Kummer on Fermat's Theorem

We return to $\mathbb{Z}(\alpha)$, at first for α a cube-root of 1, thus the solution

$$\alpha = \cos(2\pi/3) + i\sin(2\pi/3)$$

of

$$z^2 + z + 1 = 0.$$

We saw that if p is a prime number that leaves the remainder 3 on division by 3, then there is an integer a such that $a^2 + a + 1$ is divisible by p. We considered the greatest common divisor of $a - \alpha$ and p and discovered that it had to be a number π such that $p = \pi\bar{\pi}$, thus it is one of the two factors of p.

Suppose now that n is any odd prime and that we take α to be

$$\alpha = \cos(2\pi/n) + i\sin(2\pi/n),$$

thus a root of

$$Z^{n-1} + Z^{n-2} + \cdots + Z + 1 = 0.$$

The domain $\mathbb{Z}(\alpha)$ now consists of all numbers

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-2}\alpha^{n-2},$$

where the coefficients $a_0, a_1, \ldots, a_{n-2}$ are integers, thus ordinary whole numbers.

Now just as we showed that for $n = 3$ and $p \equiv 1 \pmod 3$, there is always an integer a such that $a^2 + a + 1$ is divisible by p, we can show that if p leaves the remainder 1 upon division by n, then there is an integer a such that

$$a^{n-2} + a^{n-3} + \cdots + a^2 + a + 1$$

is divisible by p. If the domain $\mathbb{Z}(\alpha)$ possessed unique factorization, we could expect that the greatest common divisor of $a - \alpha$ and p was again a prime divisor π of p.

More precisely, there are $n-1$ symmetries of the domain $\mathbb{Z}(\alpha)$, determined by

$$\begin{array}{ll}
\sigma_1 : & \alpha \to \alpha, \\
\sigma_2 : & \alpha \to \alpha^2, \\
\sigma_3 : & \alpha \to \alpha^3, \\
\ldots & \\
\sigma_{n-1} : & \alpha \to \alpha^{n-1},
\end{array}$$

The norm of a number ξ is defined to be

$$\xi \cdot \sigma_2(\xi)\sigma_3(\xi)\ldots\sigma_{n-1}(\xi).$$

We can even expect that

$$\mathrm{N}\,\pi = \pm p.$$

Kummer's first papers were on differential equations and infinite series, but in one of his earliest papers on cyclotomy, he, on the assumption that unique factorization exists in each domain $\mathbb{Z}(\alpha)$, set about finding π for each p. In a paper, written for a formal occasion and thus in Latin, on the complex numbers formed from roots of unity and whole numbers, thus on the domain $\mathbb{Z}(\alpha)$, he sets about calculating π for p up to 1000 that leave the remainder 1 upon division by n. The first values of n are 3, 5, 7, 11, 13, 17, 19 and 23. Of course, if the domain does not possess unique factorization, then his calculation will not lead to a well-defined result. He will not always arrive at a well-defined greatest common divisor; he will not always arrive at a number whose norm is p; and he will not always find a factorization of p into primes of the domain $Z(\alpha)$. He tabulates his results, from which we see in particular that for $n = 23$, there are five primes less than 1000 that cannot be factored.

The numbers in $\mathbb{Z}(\alpha)$ beside the five last primes in Kummer's tables have the following norms.

47	47^2
139	139^2
277	$277 \cdot 17159$
461	$47 \cdot 967$
967	967^2

It appears that Kummer put the wrong element of $\mathbb{Z}(\alpha)$ on the fourth line. Perhaps someone would like to find the right one. The necessary calculations are far easier now than in his day. Curiously, some reader, of the original journal article not of the collected works, appears to have corrected the preceding line. The point is that these last five numbers are exceptions. He is unable to find numbers in $\mathbb{Z}(\alpha)$ of which any of these five numbers are norms. Their squares or sometimes the products of two of them are, however, sometimes norms.

(1) Si $\lambda = 5$, et α radix æquationis $\alpha^5 = 1$.

$11 = N(2 + \alpha)$

$31 = N(2 - \alpha)$

$41 = N(3 + 2\alpha + \alpha^2)$

$61 = N(3 + \alpha)$

$71 = N(3 - \alpha + \alpha^2)$

$101 = N(3 + \alpha - \alpha^2)$

$131 = N(3 + \alpha - \alpha^4)$

$151 = N(3 + 2\alpha - \alpha^4)$

$181 = N(4 + 3\alpha)$

$191 = N(4 + \alpha + 2\alpha^2)$

$211 = N(3 - 2\alpha)$

$241 = N(4 - \alpha + \alpha^2)$

$251 = N(5 + 2\alpha + \alpha^4)$

$271 = N(3 - 3\alpha + \alpha^2)$

$281 = N(4 + \alpha - \alpha^2)$

$311 = N(3 + 2\alpha + 2\alpha^2 + \alpha^3)$

$331 = N(4 - 2\alpha + \alpha^2)$

$401 = N(4 + 3\alpha - \alpha^4)$

$421 = N(5 + 2\alpha + 2\alpha^2)$

$431 = N(4 - 2\alpha - \alpha^4)$

$461 = N(4 - \alpha - \alpha^2)$

$491 = N(5 + 3\alpha + \alpha^2)$

$521 = N(5 + \alpha)$

$541 = N(3 - 3\alpha - \alpha^2)$

$571 = N(6 + 5\alpha + 3\alpha^2)$

$601 = N(5 + 2\alpha - \alpha^2)$

$631 = N(4 - 2\alpha - \alpha^3)$

$641 = N(5 + 3\alpha + 4\alpha^2)$

$661 = N(5 + \alpha - \alpha^2 + 3\alpha^4)$

$691 = N(3 - 3\alpha - 2\alpha^2)$

$701 = N(4 - \alpha - 2\alpha^2 + \alpha^3)$

$751 = N(6 + 4\alpha + 3\alpha^2)$

$761 = N(5 - 2\alpha + \alpha^2)$

$811 = N(3 - 3\alpha - 2\alpha^2 + \alpha^3)$

$821 = N(4 - \alpha - 2\alpha^2 + 2\alpha^3)$

$881 = N(6 + 2\alpha + \alpha^2)$

$911 = N(5 + \alpha^2 - 2\alpha^4)$

$941 = N(4 + 3\alpha - 3\alpha^2 - \alpha^3)$

$971 = N(5 - 2\alpha - \alpha^4)$

$991 = N(6 + \alpha + \alpha^3)$

(2) Si $\lambda = 7$, et α est radix æquationis $\alpha^7 = 1$.

