedrich Gauss	1777–1855
Augustin Louis Cauchy	1789–1857
Gabriel Lamé	1795–1870
Carl Gustav Jacob Jacobi	1804–1851
Peter Gustav Lejeune Dirichlet	1805–1859
Joseph Liouville	1809–1882
Ernst Eduard Kummer	1810–1893
Pierre Laurent Wantzel	1814–1848
Gotthold Eisenstein	1823–1852
Leopold Kronecker	1823–1891
Bernhard Riemann	1826–1866
Adolf Hurwitz	1859–1919
Kurt Hensel	1861–1941
Hermann Minkowski	1864–1909
Harry Schultz Vandiver	1882–1973
Emil Artin	1898–1962
Harold Davenport	1907–1969
Theodore Samuel Motzkin	1908–1970

Fermat's Last Theorem

On March 1st, 1847 the French scientist Lamé, a member of the Parisian *Académie des Sciences,* made a startling announcement to his learned colleagues: he claimed to have succeeded in proving *Fermat's last theorem,* which states that there are no positive integers x, y and z with

$$x^n + y^n = z^n$$

if n is an integer greater than two. For n equal to two there are many solutions:

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2,$$
$$8^2 + 15^2 = 17^2, \quad \ldots,$$

the *Pythagorean triples.* In the margin of his copy of Diophantus' *Arithmetica,* the French jurist Fermat had written that for greater n no such triples can be found, and he had added that he had a marvellous proof for this, which, however, the margin was too small to contain:

"Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

Every other theorem which Fermat had announced in like manner had been proved by the year 1847; only this one, the *last,* was left.

Lamé attributed the basic idea of his proof to Liouville. The idea consisted of working with numbers of the shape

$$(1) \quad a_0 + a_1\zeta + \ldots + a_{n-1}\zeta^{n-1},$$
$$a_0, a_1, \ldots, a_{n-1} \text{ integers},$$

where ζ is a complex number with the properties $\zeta^n = 1$,

COMPTE RENDU

DES SÉANCES

DE L'ACADÉMIE DES SCIENCES.

SÉANCE DU LUNDI 1er MARS 1847.

PRÉSIDENCE DE M. ADOLPHE BRONGNIART.

MÉMOIRES ET COMMUNICATIONS

DES MEMBRES ET DES CORRESPONDANTS DE L'ACADÉMIE.

M. le Président annonce la perte douloureuse que l'Académie vient de faire dans la personne de M. Benjamin Delessert, décédé le 1er mars 1847.

A l'occasion du procès-verbal, M. Milne Edwards présente les observations suivantes :

« Dans notre dernière séance, M. Serres m'a adressé quelques remarques à l'occasion de la présentation des Mémoires de MM. Prevost, Lebert et Baudement; n'ayant pu avoir communication de l'article dans lequel mon savant collègue se proposait de résumer ses observations, j'ai cru devoir ajourner l'impression de ma réponse. Aujourd'hui que j'ai sous les yeux cet article, il me semble inutile de reproduire ma réplique; car, pour le lecteur des *Comptes rendus*, elle ne paraîtrait pas avoir été motivée par l'argumentation de mon savant collègue. »

MÉCANIQUE APPLIQUÉE. — *Système de chemins de fer à roues motrices horizontales.* (Note de M. Seguier.)

M. le baron Seguier place sous les yeux de ses collègues, des modèles de locomotive et de wagon d'enrayage appropriés à son système de chemin de fer à roues motrices horizontales; en les faisant plusieurs fois fonctionner sur un plan incliné très-rapide, il fait comprendre comment, à l'aide de son dispositif mécanique, la cause d'adhérence des roues motrices sur la voie peut être trouvée dans la résistance même du convoi. Il fait aussi remarquer que le même principe de construction permet d'établir un frein aussi puissant que sûr, agissant de lui-même ou à la volonté d'un garde-frein, toutes les fois que cela est nécessaire. M. Seguier croit avoir ainsi pratiquement justifié les propositions qu'il avait eu l'honneur de formuler devant l'Académie, dans ses précédentes communications à l'occasion des chemins de fer.

ANALYSE MATHÉMATIQUE. — *Démonstration générale du théorème de Fermat, sur l'impossibilité, en nombres entiers, de l'équation* $x^n + y^n = z^n$; *par* M. Lamé.

« On sait qu'il suffit de démontrer cette impossibilité pour les cas où l'exposant n est un nombre premier. On possède des démonstrations particulières, relatives aux exposants 3, 5, 7; elles sont fondées sur la décomposition en deux facteurs du premier membre de l'équation. Mais quand on passe aux exposants 11, 13, 17, 19, etc., on se trouve arrêté par la trop grande inégalité des deux facteurs. Je cherchais depuis longtemps un genre de démonstration, applicable à tous les cas, et qui fût en quelque sorte indépendant de la grandeur de l'exposant, lorsque, il y a quelques mois, j'en causai avec M. Liouville; il me parut convaincu que la propriété négative, énoncée par Fermat, devait dépendre de certains facteurs complexes, récemment étudiés par les géomètres qui s'occupent de la théorie des nombres. C'était une nouvelle voie que je n'avais pas explorée; je l'ai suivie, et je suis parvenu au mode de démonstration que je vais exposer, et qui me paraît justifier la prévision de M. Liouville.....

..... » Le théorème de Fermat, pour $n > 3$, n'est qu'un cas particulier de celui qui vient d'être démontré; car si A et B sont des entiers, ou s'ils se réduisent à α_0, β_0, M sera entier, ainsi que C, k, μ; mais μ', μ'',..., $\mu^{(n-1)}$ seront toujours des nombres complexes : seulement, leur produit devra être un module entier, c'est-à-dire que μ, μ',..., $\mu^{(n-1)}$ devront être les sous-facteurs d'un nombre entier de la forme $Y^2 \pm nZ^2$; enfin, les relations telles que (11) seront encore nécessaires, et la conclusion d'impossibilité sera la même. »

Observations de M. Liouville.

