3. _____, *On infinite series representations of real numbers*, Compositio Math. **27** (1973), 197–204. MR **48** #11026.

4. I. Niven, *Irrational numbers*, Carus Math. Monos., no. 11, Math. Assoc. of Amer.; distributed by Wiley, New York, 1956. MR **18**, 195.

5. T. Salát, *A remark on normal numbers*, Rev. Roumaine Math. Pures Appl. **11** (1966), 53–56. MR **34** #1270.

6. F. Schweiger, *Metrische Theorie einer Klasse zahlentheoretischer Transformationen*, Acta Arith. **15** (1968), 1–18. MR **40** #7219.

7. B. Volkmann, *Über Hausdorffsche Dimensionen von Mengen, die durch Zifferneigenschaften charakterisiert sind.* VI, Math. Z. **68** (1958), 439–449. MR **20** #7008.

8. _____, *Über extreme Anormalität bei Ziffernentwicklungen*, Math. Ann. **190** (1970/71), 149–153. MR **43** #6161.

BODO VOLKMANN

BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 83, Number 5, September 1977

Ernst Edward Kummer, Collected Papers (edited by André Weil), Vol. I: *Contributions to number theory*, viii + 957 pp., $40.20, Vol. II: *Function theory, geometry and miscellaneous*, Springer-Verlag, Berlin-New York, 1975, xi + 877 pp., $42.20.

1. Whatever the reason for the eighty years' delay in the publication of Kummer's collected papers,[1] they now meet an audience whose interest in the number-theoretic contributions is, one expects, undiminished. If anything, the intervening years have given that audience a chance to catch its breath, and to absorb techniques ("p-adic"[2] in particular). The broad lines of Kummer's number-theoretic ideas now form an essential part of our heritage: it is fascinating to follow the details of their evolution.

The collected works are in two volumes. Volume I consists of Kummer's number theory. It constitutes a unity of thought and spirit almost from first sentence to last. One of the joys of reading it is in the double spectacle: the steady train of mathematical content, unimpeded by lack of basic algebraic number theory; while here and there, to serve problems at hand, the deft, unobtrusive forging of pieces of present day technique. It is not hard to get into, even for those of us who have had little contact with the history of our subject. Cleft though one may think one is from historical sources, on reading Kummer one finds that the rift is jumpable, the jump pleasurable. The reader is greatly helped in this jump in two ways. Firstly, included in the volume is a continuum of well-written, moving letters from Kummer to Kronecker giving the details of many of Kummer's important discoveries as they freshly occurred to him (these, together with some letters from Kummer to his

---

[1] Weil, in his introduction, suggests that Hilbert, who dominated German mathematics in the late 19th and early 20th centuries, had little sympathy for Kummer's "p-adic" point of view, and asks whether this might not constitute a reason.

[2] Nowhere in Kummer's works will you find the word "p-adic" (nor, for that matter, "group"). The former term and concept were introduced far later by Hensel, but Kummer used the fact that formal power series in p may define numbers modulo p^n for arbitrarily high values of n. His progress seems so untrammelled by the lack of these explicit notions and so natural to describe by means of them that in the present review we will use modern language for them where suitable, although in some other respects, we shall try to be more faithful to Kummer's (explicit) ideas and choice of words.

mother, form part of a description of Kummer's work by Hensel on the occasion of the centenary of Kummer's birth, also included in the volume). Secondly, there is an excellent introduction, in which Weil describes the main lines of Kummer's work, and explains its relations to Kummer's contemporaries, and to us.[3]

Volume II is in four parts:

1. *Function theory*. Here one finds his work on the hypergeometric function, and on repeated integrals of rational functions. For a close reading of his papers on "logarithmic functions of higher order", including corrections of some errors and misprints, see [4].

2. *Algebraic geometry*. His discovery of "Kummer surfaces" (quartic surfaces in $\mathbf{P}^3$ with 16 double points) seems, curiously enough, to be an outgrowth of his interest in the optical properties of biaxial crystals, and in the "Cyclides" of Dupin. The relation between these quartic surfaces and quotients of abelian surfaces (or θ-functions) was perceived only much later. One also finds here a number of papers describing actual plaster models (of the real loci, to be sure) of particular "Kummer surfaces", with special symmetries in evidence, etc.

3. *Aerodynamics and ballistics*.

4. *Speeches and reviews*. A surprisingly broad range of topics, including a long retrospective on the life and work of Dirichlet.

Comments on the four main themes of Volume I are given in the four sections below.

Page numbers to Volume I of the collected papers are signalled by the letter K (e.g., K 539 means p. 539 of Volume I of the collected papers). "Weil's introduction" means his introduction to Volume I. Bracketed numbers refer to the bibliography at the end.

2. The discovery of ideal complex numbers (and Kummer's "reagents").

a. "*Reagents*". Kummer's "ideal complex numbers" Dedekind's "ideals", and Kronecker's "divisors" are successive, distinct discoveries. The particular intentions of the discoverers were quite different, and seen from their view, the three concepts appear to be almost independent.

Kummer's "ideal prime complex number" is, in modern language, a homomorphism from a ring of cyclotomic integers to a finite field (to be slightly more accurate, it is the associated valuation). But his homomorphisms were constructed in a very special fashion; they were conceived in an interesting way and Kummer did not know Galois' work on 'finite fields'. We shall describe the steps of Kummer's construction, flitting from his language to ours.

