RACSAM
Rev. R. Acad. Cien. Serie A. Mat.
VOL. **101** (1), 2007, pp. 1–32
Álgebra / Algebra
Artículo panorámico / Survey

Bernoulli numbers, Hurwitz numbers, p-adic L-functions and Kummer's criterion.

Álvaro Lozano-Robledo

Abstract. Let $K = \mathbb{Q}(\zeta_p)$ and let h_p be its class number. Kummer showed that p divides h_p if and only if p divides the numerator of some Bernoulli number. In this expository note we discuss the generalizations of this type of criterion to totally real fields and quadratic imaginary fields.

Números de Bernoulli, números de Hurwitz, funciones p-ádicas y criterios de Kummer.

Resumen. Sea $K = \mathbb{Q}(\zeta_p)$ y sea h_p su número de clases. Kummer demostró que p divide h_p si y solo si p divide el numerador de ciertos números de Bernoulli. En este artículo panorámico tratamos generalizaciones de este tipo de criterio para cuerpos totalmente reales y cuerpos cuadráticos imaginarios.

Contents

Presentado por José María Montesinos.
Recibido: 20 de julio de 2006. *Aceptado*: 13 de Diciembre de 2006.
Palabras clave / Keywords: Kummer's criterion, regular, irregular prime, class number divisibility
Mathematics Subject Classifications: 11R29, 11R18

1 Kummer's criterion

Let p be a prime and let ζ_p be a primitive pth root of unity. Let $F = \mathbb{Q}(\zeta_p)$ and let h_p be the class number of F. Kummer proved the following criterion:

Theorem 1 *The class number h_p is divisible by p if and only if p divides the numerator of some Bernoulli number B_j with $2 \leq j \leq p-3$ and j even.*

If p divides h_p then we say that p is irregular, otherwise we say that p is a regular prime. For example, $B_{12} = -\frac{691}{2730}$, thus by Kummer's criterion 691 divides the class number of $\mathbb{Q}(\zeta_{691})$ and $p = 691$ is an irregular prime.

The topic we want to address in this survey is the possible generalizations of Theorem 1 to other fields. The emphasis throughout this expository note is not on detailed proofs but on drawing similarities between the three known instances of the theory: Kummer's rational case, the totally real case and the quadratic imaginary case.

Section 1 provides a sketch of a modern proof of Kummer's criterion and, in Section 2, the theorem is rephrased and extended in several interesting ways (see Theorem 10). Then we move on to other fields. For example, Greenberg has shown that a similar type of theorem is true if $\mathbb{Q}$ is replaced by a totally real number field and the Bernoulli numbers are replaced by special values of Dedekind zeta functions (see Section 3 and Theorem 15 for a precise statement). In order to generalize Theorem 1 to quadratic imaginary fields, the correct point of view is to regard $\mathbb{Q}(\zeta_p)^+$, the maximal real subfield of $\mathbb{Q}(\zeta_p)$, as the maximal abelian extension of $\mathbb{Q}$ which has conductor $p\mathbb{Z}$. In other words, $\mathbb{Q}(\zeta_p)^+$ is the ray class field of $\mathbb{Q}$ of conductor $p\mathbb{Z}$. Let $K/\mathbb{Q}$ be a quadratic imaginary extension with ring of integers $\mathcal{O}_K$. For every p, we define $K(p)$ to be the ray class field of K of conductor (p), i.e. $K(p)$ is the maximal abelian extension of K of conductor $p\mathcal{O}_K$. It is possible to generalize Kummer's criterion to $K(p)$ in a remarkably similar way, this time in terms of divisibility of *Hurwitz numbers*, which we will describe in Section 4 (see Theorem 18, due to G. Robert). Section 5 of the survey is dedicated to several extensions of Robert's work, namely those of Saito, Coates-Wiles and Yager. In the last section we discuss the arithmetic applications of this type of criteria, such as Fermat's last theorem.

The theory of p-adic L-functions plays a vital role and, in fact, some of the earlier constructions of p-adic L-functions were motivated by Kummer's criterion and other related problems. The L-functions that appear in our treatment are those of Kubota, Leopoldt and Iwasawa for $\mathbb{Q}$ (Theorem 5); Serre's p-adic L-function for totally real fields (Theorem 16) and the L-function of Katz and Lichtenbaum for the quadratic imaginary case (Theorem 28).

1.1 Bernoulli numbers

The (classical) Bernoulli numbers are defined as the constants B_n which appear in a certain Taylor expansion:

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

The first few Bernoulli numbers are:

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30}, \; B_5 = 0, \quad B_6 = \frac{1}{42}, \quad \dots$$

and in fact it is not hard to show that $B_j = 0$ for all odd $j > 1$. The Bernoulli numbers may be calculated using the formula $\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$ or the following recurrence relation, due to Lehmer [23] and Carlitz [2]:

$$B_n = \frac{1}{1-n} \sum_{i=0}^{n} \binom{n}{i} (1 - 2^{1-i})(1 - 2^{i-n+1}) B_{n-i} B_i. \tag{1}$$

More generally, if χ is a Dirichlet character of conductor N, we define the generalized Bernoulli numbers $B_{n,\chi}$ to be the coefficients appearing in the formula:

$$\sum_{a=1}^{N} \frac{\chi(a) t e^{at}}{e^{Nt} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

Similarly one may define Bernoulli polynomials $B_{n,\chi}(x)$. The (classical) Bernoulli numbers satisfy some interesting congruences:

Theorem 2

- (**Congruence of von Staudt-Clausen**, [47, Thm. 5.10]) *Let n be even and positive. Then*

  $$B_n + \sum_{(p-1)|n} \frac{1}{p}$$

  is an integer, where the sum is over all p such that $p - 1$ divides n. Consequently, pB_n is p-integral for all n and all p.

- (**Kummer's congruence**, [47, Cor. 5.14]) *Suppose $m \equiv n \neq 0 \mod (p-1)$ are positive even integers. Then*

  $$\frac{B_m}{m} \equiv \frac{B_n}{n} \mod p.$$

The (generalized) Bernoulli numbers are rather important because they are essentially values of L-functions. Recall that if χ is a Dirichlet character of conductor N then

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad \text{for } \Re(s) > 1$$

is called a Dirichlet L-function. In particular, when χ_0 is the trivial Dirichlet character then $L(s, \chi_0)$ equals $\zeta(s)$, the usual Riemann zeta function. All Dirichlet L-functions have an analytic continuation to the whole complex plane, except for a simple pole at $s = 1$ when $\chi_0 = 1$ is the trivial character. Furthermore, $L(s, \chi)$ satisfies an Euler product and a functional equation (which we will not specify here; for details see [47, p. 30]). The surprising connection between L-functions and Bernoulli numbers is explained in the following two theorems:

Theorem 3 ([47, Thm. 4.2]) *Let k be an even integer and let B_k be the kth Bernoulli number. Let $\zeta(s)$ be the Riemann zeta function. Then:*

$$\zeta(k) = \frac{2^{k-1}|B_k|\pi^k}{k!}.$$

Thus, by the functional equation, $\zeta(1-n) = 0$ for odd $n \geq 3$ and for even $k \geq 2$ one has $\zeta(1-k) = -B_k/k$. More generally, for all $n \geq 1$ and for all Dirichlet characters χ, one has

$$L(1-n, \chi) = -\frac{B_{n,\chi}}{n}.$$

Remark 1 *The zeroes of the zeta function shown above, $\zeta(1-n) = 0$ for $n \geq 3$ odd, are usually called the trivial zeroes of the Riemann zeta function, while the non-trivial zeroes are those in the critical strip (the complex numbers with real part in the interval $(0,1)$). The Riemann hypothesis states that the real part of any non-trivial zero is $1/2$.*

The proof of Theorem 3 amounts to integrating

$$H(s) = \int \frac{z^{s-1}e^{(1-b)z}}{e^z - 1} dz$$

over an appropriate loop in $\mathbb{C}$. We recall the definition of $\tau(\chi)$. The Gauss sum of a Dirichlet character of conductor N is defined by

$$\tau(\chi) = \sum_{a=1}^{N} \chi(a)\, e^{2\pi i a/N}.$$

A Dirichlet character χ is said to be odd if $\chi(-1) = -1$. Otherwise, if $\chi(-1) = 1$, χ is said to be even. We will see in the next subsection that the values of Dirichlet L-functions at $s = 1$ are quite important. The following theorem provides the exact value.

Theorem 4 ([47, Thm. 4.9]) *Let χ be a non-trivial Dirichlet character of conductor N and let ζ_N be a primitive Nth root of unity. Then:*

$$L(1,\chi) = \begin{cases} \pi i \dfrac{\tau(\chi)}{N} B_{1,\overline{\chi}}, & \text{if } \chi(-1) = -1; \\ \\ -\dfrac{\tau(\chi)}{N} \sum_{a=1}^{N} \overline{\chi}(a) \log|1 - \zeta_N^a|, & \text{if } \chi(-1) = 1. \end{cases}$$

Thus, the Dirichlet L-functions may be regarded as complex analytic (meromorphic if $\chi = 1$) functions which take rational values at negative integers, and only the values of the very special (generalized) Bernoulli numbers. In other words, the Dirichlet L-functions *interpolate* the Bernoulli numbers. Let $\mathbb{Q}_p$ be the field of p-adic numbers and let $\overline{\mathbb{Q}_p}$ be a fixed algebraic closure of $\mathbb{Q}_p$. Define $\mathbb{C}_p$ to be the completion of $\overline{\mathbb{Q}_p}$ with respect to the p-adic absolute value ($\mathbb{Q}_p$ is complete, but $\overline{\mathbb{Q}_p}$ is not!). There is a notion of a p-adic analytic function which is the exact analog of a complex analytic function, i.e. a function is analytic in an open set if it can be expressed as a convergent power series. The question is: can we define p-adic analytic functions which interpolate Bernoulli numbers? The answer is that, in deed, we can and we do. The original construction [19] is due to Kubota and Leopoldt in 1964, although the version given below is due to Washington [48]. Analogous p-adic L-functions have been constructed by Coates, Fresnel, Iwasawa, Serre and Lang among others.

