News about Roots of Unity

J. Coates, G. Poitou

January 9, 2004

Abstract

This text was originally intended for non-mathematicians; during its preparation B. Mazur and A. Wiles announced the solution of the 'Main Conjecture' in the theory of cyclotomic fields. It seemed appropriate to us to try to give an explanation of what this sensational discovery is all about.

Chapter 1

Bernoulli numbers

Starting from the exponential series

$$e^x = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \frac{1}{24}x^4 + \ldots + \frac{1}{n!}x^n + \ldots$$

one finds the identity

$$\frac{e^x - 1}{x} = 1 + \frac{1}{2}x + \frac{1}{6}x^2 + \frac{1}{24}x^3 + \ldots$$

and, by computing the inverse

$$\frac{x}{e^x - 1} = 1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4 \pm \ldots$$

In fact, the function $\frac{x}{e^x-1} - \frac{x}{2}$ is even and can therefore be written in the form

$$\frac{x}{e^x - 1} - \frac{x}{2} = 1 + \frac{1}{2!}B_2 x^2 + \frac{1}{4!}B_4 x^4 + \frac{1}{6!}B_6 x^6 + \ldots$$

This is actually the definition of the Bernoulli numbers $B_2, B_4, \ldots, B_{2k}, \ldots$[1] One finds $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$ etc. The integers which appear in the numerators and denominators of these numbers appear, on first sight, to be bizarre and arbitrary, but they contain a wealth of arithmetic information which one has noticed beginning with the 19th century.

The congruences of von Staudt and Clausen (1840)

We can guess them by writing $\frac{1}{6} = 1 - \frac{1}{2} - \frac{1}{3}$, $-\frac{1}{30} = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5}$, $\frac{1}{42} = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{7}$, $\frac{5}{66} = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{1}$ etc. One is led to conjecture that the Bernoulli numbers is an integer (not always equal to 1, as the above examples seem to indicate) minus the sum of the inverses of some primes. Which primes? A careful

[1] Jakob Bernoulli (1654–1705); one can also define these numbers via the identity $x \cot x = 1 - \sum_{n=1}^{\infty} \frac{1}{2n!} B_{2n} x^{2n}$. There are recurrence formulas for computing Bernoulli numbers.

examination of our examples suggests that the primes are those dividing $2k$. The proof of this fact is not really difficult. This shows that the denominators have a very simple structure; the properties of the numerators are much more hidden. Patience! Let us first observe another phenomenon which relates the numerators and the denominators.

The Kummer congruences

Let us make an experiment with the integer 5, where we can read off the divisibility properties of an integer at the last digit. We will find that 5 divides the denominator of B_4, B_8, B_{12}, B_{16}, ... etc., and that it divides the numerator of B_{10}. Let us form the numbers $2/B_2 = 12$, $6/B_6 = 6 \cdot 42$, $10/B_{10} = 2 \cdot 66$, $14/B_{14} = 12$, $18/B_{18} = \frac{18 \cdot 798}{43867}$. The first four numbers are integers with last digit 2; as for the fifth, the numerator end with 4 and the denominator with 7; this shows that, modulo 5 (i.e. by working up to multiples of 5), it is like $\frac{4}{2} = 2$. Thus, all these numbers are in the class $2 \bmod 5$. This is the prototype of the Kummer congruences: if p is a prime and $p-1$ does not divide $2k$, then the numbers $\frac{1}{2k}B_{2k}$, $\frac{1}{2k+p-1}B_{2k+p-1}$, $\frac{1}{2k+2p-2}B_{2k+2p-2}$, ... are all in the same congruence class modulo p (of course, these numbers are fractions, but as above we can give a precise meaning to this statement by using Gauss' theory of congruences).

Euler's Relations (1755)

The famous exercises in calculus $1 + \frac{1}{4} + \frac{1}{9} + \ldots = \frac{\pi^2}{6}$, $1 + \frac{1}{8} + \frac{1}{27} + \ldots = \frac{\pi^4}{90}$ are special cases of the following theorem:

$$1 + \frac{1}{2^k} + \frac{1}{3^k} + \frac{1}{4^k} + \ldots = -\frac{(2\pi i)^{2k}}{2 \cdot (2k)!} B_{2k}.$$

The series on the left hand side is usually denoted by $\zeta(2k)$, where $\zeta(s) = 1 + 2^{-s} + 3^{-s} + \ldots$ is *Riemann's zeta function* (this function can be extended by elementary methods to all complex numbers s with real part > 1; actually it can be extended to all complex numbers $\neq 1$, but this is more difficult[2]). The fact that $\zeta(s)$ has no zeros $s \in \mathbb{C}$ with real part > 1 is an immediate consequence of the unique factorization theorem for integers; Hadamard and de la Vallée-Poussin have shown in 1896 that there are no zeros on the line $s = 1$, and used this fact to derive the 'prime number theorem': there are about $\frac{x}{\log x}$ prime numbers $\leq x$. Finally, the assertion that there are no zeros with real part $> \frac{1}{2}$ is called the 'Riemann Hypothesis' (Riemann 1859); it can be expressed in the form 'all zeros of $\zeta(s)$ with positive real part lie on the line $\Re s = \frac{1}{2}$; this has been proved for the first million zeros in the 'critical strip'.