$29 = N(1 + \alpha - \alpha^2)$

$43 = N(2 + \alpha)$

$71 = N(2 + \alpha + \alpha^3)$

$113 = N(2 - \alpha + \alpha^5)$

$127 = N(2 - \alpha)$

$197 = N(3 + \alpha + \alpha^5 + \alpha^6)$

$211 = N(3 + \alpha + 2\alpha^2)$

$239 = N(3 + 2\alpha + 2\alpha^2 + \alpha^3)$

$281 = N(2 - \alpha - 2\alpha^3)$

$337 = N(2 + \alpha - \alpha^2 - \alpha^4)$

$379 = N(3 + 2\alpha + \alpha^2)$

$421 = N(3 + \alpha + \alpha^2)$

$449 = N(2 + \alpha - \alpha^3 - \alpha^6)$

$463 = N(3 + 2\alpha)$

$491 = N(3 + \alpha + \alpha^2 - \alpha^5)$

$547 = N(3 + \alpha)$

$617 = N(2 + \alpha + \alpha^2 - \alpha^5)$

$631 = N(2 + 2\alpha - \alpha^2 + \alpha^3 + \alpha^6)$

$659 = \mathrm{N}(2 + 2\alpha - \alpha^2 + \alpha^5)$

$673 = \mathrm{N}(4 + 3\alpha + 2\alpha^2 + \alpha^4 + 2\alpha^6)$

$701 = \mathrm{N}(3 + \alpha + \alpha^4 - \alpha^5 + \alpha^6)$

$743 = \mathrm{N}(3 + 2\alpha - \alpha^3 - \alpha^4)$

$757 = \mathrm{N}(3 + 2\alpha + \alpha^5)$

$827 = \mathrm{N}(2 + 2\alpha - \alpha^4 - \alpha^5)$

$883 = \mathrm{N}(2 - \alpha^2 - 2\alpha^3 - \alpha^5)$

$911 = \mathrm{N}(3 + 2\alpha - \alpha^3 + \alpha^4)$

$953 = \mathrm{N}(3 + \alpha - \alpha^2 - \alpha^3)$

$967 = \mathrm{N}(2 + 2\alpha - \alpha^3 + 2\alpha^5)$

(**3**) Si $\lambda = 11$, et α est radix æquationis $\alpha^{11} = 1$.

$23 = \mathrm{N}(1 + \alpha + \alpha^9)$

$67 = \mathrm{N}(1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5)$

$89 = \mathrm{N}(1 + \alpha + \alpha^4 + \alpha^6)$

$199 = \mathrm{N}(1 + \alpha - \alpha^2)$

$331 = \mathrm{N}(1 - \alpha + \alpha^3 + \alpha^5)$

$353 = \mathrm{N}(1 + \alpha + \alpha^3 + \alpha^4 - \alpha^7)$

$397 = \mathrm{N}(1 + \alpha + \alpha^6 - \alpha^7)$

$419 = \mathrm{N}(1 + \alpha - \alpha^2 + \alpha^3)$

$463 = \mathrm{N}(1 - \alpha - \alpha^2 + \alpha^5 + \alpha^7)$

$617 = \mathrm{N}(2 + \alpha + \alpha^2 + \alpha^{10})$

$661 = \mathrm{N}(1 + \alpha - \alpha^2 + \alpha^4 - \alpha^5)$

$683 = \mathrm{N}(2 + \alpha)$

$727 = \mathrm{N}(1 + \alpha + \alpha^2 - \alpha^5 - \alpha^4)$

$859 = \mathrm{N}(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^7 - \alpha^5)$

$881 = \mathrm{N}(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^4 - \alpha^7 - \alpha^9)$

$947 = \mathrm{N}(2 + \alpha^3 - \alpha^5 - \alpha^6)$

$991 = \mathrm{N}(2 + \alpha + \alpha^3)$

(**4**) Si $\lambda = 13$, et α est radix æquationis $\alpha^{13} = 1$.

$53 = \mathrm{N}(1 + \alpha + \alpha^3)$

$79 = \mathrm{N}(1 - \alpha + \alpha^{10})$

$131 = \mathrm{N}(1 - \alpha + \alpha^{11})$

$157 = \mathrm{N}(1 + \alpha + \alpha^2 + \alpha^5)$

$313 = \mathrm{N}(1 - \alpha + \alpha^3 + \alpha^6)$

$443 = \mathrm{N}(1 + \alpha - \alpha^3 + \alpha^8)$

$521 = \mathrm{N}(1 + \alpha - \alpha^{12})$

$547 = \mathrm{N}(1 - \alpha - \alpha^2 + \alpha^5 + \alpha^9)$

$599 = \mathrm{N}(1 + \alpha - \alpha^7 + \alpha^8 + \alpha^{11})$

$677 = \mathrm{N}(1 - \alpha - \alpha^4 + \alpha^6 + \alpha^9)$

$959 = \mathrm{N}(1 + \alpha - \alpha^2 - \alpha^5 + \alpha^7)$

$911 = \mathrm{N}(1 + \alpha^3 + \alpha^5 - \alpha^7 - \alpha^{11})$

$937 = \mathrm{N}(1 + \alpha^3 - \alpha^7 + \alpha^8 - \alpha^{10})$

(**5**) Si $\lambda = 17$, et α est radix æquationis $\alpha^{17} = 1$.

$103 = \mathrm{N}(1 + \alpha^2 + \alpha^9)$

$137 = \mathrm{N}(1 + \alpha - \alpha^4)$

$239 = \mathrm{N}(1 + \alpha + \alpha^3)$

$307 = \mathrm{N}(1 - \alpha + \alpha^7)$

$409 = \mathrm{N}(1 - \alpha^3 + \alpha^9)$

$443 = \mathrm{N}(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^{15})$

$613 = \mathrm{N}(1 + \alpha^2 - \alpha^3)$

$647 = \mathrm{N}(1 + \alpha + \alpha^{13} + \alpha^{15})$

$919 = \mathrm{N}(1 + \alpha + \alpha^4 + \alpha^5 + \alpha^7)$

$953 = \mathrm{N}(1 + \alpha + \alpha^4 - \alpha^{12})$

(6) Si $\lambda = 19$, et α est radix æquationis $\alpha^{19} = 1$.