First we recall the definition of the Teichmüller character $\omega : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$. For $p > 2$ prime and every $a \in \mathbb{Z}_p^\times$ we define $\omega(a)$ to be the unique $(p-1)$st root of unity $\omega(a) \in \mathbb{Z}_p$ such that $a \equiv \omega(a) \mod p$. We extend the definition to $\mathbb{Z}_p$ by declaring $w(a) = 0$ whenever $p|a$. We may also consider ω as a Dirichlet character of conductor p with complex values by fixing an embedding of $\mathbb{Q}(\zeta_{p-1})$ into $\mathbb{C}$. Let χ be a Dirichlet character of conductor N. For $n \geq 1$, we define $\chi\omega^{-n}$ to be the primitive character associated to the character $\alpha : (\mathbb{Z}/\operatorname{lcm}(N,p)\mathbb{Z})^\times \to \mathbb{C}^\times$ defined by $\alpha(a) = \chi(a)\omega^{-n}(a)$.

Theorem 5 ([47, 5.11]) *Let $p > 2$ be prime and let χ be a Dirichlet character of conductor N. There exists a p-adic meromorphic (analytic if χ is non-trivial) function $L_p(s, \chi)$ on $\{s \in \mathbb{C}_p : |s| < p^{(1-\frac{1}{p-1})}\}$ such that*

$$L_p(1-n, \chi) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}$$

for $n \geq 1$. If χ_0 is trivial then $L_p(s, \chi_0)$ is analytic except for a pole at $s = 1$ with residue $(1 - 1/p)$. Furthermore, an explicit formula for $L_p(s, \chi)$ can be given.

The following congruence will be useful later on:

Proposition 1 ([47, Cor. 5.15]) *Let ω be the Teichmüller character of $\mathbb{Z}_p$.*

1. *Suppose n is odd and $n \neq -1 \mod (p-1)$. Then*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \mod p$$

   and both sides are p-integral.

2. $B_{1,\omega^{-1}} \equiv B_{1,\omega^{p-2}} \equiv \frac{p-1}{p} \mod \mathbb{Z}_p$.

The p-adic function whose existence is provided by Theorem 5 satisfies a congruence analogous to Kummer's congruence for Bernoulli numbers (cf. Theorem 2), which we will use in upcoming sections:

Proposition 2 ([47, Cor. 5.13]) *Let $p > 2$ be prime and let χ be a Dirichlet character of conductor N with N not divisible by p^2. For all $m, n \in \mathbb{Z}$:*

$$L_p(m, \chi) \equiv L_p(n, \chi) \mod p$$

and both numbers are p-integral.

1.2 The proof of Kummer's criterion

The final ingredient for the proof of Kummer's criterion is the fundamental relationship between Dirichlet L-functions and class numbers. The connection is made via the well-known analytic class number formulas.

Let K be a number field with ring of integers $\mathcal{O}_K$. The Dedekind zeta function of K is the analytic continuation of the following series:

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} (N_{\mathbb{Q}}^K(I))^{-s}$$

where I ranges over non-zero ideals of $\mathcal{O}_K$ and $N_{\mathbb{Q}}^K(I) = [\mathcal{O}_K : I]$ is the norm of I.

Theorem 6 (Class Number Formula, [22]) *Let K be a number field with $[K : \mathbb{Q}] = n = r_1 + 2r_2$, where r_1 denotes the number of real embeddings of K, and $2r_2$ is the number of complex embeddings of K. Also, let h_K be the class number, Reg_K the regulator of K, e_K the number of roots of unity contained in K and let D_K be the discriminant of $K/\mathbb{Q}$. Then $\zeta_K(s)$ converges absolutely for $\Re(s) > 1$ and extends to a meromorphic function defined for $\Re(s) > 1 - \frac{1}{n}$ with only one simple pole at $s = 1$. Furthermore:*

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot \mathrm{Reg}_K}{e_K \cdot \sqrt{\mid D_K \mid}}.$$

Hence, the residue at $s = 1$ encodes all the arithmetic information of the number field. Moreover, the Dedekind zeta function of an abelian number field factors as a product of Dirichlet L-functions as follows. Let K be an abelian number field, i.e. $K/\mathbb{Q}$ is Galois and $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. Then, by the Kronecker-Weber theorem, there is an integer n (which we choose to be minimal) such that $K \subseteq \mathbb{Q}(\zeta_n)$ where ζ_n is a primitive nth root of unity. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ and let $\chi : G \to \mathbb{C}^\times$ be a Dirichlet character. Then the kernel of χ determines a fixed field of $\mathbb{Q}(\zeta_n)$. Further, for any field K as before, there exists a group X of Dirichlet characters of G such that K is equal to the intersection of the fixed fields by the kernels of all $\chi \in X$. The order of X is $[K : \mathbb{Q}]$ and $X \cong \mathrm{Gal}(K/\mathbb{Q})$.

Theorem 7 ([47, Thm. 4.3]) *Let K be an abelian number field and let X be the associated group of Dirichlet characters. The Dedekind zeta function of K factors as follows:*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).$$

Notice that for the trivial character χ_0 one has $L(s, \chi_0) = \zeta(s)$, the Riemann zeta function, which has a simple pole at $s = 1$ with residue 1. Thus, for an arbitrary abelian number field K:

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi) = \zeta(s) \cdot \prod_{\chi_0 \neq \chi \in X} L(s, \chi)$$

where the last product is taken over all non-trivial characters $\chi \in X$. Therefore, combining this with Theorem 7 we obtain:

$$\frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot \mathrm{Reg}_K}{e_K \cdot \sqrt{\mid D_K \mid}} = \prod_{\chi_0 \neq \chi \in X} L(1, \chi). \tag{2}$$

1.2.1 Cyclotomic fields

From now on, let $p > 2$ be a prime and let $K = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_p$ is a primitive pth root of unity. The following argument generalizes to other cyclotomic fields but here we concentrate on $\mathbb{Q}(\zeta_p)$ for simplicity. The degree of the extension $K/\mathbb{Q}$ is $n = p - 1$ and K is a totally imaginary field. Thus $r_1 = 0$ and $r_2 = \frac{n}{2} = \frac{p-1}{2}$. In our case, Eq. (2) reads:

$$\frac{(2\pi)^{n/2} \cdot h_K \cdot \mathrm{Reg}_K}{e_K \cdot \sqrt{\mid D_K \mid}} = \prod_{\chi_0 \neq \chi \in X} L(1, \chi). \tag{3}$$

Let K^+ be the maximal real subfield of K, i.e. $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. If X is the group of Dirichlet characters for K, the group of characters of K^+ must be $X^+ = \{\chi \in X : \chi \text{ is even}\}$. Also, the degree of $K^+/\mathbb{Q}$ is $\frac{n}{2} = \frac{p-1}{2}$ and the extension is totally real. Thus, for K^+, Eq. (2) reads:

$$\frac{2^{n/2} \cdot h_{K^+} \cdot \mathrm{Reg}_{K^+}}{e_{K^+} \cdot \sqrt{\mid D_{K^+} \mid}} = \prod_{\chi_0 \neq \chi \in X^+} L(1, \chi). \tag{4}$$

We define the relative class number $h_p^- = h_K/h_{K^+}$. Dividing Eq. (3) by Eq. (4), we obtain a formula for h_p^- in terms of a product over the odd characters in X and some other invariants of K. By Theorem 4, we can interpret the value $L(1, \chi)$ for odd χ in terms of (generalized) Bernoulli numbers. Precisely one obtains:

$$h_p^- = e_K \prod_{\chi \text{ odd}} \left(-\frac{B_{1,\chi}}{2}\right)$$

where $e_K = 2p$. Moreover, it is not hard to see that the odd characters corresponding to $\mathbb{Q}(\zeta)$ are precisely the odd powers of the Teichmüller character, namely ω, ω^3, ω^5, ..., ω^{p-2}. Finally, using the congruences in Proposition 1 we obtain:

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \left(-\frac{B_{j+1}}{2(j+1)} \right) \mod p.$$

Therefore, we have shown:

Theorem 8 ([47, Thm. 5.16]) *The relative class number h_p^- is divisible by p if and only if p divides the numerator of one of the Bernoulli numbers B_j with $2 \leq j \leq p-3$ and j even.*

Finally, we are ready to prove:

Theorem 9 (Kummer's criterion) *Let $K = \mathbb{Q}(\zeta)$ and $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. If p divides h_{K^+} then p also divides $h_p^- = h_K/h_{K^+}$. Therefore, p divides h_K if and only if p divides the numerator of one of the Bernoulli numbers B_j for some $j = 2, 4, \ldots, p-3$.*

PROOF. By Theorem 8 it suffices to show that $p|h_{K^+}$ implies that $p|h_p^-$. The Dirichlet characters associated to K^+ are $1, \omega^2, \omega^4, \ldots, \omega^{p-3}$. Moreover, there is a p-adic analogue of Eq. (4) which reads:

$$\frac{2^{n/2-1} \cdot h_{K^+} \cdot \mathrm{Reg}_{p,K^+}}{\sqrt{|\ D_{K^+}\ |}} = \prod_{\substack{j=2 \\ j \text{ even}}}^{p-3} L_p(1, \omega^j), \tag{5}$$

where Reg_{p,K^+} is the p-adic regulator and we have substituted $e_{K^+} = 2$ into the equation. One can show (see [47, Prop. 5.33]) that

$$|\ \mathrm{Reg}_{p,K^+}\ / \sqrt{|\ D_{K^+}\ |}| \leq 1.$$

Thus, if $p|h_{K^+}$ then p divides one of the values $L_p(1, \omega^j)$ for some even $j = 2, 4, \ldots, p-3$. Now, by Proposition 2, $L_p(1, \omega^j) \equiv L_p(0, \omega^j) \mod p$ and by Theorem 5:

$$L_p(0, \omega^j) \equiv -(1 - \omega^{j-1}(p)) B_{1,\omega^{j-1}} \equiv -B_{1,\omega^{j-1}} \mod p$$

and so there is an odd $i = 1, 3, \ldots, p-4$ such that $B_{1,\omega^i} \equiv 0 \mod p$. As we have seen above

$$h^- \equiv \prod_{\substack{i=1 \\ i \text{ odd}}}^{p-4} \left(-\frac{1}{2} B_{1,\omega^i} \right) \mod p$$

and since all the B_{1,ω^i} are p-integral, h_p^- must be divisible by p, as claimed. ■

Remark 2 *It has been conjectured by Vandiver that, in fact, h_{K^+} is never divisible by p. This has been verified for all $p < 4{,}000{,}000$.*

2 Rephrasing Kummer

In this section we will rephrase Kummer's criterion (Theorem 1) in different ways, which will make more apparent the similarities with the quadratic imaginary case. In particular, we change the point of view: we regard the Bernoulli numbers as special values of L-functions.