[2]this extension, together with the 'functional equation' that goes along with it, allows us to express Euler's relations in the elegant form $-\frac{1}{2k}B_{2k} = \zeta(1-2k)$

Chapter 2

Ideal Class Numbers

Consider the following two lattices in the complex plane:
(I) the Gaussian integers $R = \{a + bi : a, b \in \mathbb{Z}\}$ and
(II) the Eisenstein integers $R = \{a + bj : a, b \in \mathbb{Z}\}$, where $j = \frac{1}{2}(-1 + i\sqrt{3}\,)$ satisfies $j^3 = 1$. These sets of numbers are closed under addition and multiplication (i.e. they form a ring). It is easy to guess what a sublattice S of R should be: a subgroup (with two points, S also contains their sum and their difference) which is not contained in a line. Let us call a sublattice *stable* if it coincides with itself after a rotation of 90^o in case (I) and 120^o in case (II). Such sublattices are easy to find: if z is an arbitrary element of R, the set zR of all products zr with $r \in R$ is a stable sublattice of R. Geometrically, multiplication by z in the complex plane produces a sublattice zR of R which is 'similar' to R, i.e. which has the same form (up to stretching and rotating). Do there exist stable sublattices which are not similar to R? An elementary argument (analogous to the one by which one shows that every subgroup of the group $\mathbb{Z}$ of integers consists of multiples of a fixed integer) shows that such sublattices do not exist! Starting with this observation, the theory of unique factorization for ordinary integers can be carried over to an analogous theory for the integers of Gauss (case I) and Eisenstein (case II).

Before going further, we need some notation. A sublattice S of R is stable (in the sense above) if and only if it is stable under multiplication by arbitrary elements of R. In general, a subring of a ring R which is stable under multiplication by elements of R is called an *ideal* of R. The ideals of the form zR are called principal, and one can formulate our results above by saying that, in our examples (I) and (II), all ideals of R are principal (just as in the ring of ordinary integers). These reassuring results, however, are misleading![1] Take R e.g. to be the lattice with basis 1 and $\theta = i\sqrt{5}$ in the complex plane; R is a ring. Let S be the subring with basis 2 and $1 + \theta$. The identities $(1 + \theta)\theta = \theta + \theta^2 = (1 + \theta) + 2(-3)$ show that S is an ideal in R. It is easy to see that S is not similar to R.

On the other hand, it can be shown that every ideal of R is similar to either

[1] The following excursion explains ideal classes in a case where they can be presented in a more visual way than in the cyclotomic case.

R or S, or, as we will say, that there are only two *ideal classes*. Consider the product UV of two ideals U and V: this is the sublattice of R generated by the products uv with $u \in U$ and $v \in V$, and it is an ideal. Forming the product is compatible with similarity, thus the ideal classes form a group. The product SS must therefore be a principal ideal, and in fact it equals $2R$.

The three examples studied so far are the special cases $a = 1, 3, 5$ of the following general situation: let $\mathbb{Q}(\sqrt{-a}\,)$ denote the imaginary quadratic number field generated (via the four arithmetic operations) by the rational numbers and the square root of the negative integer $-a$. The ring R is the ring of (algebraic) integers in this field. One could define it by brute force as the lattice generated by 1 and $\theta = \sqrt{-a}$ if $a = 1, 2, 5, 6, 10, 13, \ldots$ and by 1 and $\theta = \frac{1}{2}(1 + \sqrt{-a}\,)$ if $a = 3, 7, 11, 15, \ldots$. We are interested in the ideals of R, their similarity classes, and the number h of these classes (which is finite). Here is a little table giving the value of h as a function of a:

a	1	2	3	5	6	7	10	11	13	14	15	17	19
h	1	1	1	2	2	1	2	1	2	4	2	4	1

Let us come back to the Bernoulli numbers! It is in terms of class groups (though not of quadratic but of cyclotomic number fields) that one can see the profound connection between Bernoulli numbers and the mysteries of arithmetic. An *algebraic number field* is a set of complex numbers, closed under the four arithmetic operations, and generated by ordinary integers and finitely many algebraic numbers (roots of polynomials with integer coefficients).[2] Among all number fields, the fields generated by roots of unity play a special role (which we probably don't really understand even today). They are called cyclotomic number fields, and roots of unity are the algebraic solutions of the problem of dividing the circle into equal parts. Let $m \geq 3$ be an integer, and $\zeta = e^{2\pi i/m}$; this is a root of the polynomial $x^m - 1$, as well as of an irreducible factor (of smaller degree) of it. If m is a prime number, this factor is $x^{p-1} + x^{p-2} + \ldots + x + 1$. We denote by $\mathbb{Q}(\zeta)$ the number field generated by ζ and the rationals. In the case $m = p$, its elements can be written uniquely in the form $z = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$, where the a_i are rational numbers (wriiten in this form, it is obvious how addition is performed; as for multiplication, one reduces the result to this form by using the relation $\zeta_{p-1} + \zeta_{p-2} + \ldots + \zeta + 1 = 0$). If the a_i are integers, we say that z is an algebraic integer in this field; they form a ring which we will denote by R. Note that the case $m = 3$ coincides with example (II) above. It can be shown (even in the case of general number fields) that the ideals of R can be partitioned in a finite number of similarity classes (this definition can't be given in the same geometric form as in the quadratic case above; ideals U and V are called similar if there exist $a, b \in R \setminus \{0\}$ such that $aU = bV$), and that the classes form a multiplicative commutative group C. Here is a small table of the value of these class numbers h in terms of p:

[2] A number field is thus a 'finite extensions of the rationals $\mathbb{Q}$, i.e. a field containing $\mathbb{Q}$ as a subfield, and of finite dimension as a vector space over $\mathbb{Q}$

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
h	1	1	1	1	1	1	1	3	8	9	37	121	211	695

Let us also give a slightly enlarged table of numerators N_{2k} of the Bernoulli numbers B_{2k}, with all prime factors ≤ 4000:

2k	10	12	14	16	18	20	22
N_{2k}	5	691	7	3617	43867	$283 \cdot 617$	$11 \cdot 131 \cdot 593$

2k	24	26	28	30
N_{2k}	$103 \cdot 2294797$	$13 \cdot 657931$	$7 \cdot 339278147$	$5 \cdot 1721 \cdot 1001259881$

2k	32	34
N_{2k}	$37 \cdot 683 \cdot 305065927$	2577687858367

There are only few prime factors, especially after throwing out the divisors of k (it follows from Kummer's congruences that p divides N_{2k} if k is divisible by p but not by $p-1$). Once this is done, the only small prime factor remaining is 37. The table of class numbers h given above shows that something peculiar is happening for $p = 37$: there are 37 ideal classes in the field of 37th roots of unity! Maybe this is just accidental? After all, nothing suggests a connection between h and the Bernoulli numbers B_{2k}. This is what Kummer proved:
Theorem 1 of Kummer. The prime number p divides the class number of the fields of p-th roots of unity if and only if p divides one of the numbers N_2, N_4, …, N_{p-3}.

Such a prime number p is called *irregular*. The tables above show that 37, 103, 131 are irregular; so are 59, 67 and 101. Primes which are not irregular are called *regular*. The existence of infinitely many irregular primes has been established; for regular primes, this is still a conjecture.

Two Historical Remarks They concern the two great sources of modern algebra, namely Fermat's Last Theorem and the solution of algebraic equations by radicals, which was inspired by Galois.

Remark 1 The question posed by Fermat is whether the equation $x^m + y^m = z^m$, where $m \geq 3$ is an integer, can be solved in nonzero integers x, y, z. The relation with the fields of mth roots of unity comes via the factorization of $x^m + y^m$ into a product of factors of the form $x + y\zeta^k$. The theorem about the unique factorization into prime elements mentioned above for $m = 4$ (case (I)) and $m = 3$ (case (II)) gave the proof of Fermat's claim not only in these two cases, but also for all primes $m = p$ such that $h = 1$ (i.e. $p \leq 19$). Kummer's first spectacular result was the extension of this proof to all regular primes. See the books of Borevic-Shafarevic and of Ribenboim for more details.

Remark 2 Recall that Galois (1811–1832) has associated to every irreducible polynomial of degree n the subgroup of the group of permutations of n objects 'which conserves the roots'. If this group is commutative, the polynomial is called *abelian*. This is the case for imaginary quadratic fields, where the Galois group consists of the identity and complex conjugation. For the fields $\mathbb{Q}(\zeta)$ with $\zeta^m = 1$, the Galois group is the group of permutations of the m-th roots of unity given by $\zeta \longmapsto \zeta^a$, where a is a number coprime to m (note that only the residue class oif a modulo m counts). The group law is simply the multiplication of these classes, hence it is commutative. The field $\mathbb{Q}(\zeta)$ is therefore abelian, and it follows from Galois theory that the same holds for all of its subfields. What is more surprising is the converse (Kronecker): there are no other abelian number fields than the subfields of $\mathbb{Q}(\zeta)$. For example, the field $\mathbb{Q}(\sqrt{5}\,)$ is contained in the fields of fifth, $\mathbb{Q}(\sqrt{-5}\,)$ in the field of 20th roots of unity, etc.

Few lectures in mathematics are as well known as the one Hilbert delivered at the Congress of Mathematicians 1900 in Paris. Among the problems he posed, the 12th concerned the generalization of this theorem of Kronecker. Hilbert expressed it by saying that the abelian extensions of $\mathbb{Q}$ are generated by the values of the function $e^{2\pi x}$ at rational values of x. Then he asked if there exist analogous functions which describe those extensions of a given field K whose relative Galois groups are abelian. The elliptic functions give an answer for imaginary quadratic number fields K. Studying the class numbers of abelian extensions of K leads to numbers analogous to Bernoulli numbers: they depend on K and are called *Hurwitz numbers*.

Chapter 3

Galois Action on Class Groups

Given a prime number p, let Δ denote the set of integers $\{1, 2, \ldots, p-1\}$, with the addition law given by multiplication modulo p.[1] By specializing what we have said in Remark 2 above to the case $m = p$ we see that we may identify Δ and the Galois group of the field $\mathbb{Q}(\zeta)$ (with $\zeta^p = 1$) by associating to each $b \in \Delta$ the transformation σ_b which raises each root of unity to its bth power. This transformation acts on every element $x = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$ of the field (here the a_i are rational) via the formula $\sigma_b(x) = a_0 + a_1\zeta^b + \ldots + a_{p-2}\zeta^{b(p-2)}$. [2] Clearly Δ also acts on the integers of $\mathbb{Q}(\zeta)$ (i.e. if x is an integer, then so is $\sigma_b(x)$). Therefore, it acts on ideals and principal ideals, as well as on the group C of ideal classes. Kummer himself has recognized that the action of Δ on C holds the key to the most profound explanation of his theorem about the connection between C and the numerators of the Bernoulli numbers.