$191 = \mathrm{N}(1 + \alpha + \alpha^{16})$ $\qquad$ $457 = \mathrm{N}(1 + \alpha + \alpha^{3})$

$229 = \mathrm{N}(1 - \alpha - \alpha^{5})$ $\qquad$ $571 = \mathrm{N}(1 + \alpha + \alpha^{2} + \alpha^{3} - \alpha^{5})$

$419 = \mathrm{N}(1 + \alpha - \alpha^{5})$ $\qquad$ $647 = \mathrm{N}(1 - \alpha^{2} + \alpha^{9})$

$761 = \mathrm{N}(1 - \alpha^{2} + \alpha^{12})$

(7) Si $\lambda = 23$, et α est radix æquationis $\alpha^{23} = 1$.

$599 = \mathrm{N}(1 + \alpha^{15} - \alpha^{16})$ $\qquad$ $691 = \mathrm{N}(1 + \alpha + \alpha^{5})$

$829 = \mathrm{N}(1 + \alpha^{11} + \alpha^{20})$

Reliqui numeri primi formæ $23m + 1$ infra mille undecim factoribus primis constant, habet

47 factorem $\alpha^{10} + \alpha^{13} + \alpha^{8} + \alpha^{15} + \alpha^{7} + \alpha^{16}$

139 » $\alpha^{10} + \alpha^{13} + \alpha^{8} + \alpha^{15} + \alpha^{4} + \alpha^{19}$

277 » $2 + \alpha + \alpha^{22} + \alpha^{7} + \alpha^{16}$

461 » $\alpha + \alpha^{22} + \alpha^{10} + \alpha^{13} + \alpha^{8} + \alpha^{15} + \alpha^{9} + \alpha^{14}$

967 » $2 + \alpha^{11} + \alpha^{12} + \alpha^{4} + \alpha^{19}$.

§ XI.

Quæ de numeris complexis et de eorum factoribus primis commentati sumus ad doctrinam de sectione circuli felicissimo successu applicari possunt. In hac enim doctrina tales numeri complexi eorumque producta maximi momenti sunt, quorum vera indoles in luce clarissima ponitur si in factores primos diffinduntur.

Sit p numerus primus realis formæ $m\lambda + 1$, α radix imaginaria æquationis $\alpha^{\lambda} = 1$, g radix primitiva numeri primi p, et

$$(\alpha, x) = x + \alpha x^{g} + \alpha^{2} x^{g^{2}} + \ldots + \alpha^{p-2} x^{g^{p-2}}$$

Totius fere doctrinæ de circuli sectione caput est formæ hujus (α, x) potestas exponentis λ, quæ a radice x non pendet, sed radicis α functio rationalis integra est, ideoque numerus complexus ejus generis quod supra tractavimus. Ipsa hæc formula (α, x), quam Cl. Lagrange primus adhibuit, proprietatibus insignibus gaudet, quarum maximas Cl. Jacobi primus invenit

$$(\alpha, x)(\alpha^{-1}, x) = p,$$

$$\frac{(\alpha^{m}, x)(\alpha^{n}, x)}{(\alpha^{m+n}, x)} = \psi(\alpha) = \mathrm{A} + \mathrm{A}_{1}\alpha + \mathrm{A}_{2}\alpha^{2} + \ldots + \mathrm{A}_{\lambda-1}\alpha^{\lambda-1};$$

Maxime dolendum videtur, quod hæc numerorum realium virtus, ut in tactores primos dissolvi possint, qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quæ si esset, tota hæc doctrina, quæ magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci psset. Eam ipsam ob causam numeri complexi, quos hic tractamus, imperfecti esse videntur, et dubium inde oriri posset, utrum hi numeri complexis ceteris qui fingi possint præferendi, an alii quærendi essent, qui in hac re fundamentali analogiam cum numeris integris realibus servarent. Attamen hi numeri complexi, qui unitatis radicibus et numeris integris realibus componuntur, non ex arbitrio facti sunt, sed ex ipsa doctrina numerorum procreati, atque ipsorum ea ratio est, ut in doctrina sectionis circuli et residuorum potestatum altiorum ulterius promovenda iis carere nullo modo possimus.

De numeris complexis, qui radicibus unitatis et numeris integris realibus constant

Citation

We see with great sorrow that that virtue of ordinary numbers, that they can be resolved into prime factors that for the same number are always the same, is not possessed by complex numbers. If it were, all the theory, that is so far beset with great difficulties, would be easy to develop and to bring to completion. For this reason the complex numbers that we treat here are seen to be imperfect, so that a doubt could arise, whether other complex numbers that might be constructed are preferable, whether there are others to be investigated that in this fundamental respect would preserve the analogy with ordinary integers. Nevertheless those complex numbers that are composed from roots of unity and ordinary integers are not constructed arbitrarily, but are generated by the theory of numbers itself, which is indeed their very source, so that in developing the theory of cyclotomy and of the residues of higher powers we can in no manner neglect them.

Kummer saves the day with the introduction of *ideal* factors. I shall not give his definition, but a more modern one, which is simpler, but the wonder and brilliance is gone. The proofs are also then farther to seek. I introduce the modern definition out of expediency. We have little time left. If ξ is any number in $Z(\alpha)$, then the collection of numbers $\mu\xi$, μ being any other number in $\mathbb{Z}(\alpha)$ is such that if η and ζ are in this collection, then so are $\eta+\zeta$ and $\nu\eta$, ν being an arbitrary number in $\mathbb{Z}(\alpha)$. Thus

$$\mu_1\xi + \mu_2\xi = (\mu_1 + \mu_2)\xi, \tag{A}$$

and

$$\nu(\mu\xi) = (\mu\nu)\xi. \tag{B}$$

Our experience with the Euclidean algorithm, suggests that if, on the other hand, we have any collection of numbers with the properties (A) and (B), then it is in fact just the collection of multiples of some ξ by the numbers of $\mathbb{Z}(\alpha)$. Our experience is of course limited and leads to the wrong conclusion, but what we can do is introduce for any collection satisfying (A) and (B) an ideal number, of whose multiples the collection is imagined to exist. The value of these ideal numbers is determined by the useful properties they possess. Notice that every number in $Z(\alpha)$ determines an ideal number: the collection of all its multiples. Moreover two numbers in $Z(\alpha)$ determine the same ideal number if and only if they differ by a unit. Moreover $\mathbb{Z}(\alpha)$ itself is an ideal number, the collection of multiples of 1.

They can be multiplied. If $\mathfrak{a} = \{\mu\}$ and $\mathfrak{b} = \{\nu\}$ are two ideal numbers, then $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ consists of all numbers

$$\mu_1\nu_1 + \mu_2\nu_2 + \dots,$$

the number of terms being arbitrary, but of course finite, and μ_i lying in a and ν_i lying in b. If $\mathfrak{a}$ were just the multiples of ξ and $\mathfrak{b}$ just the multiples of η, then $\mathfrak{c}$ would just be the multiples of $\xi\eta$. If we multiply an ideal number by 1, thus by $\mathbb{Z}(\alpha)$, we just obtain the ideal number itself back. This said, the notion of a prime ideal number is clear. An ideal number is prime if when it is the product of two other ideal numbers,, one of these numbers is 1 and the other necessarily then the ideal itself.