Let $K = \mathbb{Q}(\zeta_p)$ and let $K_2 = \mathbb{Q}(\zeta_{p^2})$, where ζ_n is a primitive nth root of unity. As before, let K^+ and K_2^+ be the maximal real subfields of K and K_2, respectively. Also, we define (cf. Theorem 3):

$$\zeta^*(k) = (k-1)!(2\pi)^{-k}\zeta(k) = (-1)^{(1+k/2)} \frac{B_k}{2k}.$$

Theorem 10 (Kummer's Criterion, [4, p. 9]) *The following are equivalent:*

1. *At least one of the numbers $\zeta^*(k)$ is divisible by p, for some even $k = 2, 4, \ldots, p-3$.*
2. *The class number of K, h_p, is divisible by p.*
3. *There exists an unramified $\mathbb{Z}/p\mathbb{Z}$-extension of K.*
4. *There exists a $\mathbb{Z}/p\mathbb{Z}$-extension of K^+ which is unramified outside the prime above p and which is distinct from K_2^+.*

Parts 3 and 4 follow from part 2 and class field theory. In particular, they are consequences of the following statement: let K be a number field, h_K is its class number and let p be a prime. Then K has an everywhere unramified Galois extension of degree p if and only if h_K is divisible by p.

One can provide a much more explicit version of Kummer's criterion in terms of cyclotomic units.

2.1 Cyclotomic units

Let $K_n = \mathbb{Q}(\zeta_{p^n})$ where ζ_{p^n} is a primitive p^nth root of unity, let h_n be the class number of K_n and let $\mathcal{O}_n = \mathcal{O}_{K_n}$ be the ring of integers in K_n. Let $E_n = \mathcal{O}_n^\times$ be the group of units in K_n. The cyclotomic units are a subgroup C_n of E_n which satisfy:

- The elements of C_n are defined analytically.
- The subgroup C_n is of finite index in E_n. Furthermore, the index is h_n^+. Let E_n^+ be the group of units in K_n^+ and let $C_n^+ = C_n \cap E_n^+$. Then $[E_n^+ : C_n^+] = h_n^+$. Moreover, it can be shown that $[E_n : C_n] = [E_n^+ : C_n^+]$ because $E_n = \mu_{p^n} E_n^+$.
- The subgroups C_n behave "well" in towers. More precisely, the norm of C_{n+1} down to K_n is C_n. This follows from the fact that the norm of $\zeta_{p^{n+1}}$ down to K_n is ζ_{p^n}.

Definition 1 *Let p be prime and let $n \geq 1$.*

1. *The cyclotomic unit group $C_n^+ \subset K_n^+ = \mathbb{Q}(\zeta_{p^n})^+$ is the group of units generated by -1 and the units*

$$\xi_a = \zeta_{p^n}^{(1-a)/2} \frac{1-\zeta_{p^n}^a}{1-\zeta_{p^n}} = \pm \frac{\sin(\pi a/p^n)}{\sin(\pi/p^n)}$$

   with $1 < a < \frac{p^n}{2}$ and $\gcd(a,p) = 1$.

2. *The cyclotomic unit group $C_n \subset K_n = \mathbb{Q}(\zeta_{p^n})$ is the group generated by ζ_{p^n} and the cyclotomic units C_n^+ of K_n^+.*

Remark 3 *Let σ_a be the element of $\mathrm{Gal}(K_n/\mathbb{Q})$ defined by $\zeta_{p^n} \mapsto \zeta_{p^n}^a$. Then:*

$$\xi_a = \zeta_{p^n}^{(1-a)/2} \frac{1-\zeta_{p^n}^a}{1-\zeta_{p^n}} = \frac{(\zeta_{p^n}^{-1/2}(1-\zeta_{p^n}))^{\sigma_a}}{\zeta_{p^n}^{-1/2}(1-\zeta_{p^n})}.$$

Remark 4 *Let g be a primitive root modulo p^n, i.e. g is a generator of the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Let $a \equiv g^r \mod p^n$. Then one can rewrite ξ_a as:*

$$\xi_a = \prod_{i=0}^{r-1} \xi_g^{\sigma_g^i}.$$

In particular, ξ_g generates $C_n^+/\{\pm 1\}$ as a module over $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})^+/\mathbb{Q})]$.

Notice that in order to show that the index of C_n in K_n is finite it suffices to show that the index of C_n^+ in K_n^+ is finite. Indeed, let $[K_n : \mathbb{Q}] = 2d$. The field K_n is totally imaginary, thus by Dirichlet's unit theorem the free rank of E_n is $r_1 + r_2 - 1 = d - 1$. On the other hand, $[K_n^+ : \mathbb{Q}] = d$ and K_n^+ is totally real, thus the free rank of E_n^+ is also $d - 1$. Therefore the free ranks of E_n^+ and E_n are equal.

Theorem 11 ([47, Thm. 8.2]) *Let p be a prime and $n \geq 1$. Let h_n^+ be the class number of $\mathbb{Q}(\zeta_{p^n})^+$. The cyclotomic units C_n^+ of $\mathbb{Q}(\zeta_{p^n})^+$ form a subgroup of finite index in the full unit group E_n^+. Furthermore:*

$$h_n^+ = [E_n^+ : C_n^+] = [E_n : C_n].$$

In order to prove the previous theorem it suffices to compute the regulator of the units ξ_a in terms of values of Dirichlet L-functions associated to even characters. In particular, one calculates:

$$R(\{\xi_a\}) = \pm \prod_{\chi \neq \chi_0} \frac{1}{2}\tau(\chi)L(1, \overline{\chi}) = h_n^+ \cdot R^+$$

where the last equality follows from the properties of Gauss sums and the class number formula in terms of Dirichlet L-functions evaluated at $s = 1$. This gives that $R(\{\xi_a\})$ in non-zero, therefore the index of C_n^+ in E_n^+ is finite and

$$h_n^+ = \frac{R(\{\xi_a\})}{R^+} = [E_n^+ : C_n^+] = [E_n : C_n].$$

An immediate consequence of this is that if p divides h_n^+ then there exists a cyclotomic unit $\gamma \in C_n^+$ such that γ is a pth power in E_n^+ but not in C_n^+. The interesting consequence of the theory is that we can pin down γ exactly.

2.2 Decompositions of the full unit group

Here we concentrate on $K = \mathbb{Q}(\zeta_p)$, its full unit group $E = E_1$ and the subgroup of cyclotomic units $C = C_1$. We start by decomposing E (modulo pth powers) into $\mathbb{Z}_p[G]$ components, where $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, using orthogonal idempotents. As we pointed out before, the characters of G are ω^i for $0 \leq i \leq p - 2$ where ω is the Teichmüller character. The corresponding orthogonal idempotents for the group ring $\mathbb{Z}_p[G]$ are given by:

$$\epsilon_i = \frac{1}{|G|} \sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1} \in \mathbb{Z}_p[G].$$

As usual, the idempotents satisfy:

$$\sum_{i=0}^{p-2} \epsilon_i = 1_G \quad \text{and } \epsilon_i\epsilon_j = \begin{cases} \epsilon_i & \text{if } i = j; \\ 0 & \text{if } i \neq j. \end{cases}$$

Let N be a large enough integer such that $p^N > h_p^+ = [E^+ : C^+]$. Let $\mathcal{E}_p = E/E^{p^N}$ be the quotient of E by the p^Nth powers of E (for technical reasons we work with E/E^{p^N} instead of E/E^p). We similarly define $\mathcal{E}_p^+ = E^+/(E^+)^{p^N}$. The Galois group G clearly acts on $\mathcal{E}_p$. The group ring $\mathbb{Z}_p[G]$ acts on $\mathcal{E}_p$ as follows. If $z \in \mathbb{Z}_p$ and $z_0 \equiv z \mod p^N$ with $z_0 \in \mathbb{Z}$, and $g \in G$, $\gamma \in \mathcal{E}_p$ then $zg \cdot \gamma = g(\gamma)^{z_0}$. Thus, we may use the idempotents ϵ_i to decompose $\mathcal{E}_p$ as $\mathbb{Z}_p[G]$-module and obtain

$$\mathcal{E}_p = \bigoplus_{i=0}^{p-2} \epsilon_i\mathcal{E}_p \quad \text{and} \quad \mathcal{E}_p^+ = \bigoplus_{i=0}^{p-2} \epsilon_i\mathcal{E}_p^+.$$

This may be further simplified by noting that

$$\epsilon_0 \mathcal{E}_p = \frac{1}{p-1} \sum_{a=1}^{p-1} \sigma_a(\mathcal{E}_p) \subseteq \mathrm{Norm}(\mathcal{E}_p) \subseteq 1 \mod E^{p^N} = 1.$$

Moreover, it can be deduced from $E = \mu_p \cdot E^+$ that $\epsilon_1 \mathcal{E}_p = \langle \zeta_p \rangle$ and $\epsilon_i \mathcal{E}_p = 1 \mod E^{p^N}$ for odd i. Hence (see [47, Prop. 8.10]):

$$\mathcal{E}_p = \langle \zeta_p \rangle \oplus \bigoplus_{\substack{i=2 \\ i \text{ even}}}^{p-3} \epsilon_i \mathcal{E}_p \quad \text{and} \quad \mathcal{E}_p^+ = \bigoplus_{\substack{i=2 \\ i \text{ even}}}^{p-3} \epsilon_i \mathcal{E}_p^+.$$

Theorem 12 ([47, p. 155, 156]) *Let $(E^+/C^+)_p$ be the p-Sylow subgroup of E^+/C^+ and let $\mathcal{C}_p^+ = C^+/(C^+)^{p^N}$. Then:*

$$(E^+/C^+)_p \cong \mathcal{E}_p^+/\mathcal{C}_p^+ \cong \bigoplus_{\substack{i=2 \\ i \text{ even}}}^{p-3} \epsilon_i \mathcal{E}_p / \langle \gamma_{i,N} \rangle$$

where

$$\gamma_{i,N} = \prod_{a=1}^{p-1} \xi_g^{\omega_N(a)^i \sigma_a^{-1}}$$

and $\omega_N(a)$ is an integer congruent to $\omega(a)$ modulo p^N.