For a closer examination of the case $p = 37$, let us denote the set of integers $\{0, 1, \ldots, p-2\}$ by Ω; this is a group under addition modulo $p-1$.[3] For $b \in \Delta$ and $i \in \Omega$, the integer b^i is coprime to p, and we will also write b^i for its residue modulo p in Δ. The usual laws of exponentiation are valid in this case, thanks to elementary properties of congruences, if one multiplies elements of Δ modulo p and reduces those of Ω modulo $p-1$. In the case $p = 37$, we claim that there is a unique exponent i_0 in Ω such that

$$\sigma_b(c) = c^{b^{i_0}} \tag{3.1}$$

for every $b \in \Delta$ and all ideal classes c. If we admit the numerical fact that the group C is cyclic,[4] then this follows by elementary algebra. In fact, the group

[1] Δ is usually denoted by $(\mathbb{Z}/p\mathbb{Z})^\times$ or $(\mathbb{Z}/p)^\times$

[2] This is an automorphism of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$); this language has replaced the 'permutations of the roots' of Galois

[3] Ω is usually denoted by $\mathbb{Z}/(p-1)\mathbb{Z}$ or $\mathbb{Z}/(p-1)$

[4] A group is called cyclic if its elements are powers of one of its elements; a group of prime

Δ is cyclic itself (this is a basic result in the theory of congruences; for $p = 37$, it is easy to verify that 2 is a generator). Now let b be a fixed generator of Δ, and $c \in C$ a fixed nontrivial ideal class (thus c generates C). It is clear that (3.1) must hold for a certain $i_0 \in \Omega$. By the laws of exponentiation, (3.1) then holds (with the same i_0) for all classes in C and all elements of Δ. This has of course nothing to do with cyclotomy, but is true whenever Δ acts on a cyclic group of order p. In our case $p = 37$, computing the ideal classes yields $i_0 = 5$. What has this got to do with the Bernoulli numbers? It turns out (and has certainly been noticed by Kummer) that $5 \equiv 1 - 32 \bmod 36$, and that 32 is the only index smaller than 36 such that B_n is divisible by 37.

In order to put this observation into its proper context, let us come back to the general case and try to find the analogue of (3.1). The group C has no reason to be cyclic of prime power order anymore. We therefore replace it by the subgroup A_m of elements whose order is a power of p; let p^m be the maximum of these orders.[5] We claim that A is the direct product of $p-1$ subgroups $A^{(0)}, \dots, A^{(p-2)}$,[6] where the subgroup $A^{(i)}$ is characterized by the fact that the operation of Δ is described by

$$\sigma_b(c) = c^{b^{ip^{m-1}}} \text{ for all } b \in \Delta \text{ and all } c \in A^{(i)}. \qquad (3.2)$$[7]

This is again a purely algebraic fact which is valid whenever Δ acts on an abelian p-group and which corresponds to the decomposition of a vector space into eigenspaces with respect to a given matrix; in particular, this is not a profound statement about the groups $A^{(i)}$. Kummer seems to have been the first to notice certain arithmetic assertions which are hidden behind the orders of the groups $A^{(i)}$. The nature of these results is totally different according to the parity of i, and we will discuss the two cases separately.

3.1 The odd eigenspaces

We consider the subgroups $A^{(i)}$ with $i \in \Omega$ odd. The value $i = 1$ is a special case which can be easily dealt with. In fact, Kummer has shown that $A^{(1)}$ is always trivial (his proof makes use of the congruences of von Staudt and Clausen). Assume therefore that i is one of the numbers $3, 5, \dots, p-2$, and consider the sequence

$$B_{(p-1-i)+1}, B_{p(p-1-i)+1}, \dots, B_{p^{n-1}(p-1-i)+1}, \dots \qquad (3.3)$$

order is necessarily cyclic by Lagrange's theorem which says that the order of a subgroup divides the order of the group. Saying that 2 generates Δ thus means that Δ consists of the classes $1, 2, 2^2, \dots, 2^{p-2}$.

[5] thus p is irregular if and only if $A \neq 1$, i.e. $m \geq 1$

[6] this means that each element $\alpha \in A$ can be written uniquely as a product $\alpha = \alpha_0 \cdots \alpha_{p-2}$, where $\alpha_i \in A^{(i)}$; of course the groups $A^{(i)}$ might be trivial: for $p = 37$, we have $A^{(i)} = 1$ for all $i \neq 5$.

[7] here, we can make m as large as we please. The point is that there exists a natural character of Δ which maps b to b^{p^m} mod p^m; this character takes values in the p-adic integers, i.e. in a compatible system of homomorphisms $\Delta \longrightarrow (\mathbb{Z}/p^n)^\times$ $(n = 1, 2, \dots)$

of Bernoulli numbers. We first observe that the indices of these numbers are not divisible by $p-1$, hence p does not divide the denominators of these numbers (by von Staudt - Clausen). The numerators, however, are either all divisible by p, or none of them is (by Kummer's congruences). What can we say about higher powers of p?

Definition of $\rho_p(i)$. If p does not divide the numbers (3.3), then we put $\rho_p(i) = 0$; otherwise $\rho_p(i)$ is the biggest integer $n \geq 1$ such that p^n divides the numerator of $B_{p^{n-1}(p-1-i)+1}$.