Kummer proves, first of all, that every number has a unique factorization into ideal numbers, and expresses this theorem with a chemical analogy. We might suggest nowadays that ideal numbers are like the physicists quarks, however Kummer's analogy is more explicit and reflects better his actual construction

"I have discussed the ideal factors at length with Dirichlet and more briefly with Jacobi. I used a symbolic expression taken from chemistry: the prime factors are the elements, the ideal prime factors are those elements that do not appear alone, but only in combination with other elements, equivalent complex ideal numbers are as such the same as equivalent combining proportions of the chemical ingredients.* The search for the ideal prime factors is the chemical analysis, the complex numbers labeled ψ or Ψ in my essay are the reagents and the whole number q, which appears as a real factor, is the sediment that manifests itself upon application of the right reagent. In brief, the whole collection of notions of chemistry agrees in a striking fashion with those in which the theory of complex numbers is formulated."

* My limited knowledge of chemistry and of chemical terms in any language forces me to guess here. I suppose that two different molecules can be combined of the same elements in the same proportions, and that the reference is to this, but I do not know and would be happy for a correction or a confirmation.

Two ideal numbers $\mathfrak{a}$ and $\mathfrak{b}$ are called equivalent if there are ordinary numbers a and b in $\mathbb{Z}(\alpha)$ such that $a\mathfrak{a} = b\mathfrak{b}$. If $\mathfrak{a}$ is equivalent to $\mathfrak{b}$ and $\mathfrak{b}$ to $\mathfrak{c}$, then, as is to be expected, $\mathfrak{a}$ is equivalent to $\mathfrak{c}$. Thus the collection of all ideal numbers is decomposed into classes, one class being formed of all ideal numbers equivalent to any given one. One very important fact (or theorem) established by Kummer right at the beginning of his investigations is that the number of different classes is finite.

He also investigates, and this is easier, the units. I observe that there are very many units in $\mathbb{Z}(\alpha)$ is n is larger than 3. Some can be formed in the following way. If $1 < r < l$, then

$$\frac{1-\alpha^r}{1-\alpha} = 1 + \alpha + \alpha^2 + \cdots + \alpha^{r-2} + \alpha^{r-1}$$

is in $\mathbb{Z}(\alpha)$. If we choose s such that $rs \equiv 1 \pmod{l}$ and apply the symmetry $z \to z^s$, then this relation becomes

$$\frac{1-\alpha}{1-\alpha^r} = 1 + \alpha^s + \alpha^{2s} + \cdots + \alpha^{(r-2)s} + \alpha^{(r-1)s},$$

Uebermorgen, als den Mondtag gehen meine Vorlesungen an und zwar gleich drei auf einmal zu denen ich mich noch präpariren soll, was bei dem Anfange allemal Schwierigkeiten hat, wenn man sich nicht gleich in medias res hineinstürzen will oder kann.

Leben Sie recht wohl

Ihr

E. Kummer.

Breslau d. 14. Juni 1846.

Herzlich geliebter Freund!

... Ueber die idealen Factoren habe ich mehreres mit Dirichlet und einiges mit Jacobi verhandelt. Ich gebrauchte dabei immer die bildliche Ausdrucksweise, aus der Chemie entnommen: Die Primfactoren sind die Elemente, die idealen Primfactoren sind diejenigen Elemente welche nicht für sich darstellbar nur in Verbindung mit anderen vorkommen, äquivalente complexe ideale Zahlen sind an sich dasselbe als äquivalente Gewichtsmengen der chemischen Stoffe. Die Aufsuchung der idealen Primfactoren ist die chemische Analyse, die in meinem Aufsatze mit ψ oder Ψ bezeichneten complexen Zahlen sind die Reagentien und die ganze Zahl q, welche als realer Factor heraustritt, ist der Niederschlag welcher nach Anwendung des richtigen Reagens sich zeigt. Kurz die ganze Begriffssphäre der Chemie stimmt auf eine eclatante Weise mit derjenigen zusammen in welcher sich die Lehre von den complexen Zahlen bewegt. Dirichlet hat mich sehr ermahnt die Theorie bald fertig auszuarbeiten und Crelle zum Drucke zu übergeben. Auch hat er mir erzählt und gezeigt, nämlich aus mündlichen und schriftlichen Aeußerungen von Gauss, daß Gauss schon bei Anfertigung des Abschnittes de compositione formarum aus den Disqu. arith. etwas ähnliches wie ideale Factoren zu seinem Privatgebrauche gehabt hat, daß er dieselben aber nicht auf sicheren Grund zurückgeführt hat, er sagt nämlich in einer Note seiner Abhandlung über die Zerfällung der ganzen rat. Functionen in lineäre Factoren ohngefähr so: „Wenn ich hätte auf dieselbe Weise verfahren wollen wie die früheren Mathematiker mit dem imaginären, so würde eine andere meiner Untersuchungen die sehr schwierig ist sich auf sehr leichte Weise haben machen lassen.“ Daß hier die compositio formarum gemeint ist, hat Dirichlet später mündlich von Gauss erfahren. Ich habe ferner Dirichlet meine Vermuthung mitgetheilt daß zwischen hat. Der chemischen Verbindung entspricht für die complexen Zahlen die Multiplication; den Elementen, oder eigentlich den Atomgewichten derselben, entsprechen die Primfactoren; und die chemischen Formeln für die Zerlegung der Körper sind genau dieselben, wie die Formeln für die Zerlegung der Zahlen. Auch selbst die idealen Zahlen unserer Theorie finden sich in der Chemie, vielleicht nur allzuoft, als hypothetische Radicale, welche bisher noch nicht dargestellt worden sind, die aber, so wie die idealen Zahlen, in den Zusammensetzungen ihre Wirklichkeit haben. Das Fluor, für sich bisher nicht darstellbar und noch den Elementen zugezählt, kann als Analogon eines idealen Primfactors gelten. Die Idealität in der Chemie verhält sich aber darin wesentlich anders, als die der complexen Zahlen, daſs chemische ideale Stoffe, mit wirklichen verbunden, auch wirkliche Stoffe produciren; was bei den idealen Zahlen nicht der Fall ist. In der Chemie hat man ferner zur Prüfung der in einem unbekannten aufgelöseten Körper enthaltenen Stoffe die Reagentien, welche Niederschläge geben, aus denen die Anwesenheit der verschiedenen Stoffe sich erkennen läſst. Ganz Dasselbe findet für die complexen Zahlen Statt; denn es sind die oben mit Ψ bezeichneten complexen Zahlen ebenso die Reagentien für die idealen Primfactoren, und die reale Primzahl q, welche nach der Multiplication mit einer solchen als Factor aus dem Producte heraustritt, ist genau Dasselbe, wie der unlösliche Niederschlag, der nach Anwendung des Reagens zu Boden fällt. Auch der Begriff der Äquivalenz ist in der Chemie fast derselbe, wie in der Theorie der complexen Zahlen. So wie nämlich dort zwei Gewichtsmengen verschiedener Stoffe äquivalent heiſsen, wenn sie sich gegenseitig vertreten können, entweder zum Zwecke des Neutralisirens, oder um Isomorphie hervorzubringen: so sind zwei ideale Zahlen äquivalent, wenn sie für den Zweck, eine andere ideale Zahl zu einer wirklichen zu machen, sich gegenseitig vertreten können. — Diese hier angedeuteten Analogieen sind nicht etwa als bloſse Spiele des Witzes zu betrachten, sondern haben ihren guten Grund darin, daſs die Chemie, so wie der hier behandelte Theil der Zahlentheorie, beide denselben Grundbegriff, nämlich den der ***Zusammensetzung***, wenn gleich innerhalb verschiedener Sphären des Seins, zu ihrem Principe haben; woraus folgt, daſs auch die diesem verwandten, mit ihm nothwendig gegebenen Begriffe sich in beiden auf ähnliche Weise finden müssen. Die Chemie der natürlichen Stoffe und die hier behandelte Chemie der complexen Zahlen sind beide als Verwirklichungen des Begriffs der Zusammensetzung und der davon abhängigen Begriffs-Sphäre anzusehen: jene