> "Ideal complex numbers are comparable to the hypothetical radicals which don't exist in themselves, but only in combinations; fluor, in particular, an element which one cannot isolate, can be compared to an ideal prime

[3] A forthcoming book of H. Edwards on Fermat's Last Theorem gives a beautiful and vivid account of Kummer's times and thought and will make this subject accessible to an even wider audience. See also [1].

> factor. The notion of equivalence of ideal factors is, at bottom, the same as that of chemical equivalence . . .
>
> Comparing the methods of chemical analysis to those of decomposition of complex numbers one finds further surprising analogies. For, just as chemical reagents added to a dissolved substance yield precipitates, by means of which one determines the elements contained in the substance, so, the numbers we have denoted $\psi(\alpha)$, as reagents of complex numbers, allow one to determine the prime factors contained in complex numbers by 'putting in evidence' a prime factor q, analogous to the chemical precipitate . . . (K 443; 1851)"

b. ("*Complex numbers*"). For Kummer, α always denotes a primitive λth root of 1, and λ an odd rational prime number. A "complex number" for him[4] is an element of $\mathbf{Z}[\alpha]$ and he will denote it $f(\alpha)$, thinking of the polynomial $f(X) = \sum_{j<\lambda} a_j X^j$ which gives rise to the complex number by substitution of α for X. This gives him ready notation for the conjugates of $f(\alpha)$ ($f(\alpha^i)$, $i = 1, \ldots, \lambda - 1$). These complex numbers will sometimes be called *real* ("wirklichen") for the same notation is forced to serve the concept of *ideal* complex number.

Consider the extraordinary fortune that Kummer has in dealing with the ring $\mathbf{Z}[\alpha]$. Firstly, although Kummer does not have the general notion of algebraic integers (this subtle notion is a later discovery of Dedekind, and Kronecker; its lack is a frequent cause of confusion in early work in number theory), Kummer's "complex numbers" *are* all the cyclotomic integers. Further, all subfields of $\mathbf{Q}(\alpha)$ are completely given by the periods of Gauss. Explicitly, let γ be a primitive λth root of 1. Then, for each divisor e of $\lambda - 1$, any one of Gauss's periods $\eta_i = \sum_{j=0}^{f-1} \alpha^{\gamma^{i+ej}}$ (call these *the periods of degree e*) generate the unique subfield of degree e (call it $\mathbf{Q}(\eta)$ where $\eta = \eta_0$). But the decisive and singular luck is that, in modern language, the 'decomposition law' in $\mathbf{Z}[\alpha]$ admits a strikingly simple description: If $p \neq \lambda$ is a rational prime, of order f in the group of units mod λ, then p splits completely in $\mathbf{Q}(\eta)$ where η is a period of degree $e = (\lambda - 1)/f$ (i.e., $(p) = P_1 \cdot \ldots \cdot P_e$ where the primes P_j have residue field $\mathbf{F}_p$) and the ideals $\mathfrak{P}_j = P_j \cdot \mathbf{Z}[\alpha]$ remain prime in $\mathbf{Z}[\alpha]$. If p and η are related in this way, say that η is a *period for p*.

c. *Kummer's De numeris complexis . . .* (1844, Breslau; republished by Liouville in 1847). Let us turn now to Kummer's first published work on "complex numbers" [**10**]. The subject is that of factoring "complex numbers" into prime complex numbers. To be sure, factorizations are to be taken up to multiplication by units; there are an infinity of these ($\lambda > 3$) as Kummer knows, for he has the "cyclotomic units" (we shall call them *circular units* to avoid confusion, and we take them to be elements in the group generated by units of the form $(\alpha^i - \alpha^j)/(1 - \alpha)$; $i \neq j$). He is also aware of that other ambiguity: the failure of unique factorization: in a musing lament, beginning "Maximum dolendum videtur . . . " (to be recalled to us later (K 207) when he is in a jubilant state of mind) he bemoans this blemish on his "complex numbers", suggesting that perhaps one should seek another kind of complex

[4] The direct descendants of the "complex numbers" of Gauss and Jacobi [**3**, 6 275–280]. See also Eisenstein's *Beiträge zur Kreistheilung* (1844), p. 45, vol. i of [**2**].

number, more closely analogous to "real numbers".[5] The paper concentrates on the problem of expressing a rational prime p as a norm, $p = Nf(\alpha)$. For this to be possible, p must be congruent to 1 mod λ, a reasonable special case which avoids the encumbrance of residue field extension. It is natural for Kummer to actually *obtain* the factorization $p = Nf(\alpha)$, for large quantities of p's, for reasons which are related to the particular cast of his discovery later of ideal numbers; these reasons therefore deserve explanation. If one wishes to determine whether a general complex number $\varphi(\alpha)$ is divisible by some prime factor dividing p, there are two ways of proceeding: One may calculate the norm of $\varphi(\alpha)$ (which may be lengthy), determine whether it is divisible by p, and go on from there, or, having a factorization $p = Nf(\alpha)$ at hand, one can form $\psi(\alpha) = f(\alpha^2) \cdot f(\alpha^3) \cdot \ldots \cdot f(\alpha^{\lambda-1})$. Then, to test whether $\varphi(\alpha)$ is divisible by $f(\alpha)$ one need only check whether $\varphi(\alpha) \cdot \psi(\alpha)$ has all its coefficients divisible by p. The quantity $\psi(\alpha)$ is the first form of Kummer's "reagents". In our terms, it is a uniformizer at all primes lying above p, *except the prime* $f(\alpha)$, and it is a unit everywhere else. One might call it a *complementary uniformizer*. Multiplication by $\psi(\alpha)$ and reduction modulo p gives us the homomorphism from $\mathbf{Z}[\alpha]$ to $\mathbf{F}_p$. For this 'test-for-divisibility-by-$f(\alpha)$' to be efficient, it is natural to seek as simple as possible a $\psi(\alpha)$ (lowest coefficients). Kummer took joy in this search, investing it with craftsmanlike pride, as is clear from a glance at his table (K 206–208) which ends with $\lambda = 23$, the first case where unique factorization fails,[6] e.g., the prime 47 fails to be expressible as a norm. As one discovers by reading his collected works, Kummer's passion for elegant elementary calculation endured. For example, in 1870, he took the trouble to explain his method of finding the 'simplest' $f(\alpha)$ ("der Reinigung der complexen Zahlen von den sie behaftenden Einheiten ohne Schwierigkeit") and twice devoted short communications to providing, in a few cases,[7] simpler expressions than appeared in the extensive factorization tables ($\lambda < 1000$) of Reuschle.