Let $\gamma_i = \gamma_{i,1} = \prod_{a=1}^{p-1} \xi_g^{a^i \sigma_a^{-1}}$. Since $\omega_N(a) \equiv \omega(a) \equiv a \mod p$, it follows that $\gamma_{i,N}$ is a pth power if and only if γ_i is a pth power. Moreover, let v_p be the usual p-adic valuation, one can prove that:

$$v_p(\log_p(\gamma_{i,N})) = \frac{i}{p-1} + v_p(L_p(1, \omega_i))$$

and by Prop. 1 one has $L_p(1, \omega^i) \equiv L_p(1-i, \omega^i) \equiv -\frac{B_i}{i} \mod p$. Thus:

Theorem 13 ([47, Thm. 8.14, 8.16])

- *The class number of $\mathbb{Q}(\zeta_p)^+$, h_p^+, is divisible by p if and only if there is an even $i = 2, 4, \ldots, p-3$ such that γ_i is a pth power of a unit in E^+.*
- *If γ_i is a pth power then p divides the Bernoulli number B_i.*

Since p divides B_i for some even $i = 2, 4, \ldots, p-3$ if and only if p divides h^-, the previous result proves again that if p divides h_p^+ then p divides h^-. However, as we mentioned before, it is a conjecture of Vandiver that p does not ever divide h_p^+.

2.3 Herbrand's theorem and a converse by Ribet

In this subsection, we use the orthogonal idempotents to decompose the ideal class group modulo pth powers. Let $A = \mathrm{Cl}(\mathbb{Q}(\zeta_p))$ be the ideal class group and let $C = A/A^p$, regarded as a $\mathbb{F}_p$-vector space. It follows from the comments in the previous section that the $\mathbb{F}_p$-valued characters of $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ are the powers of $\overline{\omega}$, the reduction modulo p of the Teichmüller character. Let $\overline{\epsilon}_i$ be the mod p reduction of the $\mathbb{Z}_p[G]$ idempotents ϵ_i. Clearly, C is a $\mathbb{F}_p[G]$-module. We define the corresponding $\mathbb{F}_p[G]$-submodules by $C(\omega^i) = \overline{\epsilon}_i C$. Thus:

$$C = \bigoplus_{i \mod p-1} C(\omega^i).$$

The following famous 'if and only if' statement is a combination of the work of Herbrand [12] and Ribet [33].

Theorem 14 *Let k be even with $2 \leq k \leq p-3$ and let B_k be the corresponding Bernoulli number.*

1. (Herbrand, 1932) *If $C(\omega^{1-k}) \neq 0$ then p divides B_k.*
2. (Ribet, 1976) *If p divides B_k then $C(\omega^{1-k}) \neq 0$.*

The simplest way to prove Herbrand's theorem is using Stickelberger's theorem. The original proof of Ribet's theorem involves techniques from Galois representation theory which are used to construct unramified extensions of $\mathbb{Q}(\zeta_p)$. Since then, other proofs have been found which use elementary tools (see [47]).

3 Totally real extensions of $\mathbb{Q}$

In 1973, Greenberg [10] proved one of the first generalizations of Kummer's criterion to a large family of number fields: totally real fields. Let K be a finite totally real extension of $\mathbb{Q}$ and let $\zeta_K(s)$ be its Dedekind zeta function. It has been known since Siegel [41] and Klingen [18] that the values $\zeta_K(1-i)$ are rational numbers for $i \geq 1$. Theorem 3 treats the particular case $K = \mathbb{Q}$ and states that $\zeta_{\mathbb{Q}}(1-k) = \zeta(1-k) = -\frac{B_k}{k}$ for even $k \geq 2$.

Theorem 15 (Greenberg, [10, Thm. 1]) *Assume that $p \nmid [K : \mathbb{Q}]$ and that no prime of $K(\zeta_p + \zeta_p^{-1})$ lying over p splits in $K(\zeta_p)$. Then p divides the class number of $K(\zeta_p)$ if and only if p divides the numerator of*

$$p \cdot \prod_{\substack{i=2 \\ i \text{ even}}}^{d} \zeta_K(1-i)$$

where $d = [K(\zeta_p) : K]$.

The reader may also be interested in a related work of Kida ([17]). The proof of Theorem 15 is strikingly similar to the proof of Kummer's criterion outlined in Section 1.2 above in that the proof combines the class number formula with p-adic L-functions in order to prove the divisibility properties of the relative class number $h^- = h_{K(\zeta_p)}/h_{K(\zeta_p)^+}$. In particular, Greenberg made use of p-adic L-functions for totally real fields that had been recently described by Serre in [39]. Here, we limit ourselves to an outline of their work. We have also composed a table of examples which can be found in Table 2 of Section 6.2.

Let $K_p = K(\zeta_p)$ and let $K_p^+ = K(\zeta_p + \zeta_p^{-1})$. If F is a number field, we define:

$$\zeta_F^*(s) = \zeta_F(s) \prod_{\wp | p} (1 - (N\wp)^{-s}).$$

Notice that $\zeta_F^*(s)$ is simply the Dedekind zeta function of F with the Euler factors corresponding to primes above p removed. Also, one can define "prime to p" Dirichlet L-functions for K as follows. Let χ be any Dirichlet character of conductor p. We define:

$$L_K^*(s, \chi) = \sum_{(\mathfrak{A}, p) = 1} \frac{\chi(N\mathfrak{A})}{(N\mathfrak{A})^s}$$

where the sum is over all integral ideals of K relatively prime to p. Notice that if χ_0 is trivial then $L_K^*(s, \chi_0) = \zeta_K^*(s)$. In particular, if ω is a generator of all Dirichlet characters of conductor p then it is easy to verify:

$$\zeta_{K_p}^*(s) = \prod_{i=1}^{d} L_K^*(s, \omega^i), \quad \zeta_{K_p^+}^*(s) = \prod_{\substack{i=1 \\ i \text{ even}}}^{d} L_K^*(s, \omega^i). \tag{6}$$

A combination of the previous definitions, the class number formula for $K(\zeta_p)$ and $K(\zeta_p)^+$ and the functional equation for Dedekind zeta functions yields:

$$ah^- = \frac{e}{2^{u+1}} \prod_{\substack{i=1 \\ i \text{ odd}}}^{d} L_K^*(0, \omega^i) \tag{7}$$

where a is a power of 2 unless there exist primes of K_p^+ lying over p which split in K_p, e is the number of roots of unity in K_p and u is defined by the quotient of regulators $R/R^+ = 2^u$.

3.1 Serre's p-adic L-function for totally real fields

There are several constructions of p-adic L-functions for totally real extensions of $\mathbb{Q}$, including those of Barsky, Cassou-Noguès, Deligne-Ribet and Katz. Greenberg's proof relies on Serre's construction, which is an extension of the work of Kubota, Leopoldt and Iwasawa for the abelian case.

Theorem 16 (Serre, [39]; cf. Thm. 5) *Let $\overline{\mathbb{Q}_p}$ be a fixed algebraic closure of $\mathbb{Q}_p$ and fix an embedding of $\mathbb{Q}_p$ into $\overline{\mathbb{Q}_p}$. Let K be a finite totally real extension of $\mathbb{Q}$, let $d = [K(\zeta_p) : K]$ and let ω be a generator of the Dirichlet characters modulo p. Then there exists a continuous $\overline{\mathbb{Q}}$-valued function $L_p(s, \omega^i)$ defined for all $s \in \mathbb{Z}_p$ such that, for all $n \geq 1$:*

$$L_p(1-n, \omega^i) = L_K^*(1-n, \omega^{i-n}).$$

In particular, for all $n \equiv i \mod d$:

$$L_p(1-n, \omega^i) = \zeta_K^*(1-n).$$

Furthermore, for every i there exists a function $f_i(T)$ in the quotient field of $\mathbb{Z}_p[[T]]$ such that $L_p(s, \omega^i) = f_i((1+p)^{1-s} - 1)$ and $((1+T)^d - 1)f_i(T)$ belongs to $\mathbb{Z}_p[[T]]$.

Returning to the proof of Theorem 15, let $L_p(s, \omega^i)$ be Serre's p-adic L-function for K. Since $K(\zeta_p)^+$ is also totally real, there exists an associated p-adic L-function $L_p^+(s)$ for $K(\zeta_p)^+$ such that $L_p^+(1-n) = \zeta_{K_p^+}^*(1-n)$ for all even $n \geq 2$. In particular, by continuity and by Eq. (6):

$$L_p^+(s) = \prod_{\substack{i=2 \\ i \text{ even}}}^{d} L_p(s, \omega^i).$$

By Eq. (7) and the properties of these p-adic L-functions we obtain:

$$\frac{2^{u+1}ah^-}{e} = \prod_{\substack{i=1 \\ i \text{ odd}}}^{d} L_K^*(0, \omega^i) = \prod_{\substack{i=2 \\ i \text{ even}}}^{d} L_p(0, \omega^i) = L_p^+(0).$$

In our case $p|e$ but $p^2 \nmid e$, thus p divides h^- if and only if p divides $pL_p^+(0)$. Using the fact that $L_p(s, \omega^i) = f_i((1+p)^s - 1)$ for some $f_i(T)$ in the quotient field of $\mathbb{Z}_p[[T]]$, $((1+T)^d - 1)f_i(T) \in \mathbb{Z}_p[[T]]$ and $\gcd(p, d) = 1$, it follows that $Tf_i(T) \in \mathbb{Z}_p[[T]]$. Thus one can show that p divides $pL_p^+(0)$ if and only if p divides the product

$$\prod_{\substack{i=2 \\ i \text{ even}}}^{d} L_p(1-i, \omega^i) = \prod_{\substack{i=2 \\ i \text{ even}}}^{d} \zeta_K^*(1-i)$$

where the last equality is yet another use of the properties of the p-adic L-function. The powers of p dividing $\zeta_K^*(1-i)$ and $\zeta_K(1-i)$ are the same, which proves that p divides ah^- if and only if p divides $p\prod_{\substack{i=2 \\ i \text{ even}}}^{d} \zeta_K(1-i)$.