Remark

Those who are familiar with the techniques of the development of the theory of algebraic numbers by Kronecker and Dedekind, the successors to Kummer, will find these metaphors foreign to their own experience. Kummer's methods were different, less abstract, with a more immediate appeal. The abstract methods have by now screened the concrete, and the student is often misled. Hermann Weyl, for example, in his notes on algebraic number theory, notes I have already praised, observes after developing the abstract theory and as he is about to apply it to cyclotomic fields, the fields for which Kummer had developed his theory,

"*It is the common curse of all general and abstract theories that they have to be far advanced before yielding useful results in concrete problems.*"

I was persuaded by these lines when I first read them four decades ago, and it was not until undertaking these lectures that I appreciated the fallacy in them. There is a great deal to be said for the right abstract, general theories in mathematics and every reason to be impatient with the dull-witted who deny their value simply because they do not understand them, along the lines of the German expression,

"*Was der Bauer nicht kennt, das frißt er auch nicht.*"

None the less for the particular concrete problem that Weyl was about to consider, namely cyclotomic fields, the general and abstract theories are not necessary. It is far better and far more instructive to follow Kummer and to deal with the cyclotomic fields directly without any general tools.

The tension between the abstract and the concrete in mathematics has no final resolution, either aesthetically or practically.

so that both

$$\frac{1-\alpha^r}{1-\alpha}$$

and its reciprocal are in $\mathbb{Z}(\alpha)$. Thus it is a unit.

If $n = 3$, then all we have is

$$\frac{1-\alpha^2}{1-\alpha} = 1 + \alpha = -\alpha^2,$$

so that we do not have many units of this form. Otherwise there are many. If $n = 5$, then

$$\alpha \cdot \frac{1-\alpha^4}{1-\alpha} = \alpha(1+\alpha+\alpha^2+\alpha^3) = \alpha+\alpha^2+\alpha^3+\alpha^4 = -1,$$

so that

$$\frac{1-\alpha^4}{1-\alpha} = -\alpha^4$$

is not of much interest. On the other hand,

$$\alpha^2 \cdot \frac{1-\alpha^2}{1-\alpha} = \alpha^2(1+\alpha) = \alpha^2+\alpha^3 = -1-\alpha^1-\alpha^4$$

is $1-w$ if $w = \alpha+\alpha^4$ is the number $(-1+\sqrt{5})/2$ is the number we met when treating the regular hexagon. Thus $1-w$ is $(3-\sqrt{5})/2$ and

$$\frac{3-\sqrt{5}}{2}\frac{3+\sqrt{5}}{2} = \frac{9-5}{4} = 1$$

is in fact a unit in the domain formed from the square root of 5. If we square $1-w$, we obtain

$$\frac{9+5-6\sqrt{5}}{4} = \frac{7-3\sqrt{5}}{2}$$

Cubing we obtain

$$\frac{7-3\sqrt{5}}{2}\frac{3-\sqrt{5}}{2} = \frac{36-16\sqrt{5}}{4} = (9-4\sqrt{5})(9+\sqrt{5}) = 81-16.5-1.$$

Thus we obtain a solution of Pell's equation,

$$1+5x^2 = y^2, \quad x = 4, \quad y = 9.$$

In a letter to Kronecker dated April 2, 1847 Kummer described how he could prove Fermat's theorem if he made two assumptions, one on the number of classes and one on the units. These assumptions are not always satisfied, so that he was not to obtain in this way a general proof of Fermat's theorem, but he would in the course of years, verify that they were satisfied in many cases, and would in addition show that weaker hypotheses sufficed. Kummer denotes n by λ, but I keep to our notation.

I) *If a unit has the form $c + n\xi$, where c is an ordinary whole number and ξ is in $\mathbb{Z}(\alpha)$, then it is the n-th power of another unit.*

II) *If $\mathfrak{a}$ is any ideal number then the ideal number $\mathfrak{a}^n$ is the ideal number associated to a number in $\mathbb{Z}(\alpha)$ only if this is already true for $\mathfrak{a}$ itself, or better, as it is stronger, the number of classes of ideal numbers is not a multiple of n.*

If $n = 3$, then there are six units, of which two, ± 1 are certainly third powers, and of which the other four, $\pm\alpha$ and $\pm\alpha^2 = \mp(1+\alpha)$ are not of the form envisaged in the first hypothesis. They are also not third powers. If $n = 2$, then $\mathbb{Z}(\alpha)$ is just the domain $\mathbb{Z}$ of whole numbers but -1 is not a square. So the first hypothesis is not satisfied in this case. For $n = 2$ and $n = 3$, there is a single class. So the number of classes is 1 which is not divisible by n. As we shall see, the proof uses, however, the additional assumption $n > 2$. The stronger form of the second hypothesis is what is usually proved.