d. *Kummer's unpublished* 1844 *manuscript.*[8] An unpublished earlier paper of Kummer (*Über die complexen Primfaktoren der Zahlen und deren Anwendung in der Kreisteilung*) submitted to the Berlin Academy of Sciences on April 21, 1844, and withdrawn shortly afterwards, has just been brought to light by Edwards [**1**]. In this paper, Kummer claims (wrongly, of course) to prove that every prime number p congruent to 1 modulo λ can be expressed as a norm $p = Nf(\alpha)$. This was therefore written before he had made his famous calculation for $\lambda = 23$. This paper is undoubtedly also the one referred to in a

[5] "Real numbers" means rational integers.

[6] From then on it always fails [**5**], [**9**].

[7] $\lambda = 29, 31$; in these cases the ideal class group is noncyclic and Kummer wished to obtain its structure in an efficient manner. Despite the lack of (explicit) group theory, Kummer was sensitive to the question of noncyclicity of the ideal class group (this goes under the heading "sehr mysteriösen Irregularität von Determinanten") and he determined all the instances of this phenomenon for low values of λ. See especially [**15**] (also footnote K 956) and its application to $\lambda = 41$ whose ideal class group is of type (11, 11).

[8] Not included in the collected papers. See [**1**].

letter from Eisenstein to Stern [2, p. 793, vol. II] (English transl. [1]), in which he discusses his own work on higher reciprocity[9]:

> ... You can hardly imagine how delicate these investigations are. There are difficulties in the very first elements of complex numbers, about which one knows nothing.
>
> Professor Kummer was fortunately able to take back his beautiful theory of complex numbers from the Academy ... in time; it contained so much revolutionary material that I for one would have gone crazy; one can use it to prove that there is only one quadratic form for each determinant and other such nonsense ... If one had the theorem which states that the product of two complex numbers can be divisible by a prime number only when one of the factors is–which seems completely obvious–then one would have the whole theory [referring to higher reciprocity laws] at a single blow; but this theorem is totally false and entirely new principles must be applied ...

Eisenstein's letter implies that he knew of the failure of unique factorization, and its relation to Gauss's theory of binary quadratic forms, before Kummer's 1844 paper. In contrast, this was unknown to the French Academy until 1847 when Kummer, motivated by Lamé's announcement of a proof of Fermat's last theorem, wrote a letter to Liouville (K 298) informing him, firstly, of the failure of unique factorization for complex numbers, and secondly of its resuscitation ("on peut le sauver") by means of ideal complex numbers. It was Kummer's letter that led Liouville to republish Kummer's 1844 paper [10] side-by-side with Lamé's purported proof. Liouville heralded this mathematical joust with a note (K 298) which ends: "C'est au temps à fixer la valeur de leurs travaux et à mettre toute chose à sa place."

e. *Homomorphisms.* Kummer's next step is to investigate complex prime factors of norm p^f (letter to Kronecker of Oct. 2, 1844). For these, the natural intermediate field to work in is $\mathbf{Q}(\eta)$ where η is a Gauss period of order e, $ef = \lambda - 1$. As we know, given a complex prime factor $f(\alpha)$ of norm p^f, one can associate to it a homomorphism from $\mathbf{Z}[\eta, \eta_1, \ldots, \eta_{e-1}]$ to $\mathbf{F}_p$ (the one determined by the prime of $\mathbf{Q}(\eta)$ 'over which $(f(\alpha))$ lies'). In the course of [11] Kummer produces such homomorphisms. If u_j is the image of η_j, then he will indicate this 'homomorphism' by "$\eta = u$, $\eta_1 = u_1$, ... etc." He uses, however, a fallacious argument when the prime of $\mathbf{Q}(\eta)$ divides the norm of $\eta - \eta_i$.[10] This argument persists in his early papers, and it is only in 1856 that

[9] In his introduction (written before the withdrawn article was unearthed), Weil suggests that Eisenstein's letter might be alluding to an incorrect proof of Fermat's last theorem that Kummer supposedly submitted to Dirichlet (see Hensel's 'biography' of Kummer (K 54)). For a spirited account of these, and related historical matters, see [1].

[10] He produces the u_j's by working with a matrix with integral coefficients and attempting to invert it modulo p. Although the matrix has a nonzero determinant D, it may very well happen that $D \equiv 0 \bmod p$ .... For a discussion of this, related errors, and the ultimate correct argument replacing them, see [1] and Weil's introduction and notes.