It is true, though not obvious, that the $\rho_p(i)$ are finite. We will not prove this here, but the reader may guess that this has got something to do with the convergence of the series (3.3), not in the usual sense, but in the p-adic metric, where two numbers are considered to be close if their difference is divisible by a high power of p. Kummer himself has obtained two results which connect the integers $\rho_p(i)$ with the orders of the groups $A^{(i)}$. The first is known as the analytic class number formula; as the corresponding formula for imaginary quadratic number fields by Dirichlet, it uses a generalization of the zeta function $\zeta(s)$.

Theorem 2 of Kummer The product of the orders of the groups $A^{(i)}$ ($i = 3, 5, \ldots, p-2$) is equal to the product of the numbers $p^{\rho_p(i)}$ ($i = 3, 5, \ldots, p-2$).

The second result does not occur explicitly in the papers of Kummer, but he was in possession of all the necessary tools. It was rediscovered by J. Herbrand[8] and maybe others.

Theorem 3 of Kummer For each $i = 3, 5, \ldots, p-2$, the order of $A^{(i)}$ divides $p^{\rho_p(i)}$. In particular, the groups $A^{(i)}$ are trivial if p does not divide the numerators of the Bernoulli numbers (3.3), i.e. of the B_{p-i}.

A very poor illustration of this theorem is provided by the case $p = 37$, where $A^{(i)} = 1$ if $i \neq 5$, and $A^{(5)} \neq 1$.

In light of these results, it is natural to conjecture that $p^{\rho_p(i)}$ is the exact order of $A^{(i)}$. Let us sketch the history of this conjecture. Several authors have shown that this is true under some strong additional hypotheses for p, for example 'Vandiver's Conjecture' (see below). Without such hypotheses, the problem seemed intractable by the classical methods until very recently. The fundamental difficulty is that one has to construct non-trivial ideal classes of order $p^{\rho_p(i)}$ in $A^{(i)}$, and this could not been done by known methods. The first real progress on this question was made by Ribet[9] in 1976. Using modular curves, he could show that $A^{(i)} \neq 1$ if $\rho_p(i) > 0$. Recently, Wiles[10] saw how to improve Ribet's ideas in a decisive way by using work of Mazur[11] on modular curves. He obtained the conjectured equality for those $A^{(i)}$ which are cyclic. One has to remark that numerical experiments have not revealed any example

[8]Journal de Math. pures et appliquées, 11 (1932)
[9]Inventiones mathematicae, 34 (1976), 151–162
[10]Inventiones mathematicae, 58 (1980), 1–35
[11]Publ. Math. I.H.E.S. 47 (1978)

of a non-cyclic $A^{(i)}$, but there is no reason to suspect that this is always true.[12] The whole problem has been resolved completely by Mazur and Wiles,[13] who proved the history-making result

First Theorem of Mazur and Wiles For each $i = 3, 5, \ldots, p-2$, the subgroup $A^{(i)}$ has order $p^{\rho_p(i)}$.

Of course the proof is difficult. We will say a few words about it in Chapter 4 below. Now we will return to the decomposition of the class group.

3.2 The even eigenspaces

One of the big mysteries in the theory of cyclotomic number fields is the relation between the order of the subgroup $A^{(i)}$ for *even* index i and the order of a completely different (but equally important) group, namely the group of *positive units modulo the cyclotomic units*. Recall that R denotes the ring of integers in $\mathbb{Q}(\zeta)$. By a *unit* of this field we understand actually a unit in R, i.e. an element $\varepsilon \neq 0$ such that $1/\varepsilon$ is also an element of R. It turns out that it is easy to write down explicitly a set of units in $\mathbb{Q}(\zeta)$. We leave it as an exercise to the reader to prove that each of the $r = \frac{1}{2}(p-3)$ numbers

$$\eta_k = \frac{\sin\left(\frac{(k+1)\pi}{p}\right)}{\sin\left(\frac{\pi}{p}\right)} \qquad (k = 1, 2, \ldots, r)$$

is a unit in $\mathbb{Q}(\zeta)$.[14] Let D denote the multiplicative subgroup of $\mathbb{Q}(\zeta)$ generated by these units. Every element of D is a real positive unit, since each generator is. We call D the group of cyclotomic units.[15] Let E be the multiplicative group of all real positive units in $\mathbb{Q}(\zeta)$; they are actually contained in the maximal real subfield $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{p})$. What can we say about the factor group E/D? This is the point where we have to invoke Dirichlet's celebrated theorem[16] (which holds more generally for arbitrary number fields), according to which E is a free abelian group of rank $r = \frac{1}{2}(p-3)$. This means that there exist units

[12] There are 11 734 primes $p \leq 125\,000$, and 4605 among them are irregular; more than 3/4 do only have one non-trivial component (like $p = 37$), and this component is cyclic of order p (Wagstaff, 1978)

[13] On a conjecture of Iwasawa, to appear

[14] The first nontrivial case, $p = 5$, yields the unit $\eta_1 = 2\cos\frac{\pi}{2}$, which equals the 'golden ratio' $\frac{1}{2}(1+\sqrt{5})$. It is well known that this number generates the group of positive units of the field $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$, which, in accordance with Theorem 4 below, has class number 1

[15] In the 'elliptic' theory which we have hinted at in Remark 2 of Chapter 2, and where the base field Q is replaced by an imaginary quadratic number field K, the analogue of D is the group of 'elliptic units' by Gilles Robert.