The final step is to show that if p divides $h^+ = h_{K_p^+}$ then p divides the relative class number h^-, i.e. an analogue of Theorem 9 in the totally real case. Greenberg tackles this part in a short proof by using class field theory and Kummer theory.

4 The quadratic imaginary case

At this point we turn to the quadratic imaginary case. Let K be a quadratic imaginary number field with ring of integers $\mathcal{O}_K$, let h_K be the class number of K and let $p > 2$ be a prime. Let $K(p)$ be the ray class field of K of conductor p and let h_p be the class number of $K(p)$. The goal is to describe a criterion to decide whether h_p is divisible by p or not.

4.1 Hurwitz numbers

Since the time of Kronecker and Weber, it has been well known that the abelian extensions of a quadratic imaginary field K are intimately connected to the arithmetic of elliptic curves with complex multiplication by K. Let A be an elliptic curve defined over K and with complex multiplication by $\mathcal{O}_K$ (in other words, the endormorphism ring of A is isomorphic to $\mathcal{O}_K$), and let $j(A)$ be the j-invariant of A. The theory of complex multiplication, for example, shows that $K(j(A))$ is the Hilbert class field of K. Furthermore, let e be the number of roots of unity in K, let $\mathfrak{A}$ be an integral ideal in $\mathcal{O}_K$ and let $x^{e/2}(A[\mathfrak{A}])$ be the set of x-coordinates of all $\mathfrak{A}$-torsion points on A, raised to the $\frac{e}{2}$th power. Then $K(j(A), x^{e/2}(A[\mathfrak{A}]))$ is the ray class field of K of conductor $\mathfrak{A}$ (see [43, Chapter II], for an account of the CM theory of elliptic curves).

Let $L \subset \mathbb{C}$ be the lattice associated to the elliptic curve A (that is, $A(\mathbb{C}) \cong \mathbb{C}/L$) and let G_k be the Eisenstein series of weight $k > 2$. The *Hurwitz numbers* attached to the elliptic curve A are the numbers:

$$G_k(L) = \sum_{\lambda \in L}{}' \frac{1}{\lambda^k}$$

where the sum is over all the non-zero elements of L, and $k > 2$ is divisible by e, the number of roots of unity in the field of complex multiplication K (in particular k must be even). For $k = 2$, $G_2(L)$ is defined in a slightly different manner, namely $G_2(L) = \lim_{s \to 0^+} \sum_{\lambda \in L \setminus \{0\}} 1/\lambda^2 |\lambda|^{2s}$. Table 1 exhibits the values of $G_2(L)$ for quadratic imaginary fields K of class number $h_K = 1$ and discriminant D_K.

Table 1. Values of $G_2(L)$

D_K	-3	-4	-7	-8	-11	-19	-43	-67	-163
$G_2(L)$	0	0	$1/2$	$1/2$	2	2	12	$2 \cdot 19$	$4 \cdot 181$

It is worth remarking that the Hurwitz numbers are essentially the coefficients of the Laurent expansion of the Weierstrass $\wp$-function (see [42, VI.3.5.a]; compare with the definition of the Bernoulli numbers):

$$\begin{aligned} \wp(z; L) &= \frac{1}{z^2} + \sum_{w \in L \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) \\ &= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(L) z^{2k}. \end{aligned} \tag{8}$$

A related fact is that, if we define $g_2 = 60G_4(L)$ and $g_3 = 140G_6(L)$, then the elliptic curve A may be retrieved from the Hurwitz numbers, for A is given by the Weierstrass equation $y^2 = 4x^3 - g_2 x - g_3$. The

Hurwitz numbers are also the Fourier coefficients of the Weierstrass ζ function:

$$\zeta(z,L) = \frac{1}{z} + \sum_{w \in L \setminus \{0\}} \left(\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right) = \frac{1}{z} - \sum_{k=1}^{\infty} G_{2k+2}(L) z^{2k+1}.$$

This follows from the fact that $\frac{d}{dz}\zeta(z,L) = -\wp(z,L)$. Recall that the Bernoulli numbers appear as coefficients in the expansion of $t/(e^t-1)$. The similitude between $\zeta(z,L)$ and an alternate expansion of $1/(e^t-1)$ is striking:

$$\begin{aligned} \frac{1}{e^{2\pi i t}-1} &= \sum_{n=0}^{\infty} \frac{B_n (2\pi i)^{n-1} t^{n-1}}{n!} \\ &= \frac{1}{2\pi i t} - \frac{1}{2} - \frac{1}{\pi i} \sum_{n=1}^{\infty} \zeta(n+1) t^n \\ &= -\frac{1}{2} + \frac{1}{\pi i} \left(\frac{1}{2t} - \sum_{k=1}^{\infty} \left(\frac{1}{k-t} - \frac{1}{k} \right) \right). \end{aligned}$$

Remark 5 *In some pieces of literature (e.g.* [14]*) the term Hurwitz number refers only to*

$$E_n = 2^{-4n}(4n)! G_{4n}(L)$$

where the associated elliptic curve is the lemniscate curve $y^2 = 4x^3 - 4x$ and $K = \mathbb{Q}(i)$, which is the example that Hurwitz actually used in his work [13]*. Katz defines the Bernoulli-Hurwitz numbers to be* $\mathrm{BH}_k(L) = k! G_k(L)$.

The Hurwitz numbers $G_k(L)$ with $k \geq 8$ can be calculated from G_4 and G_6 using the following relation (cf. Eq (1) in Section 1.1).

Proposition 3 ([36, Formula (D.10)]) *The Hurwitz numbers $G_k = G_k(L)$, with $k > 2$, satisfy the recurrence relation:*

$$G_k = \frac{6}{(k-6)(k+1)(k-1)} \sum_{\substack{j=4 \\ j \text{ even}}}^{k-4} (j-1)(k-j-1) G_j G_{k-j}.$$

PROOF. The recurrence follows from the Laurent expansion in Eq. (8) and identifying the coefficients of z^{k-4} in the differential equation:

$$2\frac{d^2}{dz^2}\wp(z,L) = 12\wp(z,L)^2 - 60G_4(L). \quad \blacksquare$$

The Hurwitz numbers are closely related to the Bernoulli numbers because the q-expansion of the Eisenstein series is:

$$\frac{(k-1)!}{2} G_k(q) = -\frac{B_k}{2k} + \sum_{n \geq 1} q^n \sum_{d|n} d^{k-1}$$

for even $k \geq 4$. Furthermore, the Hurwitz numbers also satisfy interesting congruences, analogous to those of Kummer and Clausen-von Staudt for the Bernoulli numbers.

Theorem 17 ([14], cf. Thm. 2) *Let A be an elliptic curve with lattice $L \subseteq \mathbb{C}$ and let $p > 2$ be a prime of good reduction for A. Let $\mathcal{O}_p = \mathcal{O}_K \otimes \mathbb{Z}_p$ and let $\alpha_p \in \mathcal{O}_p/p\mathcal{O}_p$ be the Hasse invariant of A modulo p. For even $k \geq 2$ we define* $\mathrm{BH}_k(L) = k! G_k(L)$*. Then:*

1. *If $p-1$ divides k, then $p\,\mathrm{BH}_k \equiv \alpha_p^{k/p-1} \mod p\mathcal{O}_p$;*
2. *If $p-1$ does not divide k, then $\mathrm{BH}_k/k \in \mathcal{O}_p$, and*

$$\frac{\mathrm{BH}_{k+p-1}}{k+p-1} \equiv \alpha_p \cdot \frac{\mathrm{BH}_k}{k} \mod p\mathcal{O}_p.$$

For a proof see [14]. The Hasse invariant of A/K is computed as follows. Let k be the residue field of $\mathcal{O}_p$ and let A/k be given by the Weierstrass equation $y^2 = f(x)$. Then α_p is the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$.

Lemma 1 ([36, Cor. 14, Prop. 16]) *Let $p \geq 5$ be unramified in K, let $\wp$ be a prime of K lying above p and let $0 < k < N(\wp) - 1$ be divisible by e, the number of roots of unity in K. If $k \neq p+1$ then $G_k(L)$ is p-integral. If $k = p+1$ then $pG_k(L)$ is p-integral and, in fact, it is a p-unit ($pG_k(L) \neq 0 \mod p$).*

4.2 Robert's criterion

In 1978, Robert published his article [36] which establishes the first general Kummer-type criterion for $K(p)$, greatly improving results of Novikov (who had proved in [28] similar results for $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\sqrt{-3})$) and his own previous results [35].