This is one of Kummer's errors that Weil discusses in some detail. Weil points out that Kummer's papers are surprisingly free of errors. He doesn't go into the questions raised by Vandiver concerning gaps in Kummer's later papers and it is reasonable not to do so. Neither does he correct the known errors in Kummer's tables, some of which were later corrected by Kummer himself. These numerical errors, however, could have easily been footnoted on the pages on which they occurred.

he produces a correct argument. It is this error, also occurring in Kummer's expository paper (1851; J. Math. Pures Appl.) which is the subject of a letter from Liouville to Dirichlet recently found by Edwards [1].

> "Ouvrons, je vous prie, le Mémoire de M. Kummer à la page ... de mon journal ... " says Liouville, putting his finger on the problematic formula, and an accompanying "on en conclut aisément ... " in the text. He then laments that neither he nor Cauchy nor anyone else he knows can make the conclusion *easily*, imploring Dirichlet for a proof ... "aisément ou non".

The pressing cause for Liouville's concern was that the Paris Academy was, at that time, preparing to award Kummer their prize for a proof of Fermat's last theorem (offered in 1850, but, to be sure, unclaimed) even though Kummer himself had not officially entered the competition.

f. *Ideal prime factors.* Things are now set for that double stroke of insight which gushes forth a year later in the jubilant letter to Kronecker and the corresponding public communications: one can construct the test-for-divisibility-by-$f(\alpha)$ without actually having $f(\alpha)$–in fact, whether or not $f(\alpha)$ exists–and that these test *themselves* should be taken as *ideal* prime factors of p. Kummer saw that one can make do with far less than $f(\alpha)$. What he wanted, in present-day language, is a *local* uniformizer for the prime of $\mathbf{Q}(\eta)$ corresponding to the above homomorphism, which is a unit at all other primes of norm p^f and where η is a period for p (cf. **b** above). As Kummer put it, one must find a $\psi(\alpha)$ such that $\psi(\eta) \equiv 0 \bmod p$ for the substitution $\eta = u$, and such that $\psi(\eta)\psi(\eta^2)\cdot \ldots \cdot \psi(\eta^{e-1})$ which is divisible by p, is not divisible by p^2. Then, set: $\Psi(\eta) = \psi(\eta^2)\cdot \ldots \cdot \psi(\eta^{e-1})$ (one is tempted to call $\Psi(\eta)$ a *'complementary' local uniformizer*) and, by definition, the general complex number $\varphi(\alpha)$ *contains the ideal prime factor belonging to* $\eta = u$ *m times* if m is the largest integer such that $\varphi(\alpha)\cdot \Psi(\eta)^m$ is divisible by p^m. Let us quote his definition of ideal prime factor (ignoring "multiplicities") and the flood of analogies illuminating it from his 1851 expository paper [13].

> If a complex number $f(\alpha)$ satisfies the condition
>
> $$f(\alpha) \equiv 0 \pmod{q} \quad \text{for } \eta = u_r,$$
>
> we will say that $f(\alpha)$ contains the *ideal prime factor of the number q which belongs to the substitution* $\eta = u_r \cdots$ we believe that these factors render visible, so to speak, the internal constitution of numbers, so that their essential properties are brought to light. A complex number satisfying several of the above type conditions, even if it is not decomposable in complex factors, behaves rather like a composite number ... Algebra, Arithmetic and Geometry offer numerous analogies to our theory. One decomposes, for example, rational and polynomial functions of one variable in linear factors, although these isolated factors exist only in special cases; it is to this end that imaginary quantities were created. In geometry one speaks of a line passing through the intersection points of two circles, even when these intersection points don't exist. In this example, the general property that the tangents drawn from an arbitrary point of this line to the two circles are equal (in length) is the analogue to the general property of the complex number "$f(\alpha) \equiv 0 \pmod{q}$ for $\eta = u_r$", while the accidental property of this

> line (that of passing through the intersection points of the two circles) is the analogue of the accidental property that the complex number $f(\alpha)$ have an *existant* prime factor $\varphi(\alpha)$.
>
> Finally the idea of considering ideal factors of complex numbers is, at bottom, the same as that which produced the complex numbers themselves . . .

It is interesting at this point to turn to Dedekind who, in 1876, when describing the features of his own concept of *ideal*, says that he has no need of *any new creation* like that of Kummer's ideal numbers; for him it completely suffices to consider the system of *really existing numbers* which he calls an ideal. His curious objection to Kummer is that Kummer hasn't defined ideal complex numbers *themselves* but only the notion of *divisibility by these numbers*.

To be sure, Dedekind, who had already conceived his "cut" definition of real numbers, had a predilection for grounding existence in set-theoretic constructions.

The boldness of Kummer's discovery is surpassed only by the boldness with which he makes use of it. The reader is struck by the swift emergence in his papers of much of what is now algebraic number theory (in cyclotomic domains, to be sure) as crown and corollary of the theory of ideal complex numbers: equivalence, ideal class 'groups', finiteness of the class number, analytic techniques (the 'analytic formula' inspired by Dirichlet) and, more singularly unique to Kummer, p-adic analytic techniques.