« Dans la communication qu'il vient de faire à l'Académie, M. Lamé a bien voulu déclarer qu'il a suivi une idée dont je lui avais fait part autrefois : celle d'introduire des nombres complexes dérivés de l'équation binôme $r^n - 1 = 0$ dans la théorie de l'équation $x^n - y^n = z^n$, pour essayer d'en conclure l'impossibilité de cette dernière équation, soit en nombres entiers ordinaires, soit même en nombres complexes de la forme indiquée. Une telle idée n'a rien de neuf en soi, et a dû se présenter naturellement aux géomètres d'après la forme du binôme $x^n - y^n$. Je n'en ai d'ailleurs déduit aucune démonstration satisfaisante, et, à vrai dire, je ne me suis même jamais occupé sérieusement de l'équation $x^n - y^n = z^n$. Toutefois, quelques essais me portaient à croire qu'il faudrait d'abord chercher à établir pour les nouveaux nombres complexes un théorème analogue à la proposition élémentaire pour les nombres entiers ordinaires, qu'un produit ne peut être décomposé en facteurs premiers que d'une seule manière. L'analyse de M. Lamé me confirme dans ce sentiment; elle a besoin, ce me semble, du théorème dont je parle : et pourtant je ne vois pas que notre confrère soit entré, à ce sujet, dans les détails que la matière paraît exiger. N'y a-t-il pas là une lacune à remplir? Je soumets cette observation à notre confrère, mais en exprimant la ferme espérance qu'il viendra à bout de toutes les difficultés, et qu'il obtiendra un nouveau et plus éclatant triomphe dans cette question épineuse où il s'est déjà tant distingué. Je rappellerai, en terminant, que depuis M. Gauss, et même depuis Euler et Lagrange, les géomètres se sont souvent occupés de nombres complexes. Le tome XVII de nos Mémoires renferme un grand travail de M. Cauchy, où ceux de ces nombres qui se rattachent à l'équation $r^n - 1 = 0$, jouent un rôle important. Mais pour le point spécial que j'ai signalé tout à l'heure, c'est surtout dans un article de M. Jacobi (*Journal de Mathématiques*, tome VIII, page 268), que l'on pourra trouver des renseignements utiles. »

A la suite de la lecture faite par M. Lamé, M. Cauchy prend aussi la parole et rappelle un Mémoire qu'il a présenté à l'Académie dans une précédente séance (19 octobre 1846), et qui a été paraphé, à cette époque, par l'un de MM. les Secrétaires perpétuels. Dans ce Mémoire, M. Cauchy exposait une méthode et des formules qui étaient, en partie, relatives à la théorie des nombres, et qui lui avaient semblé pouvoir conduire à la démonstration du dernier théorème de Fermat. Détourné par d'autres travaux, M. Cauchy n'a pas eu le temps de s'assurer si cette conjecture était fondée. D'ailleurs, la méthode dont il s'agit était très-différente de celle que M. Lamé paraît avoir suivie, et pourra devenir l'objet d'un nouvel article.

PHYSIOLOGIE. — *Sur la découverte du siége distinct de la sensibilité et de la motricité; par* M. Flourens.

$\zeta \neq 1$. Here, Lamé supposed n to be an odd prime number, which assumption, as had already been known for some time, does not involve any essential restriction in the proof of Fermat's last theorem. With the aid of these numbers, $x^n + y^n$ may be split into n factors:

$$x^n + y^n = (x + y)(x + \zeta y) \ldots (x + \zeta^{n-1} y)$$

and Fermat's equation then assumes the shape

$$(2) \quad (x + y)(x + \zeta y) \ldots (x + \zeta^{n-1} y) = z^n.$$

To this Lamé applied the following principle, a classic method from the theory of *diophantine equations*:

(3) If the product of two numbers that have no factor in common is an n-th power, then each of the two numbers is an n-th power.

For positive integers one readily sees the validity of this principle on splitting the numbers into their prime factors and checking the contribution of each distinct prime.

Lamé assumed that (3) would also hold for numbers of the shape (1), and with the help of an argument that is of little matter here he reached the conclusion that (2) is possible only if one of the numbers x, y, z is zero. The truth of Fermat's last theorem follows from this.

After Lamé, the meeting was addressed by Liouville. The idea attributed to him of considering complex numbers (1), he said, was nothing new; one could already meet such numbers in the work of Euler, Lagrange, Gauss and Jacobi. Moreover, it seemed to him, said Liouville, that Lamé implicitly assumed that unique factorisation into prime factors also holds for the numbers (1). At this point Liouville made the remark quoted at the head of this article.

Thus Fermat's last theorem gives rise to a question which perhaps is more interesting than is Fermat's last theorem itself:

(4) Does unique factorisation into primes also hold for numbers of the shape (1)?

In this section we concern ourselves principally with the methods applied by Liouville's contemporaries to answering this question.

A second difficulty that Liouville drew to Lamé's attention derives from the existence of divisors of 1: numbers which divide 1, or *units*, as they are called nowadays. That these play a role in an assertion such as (3) can be seen in the example

$$-4 \cdot -9 = 6^2.$$

The two numbers -4 and -9 have no factor in common, their product is a square, but nevertheless neither -4 nor -9 is the square of an integer. However, each is a unit, namely -1, times a square.