Let K be a quadratic imaginary field and let A and $L \subset \mathbb{C}$ be as before. Let $\wp$ be a prime of K lying above p, so that $p\mathcal{O}_K = \wp$ if p is inert in K and $p\mathcal{O}_K = \wp\overline{\wp}$ if p splits in K. Let H_0 be the Hilbert class field of K and let $H = K(\wp)$ be the ray class field of K of conductor $\wp$. Let h_H and h_{H_0} be the class numbers of H and H_0 respectively. It is easy to see that h_{H_0} divides h_H. Robert's criterion establishes sufficient conditions for the quotient h_H/h_{H_0} to be relatively prime to p (although he also provides some partial necessary conditions in his work; see Theorem 25 in this survey). His work is valid for the most general case (i.e. h_{H_0} is arbitrary). Here we state his results (as announced in [35]) for the case $h_K = h_{H_0} = 1$ for simplicity:

Theorem 18 (Robert, [36]) *Let $p \geq 5$ be an unramified prime of K and suppose that every k divisible by e with $0 < k < N(\wp) - 1$ satisfies:*

1. *If $k = p+1$, $pG_k(L) \neq 0 \mod p$;*
2. *If $(p+1)|k$ but $k \neq p+1$, $G_k(L) \neq 0 \mod p$;*
3. *If $(p+1) \nmid k$ and p splits in K then $G_k(L) \neq 0 \mod p$;*
4. *If $(p+1) \nmid k$ and p is inert in K then either $G_k(L) \neq 0 \mod p$ or $G_{p(k)}(L) \neq 0 \mod p$, where $0 < p(k) < p^2 - 1$ is an even integer congruent to $pk \mod p^2 - 1$.*

Then h_H is not divisible by p.

In the general case (h_K is arbitrary) the criterion is given in terms the $\mathcal{O}_K/\wp$-linear independence of the numbers $G_k(\mathfrak{A}_i^{-1}L)$ where the integral ideals of K in the list $\{\mathfrak{A}_i : i = 1, \ldots, h_K\}$ are relatively prime to $6\wp$ and form a complete system of representatives for $\mathrm{Cl}(K)$.

Remark 6 *A word of caution: the converse of Robert's criterion is in fact not true, in stark contrast with Kummer's criterion. Indeed, let $K = \mathbb{Q}(\sqrt{-19})$ and $p = 17$. Then $G_{12}(L) \equiv 0 \mod 17$. However, one can use bounds of class numbers (an application of Odlyzko's work* [29] *on bounds of discriminants) to show that h_H is not divisible by* 17*. In fact, if p splits in K, Robert (*[36, §6, Prop. 57, see also Appendix B, p. 363]*) shows that those numbers k divisible by e and $0 < k < p-1$ such that $G_k(L) \equiv 0 \mod p$ correspond to abelian extensions of degree p of $K(\wp)$, unramified outside $\wp$ and wildly ramified at $\wp$ (see also Theorem 25 in this note).*

The proof of Theorem 18 rests on Robert's work on the theory of elliptic units, which we describe next.

4.3 Elliptic units

In 1973, building on ideas by Kronecker and Weber, Siegel [40], Ramachandra [32] and Novikov [28], Robert constructed a group of *elliptic units*, an analogue of the group of cyclotomic units which replaces the role of $\mathbb{Q}(\zeta_p)$ by $K(p)$. His work was later generalized by Kubert and Lang in their book *Modular Units* [20].

Before stating the main theorems we introduce the Siegel functions. We follow Robert and Kubert-Lang in defining invariants as in [34] and [20], respectively.

Definition 2 *Let L be a lattice in $\mathbb{C}$.*

1. *The Siegel functions are defined by*
$$g^{12}(z,L) = \mathfrak{k}^{12}(z,L)\Delta(L)$$
where $\mathfrak{k}(z,L) = e^{\eta(z,L)z/2}\sigma(z,L)$ is a Klein form and $\Delta(\tau)^{1/12} = (2\pi i)\cdot\eta(w)^2$. In particular, $g^{12}(\zeta z, L) = g^{12}(z,L)$ for any root of unity $\zeta \in K$(see [20, p. 26-29]).

2. *Let I be the free abelian group on ideals of K which are prime to $6p$. We express $a \in I$ as formal sums $a = \sum_{\mathfrak{A}} a(\mathfrak{A})\mathfrak{A}$ with $a(\mathfrak{A}) \in \mathbb{Z}$ for all ideals $\mathfrak{A} \subseteq \mathcal{O}_K$, and define the degree and norm of a by the formulas $\deg(a) = \sum_{\mathfrak{A}} a(\mathfrak{A})$, $N(a) = \sum_{\mathfrak{A}} a(\mathfrak{A})\mathbf{N}(\mathfrak{A})$ where $\mathbf{N}(\mathfrak{A}) = |\mathcal{O}_K/\mathfrak{A}|$ denotes the absolute norm of the ideal $\mathfrak{A}$. Also, for $a \in I$ write:*
$$g_p^{12}(a;\mathcal{O}_K) := \prod_{\mathfrak{A}=(\alpha)} g^{12}\left(\frac{\alpha}{p},\mathcal{O}_K\right)^{a(\mathfrak{A})}.$$
The primitive Robert group $\mathfrak{R}_p^*$ is the group of all elements:
$$g_p^{12}(a;\mathcal{O}_K), \quad a \in I \text{ such that } \deg(a) = 0,\ N(a) = 0.$$
If p splits in K, the Robert group of units for $K(\wp)$, denoted by $\mathfrak{R}_\wp^*$, is defined to be $\mathfrak{R}_\wp^* = N_{K(\wp)}^{K(p)}(\mathfrak{R}_p^*)$, i.e. the norm of $\mathfrak{R}_p^*$ down to $K(\wp)$.

Remark 7 *The elements of the primitive Robert group $\mathfrak{R}_p^*$ are usually referred to as "elliptic units", although other elements constructed in a similar manner receive the same name. The terminology comes from the fact that the Siegel functions are elliptic functions. As in the cyclotomic case, the elliptic units are analytically defined, the index in the full unit group of $K(p)$ is finite and the index itself is quite interesting (see below). Moreover, these units may be defined for all ray class fields of the form $K(p^n)$ and they behave nicely under relative norms.*

Let E be the group of units in $K(p)$. Notice that E contains μ_p, the group of pth roots of unity because, by definition, $K(p)$ is the ray class field of K of conductor (p), thus $\mu_p \subseteq K[\mu_p] \subseteq K(p)$. Similarly, if p splits in K, let $E_\wp$ be the full unit group inside $K(\wp)$. For $p \geq 5$, the group of Robert units $\mathfrak{R}_p^*$ also contains μ_p (see [25], Lemma 4.3), however when p splits $\mathfrak{R}_\wp^*$ does not contain the pth roots of unity. The following is a theorem due to Robert ([34]), although we are using the notation of Kubert-Lang (for details about the dictionary of invariants, see [25, Thm. 4.5]).

Theorem 19 ([34, §6.5, Thm. 16]) *The Robert groups of elliptic units $\mathfrak{R}_p^*$ (resp. $\mathfrak{R}_\wp^*$ if p is split) is a subgroup of E (resp. $E_\wp$). Moreover, the index is finite and given by*
$$[E\colon \mathfrak{R}_p^*] = \lambda \cdot h_p, \quad [E_\wp\colon \mathfrak{R}_\wp^*] = \lambda' \cdot h_\wp$$
where λ and λ' are integers only divisible by 2 and 3, and h_p and $h_\wp$ are the class numbers of $K(p)$ and $K(\wp)$ respectively.

The reader should compare the previous theorem with Theorem 11 of Section 2.1. In the work of Kubert-Lang (and improvements by Kersey) a larger, more refined subgroup of elliptic units is defined so that the index in the full unit group is precisely the class number.

4.3.1 Kronecker limit formulas

The so-called Kronecker limit formulas relate the class numbers of ray class fields of K, the value of certain Dirichlet L-functions at $s = 1$ and the logarithms of elliptic units. The formulas date back to Meyer [27], Siegel [40] and Ramachandra [32] and play an essential role in the proof of the index of the subgroup of elliptic units in the full unit group. These formulas constitute a remarkable analogue of Theorem 4.

Definition 3 (cf. [20, p. 234]) *Let $\mathfrak{f} \neq (1)$ be an integral ideal of $\mathcal{O}_K$ and let $f \geq 0$ be the smallest positive integer in the ideal $\mathfrak{f}$. Let C be a class in $\mathrm{Cl}(K, \mathfrak{f})$, the ray class group of K of conductor $\mathfrak{f}$, and let $\mathfrak{A}$ be an ideal in C. We define the number:*

$$g_{\mathfrak{f}}(C) = g^{12f}(1, \mathfrak{f}\mathfrak{A}^{-1}).$$

It can be shown that $g_{\mathfrak{f}}(C)$ does not depend on the choice of ideal $\mathfrak{A} \in C$ and $g_{\mathfrak{f}}(C) \in K(\mathfrak{f})$, the ray class field of K of conductor $\mathfrak{f}$ (see [20, Thm. 1.1, p. 234]). Next we define the appropriate L-functions.

Definition 4 *Let $\mathfrak{f} \neq (1)$ be an integral ideal of K and let χ be a character of $\mathrm{Cl}(K, \mathfrak{f})$. We define the L-function attached to (K, χ) by*

$$L_K(s, \chi) = \sum_{\mathfrak{A} \neq (0)} \frac{\chi(\mathfrak{A})}{N(\mathfrak{A})^s}$$

for $\Re(s) > 1$, where the sum is over all non-zero integral ideals of K. Let D_K and $\mathfrak{D}_K$ be the discriminant and different of K respectively and let $\gamma \in K$ be such that the ideal $\gamma\mathfrak{D}_K\mathfrak{f}$ is prime to $\mathfrak{f}$. We define a Gauss sum $\tau(\chi)$ by

$$\tau(\chi) = \sum_{\lambda \mod \mathfrak{f}} \bar{\chi}(\lambda\gamma\mathfrak{D}_K\mathfrak{f}) e^{2\pi i \operatorname{Tr}(\lambda\gamma)}.$$

The quotient $\rho(\chi) = \tau(\chi)/N(\mathfrak{f})^{1/2}$ is one.