The only application of his theory given in his first two papers on ideal complex numbers is to determine the (ideal) prime decomposition of the λth power of the 'Lagrange resolvents':[11]

$$x + \alpha x^g + \alpha^2 x^{g^2} + \cdots + \alpha^{p-2} x^{g^{p-1}}$$

(here p is a prime number congruent to 1 mod λ, x is a primitive pth root of 1, and g is a primitive root modulo p), generalizing a formula of Jacobi. Except for the introduction of ideal numbers, Kummer had already obtained this decomposition formula in his 1844 paper. By means of this decomposition formula (viewing it at a slant) one may obtain an ideal in the integral group ring of

$$\mathrm{Gal}\big(\mathbf{Q}(\exp(2\pi i/\lambda))/\mathbf{Q}\big) = (\mathbf{Z}/\lambda\mathbf{Z})^*$$

which annihilates the ideal class group. (Anticipating Stickelberger's generalization [**8**] we shall call it the *Kummer-Stickelberger* ideal $\mathfrak{S}$ which is essentially (cf. [**6**]) generated by one element, the *Kummer-Stickelberger element*,

$$s = \frac{1}{\lambda} \sum_0^{\lambda-1} a \cdot \sigma_a^{-1} \in \mathbf{Q}\big[(\mathbf{Z}/\lambda\mathbf{Z})^*\big]$$

where σ_a is the image of the integer a in $(\mathbf{Z}/\lambda\mathbf{Z})^*$. Explicitly:

$$\mathfrak{S} = \mathbf{Z}\big[(\mathbf{Z}/\lambda\mathbf{Z})^*\big] \cap s \cdot \mathbf{Z}\big[(\mathbf{Z}/\lambda\mathbf{Z})^*\big].)$$

---

[11] Stickelberger [**8**] refers to this (or rather its generalization to composite λ) as the "Kreistheilungsresolvente"; Hilbert refers to it as a "Wurzelzahl"; modern authors call it a "Gauss sum".

Except for the modern formulation, Kummer proves this. It is not surprising that Kummer should be seized by the importance of the 'Kummer-Stickelberger' element, for it dominates the study of the ideal class group; it is the link between the properties of that group and the Bernoulli numbers: it remains to the present day the (still poorly understood) keystone of p-adic analytic number theory.

3. Kummer's congruence. This is usually stated as the following congruence between p-integers:

$$B_m/m \equiv B_{m+(p-1)p^n}/m + (p-1)p^n \mod p^{n+1},$$

where B_m is the mth Bernoulli number and $m \geqslant \max(2, n)$, and $m \not\equiv 0 \mod p-1$. ($B_{2n+1} = 0$; $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42, \ldots$; here we have departed from Kummer's indexing.)

Although one does find the above congruence for $n = 0$ in [**13**], Kummer fell upon a slightly different form of the general congruence ("ein ganz nettes Früchtchen meiner Untersuchungen") in the course of other pursuits and quickly saw that the above congruence is but the symptom of far broader relations; these broader relations have resurfaced recently to general mathematical consciousness (beginning with the work of Kubota-Leopoldt) in terms of p-adic interpolation of values of the zeta function.

For $k \geqslant 3$ an odd integer, and c a p-adic unit, consider the following 'modified' value of the Riemann zeta function at $s = -k$:

$$\zeta_c^{(p)}(-k) = (1 - c^{k+1})(1 - p^k)\zeta(-k),$$

where $\zeta(-k) = -B_{k-1}/(k-1)$ is the value of the ordinary Riemann zeta function at $-k$.

Now the "generalized Kummer congruences"[12] imply that if $f(X) = \sum a_k X^k \in \mathbf{Z}[X]$ is a polynomial whose values are congruent to zero mod p^{n+1} for all $x \in \mathbf{Z}_p^*$, then $\sum a_k \zeta_c^{(p)}(-k) \equiv 0 \mod p^{n+1}$. [To obtain the congruences which occur in Kummer's paper (K 361) from the generalized Kummer congruences, the reader should use the polynomial

$$f(X) = X^{2\nu}(1 - X^{p-1})^{n+1}$$

Note the relation $f(x) \equiv 0 \mod p^{n+1}$ for $x \in \mathbf{Z}_p$ provided $2\nu \geqslant n+1$.]

The most fluid language to express such relations is that of $\mathbf{Z}_p$-valued measures $d\mu$ on $\mathbf{Z}_p^*$ (namely: bounded $\mathbf{Z}_p$-valued functions $f \mapsto \int_{\mathbf{Z}_p^*} f \cdot d\mu$ on the space of continuous $\mathbf{Z}_p$-valued functions on $\mathbf{Z}_p^*$; equivalently: $\mathbf{Z}_p$-valued finitely additive functions on open and closed subsets of $\mathbf{Z}_p^*$). It is evident that if two functions on $\mathbf{Z}_p^*$ enjoy the congruence $f \equiv f' \mod p^{n+1}$, then the same congruence holds for their integrals:

$$\int_{\mathbf{Z}_p^*} f \cdot d\mu \equiv \int_{\mathbf{Z}_p^*} f' \cdot d\mu \mod p^{n+1}.$$

The "generalized Kummer congruences" are equivalent to the assertion

[12] As elegantly explained by Katz in his lectures at the conference on modular forms (Bonn, 1976).

that (for any choice of p-adic unit c) there is a measure $d\mu^c$ on $\mathbf{Z}_p$ such that

$$\int_{\mathbf{Z}_p} x^k \, d\mu^c = (1 - c^{k+1})\zeta(-k) \quad \text{and} \quad \int_{\mathbf{Z}_p^*} x^k \, d\mu^c = \zeta_c^{(p)}(-k)$$

for all odd $k \geqslant 3$.[13]

From this vantage point it is clear that the shape of such congruences is not restricted to Bernoulli numbers, but follows more generally from the existence of a measure. This is not far from the spirit of Kummer's explanation [13].