[16] 1846. According to this theorem, an imaginary quadratic number field only has finitely many units; in real quadratic fields, the positive units are all powers of one unit - which is actually a solution of 'Pell's equation'

$\varepsilon_1, \ldots, \varepsilon_r$ in E such that each element $\varepsilon \in E$ can be written uniquely in the form

$$\varepsilon = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r},$$

where the n_i are rational integers. Of course, in general we cannot write down explicit expressions for $\varepsilon_1, \ldots, \varepsilon_r$; nevertheless it is clear that the factor group E/D is finite if and only if there does not exist a non-trivial multiplicative relation among the η_i; equivalently, the equation $\eta_1^{k_1} \cdots \eta_r^{k_r} = 1$ with integers k_i has only the trivial solution $k_1 = \ldots = k_r = 0$. Kummer has shown that this is true, by making use of Dirichlet's L-functions $L(s, \chi)$ in an essential way (these generalize the function $\zeta(s)$). It is remarkable that we still do not possess a direct proof of this fact. Actually, Kummer obtained a much stronger result: he computed the order of the group E/D:

Theorem 4 of Kummer The index of the group D of cyclotomic units in the group E of real positive units of $\mathbb{Q}(\zeta)$ equals the order of the ideal class group C^+ of the field $\mathbb{Q}(\zeta + \zeta^{-1})$.

We are interested in the p-components of the ideal class group. Let B denote the subgroup of E/D which consists of all elements whose order is a power of p.

Corollary. The order of B is the product of the orders of the $A^{(i)}$ for $i = 0, 2, 4, \ldots, p-3$. In fact, the product of these groups $A^{(i)}$ is the p-part of C^+.

Let us now introduce the action of the Galois group. Although a positive unit in general has conjugates which are not positive, one can show that Δ acts on the group B. Since each element of B has p-power order, the algebraic situation is as above, and we can write B as the product $B = B^{(2)} B^{(4)} \cdots B^{(p-3)}$ of the subgroups $B^{(i)}$, which is characterized by the fact that the operation of Δ corresponds to (11). Since all the units we consider are real, it follows easily that $B^{(i)} = 1$ for odd values of i. Thus the corollary above says that the product of the orders of the $B^{(i)}$ with even index equals the corresponding product of the orders of the $A^{(i)}$. Again, the principal question since Kummer is: do $A^{(i)}$ and $B^{(i)}$ have the same order?[17] The essential difficulty here is that Kummer's proof of Theorem 4 does not yield a natural map between E/D and the class group C^+ of $\mathbb{Q}(\zeta + \zeta^{-1})$. The first real progress was made by Wiles,[18] who showed (using the theory of modular curves) that $A^{(i)} = 1$ implies $B^{(i)} = 1$. The collaboration of Mazur and Wiles[19] has now led to a complete answer to this problem:

Second Theorem of Mazur and Wiles For each $i = 0, 2, 4, \ldots, p-3$, the subgroups $A^{(i)}$ and $B^{(i)}$ have same order.

It is appropriate to remark that numerical computations have never produced a prime p with $B^{(i)} \neq 1$ for some even i. Although the calculations have

[17] For a generalization to general real abelian number fields, see the conjecture of Gras in Ann. Inst. Fourier 27 (1977), 1–66, Greenberg's answer in Bagoya Math. J. 67 (1977), 139–158, and Gillard, Seminaire Delange-Pisot-Poitou, 3 janvier 1977.

[18] op. cit.

[19] op. cit.

now covered all primes $p \leq 125\,000$, this number should not be considered as very big, and there do not exist good reasons for believing Vandiver's conjecture that we always have $B^{(i)} = 1$, or, in other words, that p never divides the order of C^+.

Chapter 4

Comments on the Methods

The proofs of Mazur and Wiles depend on subtle combinations of ideas in the arithmetic of number fields and the geometry of certain algebraic curves[1] which occur naturally in the theory of modular elliptic functions. In a very clear sense, their work may be considered as a natural variation of one of the great subjects of 19th century mathematics, namely the (extraordinarily rich and profound) connection between modular elliptic functions and number theory.[2] It is of course impossible to give only the slightest account of their arguments, but we think that we can at least give an aspect of the theory of cyclotomic fields which is absolutely essential in their approach, and which was discovered by Iwasawa in the last twenty years. The two theorems of Mazur and Wiles cited above concern the field of p-th roots of unity. It seems that, in order to obtain them, one has to consider the whole tower of fields $\mathbb{Q}(e^{2\pi i/p^n})$, $n = 1, 2, 3, \ldots$. At first sight, analogous questions for these fields lead to the following difficulty: for $n \geq 2$, the order of the Galois group of such fields is divisible by p, and its action on a p-primary abelian group cannot be described by a decomposition into eigenspaces (see our remarks in Chapter 3). Nevertheless, more complex algebraic arguments allow us to attach interesting invariants to such a group action. These invariants have been defined earlier by Fitting,[3] but here we shall follow the version due to Iwasawa[4] and Serre,[5] where the passage to the limit simplifies things considerably.