Theorem 20 (Kronecker Limit Formulas, [34, Thm. 3]) *Let $\mathfrak{f} \neq (1)$ be an integral ideal of K. Let $\chi \neq 1$ be a character of $\mathrm{Cl}(K, \mathfrak{f})$. Then there exists an integral ideal $\mathfrak{f}_\chi$ which divides $\mathfrak{f}$ and a primitive character χ' of $\mathrm{Cl}(K, \mathfrak{f}_\chi)$ associated to χ. Let $e_{\mathfrak{f}_\chi}$ be the number of roots of unity in $K(\mathfrak{f})$ which are congruent to 1 modulo $\mathfrak{f}$ and let f_χ be the smallest positive integer in $\mathfrak{f}$. Then:*

1. $$L_K(1, \chi')\tau(\chi') = -\frac{2\pi}{6 f_\chi e_{\mathfrak{f}_\chi} \sqrt{|D_K|}} \sum_{C \in \mathrm{Cl}(K, \mathfrak{f}_{\chi'})} \bar{\chi}(C) \log |g_{\mathfrak{f}_{\chi'}}(C)|.$$

2. *Let H be an abelian extension of K of conductor $\mathfrak{f}$. Let h_H and R_H be the class number and regulator of H, respectively. Let e_H and e be the number of roots of unity in H and K, respectively. Then:*

$$\frac{h_H \cdot R_H \cdot e}{h \cdot e_H} = \prod_\chi \frac{-1}{6 f_\chi e_{\mathfrak{f}_\chi} \rho(\chi')} \sum_{C \in \mathrm{Cl}(K, \mathfrak{f}_{\chi'})} \bar{\chi}(C) \log |g_{\mathfrak{f}_{\chi'}}(C)|.$$

The reader can find a proof in [40] or [21, Chapter 20, §5].

4.4 The proof of Robert's criterion

In this subsection we sketch the proof of Theorem 19, as given in [36], but specialized to the case $h_K = 1$. The approach is closely related to the proof of Theorem 12 outlined in Section 2.2, i.e. it combines a decomposition of an appropriate module with the index formula and logarithmic derivatives modulo $\wp$. We start by describing the characters of $\mathrm{Gal}(K(\wp)/K) \cong (\mathcal{O}_K/\wp\mathcal{O}_K)^\times/\{\pm 1\}$.

Lemma 2 *Let $p \geq 5$ be unramified in K and let $G = (\mathcal{O}_K/\wp\mathcal{O}_K)^\times/\{\pm 1\}$. Let $\sigma^k \colon G \to (\mathcal{O}_K/\wp\mathcal{O}_K)^\times$ be defined such that $\sigma^k(\alpha) = \alpha^k$, with k divisible by e and $e \leq k \leq N(\wp) - 1$. The irreducible representations of G over $\mathbb{F}_p$, up to equivalence, are:*

1. *If p splits in K the linear irreducible representations of G are the homomorphisms $\sigma^k : G \to \mathbb{F}_p^\times$ with $e|k$ and $e \leq k \leq p-1$. They are all of degree 1.*
2. *If p is inert and $(p+1)|k$ then $\sigma^k \colon G \to \mathbb{F}_p^\times$ is a group character of degree 1. Notice that $\alpha^{p+1} \equiv N(\alpha) \mod p$. Thus, for $k \equiv 0 \mod p+1$, the map σ^k is given by*
$$\alpha \mapsto (N(\alpha))^{\frac{k}{p+1}} \mod p.$$
3. *If p is inert and $(p+1) \nmid k$: in this case $\sigma^k \colon G \to \mathrm{GL}(\mathcal{O}_K/(p))$ is of degree 2 and the character of σ^k is $\chi_k(\alpha) = \mathrm{Trace}(\sigma^k(\alpha)) = \alpha^k + \alpha^{pk} \equiv 2\Re(\alpha) \mod p$.*

The previous lemma is stated and proved in [36, *Lemme* 9, p. 305]. Let χ_k, with $2 \leq k \leq N(\wp) - 1$, be the set of all irreducible characters attached to the representations σ^k. We define a system of orthogonal idempotents by:
$$\epsilon_{\chi_k} = \frac{1}{|G|} \sum_{g \in G} \chi_k(g^{-1}) g \in \mathbb{F}_p[G]$$
so that $\sum_k \epsilon_{\chi_k} = 1 \in \mathbb{F}_p$, where the sum is over all even k as above. Moreover, if $\mathcal{S}$ is a $\mathbb{F}_p[G]$-module, we define submodules $\mathcal{S}^\chi := \epsilon_\chi \cdot \mathcal{S}$ and one has a direct sum decomposition:
$$\mathcal{S} = \bigoplus_\chi \mathcal{S}^\chi.$$

Let $\wp$ be a prime of K lying above p and let $E_\wp$ be the full group of units in $K(\wp)$. The $\mathbb{F}_p$-vector space $\mathcal{E}_p = E_\wp/(E_\wp)^p$ is clearly an $\mathbb{F}_p[G]$-module. Although not obvious, the space $\mathcal{R}_p = \mathfrak{R}_\wp^*/\mathfrak{R}_\wp^* \cap E_\wp^p$ is also an $\mathbb{F}_p[G]$-module. To see this, we make use of the isomorphism $(\mathcal{O}_K/p)^\times/\{\pm 1\} \to \mathrm{Gal}(K(p)/K)$ given by the Artin map $(\alpha) \mapsto ((\alpha), K(p)/K)$. The action of Galois on values of the Siegel function is as follows (see [20]):
$$g^{12}\left(\frac{\beta}{p}, \mathcal{O}_K\right)^{((\alpha),K(p)/K)} = g^{12}\left(\frac{\alpha \cdot \beta}{p}, \mathcal{O}_K\right). \tag{9}$$

Hence $g_p^{12}(a; \mathcal{O}_K)^{((\alpha),K(p)/K)} = g_p^{12}(\alpha \cdot a; \mathcal{O}_K)$. If we define another $\mathbb{F}_p[G]$-submodule by $\mathcal{S} = E_\wp/\mathfrak{R}_\wp^* E_\wp^p$ we obtain exact sequences:
$$\{0\} \to \mathcal{R}_p \to \mathcal{E}_p \to \mathcal{S} \to \{0\}, \quad \{0\} \to \mathcal{R}_p^\chi \to \mathcal{E}_p^\chi \to \mathcal{S}^\chi \to \{0\} \tag{10}$$
for each character χ of G. By Theorem 19 one has $[E_\wp : \mathfrak{R}_\wp^*] = \lambda \cdot h_\wp$ (where $h_\wp$ here is the class number of $K(\wp)$), thus $p \nmid h_\wp$ (for $p \geq 5$) if and only if $\mathcal{S}^\chi = 0$ for all irreducible characters χ. We record this as a lemma.

Lemma 3 *The class number $h_\wp$ is prime to p if and only if $\mathcal{S}^\chi = 0$ for all irreducible characters χ of G.*

Moreover, we can calculate the dimension of $\mathcal{E}_p^\chi$, call it $e(\chi)$, over the finite field $\epsilon_\chi \mathbb{F}_p[G]$.

Lemma 4 ([36, Lemma 11, p. 307]) *Let $p \geq 5$ be prime and let χ be an irreducible character of G over $\mathbb{F}_p$. Let h_K be the class number of K. Then:*

1. *If $\chi = 1$ then $e(\chi) = \dim_{\epsilon_\chi \mathbb{F}_p[G]}(\mathcal{E}_p^\chi) = h_K - 1$;*
2. *If $\chi = \chi_{p+1}$ then $e(\chi) = h_K + 1$;*

3. *In all other cases* $e(\chi) = h_K$.

Since in this section the attention is restricted to the case $h_K = 1$, the possibilities for $e(\chi)$ are 0, 1 or 2. The last fundamental ingredient is the construction of a logarithmic derivative modulo $\wp$.

Let $\mathfrak{X} = \mathcal{O}_K/\wp\mathcal{O}_K$ and let $\widehat{\mathfrak{X}} = \mathfrak{X}^{\oplus(N(\wp)-1)/e}$ denote the direct sum of $(N(\wp)-1)/e$ copies of $\mathfrak{X}$. Notice that for an integral ideal $\mathfrak{A} = (\alpha) \subset \mathcal{O}_K$ the logarithmic derivative of

$$g^{12}(z, L; \mathfrak{A}) := \frac{g^{12}(z, L)^{N(\mathfrak{A})}}{g^{12}(z, \mathfrak{A}^{-1}L)}$$

is given by (see [36, p. 299]):

$$z\frac{\partial}{\partial z}\log g^{12}(z, L; \mathfrak{A}) = 12(N(\mathfrak{A}) - 1 + \sum(G_k(\mathfrak{A}^{-1}L) - N(\mathfrak{A})G_k(L))z^k)$$

where the sum is over all $k > 0$ divisible by e. Put $G_k^*(\mathfrak{A}, L) = G_k(\mathfrak{A}^{-1}L) - N(\mathfrak{A})G_k(L)$ and notice that if $\mathfrak{A} = (\alpha)$ is principal (and all ideals in K are principal, by assumption) then $G_k^*((\alpha), L) = (\alpha^k - N(\alpha))G_k(L)$. We are ready to describe the desired mod $\wp$ logarithmic derivative:

Theorem 21 ([36, Thm. 12]) *Let A/K and $L \subset \mathbb{C}$ be as before. Let k be divisible by e and $e \leq k \leq N(\wp) - 1$. There exist a homomorphism φ_k from $K(\wp)^\times$ to the additive group $\mathfrak{X}$, such that:*

1. *The kernel of φ_k, for $k \neq N(\wp) - 1$, and the kernel of $\varphi_{N(\wp)-1}$ restricted to E, are G-stable.*
2. *For all $u \in K(\wp)^\times$ and all $g \in G$ one has $\varphi_k(u^g) = \sigma^k(g)\varphi_k(u)$, where σ^k is the irreducible representation described in Lemma 2.*
3. *Let ρ be an element of $\wp^{-1}L$ such that $\rho \notin L$. If $k \neq N(\wp) - 1$ and $\mathfrak{A} = (\alpha) \subset \mathcal{O}_K$ is an integral ideal prime to $\wp$ then:*

$$\varphi_k\left(g^{12}(\rho, L; \mathfrak{A})\right) \equiv 12G_k^*(\mathfrak{A}, L) \equiv 12(\alpha^k - N(\alpha))G_k(L) \mod \wp.$$

Moreover, if $k \neq p + 1$ then $\alpha^k - N(\alpha) \neq 0 \mod \wp$.