4. Fermat's last theorem.

> "Fermat's last theorem is, to be sure, more of a curiosity than a pinnacle of Science . . . " (K 281).

A month after Lamé presented his purported proof of Fermat's last theorem to the Paris academy, Kummer sent the details of his own version to Kronecker. Soon afterwards the *Beweis des Fermat'schen Satzes der Unmöglichkeit von* $x^\lambda + y^\lambda = z^\lambda$ *für eine unendliche*[14] *Anzahl Primzahlen* λ [12] appeared.

He initially proves the Fermat theorem under two hypotheses:

A. The class number h of $\mathbf{Q}(\alpha)$ is not divisible by λ.

B. Every unit in $\mathbf{Z}[\alpha]$ which is congruent to a rational integer modulo λ is a λth power of a unit.

But these hypotheses immediately change their form (see Dirichlet's response to Kummer's communication and Kummer's response to Dirichlet, all in [12]). Hypothesis B follows from A, and hypothesis A admits further analysis leading Kummer to a deep study of the class number: One may separate the study of h into two parts which have strikingly different behavior $h = h^- \cdot h^+$. We have departed, again, from Kummer's notation. Kummer calls h^- the *first* and h^+ the *second* factor. One can show that the ideal class group H^+ of the maximal totally real subfield $\mathbf{Q}(\alpha + \alpha^{-1})$ of $\mathbf{Q}(\alpha)$ injects into the ideal class group H of $\mathbf{Q}(\alpha)$. Letting $H^- = H/H^+$ define h^+ and h^- to be the orders of H^+ and H^-, respectively. The element σ_{-1} of $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ (cf. §2f) acts as ± 1 on $H^\pm$.

The first factor h^- is amenable to analysis.[15] Using the fact that the Kummer-Stickelberger ideal annihilates H^-, the hypothesis that $h^- \equiv 0 \bmod \lambda$ implies a congruence of the form $\sum_{a=1}^{p-1} \chi^{-1}(a) \cdot a \equiv 0 \ (\lambda^2)$ for some odd Dirichlet character χ of conductor p. This, in turn, is equivalent (after an elementary calculation) to saying that one of the first $(\lambda - 3)/2$ Bernoulli numbers (of even index in my notation) are divisible by λ. Indeed, Kummer shows that h^- is not divisible by λ if none of the first $(\lambda - 3)/2$ Bernoulli numbers is divisible by λ.

---

[13] The existence of these measures is equivalent to the existence of the p-adic Kubota-Leopoldt zeta function possessing the standard properties.

[14] One still does not know an infinity of λ for which Fermat's last theorem is true. See footnote 17 below. Weil's comment about this is: "after such a step forward, Kummer was entitled to some optimism".

[15] h^- is essentially determined by an appropriate norm of the Kummer-Stickelberger ideal [6].

The second factor h^+ is the hard one. It is equal to the index of the circular units in the group of all units, but neither the direct definition of h^+, nor this fact helps significantly in calculating it. A moment's reflection will show that one learns nothing about H^+ from the fact that the Kummer-Stickelberger ideal annihilates it.

It is therefore a piece of luck for Kummer that he can show that if h^- is not divisible by λ, then neither is h^+.[16] He thus reduces hypotheses A and B (and hence the truth of the Fermat theorem) to the hypothesis that λ does not divide any of the first $(\lambda - 3)/2$ Bernoulli numbers.

We call such primes λ *regular*; Kummer had no special term for them, but would usually refer to the irregular ones as "diese besondere Art von Primzahlen" or "Ausnahmzahlen".[17]

Kummer's proof that hypotheses A and B imply the truth of Fermat's theorem for regular λ occurs in various places in the collected works, is quite readable, and is, moreover, extremely well known. It would serve little purpose to repeat it here. Nevertheless a loose translation into geometric language of Kummer's method of descent may be helpful to some readers. We discuss only the "second case"[18] of Fermat's theorem, which is the one requiring a 'descent'. The first case, however, also requires regularity of λ.

The second case. Here one considers the (finite) package of equations (curves over $\mathbf{Q}(\alpha)$): $\mathfrak{F}_u$: $x^\lambda + y^\lambda = u \cdot z^\lambda$ where u runs through a complete system of representatives for units modulo λth powers in $\mathbf{Z}[\alpha]$. One supposes a solution given $\xi = (x_0, y_0, z_0)$ where $z_0 = (1 - \alpha)^m z_0'$, and $x_0, y_0, z_0' \not\equiv 0 \bmod(1 - \alpha)$. Call m the *order of contact* of ξ. We are in the *second case* if $m > 0$. By multiplication of x_0, y_0 by suitable powers of α we may suppose that they are both congruent to rational integers modulo $(1 - \alpha)^2$.