In the case of numbers of the shape (1) many more units occur. For example from

$$(\zeta + \zeta^{n-1})(\zeta + \zeta^5 + \zeta^9 + \ldots + \zeta^{2n-1}) = 1,$$
$$(n \text{ odd}, n > 1)$$

one sees that each factor on the left is a unit. Properties of divisibility by $\zeta + \zeta^{n-1}$ play an important role in Lamé's proof. But this number divides 1, thus it also divides every other number. This present observation vitiates Lamé's entire argument even were we to assume unique factorisation.

We pause no further at the matter of units. Later developments have shown that questions on this topic are more difficult to deal with than are questions concerning uniqueness of factorisation. But it is worth mentioning that, even today, several authors of number theory texts seem to forget that in order to draw conclusions such as (3) one must know about units as well as about factorisation into primes.

Two weeks after Lamé's pronouncements Wantzel produced a method for answering Liouville's question. Until the beginning of this century, Wantzel enjoyed some fame for having provided a simplified proof of the unsolvability of the equation of the 5-th degree. As well, his was the first published proof of the impossibility of trisecting an angle, and of doubling a cube. Because he died young Wantzel never fulfilled the promise he had shown – these days he is entirely forgotten.

Wantzel's idea boils down to the following. Let n be an arbitrary integer $\geqslant 3$ and let ζ be a primitive root of $\zeta^n = 1$, for example $\zeta = e^{2\pi i/n}$. Wantzel argued that in order to show that the numbers (1) have unique factorisation, it suffices to find a substitute for the well-known concept of *division with remainder* valid for ordinary integers: for then one can call on arguments going back to Euclid which lead to the desired theorem of unique factorisation into prime factors.

To illustrate just how one finds such a substitute Wantzel first considers the case $n = 4$. In this case the numbers (1) are just the numbers $a + b\sqrt{-1}$ with a and b integral, and one defines the *norm* of such a number by

$$N(a + b\sqrt{-1}) = (a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2.$$

Now to divide $a + b\sqrt{-1}$ by $c + d\sqrt{-1}$, with c and d not both zero, one notes that

$$\frac{a + b\sqrt{-1}}{c + d\sqrt{-1}} = t + u\sqrt{-1}$$

with

$$t = (ac + bd)/(c^2 + d^2), \quad u = (bc - ad)/(c^2 + d^2).$$

This does not mean that we divide exactly, because of course t and u need not be integral. But we can always approximate t and u by integers t', u' such that

$$t = t' + v, \quad u = u' + w,$$

with

$$|v| \leqslant \tfrac{1}{2}, \quad |w| \leqslant \tfrac{1}{2}.$$

Then we have

$$a + b\sqrt{-1} = (t' + u'\sqrt{-1}) \cdot (c + d\sqrt{-1}) + \\ + (v + w\sqrt{-1}) \cdot (c + d\sqrt{-1}).$$

If we write $r = vc - wd$, $s = vd + wc$ this becomes

$$(5) \quad a + b\sqrt{-1} = (t' + u'\sqrt{-1}) \cdot (c + d\sqrt{-1}) + \\ + (r + s\sqrt{-1}).$$

So one may consider $t' + u'\sqrt{-1}$ to be the *quotient* and $r + s\sqrt{-1}$ to be the *remainder* of $a + b\sqrt{-1}$ on division by $c + d\sqrt{-1}$. In order that $r + s\sqrt{-1}$ deserve the name *remainder* and – we must not forget – in order that Euclid's arguments may operate, $r + s\sqrt{-1}$ must be *smaller* than the number $c + d\sqrt{-1}$ by which we divide. Here we will measure size by means of the norm; and indeed we have

$$\begin{aligned} N(r + s\sqrt{-1}) &= (r + s\sqrt{-1}) \cdot (r - s\sqrt{-1}) \\ &= (v + w\sqrt{-1}) \cdot (c + d\sqrt{-1}) \cdot \\ &\quad \cdot (v - w\sqrt{-1}) \cdot (c - d\sqrt{-1}) \\ &= (v^2 + w^2) \cdot N(c + d\sqrt{-1}) \\ &\leqslant ((\tfrac{1}{2})^2 + (\tfrac{1}{2})^2) \cdot N(c + d\sqrt{-1}) \\ &< N(c + d\sqrt{-1}). \end{aligned}$$

So much for the case $n = 4$. Nowadays we describe all this by saying that Wantzel proves that the numbers $a + b\sqrt{-1}$, with a and b integral, form a *euclidean ring* with respect to the norm. The arguments of Euclid, which we have already mentioned a number of times, show that the theorem of unique factorisation into primes holds in a euclidean ring.

For a second example Wantzel takes the case $n = 3$. Then one has $\zeta^2 = -1 - \zeta$, so the numbers (1) may be written as $a + b\zeta$ with a and b integers. The norm – *module*, in Wantzel's terminology – is now defined by

$$N(a + b\zeta) = (a + b\zeta) \cdot (a + b\zeta^2) = a^2 - ab + b^2.$$

In an entirely analogous fashion one now finds on dividing $a + b\zeta$ by $c + d\zeta$ that

$$a + b\zeta = (t' + u'\zeta)(c + d\zeta) + (r + s\zeta),$$

with t', u', r, s integers and

$$r + s\zeta = (v + w\zeta) \cdot (c + d\zeta)$$
$$|v| \leqslant \tfrac{1}{2}, \; |w| \leqslant \tfrac{1}{2}.$$

That $r + s\zeta$ deserves to be called a remainder is easy to check:

$$\begin{aligned} N(r + s\zeta) &= (v^2 - vw + w^2) \cdot N(c + d\zeta) \\ &\leqslant \tfrac{3}{4} \cdot N(c + d\zeta) < N(c + d\zeta). \end{aligned}$$

This deals with the case $n = 3$. For general n Wantzel gave somewhat less detail:

"On voit facilement que le même mode de démonstration s'applique aux nombres complexes de forme plus compliquée qui dépendent des racines de $r^n = 1$ pour n quelconque. Il suffira d'établir que le module de l'expression

$$\alpha + \beta r + \gamma r^2 + \ldots + \mu r^{n-1}$$

est toujours moindre que 1 quand $\alpha, \beta, \gamma, \ldots, \mu$ sont compris entre 0 et 1; ce qui se vérifie de plusieurs manières."