I do not want to offer here all of the proof given by Kummer in his letter to Kronecker that Fermat's theorem follows from these two hypotheses. Let me present none the less one of the main ideas. He supposes that

$$(C) \qquad x^n + y^n = z^n, \quad xyz \neq 0$$

and shows that one of the three numbers x, y or z is necessarily divisible by n, just as we did for $n = 3$. Now we saw for $n = 3$ that n was a unit times $(1-\alpha)^{n-1}$. This is so in general because

$$(1-\alpha)^{n-1} = n\frac{1-\alpha}{1-\alpha}\frac{1-\alpha}{1-\alpha^2}\frac{1-\alpha}{1-\alpha^3}\cdots\frac{1-\alpha}{1-\alpha^{n-1}},$$

as we see on substituting $x = 1$ in the relation

$$(x-\alpha)(x-\alpha^2)\dots(x-\alpha^{n-1}) = x^{n-1} + x^{n-2} + \dots x + 1.$$

Thus, as we take n odd, (C) implies a relation

$$(D) \qquad u^n - v^n = E(1-\alpha)^{mn}w^n, \quad m > 0, \quad uvw \neq 0$$

with E a unit and he shows that such a relation cannot be satisfied even with numbers u, v and w in $\mathbb{Z}(\alpha)$, at least not with numbers satisfying

$$(E) \qquad u = c + (1-\alpha)^{mn-n+1}\Phi, \quad v = c + (1-\alpha)^{mn-n+1}\Psi,$$

where Φ and Ψ are in $\mathbb{Z}(\alpha)$ and c is an ordinary whole number. Just as for $n = 3$, there are two steps. It has to be shown that (D) is impossible for $m = 1$. Then it has to be shown that if it is possible for $m > 1$ then it is possible with m replaced by $m - 1$. I consider only the second step, as this make clear the role of the second hypothesis and the hypothesis $n > 2$.

We can factor $u^n - v^n$ as

$$(F) \qquad u^n - v^n = (u-v)(u-\alpha v)(u-\alpha^2 v)\dots(u-\alpha^{n-1}v).$$

To see this divide both sides by v^n to obtain with $x = u/v$

$$x^n - 1 = (x-1)(x-\alpha)\dots(x-\alpha^{n-1}).$$

This relation just expresses the fact that

$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

are all the roots of $x^n - 1 = 0$.

Now we factor (F) into ideal prime factors and use the second hypothesis and the relation (D). Just as for $n = 3$, we see that the factors appearing on the right side of (F) have at most the prime factor associated to $1 - \alpha$ in common. This number does indeed determine a prime ideal. That is easily verified as its norm is n. It is the number we denoted λ for $n = 3$. That means again that one of the numbers on the right side of (F) is divisible by $(1-\alpha)^{mn-n+1}$ and by no higher power, the others being exactly divisble by $1-\alpha$. All of this is exactly the same as for $n = 3$. Once again, we can replace u by $\alpha^k u$ with any k as $\alpha^n = 1$. Making use of such a replacement, we may suppose that it is $u - v$ that is exactly divisible by $(1-\alpha)^{mn-n+1}$. This we did for $n = 3$ as well. Thus we have

$$u - v = e(1-\alpha)^{mn-n+1}w_1^n,$$

where at first ew_1^n is only the n-th power of an ideal number $\mathfrak{w}$. But the second hypothesis asserts that if the n-th power of an ideal number is the ideal number associated to an ordinary number, then that is true of the original ideal number. Consequently $\mathfrak{w}$ is associated to w_1 and the equation (F), in which e is a unit, results.

For similar reasons we have

$$u - \alpha^r v = e_r(1-\alpha^r)t_r^n, \quad r = 1, \dots, n-1$$

in which e_r is again a unit.

Kummer has then to make use of the condition (E) and the first hypothesis to ensure that each e_r is an n-th power, $e_r = f_r^n$, and to replace $e_r t_r^n$ by z_r^n, $z_r = f_r t_r$. Finally he uses two of the equations

$$(G) \qquad u - \alpha^r v = (1-\alpha^r)z_r^n,$$

but to have two of them, he needs $n > 2$ for $0 < r < n$. Consider then (G) and

$$(H) \qquad u - \alpha^s v = (1-\alpha^s)z_s^n.$$

Mutiply the first by $1-\alpha^s$ and the second by $1-\alpha^r$ and subtract. On the left we obtain

$$(J) \qquad \begin{aligned} (1-\alpha^s)(u-\alpha^r v) - (1-\alpha^r)(u-\alpha^s v) &= (\alpha^r - \alpha^s)(u-v) \\ &= (\alpha^r-\alpha^s)e(1-\alpha)^{mn-n+1}w_1^n, \end{aligned}$$

and on the right

$$(I) \qquad (1-\alpha^r)(1-\alpha^s)(u_1^n - v_1^n).$$

where, following Kummer, we have set $z_r = u_1$ and $z_s = v_1$.

We want to deduce from the equality of (I) and (J) a relation of the form (D), with u_1, v_1 and w_1 replacing u, v and w and with m replaced by $m-1$. What (I) and (J) give is a relation

$$(K) \qquad u_1^n - v_1^n = \frac{(\alpha^r-\alpha^s)(1-\alpha)}{(1-\alpha^r)(1-\alpha^s)}e(1-\alpha)^{mn-n}w_1^n.$$

If

$$(L) \qquad \frac{(\alpha^r-\alpha^s)(1-\alpha)}{(1-\alpha^r)(1-\alpha^s)}$$

erscheint allerdings günstiger für wissenschaftliche Studien, aber Geldgeschäfte schließen dieselben auch nicht aus. Ich selbst habe in diesem Jahre vielleicht noch weniger mathematisch gearbeitet als Sie. Ich habe nämlich noch keinen neuen Stoff gefunden, und um doch etwas zu thun, werde ich eine Recension über die von JACOBI herausgegebenen dem Könige dedicirten Abhandlungen schreiben. ... — Ich hoffte immer Sie in kurzem einmal hier zu sehen, denn ich denke, die Geschäfte müssen Sie bald einmal herführen, sollten diese es nicht thun, so thun Sie es doch selbst recht bald. Die besten Grüße von den Meinen an Sie und die Ihrigen Ihr Sie herzlich liebender

E. KUMMER.

Breslau, d. 2. April 1847.

Herzlich geliebter Freund!