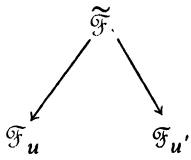
The structure of Kummer's proof is as follows: By methods of congruence one shows that there is no such solution ξ with $m = 1$ (even over the $(1 - \alpha)$-adic completion). Next suppose $m > 1$; one constructs a diagram of curves over $\mathbf{Q}(\alpha)$,

---

[16] His approach to this is not the modern one . . . to compare class field theory with "Kummer theory" via the 1-dimensional Galois cohomology isomorphism induced by the morphism of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\alpha))$-modules $\mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} \mu_p$ ($= p$th roots of 1), which conveniently reverses the signs of the characters of the action of $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ . . . Rather, Kummer supposes that h^+ is divisible by λ. Then, some circular unit, which is not a λth power in the group of circular units, *is* a λth power in the full group of units. Using this fact he deduces certain congruences which he shapes into the form of the appropriate congruences for Kummer-Stickelberger elements to insure that h^- is divisible by λ. His later paper where he shows, among other things, that if h^+ is even, then so is h^-, is an impressive elaboration of that calculation.

[17] At first, Kummer was disposed to regard irregularity as a rare phenomenon, for he had calculated the class number for all $\lambda < 100$ ("nicht ohne grosse Mühe") and found only three such. That he held this opinion helps to explain why he was content to treat λ-power reciprocity only for regular λ (see §5). Volume I ends, however, with his conclusions following a similar class number calculation for the range $101 \leqslant \lambda \leqslant 163$ where there are five irregular primes. There, he guesses that, asymptotically, half the primes are regular, but this guess has undergone subsequent modifications.

[18] The separation of Fermat's last theorem into cases seems to stem from the work of Sophie Germain who gave an easily applied sufficient condition for the *first* case to be true.



where $\tilde{\mathfrak{F}} \to \mathfrak{F}_u$ is a p-cyclic covering, unramified over $\mathbf{C}$, and $\tilde{\mathfrak{F}} \to \mathfrak{F}_{u'}$ is a projection to (possibly) another "Fermat" curve in the above package. There are, in fact, many such diagrams, and which one is to be chosen (the one which enjoys the excellent properties **(i)** and **(ii)** to be described below) depends upon the properties of the particular solution ξ that one has (hypothetically) at hand.

Kummer now lifts the solution ξ of $\mathfrak{F}_u$ to a solution $\tilde{\xi}$ of the p-cyclic cover $\tilde{\mathfrak{F}}$ and this solution *remains defined over the field* $\mathbf{Q}(\alpha)$. Here he makes use of regularity of the prime λ (in the form of *both* hypotheses A and B), but if we grant ourselves class field theory, we can "comprehend" this step geometrically by noting that $\tilde{\xi}$ must be defined over a p-cyclic extension of $\mathbf{Q}(\alpha)$ unramified outside $(1-\alpha)$ and (i) that the congruence hypotheses on ξ rule out ramification at $(1-\alpha)$ as well. Thus $\tilde{\xi}$ is defined over an everywhere unramified p-cyclic extension of $\mathbf{Q}(\alpha)$ which is trivial, by the hypothesis of regularity of λ.

Lettinq ξ' denote the image of ξ in $\mathfrak{F}_{u'}$ one obtains *another* solution of (possibly) another "Fermat" curve. Kummer then calculates (ii) the *order of contact* of ξ' to be $m-1$. Downwards induction on the order of contact m then concludes the proof of the second case.

As everyone knows, the arithmetic of Fermat curves (indeed of most curves over $\mathbf{Q}$) remains as problematic today as it was in Kummer's time.

The Fermat curves themselves have been observed by Fricke to be representable in a natural way as quotients of the upper half plane by (noncongruence) subgroups of finite index in $\mathrm{SL}_2\mathbf{Z}$. In this representation, the "trivial solutions" are precisely the cusps. Some effort has recently been devoted to connecting the Fermat curves and modular (congruence) subgroups; it is yet too early to say what concrete applications to arithmetic may be obtained by this connection.

For a modern reader the temptation is great to try to 'understand' Kummer's descent in terms of a descent argument on the Jacobian varieties J_λ of the "Fermat" curves.

To treat Fermat's last theorem for special cases of irregular λ, Kummer [**16**] was naturally led to a closer study (i.e., mod λ^2) of the 'λ-adic regulator', forcing further congruence relations on Bernoulli numbers, once a hypothetical nontrivial solution of the Fermat equation is given. Kummer's conditions on λ require that there be a unique λ-cyclic unramified extension of $\mathbf{Q}(\alpha)$ and Kummer obtains it explicitly as a 'Kummer extension', but here it seems harder to find "geometric language" to lighten the reading.[19] Will such

[19] The reader will be amused to find, in the midst of this thicket, a discursive three-page digression on what is, in effect, the theory of finite abelian groups. In modern terms, Kummer produces filtrations in finite abelian groups with cyclic successive quotients.

calculations find their systematization in the theory of the λ-adic L series associated to the Grössencharaktere coming from Jacobi sums?

5. Higher reciprocity. Let us consider cubic reciprocity, as an example of a higher reciprocity law. It is customary (following Jacobi) to work over the quadratic field $\mathbf{Q}(\alpha)$ where α is a primitive cube root of 1.