For each integer $n \geq 0$, put $\zeta_n = e^{2\pi i/p^{n+1}}$, let F_n denote the field $\mathbb{Q}(\zeta_n)$, and let Δ_n be the Galois group of F_n. As above, we may identify Δ_n with the set of integers b between 0 and p^{n+1} which are coprime to p, with addition on this set being addition modulo p^{n+1}. Under this identification, b corresponds to the unique automorphism σ_b of F_n such that $\sigma_b(\zeta_n) = \zeta_n^b$. What structure does

[1] for example, the curve $X_i(p)$, which is obtained from Poincaré's upper half plane (complex numbers z with $\operatorname{Im} z > 0$) by taking the quotient with respect to the transformations $(az + b)/(cz + d)$, where a, b, c, d are integers with $ad - bc = 1$ and $a \equiv d \equiv 1 \bmod p$, $c \equiv 0 \bmod p$.

[2] The theorem of Kronecker-Weber we have talked about earlier belongs here.

[3] Jahresbericht Deutsch. Math. Verein. 46 (1936), 195–228

[4] Bull. Amer. Math. Soc. 65 (1959)

[5] Séminaire Bourbaki, 1958

Δ_n have? The restriction of automorphisms from the field F_n to F_0 defines a group homomorphism $\Delta_n \longrightarrow \Delta_0 =: \Delta$, and one verifies immediately that the kernel of this homomorphism is a cyclic group of order p^n, which is generated by σ_{1+p}. Since the order of Δ is prime to p, we can identify Δ with a subgroup of Δ_n and thus obtain a decomposition into a direct product

$$\Delta_n \simeq \Delta \times \Sigma. \tag{4.1}$$

In light of the passage to the limit, the algebraic situation can be described by giving a sequence X_n ($n = 0, 1, \ldots$) of finite p-primary abelian groups which are acted on by Δ_n, together with a family $\Phi_{n,m} : X_n \longrightarrow X_m$ of homomorphism (with $n \leq m$) which are compatible in an obvious sense with the restriction of the automorphisms from Δ_m to Δ_n. Which invariants can we extract from this situation? Let us first look at the action of Δ, then study the chain of the Σ_n. In fact, from (4.1) we see that X_n can be viewed as a Δ-module, thus we can decompose it (as above) into a product of eigenspaces $X_n^{(i)}$, $i \in \Omega$. Let us fix $i \in \Omega$ and consider the sequence $X_0^{(i)}, X_1^{(i)}, \ldots, X_n^{(i)}, \ldots$ with the homomorphisms deduced from the $\Phi_{n,m}$ and the compatible action of Σ_n on $X_n^{(i)}$. Recall that Σ_n is a cyclic group of order p^n, generated by the remarkable automorphism σ_{1+p} (for which we do not need an index n); in fact the element σ_{1+p} in Σ_n is simply the restriction of σ_{1+p} in Σ_m.

Is it possible to find an analogue for the characteristic polynomial of a matrix if one considers the action of σ_{1+p} on the abelian groups $X_n^{(i)}$? The answer is no if we fix n, but Iwasawa has shown that the answer is yes for a certain limit space formed from the sequence $X_0^{(i)}, X_1^{(i)}, \ldots$ We cannot give the details here; suffice it to say that the result differs in two aspects from what one may expect naively. First, one does not obtain a characteristic polynomial for σ_{1+p}, but a *characteristic series*[6] of the form

$$f_i(T) = a_0(i) + a_1(i)T + \ldots + a_k(i)T^k + \ldots$$

Second, the coefficients $a_k(i)$ are not ordinary integers in $\mathbb{Z}$ but lie in $\mathbb{Z}_p$, its completion with respect to the p-adic metric.[7]

Let us now apply these algebraic remarks to the $X_n = A_n$ ($n = 0, 1, \ldots$), where A_n is the p-primary subgroup of the ideal class group of F_n. The action of the Galois group Δ_n on A_n is the natural action (we have looked at the case $n = 0$ before). For $n \leq m$, the homomorphism $\Phi_{n,m} : A_n \longrightarrow A_m$ is induced by a homomorphism on the ideal groups, which map an ideal $\mathfrak{a}$ in F_n to the ideal generated by $\mathfrak{a}$ in F_m. The algebraic theory we just described can be applied now, and it yields the characteristic series $f_i(T)$ for $i = 0, 1, \ldots, p-2$. Iwasawa

[6] This series is commonly called the *Iwasawa series* of the system $X_n^{(i)}$; it is defined up to factors of units in the ring of formal power series with coefficients in $\mathbb{Z}_p$.

[7] The elements of Z_p (p-adic integers) are the limits of Cauchy sequences of ordinary integers with respect to the p-adic metric mentioned earlier; one can also view them as the sums of series $a_0 + a_1 p + \ldots + a_k p^k + \ldots$, where the a_k are ordinary integers between 0 and $p-1$. These series converge in the p-adic metric.

has noticed that several classical problems in the theory of cyclotomic fields (including those discussed above for $n = 0$) would follow from a remarkable conjecture about the $f_i(T)$ with odd index i.

In order to explain some details, we first recall an important theorem of Iwasawa[8] on Bernoulli numbers. As above, we exclude the case $i = 1$; in fact, one can show that $f_1(T) = 1$ is always trivial. Let Λ denote the ring of formal power series in one variable T with coefficients in $\mathbb{Z}_p$ (the characteristic series $f_i(T)$ mentioned above are elements of Λ). It is possible to transform these formal power series into converging series by substituting an ordinary integer divisible by p for T, and by recalling that convergence is to be understood in the p-adic sense.[9]

Theorem (Iwasawa). For each $i = 3, 5, \ldots, p-2$, there exists a series $g_i(T)$ [10] in Λ such that

$$g_i((1+p)^n - 1) = -(1-p^n)\frac{B_{n+1}}{n+1} \tag{4.2}$$

for each $n \in \mathbb{N}$ with $n \equiv p-1-j \bmod (p-1)$.