Versetzen Sie sich wieder einmal in die complexen Zahlen und Einheiten, wo λ, α, u. s. w. lauter bekannte Zeichen sind. Nehmen Sie auch vorläufig einmal folgenden Satz als bewiesen an:

I. „Wenn eine Einheit $E(\alpha)$ die Form hat $E(\alpha) = c + \lambda f(\alpha)$, ($c$ reale g. Z.), so ist $E(\alpha)$ eine λ^{te} Potenz einer andern Einheit."

Der umgekehrte Satz versteht sich ganz von selbst, aber auch dieser ist für $\lambda = 5$ und $\lambda = 7$ sehr leicht zu beweisen, und so überall wo man die Fundamental-Einheiten kennt. Einen allgemeinen Beweis habe ich bisher noch nicht.

II. Es sei ferner λ eine solche Primzahl, für welche die Anzahl aller nicht äquivalenten Formen (oder nach meiner Auffassung der nicht äquivalenten idealen complexen Zahlen) nicht durch λ selbst theilbar ist. Dieß gilt offenbar wieder für $\lambda = 5$, $\lambda = 7$, und für unendlich viele Primzahlen λ, ich weiß nicht ob für alle. Es wird unter dieser Voraussetzung, wenn $(f(\alpha))^\lambda$ eine wirkliche complexe Zahl ist, allemal auch $f(\alpha)$ selbst eine wirkliche complexe Zahl sein; denn die Potenz, welche die ideale Zahl zur wirklichen macht, hat stets mit der Anzahl der nicht äquivalenten Formen einen gemeinschaftlichen Factor.

Für alle diejenigen Primzahlen λ, welche diesen beiden Bedingungen I und II genügen kann ich nun die Unmöglichkeit der Gleichung $x^\lambda - y^\lambda = z^\lambda$ vollständig beweisen wie folgt.

Zunächst beweise ich, daß wenn $x^\lambda - y^\lambda = z^\lambda$ Statt haben soll, eine der drei Zahlen durch λ theilbar sein muß. Sei x nicht durch λ theilbar, so giebt $x^\lambda = z^\lambda + y^\lambda$ folgende Gleichungen:

$$z + y = a^\lambda \quad \text{und} \quad z + \alpha^r y = E(\alpha) f(\alpha)^\lambda$$

ich verwandle α in α^{-1}, wodurch

$$z + \alpha^{-r} y = E(\alpha^{-1}) f(\alpha^{-1})^\lambda$$

es ist aber

$$E(\alpha^{-1}) = \pm\, \alpha^\varkappa E(\alpha), \quad \text{also} \quad z + \alpha^{-r} y = \pm\, \alpha^\varkappa E(\alpha) f(\alpha^{-1})^\lambda$$

also wenn $E(\alpha)$ eliminirt wird

$$\pm\, \alpha^\varkappa (z + \alpha^r y) f(\alpha^{-1})^\lambda = (z + \alpha^{-r} y) f(\alpha)^\lambda.$$

Hieraus eine Congruenz mod λ gemacht, giebt $f(\alpha)^\lambda \equiv c$ mod λ, ebenso $f(\alpha^{-1}) \equiv c$ mod λ also, weil c nicht durch λ theilbar ist,

$$\pm\, \alpha^\varkappa (z + \alpha^r y) \equiv z + \alpha^{-r} y \quad \text{mod } \lambda$$

oder

$$0 \equiv z + \alpha^{-r} y \mp \alpha^\varkappa z \mp \alpha^{\varkappa + r} y \quad \text{mod } \lambda.$$

Diese Congruenz kann nicht bestehen, ohne daß eine der Zahlen z oder y durch λ theilbar ist. q. e. d. Es sei also z die durch λ theilbare Zahl.

Anstatt der Gleichung $x^\lambda - y^\lambda = z^\lambda$, wo z durch λ theilbar ist, behandle ich die allgemeinere Gleichung für complexe Zahlen:

1) $$u^\lambda - v^\lambda = E(\alpha)(1-\alpha)^{m\lambda} w^\lambda \quad (E(\alpha) \text{ Einheit})$$

wo u, v, w complexe Zahlen sind, w den Factor $1 - \alpha$ nicht weiter enthaltend, und ich setze von u und v nur das voraus, daß sie in folgende Form gebracht werden können:

2) $$u = c + (1-\alpha)^{m\lambda - \lambda + 1} \cdot \Phi(\alpha); \quad v = c + (1-\alpha)^{m\lambda - \lambda + 1} \cdot \Psi(\alpha). \quad (c \text{ real}).$$

Ich zerlege nun $u^\lambda - v^\lambda$ in seine λ complexen Factoren, $u - v$, $u - \alpha v$, $u - \alpha^2 v$, etc. Diese Factoren haben unter sich keinen gemeinschaftlichen Factor außer $1 - \alpha$, diesen aber haben sie alle und zwar jedes nur einmal, eins aber hat ihn alle übrigen male, und dieß ist nach der Voraussetzung (siehe 2)) $u - v$ es ist also

3) $$u - v = e(\alpha)(1-\alpha)^{m\lambda - \lambda + 1} \cdot w_1^\lambda$$

4) $$u - \alpha^r v = e_r(\alpha)(1 - \alpha^r) t_r^\lambda$$

$e(\alpha)$ und $e_r(\alpha)$ sind Einheiten, w_1 und t_r complexe Zahlen.

(Der Satz: „wenn eine Potenz einer complexen Zahl in Factoren zerlegt wird, welche relative Primzahlen sind, so müssen diese Factoren selbst ebensolche Potenzen sein, multiplicirt mit Einheiten", folgt klar aus meinen früheren Untersuchungen, noch ist zu bemerken, daß weil w_1^λ und t_r^λ wirkliche complexe Zahlen sind, auch w_1 und t_r selbst solche sein müssen, nach der obigen Voraussetzung.)

Ich substituire in 4) die Werthe des u und v aus 2), so wird, wenn durch $1-\alpha^r$ dividirt ist:

5) $$c+(1-\alpha)^{m\lambda-\lambda}\cdot\left(\frac{1-\alpha}{1-\alpha^r}\right)(\Phi(\alpha)-\alpha^r\Psi(\alpha))=e_r(\alpha)\,t_r^\lambda$$

Hieraus mache ich eine Congruenz modulo λ und bemerke, daß $(1-\alpha)^{m\lambda-\lambda}$ durch λ theilbar ist, wenn $m>1$, welches hier vorausgesetzt wird, so ist

$$c\equiv e_r(\alpha)\,t_r^\lambda \quad \text{mod } \lambda;$$

es ist aber die λ^{te} Potenz der complexen Zahl allemal einer realen Zahl congruent, also $t_r^\lambda\equiv b$ mod λ folglich

$$c\equiv e_r(\alpha)b \quad \text{mod } \lambda,$$

und weil $e_r(\alpha)$ einer realen Zahl congruent ist modulo λ, so ist, nach dem oben angenommenen Satze, $e_r(\alpha)$ gleich einer λ^{ten} Potenz einer andern Einheit, also $e_r(\alpha)t_r{}^\lambda$ gleich einer λ^{ten} Potenz, gleich $u_1{}^\lambda$.