If $f(\alpha)$ is a prime in $\mathbf{Z}[\alpha]$, and $\varphi(\alpha)$ is an arbitrary element of $\mathbf{Z}[\alpha]$ such that both are prime to 3, and mutually relatively prime, one sets $\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)$ equal to that power of α which is congruent to $\varphi(\alpha)^{(Nf(\alpha)-1)/3} \bmod 1-\alpha$. One then sees that $\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)=1$ if and only if $\varphi(\alpha)$ is a cubic residue modulo $f(\alpha)$. The symbol $\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)$ is a natural generalization of the Legendre symbol. One says that an element $\varphi(\alpha)$ is *primary*, or *in primary form* if it is prime to 3, and congruent to a rational integer modulo 3. Any ideal prime to 3 in $\mathbf{Z}[\alpha]$ has a unique primary generator. The *cubic reciprocity law for ideals prime to* 3 then states that if $f(\alpha)$ and $\varphi(\alpha)$ are primes in $\mathbf{Z}[\alpha]$ which are in primary form, and which are mutually relatively prime, and prime to 3, we have

$$\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)=\left(\frac{f(\alpha)}{\varphi(\alpha)}\right).$$

Kummer's work on reciprocity may be viewed as a generalization of the above cubic case to λ-power reciprocity, where λ is a regular prime.

Nowadays, following Hilbert, we have the norm residue symbol, and 'reciprocity laws' are conveniently viewed as a particular legacy of class field theory for an arbitrary number field K. This theory neatly separates what is 'local' from what is 'global' and most decidedly does not shun the maximal abelian extension (the Hilbert class field) of K; rather, the Hilbert class field has center stage. A major objective of class field theory is to explain (and perhaps even to display) it. The idiosyncratic character of Kummer's reciprocity laws, from our viewpoint, is that he utterly suppresses that which is our foreground, by working with λ-power reciprocity over $K=\mathbf{Q}(\alpha)$ where λ is *hypothesized* to be a regular prime. This hypothesis enables him to formulate his power residue symbols in a way which is strange to us, but probably appeared to him to be *the* natural generalization of symbols of Legendre, Jacobi, and Eisenstein. Namely, if $f(\alpha)$ is a "complex prime number" ("real" or "ideal"), prime to λ, and $\varphi(\alpha)$ a "complex number" prime to λ ("real" for the moment), let $\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)$ denote that power of α which is congruent to $\varphi(\alpha)^{Nf(\alpha)-1/\lambda}$ modulo $f(\alpha)$.

Kummer now proceeds to modify his symbol, and by using regularity of λ, to attach a meaning to the symbol $\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)$ when $\varphi(\alpha)$ is an ideal complex number. For principal ideals prime to λ he pinpoints a specific generator $\varphi(\alpha)$ (in *primary* form) by suitable congruence conditions: $\varphi(\alpha)\cdot\varphi(\alpha^{-1})$ must be congruent to a rational integer mod λ and $\varphi(\alpha)$ must be congruent to a rational integer mod$(1-\alpha)^2$. For ideal complex numbers $\varphi(\alpha)$ let us now

modify the symbol by setting

$$\left(\frac{\varphi(\alpha)}{f(\alpha)}\right) = \left(\frac{x}{f(\alpha)}\right)^{1/h}$$

where x is a *primary* generator of the (principal) ideal $\varphi(\alpha)^h$ where h is the class number. Kummer's reciprocity law then states

$$\left(\frac{\varphi(\alpha)}{f(\alpha)}\right) = \left(\frac{f(\alpha)}{\varphi(\alpha)}\right)$$

if $f(\alpha)$ and $\varphi(\alpha)$ are ideal prime complex numbers, mutually relatively prime, and prime to λ. Moreover, always under the hypothesis that λ is regular, Kummer gives p-adic formulae for the symbols $\left(\frac{e}{f(\alpha)}\right)$ where e is a unit. We may most easily understand Kummer's work here, perhaps, by seeing how it can be derived with more modern techniques (norm residue symbols and class field theory). Weil's introduction explains this with great care.

6. In summary, Kummer's number-theoretic concerns are impressively close to the concerns of modern students of number theory. The progression of his thought deserves and rewards close reflection.

References

1. H. M. Edwards, *The background of Kummer's proof of Fermat's last theorem for regular primes*, Arch. History Exact Sci. **14** (1975), no. 3, 219–236.

2. G. Eisenstein, *Mathematische Werke*, Chelsea, New York, 1975.

3. C. G. J. Jacobi, *Gesammelte Werke*, Reimer, Berlin, 1890.

4. L. Lewin, *Dilogarithms and associated functions*, Macdonald, London, 1958. MR **21** #4264.

5. J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization* (to appear).

6. K. Iwasawa, *A class number formula for cyclotomic fields*, Ann. of Math. (2) **76** (1962), 171–179. MR **27** #4806.

7. ———, *On p-adic L functions*, Ann. of Math. (2) **89** (1969), 198–205. MR **42** #4522.

8. L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, Math. Ann. **37** (1890), 321–367.

9. K. Uchida, *Class numbers of imaginary abelian number fields.* III, Tôhoku Math. J. (to appear).

Published papers of Kummer referred to, with dates of publication:

(and their numbers in Lampe's bibliography (K 21–28)):

10. *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant*, 1844 (republished, 1847), L(ampe) 20.

11. *Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen*, 1846, L 23.

12. *Beweis des Fermat'schen Satzes der Unmöglichkeit von* $x^\lambda + y^\lambda = z^\lambda$ *für eine unendliche Anzahl Primzahlen* λ, 1847, L 24.

13. *Über eine allgemeine Eigenschaft der rationalen Entwickelungscoefficienten einer bestimmten Gattung analytischer Functionen*, 1851, L 38.

14. *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers*, 1851, L 39.

15. *Über die Irregularität von Determinanten*, 1853. Not in Lampe's bibliography!

16. *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen, für den Fall, dass die Klassenzahl durch* λ *theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, 1857, L 45.

BARRY MAZUR