Here the term *module* (norm) of the expression

$$(6) \quad u_0 + u_1\zeta + \ldots + u_{n-1}\zeta^{n-1},$$
$$u_0, u_1, \ldots, u_{n-1} \text{ real},$$

is to be interpreted as the product of the numbers obtained from (6) as ζ runs through the different primitive roots of $\zeta^n = 1$. In this context a root ζ of $\zeta^n = 1$ is said to be *primitive* if there is no m such that $\zeta^m = 1$ and $0 < m < n$. One can show that, if $u_0, u_1, \ldots, u_{n-1}$ are integers, then the norm is an integer $\geqslant 0$, and is zero only if the expression (6) itself is zero.

The remarkable aspect of Wantzel's assertion is that it is not even valid in the case $n = 4$, which he himself had presented as an example. Surely no one could maintain that the norm

$$N(v + w\sqrt{-1}) = v^2 + w^2$$

is smaller than 1 whenever v and w both lie between 0 and 1? But even were we to take all of $\alpha, \beta, \gamma, \ldots, \mu$ as lying between $-\frac{1}{2}$ and $+\frac{1}{2}$, Wantzel's claim does not hold for general n, as Cauchy was to show later by producing a counterexample.

Already on March 1st, the day of Lamé's announcement, Cauchy, with apparent faith in Lamé's approach, had demanded some of the likely credit for himself. He had, so he claimed, notified the Academy several months earlier of a method which would possibly lead to a proof of Fermat's last theorem.

"Détourné par d'autres travaux, M. Cauchy n'a pas eu le temps de s'assurer si cette conjecture était fondée."

The series of notices which Cauchy now had appear in the *Comptes Rendus* of the Academy are principally directed at attempting to answer Liouville's question (4) in the positive sense. Moreover, assuming that he would succeed in this attempt, Cauchy deduced a number of consequences of unique factorisation which seemed to him to be relevant to Fermat's theorem. For reasons which will become clear we make no further comment concerning these consequences. In any event the common belief that Cauchy supposed unique factorisation of the numbers (1) to be self-evident is totally unjustified.

Cauchy commenced by rapping Wantzel over the knuckles: the analysis of the case $n = 4$ could already be found in the work of Dirichlet; and indeed those arguments also work for the case $n = 3$,

mais une objection s'élève contre le passage où il assure qu'on peut aisément étendre le même mode de démonstration aux nombres complexes de forme plus compliquée qui dépendent des racines de l'équation binôme

$$x^n = 1,$$

n étant un nombre entier quelconque.

Cauchy then gave a number of examples counter to the claim of Wantzel that we have already quoted, and he concluded:

» On voit, par ce qui précède, que la théorie générale des nombres complexes est encore à établir.

For several months Cauchy busied himself with this problem, achieving only partial results. He showed that the numbers (1) do in fact form a euclidean ring in the cases

$$n = 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15.$$

Cauchy apparently overlooked the fact that when k is odd the numbers (1) for $n = k$ coincide with those for $n = 2k$; for the primitive roots of $\zeta^{2k} = 1$ only differ by a minus sign from the primitive roots of $\zeta^k = 1$. Be this as it may; Cauchy's result is correct. His proof is probably not correct, but its sketchiness makes this difficult to confirm.

In addition to these results for small n, Cauchy found analytical arguments which convinced him that also for large n – say, n greater than 10 – the numbers (1) constitute a euclidean ring. But notwithstanding repeated attempts he was not able to obtain a decisive proof.

The explanation for this failure of Cauchy's came, by post, from Germany. One can deduce the relative strengths of German and French mathematics at the time from the words below. The passage is taken from a review written by Kummer in 1847 of the first volume of Jacobi's *Mathematische Werke*. Having sung the praises of Gauss, Jacobi and of Dirichlet, Kummer writes:

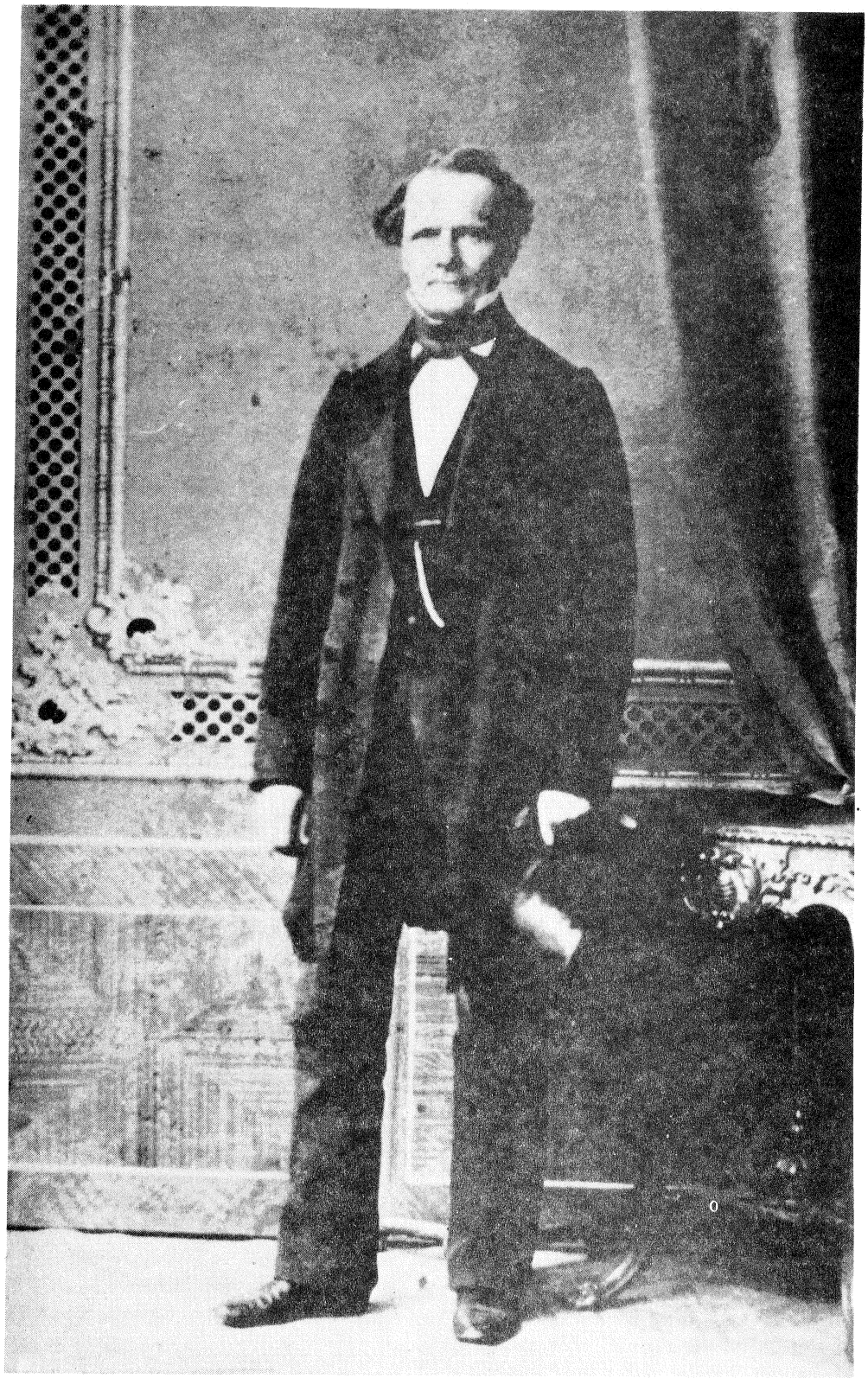
Wir könnten nach diesen noch eine treffliche Reihe deutscher Mathematiker aufführen, welche das neu erwachte Leben entweder mit anfachen halfen, oder von demselben beseelt wurden, aber die Hauptmacht und der Principat, welchen Deutschland in dieser Wissenschaft jetzt behauptet, liegt allein in den genannten drei Namen Gauss, Jacobi und Dirichlet. In Frankreich lebt jetzt nur einer, welcher diesen an die Seite gestellt werden kann, nämlich Cauchy, dessen aussrordentlich productiver Geist in den elementarsten, sowie in den sublimsten Sphären der Mathematik neues schafft, und in allem, was er unternimmt, einen Fortschritt der Erkenntniss bewirkt. Wenn wir nun in den Mathematikern ersten Ranges das entschiedene Übergewicht über die Franzosen haben, da uns drei Sterne erster Grösse glänzen, jenen nur einer, so können wir ihnen gern zugestehen, dass sie unter den mathematischen Sternen zweiter und dritter Grösse mehr ausgezeichnete Namen nachzuweisen haben, als wir, und dass dieses Übergewicht weiter hinab bis zu den teleskopischen Sternen, selbst bis zu denen sechszehnter Grösse immer mehr zunimmt.

In this situation it is little wonder that a question being puzzled over in Paris had already been answered for some time in Germany. On April 28th 1847 Kummer wrote to Liouville:

Quant à la proposition élémentaire pour ces nombres complexes, *qu'un nombre complexe composé ne peut être décomposé en facteurs premiers que d'une seule manière*, que vous regrettez très-justement dans cette démonstration défectueuse en outre en quelques autres points, je puis vous assurer qu'*elle n'a pas lieu généralement* tant qu'il s'agit de nombres complexes de la forme $\alpha_0 + \alpha_1 r + \alpha_2 r^2 + \ldots + \alpha_{n-1} r^{n-1}$, mais qu'on peut la sauver en introduisant un nouveau genre de nombres complexes, que j'ai appelé *nombre complexe idéal*.

Cauchy's reaction:

"Si M. Kummer a fait faire à la question quelques pas de plus, si même il était parvenu à lever tous les obstacles, j'applaudirais le premier au succès de ses efforts; car ce que nous devons surtout désirer, c'est que les travaux de tous les amis de la science concourent à faire connaître et à propager la vérité."



Ernſt Eduard Kummer

In one of the next *Comptes Rendus* Cauchy showed, following Kummer, that for $n = 23$ the numbers (1) do not possess the property of unique factorisation into primes. With this we close our report of the doings of the Parisian Academy in the first half of 1847. For further details one should consult the *Comptes Rendus de l'Académie des Sciences*, vol. 24, 1847.

In Germany a similar development had taken place a few years earlier, though in a somewhat less straightforward way.