Dieß in der Gleichung (4) substituirt, giebt

6) $$u-\alpha^r v=(1-\alpha^r)u_1^\lambda$$

ebenso hat man für irgend einen anderen Werth des r, welchen ich s nenne

7) $$u-\alpha^s v=(1-\alpha^s)v_1^\lambda$$

und wenn noch die Gleichung 3) hinzugenommen wird:

3) $$u-v=e(\alpha)(1-\alpha)^{m\lambda-\lambda+1}\cdot w_1^\lambda$$

und aus diesen u und v eliminirt werden, so erhält man

$$u_1{}^\lambda-v_1{}^\lambda=\frac{(\alpha^r-\alpha^s)e(\alpha)(1-\alpha)^{m\lambda-\lambda+1}\cdot w_1^\lambda}{(1-a^r)(1-a^s)}$$

und wenn

$$\frac{(\alpha^r-\alpha^s)(1-\alpha)}{(1-\alpha^r)(1-\alpha^s)}\,e(\alpha)=E_1(\alpha)$$

gesetzt wird

8) $$u_1{}^\lambda-v_1{}^\lambda=E_1(\alpha)\,(1-\alpha)^{(m-1)\lambda}\cdot w_1{}^\lambda\,.$$

Diese Gleichung 8) ist nun dieselbe als 1) nur $m-1$ statt m gesetzt. Um aber zu zeigen, daß dieselbe Verwandlung sich wieder mit dieser Gleichung vornehmen läßt, müssen wir auch noch beweisen, daß die is a unit, then its product with e is again a unit e_1 and the relation (K) becomes

$$u_1^n - v_1^n = e_1(1-\alpha)^{(m-1)n} w_1^n,$$

which is exactly like (D) but with m replaced by $m-1$. Of course the conditions (E) have still to be verified, but that we leave to Kummer.

The expression in (L) is

$$\alpha^r \cdot \frac{1-\alpha^{s-r}}{1-\alpha} \frac{1-\alpha}{1-\alpha^r} \frac{1-\alpha}{1-\alpha^s},$$

thus the product of four expressions, all of which is a unit. So it is a unit.

Kummer was able to verify the two hypotheses for a large number of primes. They are true for all primes less than 100 except 37, 59 and 67, but it is not known that they are true for an infinite number of primes.

We do not have time to discuss Kummer's efforts to verify his hypotheses. Nor do we have time, or perhaps even the inclination, to discuss the methods introduced by Kummer and others to circumvent the difficulties entailed by the lack of general validity of these hypotheses. Kummer's claims to greatness rest as much on his creation of a rich theory of algebraic numbers and on discoveries that remain, even after the resolution of Fermat's theorem, very near mysteries that are at core of modern number theory as they do on his very bold, highly acclaimed, but ultimately only partially successful treatment of Fermat's theorem. I had hoped initially to offer in these lectures a glimpse of these mysteries to a lay audience and at the same time, by removing them from an abstract, theoretical sphere burdened with definitions to a plane where their significance would be immediately comprehensible, to acquire myself some adequate insight into their meaning. Frankly, in this respect, I have not come very far along, and am still about where I was a year ago. With the first set of lectures behind me, I can perhaps(!) now begin to think about a second in which I try again.

The mysteries to which I refer are to a large extent conjectures about the relation between numbers defined in one way or another by attempts to analyze the solutions of equations in integers or rational numbers and numbers defined by analytic expressions, thus expressions whose formation requires integrals and infinite series, but which can nevertheless, in contrast to the first class of numbers, be – provided various other conjectures can be established – calculated readily. Kummer was one of the first to discover such relations. The number of ideal classes of $\mathbb{Z}(\alpha)$ is a number of the first type.

It is by no means clear how to calculate it, yet Kummer, for his purposes, needs to show that it is prime to n. This is his second hypothesis. What he eventually showed is that his two hypotheses are valid if and only if the prime n does not divide the numerator of a certain collection of numbers, called Bernoulli numbers. These numbers can be defined in an elementary way, and I shall do so. Not only can they be readily calculated as we shall see, but also they are, in essence, the value of a very famous function, the Riemann zeta function, at negative integers. This function is defined by summing an infinite series.

There are many relations of this sort presently conjectured. The conjectures are magnificent, and it is a still outstanding task of the modern mathematician not only to prove them but also to explain them to himself and to the rest of the world.

The Bernoulli numbers B_0, B_1, B_2, and so on, can be defined in a simple way. First of all, $B_0 = 1$. Then, in general,

$$B_n = -\frac{1}{n+1}\left(B_0 + (n+1)B_1 + \cdots + \frac{n(n+1)}{2}B_{n+1}\right).$$

Thus

$$\begin{aligned}
B_1 &= -\frac{1}{2}B_0 = -\frac{1}{2},\\
B_2 &= -\frac{1}{3}\left(1 + 3\left(-\frac{1}{2}\right)\right) = \frac{1}{6},\\
B_3 &= -\frac{1}{4}\left(1 + 4\left(-\frac{1}{2}\right) + 6\left(\frac{1}{6}\right)\right) = 0,\\
B_4 &= -\frac{1}{5}\left(1 + 5\left(-\frac{1}{2}\right) + 10\left(\frac{1}{6}\right) + 10(0)\right) = -\frac{1}{30}.
\end{aligned}$$

The numbers grow rapidly, except that B_k, k odd, is always 0. For example,

$$B_{30} = \frac{8615841276005}{14322}.$$

Kummer's criterion fora prime n to satisfy his two hypotheses is that n does not divide the numerator of the numbers $B_2, B_4, \ldots, B_{n-3}$. For example 5 does not divide the numerator of B_2 which is 1 and 7 does not divide the numerator of B_2 or of B_4, which is 1. Since, for example,

$$B_6 = \frac{691}{2730},$$

the prime 691 will not satisfy Kummer's hypotheses. We also have

$$B_{32} = \frac{7709321041217}{510}$$

and

$$7709321041217 = 37 \times 683 \times 305065927,$$

so that $n = 37$ does not satisfy Kummer's hypotheses.