We observe immediately that the two facts on Bernoulli numbers which we have used before (the Kummer congruences and the finiteness of the $\rho_p(i)$) are easy consequences of this theorem: in fact, let

$$g(T) = b_0 + b_1 T + \ldots \tag{4.3}$$

be a series in Λ, i.e. with coefficients $b_i \in \mathbb{Z}_p$. If one substitutes $T = (1+p)^n - 1$, it is clear that all terms except b_0 are divisible by p, and we get

$$g((1+p)^n - 1) \equiv b_0 \equiv g((1+p)^m - 1) \bmod p$$

for arbitrary integers m, n. If we apply this observation to the series $g_i(T)$ above, we get the Kummer congruences.

Now, let us fix i and put $n_k = p^{k-1}(p-i-1)$, where k is an integer ≥ 1. We see that $(1+p)^{n_k} - 1$ is divisible by p^k. Therefore, all terms in the series(4.3) except b_0 are divisible by p^k, and we find

$$g_i((1+p)^{n_k} - 1) \equiv b_0 \equiv g(0) \bmod p^k, \qquad (k = 1, 2, \ldots)$$

Let k tend to infinity. Then two things can happen: either $g(0) \neq 0$; then thre exists a greatest integer k such that p^k divides $g(0)$, and this is also the

[8] Ann. of Mth. 89 (1969), 198–205)

[9] In this metric, the converging series $\sum a_n$ are those for which $a_n \longrightarrow 0$, i.e. for which the a_n are divisible by a power of p which tends to infinity.

[10] We have seen in the first part that $-\frac{1}{2k}B_{2k}$ can be viewed as $\zeta(1-2k)$. What we have here can therefore be regarded as a 'p-adic interpolation of Riemann's zeta function at negative integers', also known as the 'p-adic L-functions of Kubota and Leopoldt'. We remark that the extension of this theory from Riemann's ζ-function to Dedekinds ζ-function and even to abelian L-series of totally real number fields has been developed (in the direction explained by Serre in a lecture at Anvers 1972) by Deligne and Ribet, and, using completely different methods, by Barsky and Pierette Cassou-Noguès. See Ribet's report at the Journées Arithmétiques de Luminy (1978), Astérisque 61.

greatest integer k such that p^k divides $g_i((1+p)^{n_k}-1)$. Or $g(0)=0$, and $g_i((1+p)^{n_k}-1)$ is divisible by p^k for all $k \geq 1$. Let us apply this to the series $g_i(T)$ in Iwasawa's theorem: then we see that the index $\rho_p(i)$ introduced in Chapter 3 is nothing but the exponent of the exact power of p which divides $g(0)$. In particular, the finiteness of $\rho_p(i)$ is equivalent to $g(0) \neq 0$; this can be proved, but it is not obvious. Actually, one can view $g_i(0)$ as the value at $s=0$ of a Dirichlet L-function $L(s,\chi)$, and the functional equation of $L(s,\chi)$ then relates the non-vanishing of $g_i(0)$ to the non-vanishing of Dirichlet's L-function $L(s,\chi)$ at $s=1$.[11]

Thus, starting with the Bernoulli numbers we have constructed the series $g_i(T)$, and the Galois modules $A_0^{(i)}, A_1^{(i)}, \ldots$ have given rise to the series $f_i(T)$. Are these series related? Iwasawa made the guess that they are, and that one has in fact an equality $f_i(T) = g_i(T)$ if the characteristic series are suitably chosen. Moreover he showed that this assertion is a consequence of a reinterpretation of classical results, if one assumes some rather strong hypotheses like 'Vandiver's conjecture'. But the classical methods did not allow to solve the general problem: this was just done by Mazur and Wiles.

Main Theorem of Mazur and Wiles. For each $i = 3, 5, \ldots, p-2$, the suitably chosen characteristic series $f_i(T)$ of the Galois modules $A_0^{(i)}, A_1^{(i)}, \ldots$ coincide with the series $g_i(T)$ defined by (4.2).

The two theorems of Mazur and Wiles cited in Chapter 3 follow from this result, the first immediately, the second by combination with a deep theorem of Iwasawa on cyclotomic units. Instead of citing this theorem, we conclude by remarking that only by studying the whole tower of fields $F_n = \mathbb{Q}(e^{2\pi i/p^{n+1}})$ one can derive these corollaries, which concern only the ideal classes and units of the field $F_0 = \mathbb{Q}(e^{2\pi i/p})$, but which establish extremely precise relations between apparently pretty obscure arithmetical objects.

[11] The non-vanishing of the numbers $L(1,\chi)$ is an essential ingredient in the proof of the 'theorem about primes in arithmetic progressions': there exist infinitely many primes of the form $a+nb$ $(n = 1, 2, \ldots)$ if a and b are coprime.

The original appeared as

Du nouveau sur les racines de l'unite. (French)
Gaz. Math., Soc. Math. Fr. 15, 5-26 (1980).
ISSN: 0224-8999
Zbl 476.12007

Translation by Franz Lemmermeyer
Thanks to David Van Vactor for corrections.