The interest in numbers of the shape (1) in Germany did not arise from the wish to prove Fermat's last theorem – though there was the awareness of a possible application in this direction – but from the desire to generalise the *law of quadratic reciprocity* of Gauss (1801). The law of quadratic reciprocity says that if p and q are a pair of distinct odd primes then the two congruences

$$x^2 \equiv p \bmod q$$

$$y^2 \equiv q \bmod p$$

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

Gauss himself had shown in 1832 that in order to be able to adequately formulate such a rule for fourth powers one needs the numbers (1) with $n = 4$. In 1836 Jacobi gave a simple proof of the theorem stated by Gauss, and moreover was able to establish a cubic (third-power) reciprocity law using the numbers (1) with $n = 3$. His results suggested that for higher n one must firstly pose the following question:

(7) can every prime p that is congruent to 1 modulo n be written as the norm of a number (1)?

In the cases $n = 4$ and $n = 3$ this was known, and for $n = 5$, 8, and 12 Jacobi answered the question in the affirmative in 1839 without, however, publishing his proof.

In the developments in Germany (7) occupied the position which in France would be taken by Liouville's question (4). The two problems are closely related: if one assumes uniqueness of factorisation into primes for the numbers (1) then it is not difficult to show that the property described by (7) does indeed hold. There can be no doubt that Jacobi and, some years later, Eisenstein had the insight to realise that the converse must also be true: an affirmative answer to (7) implies unique factorisation. For n prime, a beautiful proof of this converse was given by Kummer in 1847 (see [11, vol. I, pp. 241–243]).

But this wasn't Kummer's first contribution to the problem: in 1844 he submitted to the Berlin Academy a manuscript in which he thought he had proved for all prime n that the answer to (7) is *yes*. His argument did not depend on unique factorisation, but it contained a different error. In any case, Kummer came to a timely discovery that (7) is false for $n = 23$, likely on the suggestion of Jacobi, and the erroneous proof was published only in 1977, see [7, Postscript].

It seems that this incident, after having been passed on by word of mouth for 66 years, received the form in which it is now known to the mathematical world in a speech of Hensel in 1910: Kummer was said to have thought that he had proved Fermat's last theorem but was shown by Dirichlet that the proof depended on the unjustified assumption of unique factorisation. Were this story, which incidentally is rather badly documented, to be based on some incident other than the one referred to above then Kummer would have made much the same mistake twice, and this is difficult to believe. Concerning all this one may consult the paper of H. M. Edwards cited at the end of this note.

Battered, but not defeated – so goes the story, which is now more dependable – Kummer, in 1845, managed to find a satisfactory theory by introducing *ideal complex numbers* (compare his previously cited letter to Liouville). And in March, 1847, just when in Paris people were beating their heads against the wall of unique factorisation, Kummer came to the idea of applying his ideal theory to Fermat's last theorem. From his correspondence with Kronecker one gets the impression that Kummer could not find anything better to do; and when he announces his results to the Berlin Academy he writes:

Der Fermatsche Satz ist zwar mehr ein Curiosum als ein Hauptpunkt der Wissenschaft,

Kummer managed to prove Fermat's last theorem for a large, probably for an infinite, class of prime numbers n. Whether this class of prime numbers is in fact infinite, as Kummer did at the time assert, is unknown. His methods, and the later refinements thereof, in particular those of Vandiver, recently allowed Wagstaff, with the aid of an electronic computer, to prove Fermat's last theorem for all $n < 125{,}000$. The general case remains unproved. In concluding our discussion of Fermat's last theorem it seems worthwhile to quote a remark of Knuth. In his *The Art of Computer Programming*, he illustrates his rating system for exercises with the following problem:

"[M50] Prove that when n is an integer, $n > 2$, the equation $x^n + y^n = z^n$ has no solution in positive integers, x, y, z."

In the *Answers to Exercises* one finds:

"(Note: One of the men who read a preliminary draft of the manuscript for this book reported that he had discovered a truly remarkable proof, which the margin of his copy was too small to contain.)"

We pause no further at Fermat's last theorem, nor at the subject for which Kummer had created his theory: the n-th power reciprocity laws which he was to prove in the future, and which he himself valued far more highly than the results on Fermat's theorem to which he owes his current fame. Compare his words of 1850:

Bei meinen Untersuchungen über die Theorie der complexen Zahlen und den Anwendungen derselben auf den Beweis des Fermàtschen Lehrsatzes, welchen ich der Akademie der Wissenschaften vor drei Jahren 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.

Instead we turn back to a relatively minor point to which Kummer had given some attention in 1844.

As we have seen, for $n = 23$ the answer to both (4) and (7) is *no*. The proof that was given of this is not difficult: with the aid of the *periods of Gauss* one showed that $p = 47$ cannot be the norm of a number of the shape (1) with $n = 23$. Kummer, who first considered only the case n prime, asked himself: is 23 the first example? For $n = 5$, 7, 11, 13, 17, 19 his calculations showed that indeed each prime $p \equiv 1 \bmod n$ and smaller than 1,000 is the norm of a number (1). But how could one prove this for *all* primes $p \equiv 1 \bmod n$? Kummer noted that it would be sufficient to prove uniqueness of factorisation and for this he turned to the method that also Wantzel would apply: the euclidean division algorithm.

From the summary that we have given of Wantzel's argument it is plain that the problem comes down to approximating an arbitrary expression

$$u_0 + u_1\zeta + \ldots + u_{n-1}\zeta^{n-1},$$

$$u_0, u_1, \ldots, u_{n-1} \text{ rational},$$

by a number

$$u'_0 + u'_1\zeta + \ldots + u'_{n-1}\zeta^{n-1},$$

$$u'_0, u'_1, \ldots, u'_{n-1} \text{ integral},$$

so that the difference

$$(u_0 - u'_0) + (u_1 - u'_1)\zeta + \ldots + (u_{n-1} - u'_{n-1})\zeta^{n-1}$$

has norm less than 1.

Kummer solved this problem for $n = 5$ in a letter to Kronecker dated October 2nd 1844. A simplified proof that he found a few days later may be reconstructed as follows.

The norm of $f(\zeta) = u_0 + u_1\zeta + u_2\zeta^2 + u_3\zeta^3 + u_4\zeta^4$ is defined by

$$N(f(\zeta)) = f(\zeta) \cdot f(\zeta^2) \cdot f(\zeta^3) \cdot f(\zeta^4).$$

Here one has $\overline{f(\zeta)} = f(\zeta^4)$ and $\overline{f(\zeta^2)} = f(\zeta^3)$; thus both $f(\zeta)f(\zeta^4)$ and $f(\zeta^2)f(\zeta^3)$ are real numbers $\geqslant 0$. The inequality of the means (relating the arithmetic and geometric means) now yields

$$\sqrt{N(f(\zeta))} \leqslant \tfrac{1}{2}(f(\zeta) \cdot f(\zeta^4) + f(\zeta^2) \cdot f(\zeta^3)).$$

It follows from an easy calculation that the right hand side is equal to

$$\tfrac{1}{4} \cdot \sum_{0 \leqslant i < j \leqslant 4} (u_i - u_j)^2.$$

To solve the problem with $n = 5$ it thus suffices to prove the following claim, in which we have written $v_i = u_i - u'_i$:

(8) for every choice of five real numbers u_0, u_1, u_2, u_3, u_4 one can find real numbers v_0, v_1, v_2, v_3, v_4 so that

(9) $u_i - v_i$ is integral, for $i = 0, 1, 2, 3, 4$

and

$$(10) \quad \sum_{0 \leqslant i < j \leqslant 4} (v_i - v_j)^2 < 4.$$

An inequality useful to the proof is that for arbitrary real v:

$$\sum_{0 \leqslant i < j \leqslant 4} (v_i - v_j)^2 = 5 \cdot \sum_{i=0}^{4} (v_i - v)^2 - \left(\sum_{i=0}^{4} (v_i - v) \right)^2 \leqslant 5 \cdot \sum_{i=0}^{4} (v_i - v)^2.$$

Now we choose the v_i so that (9) holds, and $0 \leqslant v_i < 1$. Then, with $v = \frac{1}{2}$ it follows from the above inequality that

$$\sum_{0 \leqslant i < j \leqslant 4} (v_i - v_j)^2 \leqslant 5 \cdot ((\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2) = 6\tfrac{1}{4}$$

which is not good enough to give (10). To obtain a better result we note that we may suppose that there are k and l, $0 \leqslant k < l \leqslant 4$, with $|v_k - v_l| \leqslant \frac{1}{5}$. This is clear if the v_i all lie in an interval of length $\leqslant \frac{4}{5}$ and if the interval is longer (but < 1), we subtract 1 from the largest v_i; this does not disturb the validity of (9).

If we now take v to be the average of v_k and v_l we obtain $|v_k - v| \leqslant \frac{1}{10}$, $|v_l - v| \leqslant \frac{1}{10}$. To the remaining v_i we add, if necessary, $+1$ or -1 so as to obtain $|v_i - v| \leqslant \frac{1}{2}$. We find that

$$\sum_{0 \leqslant i < j \leqslant 4} (v_i - v_j)^2$$

$$\leqslant 5 \cdot ((\tfrac{1}{10})^2 + (\tfrac{1}{10})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2) = 3.85 < 4,$$

so demonstrating (10). Thus for $n = 5$ the numbers (1) form a euclidean ring.

Kummer claimed to be able to deal with the case $n = 7$ in a similar way. So for given $u_0, u_1, \ldots, u_6$ one should be able to find numbers $v_0, v_1, \ldots, v_6$ with $u_i - v_i$ integral ($i = 0, 1, \ldots, 6$) and

$$(11) \quad \sum_{0 \leqslant i < j \leqslant 6} (v_i - v_j)^2 < 6.$$

But the argument we have given for $n = 5$ now provides only

$$\sum_{0 \leqslant i < j \leqslant 6} (v_i - v_j)^2 \leqslant 8\tfrac{23}{28}.$$

Nevertheless it is believable that Kummer did prove (11). This becomes apparent if one investigates just what is the best possible result for n numbers, rather than 5 or 7. One then finds (see [13]):

$$\sum_{0 \leqslant i < j < n} (v_i - v_j)^2 \leqslant \frac{n^2 - 1}{12},$$

where the equality sign is needed, for example, if $u_i = i/n$ for $i = 0, 1, \ldots, n-1$. In particular < 4 in (10) can be replaced by $\leqslant 2$ and < 6 in (11) can be replaced by $\leqslant 4$. When $n = 11$ one obtains $\leqslant 10$, and, apart from a small problem with the equality sign, this is just what is needed for the proof that also in the case $n = 11$ the numbers (1) form a euclidean ring. This result is not noted by Kummer. The cases $n = 13$, 17 and 19 remain undetermined by the present method.

Once Kummer had developed his ideal theory the questions occupying us here receded from the spotlight. We will not delve further into the history of the subject but shall restrict ourselves to a brief discussion of the results now known.

A few years ago Masley and Montgomery, see [16], determined all those n for which the numbers (1), with ζ a primitive root of $\zeta^n = 1$, have the property of unique decomposition into prime factors. As we saw in discussing Cauchy's results we can restrict ourselves to the case where n is not 2 modulo 4. For such n the answer to (4) is *yes* if and only if n takes one of the following thirty values:

(12) 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 difficult part of this theorem is the *only if* portion: the proof that the answer to (4) is *no* for all other values of n, $n \not\equiv 2 \bmod 4$. The proof of the *if* portion becomes routine if one applies methods developed by Minkowski; the concept *euclidean ring* plays no role whatsoever.

For thirteen of the thirty values (12) it is known that the numbers (1) form a euclidean ring with respect to the norm. These are

(13) 1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 16, 20, 24.

The remaining seventeen values appear never to have been investigated, with the exception of $n = 32$. In this case the euclidean property does not hold: if ζ is a primitive root of $\zeta^{32} = 1$, then it is impossible to so divide $1 + (1 + \zeta)^5$ by $(1 + \zeta)^6$ that the remainder has norm smaller than $N((1 + \zeta)^6) = 64$.

The numbers (13) are exactly all the n, $n \not\equiv 2 \bmod 4$ for which $\varphi(n) \leqslant 10$. Here $\varphi(n)$ denotes the number of integers m with $1 \leqslant m \leqslant n$ which are relatively prime to n. It is easy to see that $\varphi(n)$ is exactly the number of primitive roots of $\zeta^n = 1$. Moreover, $\varphi(n)$ turns out to be the smallest number d with the property that all the numbers (1) can be expressed as

$$a_0 + a_1\zeta + \ldots + a_{d-1}\zeta^{d-1},$$

$a_0, a_1, \ldots, a_{d-1}$ integers.

One can therefore take $\varphi(n)$ as a measure of how *many* numbers (1) there are, and view the thirteen cases (13) as the thirteen simplest.

Euclid noted that one has a euclidean ring when $n = 1$. The case $n = 4$ can be found in Gauss [9, pp. 117–118] and Dirichlet [6, vol. I, pp. 540–541]. That the case $n = 3$ is similar was generally known, but prior to Wantzel [3, pp. 430–434] no one seems to have found it worthwhile to write a proof. A proof can also be found in Gauss' posthumous papers [9, pp. 391–393]. The case $n = 5$ was first published by Ouspensky [18], a few years before Kummer's proof appeared. Eisenstein [8, vol. II, pp. 585–595] dealt with the case $n = 8$, see also [12] and [15]. A remark of his suggests he could also cope with the case $n = 12$, but I have not been able to find a proof published before 1972, see [12]; see also [15]. Proofs for $n = 7, 9, 11, 15, 20$ can be found in [13]. Ojala [17] found a long proof – one hour of computing time on a UNIVAC 1108 – for the case $n = 16$. Finally, the case $n = 24$ has been handled with the help of properties of the lattice Γ_8, see [14].

References

1. F. Cajori, Pierre Laurent Wantzel, *Bull. Amer. Math. Soc.* 24 (1918), 339–347
2. A. Cauchy, *Oeuvres complètes*, sér. 1, tome X, Gauthier-Villars, Paris 1897.

3. *Comptes Rendus de l'Académie des Sciences* 24 (1847)
4. L. E. Dickson, *History of the theory of numbers,* vol. II, Ch. XXVI, Chelsea, New York 1952 (reprint)
5. L. E. Dickson et al., *Algebraic numbers,* Chelsea, Bronx, n. d. (reprint)
6. G. Lejeune Dirichlet, *Werke,* Chelsea, Bronx 1969 (reprint)
7. H. M. Edwards, The background of Kummer's proof of Fermat's last theorem for regular primes, *Arch. History Exact Sci.* 14 (1975), 219–236; Postscript, ibid. 17 (1977), 381–394
8. G. Eisenstein, *Mathematische Werke,* Chelsea, New York 1975
9. C. F. Gauss, *Werke,* Zweiter Band, Göttingen 1876
10. C. G. J. Jacobi, *Gesammelte Werke,* Sechster Band, Chelsea, New York 1969 (reprint)
11. E. E. Kummer, *Collected Papers,* Springer, Berlin 1975
12. R. B. Lakein, Euclid's algorithm in complex quartic fields, *Acta Arith.* 20 (1972), 393–400
13. H. W. Lenstra, Jr., Euclid's algorithm in cyclotomic fields, *J. London Math. Soc.* (2) 10 (1975), 457–465
14. H. W. Lenstra, Jr., Quelques exemples d'anneaux euclidiens, *C. R. Acad. Sc. Paris,* Sér. A, 286 (1978), 683–685
15. J. M. Masley, On Euclidean rings of integers in cyclotomic fields. *J. Reine Angew. Math.* 272 (1975), 45–48
16. J. M. Masley, H. L. Montgomery, Cyclotomic fields with unique factorization, *J. Reine Angew. Math.* 286/287 (1976), 248–256
17. T. Ojala, Euclid's algorithm in the cyclotomic field $\mathbb{Q}(\zeta_{16})$, *Math. Comp.* 31 (1977), 268–273
18. J. Ouspensky, Note sur les nombres entiers dépendant d'une racine cinquième de l'unité, *Math. Ann.* 66 (1909), 109–112. Cf. *Jbuch Fortschr. Math.* 37 (1906) 241
19. H. J. S. Smith, *Report on the theory of numbers,* Chelsea, Bronx 1965 (reprint)
20. S. S. Wagstaff, Jr., The irregular primes to 125,000, *Math. Comp.* 32 (1978), 583–591
21. A. Weil, La cyclotomie jadis et naguère, *Sém. Bourbaki* (1973/74), exp. 452, *Lecture Notes Math.* 431. Springer, Berlin 1975

H. W. Lenstra, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam
Netherlands

A. J. van der Poorten
School of Mathematics and Physics
Macquarie University
North Ryde
NSW 2113 Australia