Let Ψ be the subgroup of $K(\wp)^\times$ generated by elements of the form $g^{12}(\rho, L; \mathfrak{A})$ and let $\Theta = E_\wp \cap \Psi$. Also we define an extra $\mathbb{F}_p[G]$-module by $\Theta_p = \Theta/\Theta \cap E_\wp^p$. In particular, let $f_\chi : G \to \mathbb{Z}$ be a function such that $f_\chi(g) \equiv \chi(g) \mod p$ and $\sum_g f_\chi(g) = 0$ and define (compare with Theorem 12):

$$\xi_\chi(\mathfrak{A}) = \prod_{g \in G} g^{12}(\rho, L; \mathfrak{A})^{f_\chi(g^{-1})g}.$$

Then $\xi_\chi(\mathfrak{A}) \in \Psi$. In fact, one can show that $\xi_\chi(\mathfrak{A}) \in \Theta$ and

$$\varphi_k(\xi_\chi(\mathfrak{A})) \equiv 12G_k^*(\mathfrak{A}, L) \mod \wp.$$

Furthermore:

Lemma 5 ([36, Prop. 22, Lemma 24])

1. *If χ is of degree 1 and $\chi \neq \chi_{p+1}$ then $\varphi_k(\Theta_p^\chi)$ is generated over $\mathbb{F}_p$ by $G_k(L) \mod \wp$;*
2. *If $\chi = \chi_{p+1}$ then $\varphi_k(\Theta_p^\chi)$ is generated over $\mathbb{F}_p$ by $pG_k(L)$;*
3. *If χ is of degree 2 then $(\varphi_k, \varphi_{p(k)})(\Theta_p^\chi)$ is generated over $\mathcal{O}_K/\wp$ by the pair $(G_k(L), G_{p(k)}(L))$, where $0 < p(k) < p^2 - 1$ is an even integer congruent to $pk \mod p^2 - 1$.*

Since φ_k is an homomorphism, $\dim(\varphi_k(\Theta_p^\chi)) \leq \dim(\Theta_p^\chi)$. Moreover Θ_p^χ is a submodule of $\mathcal{R}_p^\chi$. If we combine these two facts with the exact sequence in Eq. (10) we obtain:

$$\dim(\varphi_k(\Theta_p^\chi)) \leq e(\chi) = \dim(\mathcal{E}_p^\chi), \quad \dim \mathcal{S}^\chi \leq e(\chi) - \dim(\varphi_k(\Theta_p^\chi)).$$

Finally, since $e(\chi) = 0$, 1 or 2 by Lemma 4, if the appropriate Hurwitz numbers are not zero modulo p then $\dim \mathcal{S}^\chi = 0$ for all χ, by Lemma 5 and the previous inequalities. Hence, by Lemma 3, $h_\wp$ is not divisible by p which ends the proof of Robert's criterion.

5 Rephrasing Robert

The objective of this section is to rephrase Robert's criterion (Theorem 18) in a similar way to the generalizations of Kummer's criterion discussed in Section 2. The reader should keep in mind that the converse of Robert's criterion is false (see Remark 6). The first step is to express the Hurwitz numbers as values of Hecke L-functions attached to the powers of certain Grössencharacter.

5.1 Grössencharacters, L-functions and Hurwitz numbers

Let F be a number field and let $\mathcal{A}_F^*$ be the idele group of F, i.e. $\mathcal{A}_F^* = \prod_\nu' F_\nu^*$ where the product is a restricted direct product running over all places (infinite and finite) of F. Recall that F^* embeds into $\mathcal{A}_F^*$ diagonally $x \in F^* \mapsto (x_\nu)_\nu$ where x_ν is the image of x under the embedding of F into its completion at the place ν, F_ν.

Definition 5 *A Grössencharacter ψ on F is a continuous homomorphism $\psi : \mathcal{A}_F^* \to \mathbb{C}^*$ which is trivial on F^*, i.e. if $x \in F^*$ then $\psi((x_\nu)_\nu) = 1$. We say that ψ is unramified at a prime $\wp$ of F if $\psi(\mathcal{O}_\wp^*) = 1$, where $\mathcal{O}_\wp$ is the ring of integers inside $F_\wp$. Otherwise we say that ψ is ramified at $\wp$.*

Let $\mathcal{O}_F$ be the ring of integers in F. We may define a homomorphism on the (multiplicative) group of non-zero fractional ideals of F as follows. Let $\wp$ be a prime of F, let π be a uniformizer of $F_\wp$ and let $\alpha_\wp \in \mathcal{A}_F^*$ be the element which is π at the place $\wp$ and 1 at all other places. We define:

$$\psi(\wp) = \begin{cases} 0, & \text{if } \psi \text{ is ramified at } \wp; \\ \psi(\alpha_\wp), & \text{otherwise.} \end{cases}$$

Definition 6 *The Hecke L-series attached to a Grössencharacter ψ of F is given by the Euler product over all primes of F:*

$$L(s,\psi) = \prod_\wp \left(1 - \frac{\psi(\wp)}{(N_{\mathbb{Q}}^F(\wp))^s}\right)^{-1}.$$

Hecke L-series of this form have an analytic continuation and satisfy a certain functional equation. This fact was first proved by Hecke himself but it was later vastly generalized by Tate using Fourier analysis on the adeles $\mathcal{A}_F$ (what is usually called Tate's thesis, see [22]).

Now let K be a quadratic imaginary field and let A/F be an elliptic curve defined over a number field F (such that $K \subset F$), with complex multiplication by K. The so-called 'Main Theorem of Complex Multiplication' ([43, Thm. 8.2]) implies the existence of a Grössencharacter of F, $\psi_{A/F} : \mathcal{A}_F^* \to \mathbb{C}^*$ associated to the curve A/F satisfying several interesting properties which we collect in the following statement.

Theorem 22 ([43, Thm. 9.1, Prop. 10.4, Cor. 10.4.1]) *Let $\wp$ be a prime of F of good reduction for A/F, i.e. the reduction $\widetilde{A}/F$ of A modulo $\wp$ is smooth. There exists a Grössencharacter of F, $\psi_{A/F} : \mathcal{A}_F^* \to \mathbb{C}^*$, such that:*

1. *$\psi_{A/F}$ is unramified at a prime $\mathfrak{Q}$ of F if and only if A/F has good reduction at $\mathfrak{Q}$;*
2. *$\psi_{A/F}(\wp)$ belongs to $\mathcal{O}_K$, thus multiplication by $[\psi_{A/F}(\wp)]$ is a well defined endomorphism of A/F. Moreover $N_{\mathbb{Q}}^F(\wp) = N_{\mathbb{Q}}^K(\psi_{A/F}(\wp))$;*
3. *The following diagram is commutative*

$$\begin{array}{ccc} A & \xrightarrow{[\psi_{A/F}(\wp)]} & A \\ \downarrow & & \downarrow \\ \widetilde{A} & \xrightarrow{\phi_\wp} & \widetilde{A} \end{array}$$

where $\phi_\wp : \widetilde{A} \to \widetilde{A}$ be the $N_{\mathbb{Q}}^F(\wp)$-power Frobenius map and the vertical maps are reduction mod $\wp$;

4. *Let $|\widetilde{A}(\mathcal{O}_F/\wp)|$ be the number of points in $\widetilde{A}$ over the finite field $\mathcal{O}_F/\wp$ and put $a_\wp = N_{\mathbb{Q}}^F(\wp) + 1 - |\widetilde{A}(\mathcal{O}_F/\wp)|$. Then*
$$a_\wp = \psi_{A/F}(\wp) + \overline{\psi_{A/F}(\wp)} = 2 \cdot \Re(\psi_{A/F}(\wp)).$$

5. *(due to Deuring) Let $L(A/F, s)$ be the L-function associated to the elliptic curve A/F. If $K \subset F$ then $L(s, A/F) = L(s, \psi_{A/F})L(s, \overline{\psi_{A/F}})$. If $K \not\subseteq F$, and $F' = FK$, then $L(s, E/F) = L(s, \psi_{A/F'})$.*

In particular, if $h_K = 1$ then A is defined over K (actually, it can be defined over $\mathbb{Q}$), $\psi_{A/K}(\wp)$ is a generator of $\wp$ by part 2 and the explicit generator can be pinned down using part 4. Thus, if e is the number of roots of unity in K, then $\psi_{A/K}^k(\wp) = \alpha^k$ where α is *any* generator of $\wp$. Also, by part 5, $L(s, A/\mathbb{Q}) = L(s, \psi_{A/K})$. In 1970, Damerell proved that certain special values of the Hecke L-functions attached to the Grössencharacter $\psi_{A/K}$ are algebraic numbers.

Theorem 23 (Damerell's Theorem, [7]) *Let $A/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}$, an order in a quadratic imaginary field K of class number $h_K = 1$. Let L be the period lattice and let $\Omega \in L$ be such that $L = \Omega\mathcal{O}$ (such an Ω exists because $h_K = 1$). Let $\psi = \psi_{A/K}$ be the Grössencharacter attached to A/K and let $L(s, \bar{\psi}^k)$ be the Hecke L-function attached to the powers of $\bar{\psi}$, with $k \geq 1$. Then the numbers*
$$L^*(k, \bar{\psi}^{k+j}) := \left(\frac{2\pi}{\sqrt{D_K}}\right)^j \frac{L(k, \bar{\psi}^{k+j})}{\Omega^{k+j}}, \quad k \geq 1,\ j \geq 0$$
belong to $\overline{K}$, the algebraic closure of K. Moreover, if $0 \leq j < k$ then $L^*(k, \bar{\psi}^{k+j})$ belongs to K.

Since then, a great deal has been discovered about the special values of Hecke L-functions. For example, Yager [45] has shown that $L^*(k, \bar{\psi}^{k+j})$, with $k \geq 1, j \geq 0$ belongs to $K_\wp$, the completion of K at $\wp$, and are $\wp$-integral if $0 \leq j \leq p-1$ and $1 < k \leq p$. On the other hand, the vanishing of $L(1, \bar{\psi})$ (i.e. the case $j = 0$ and $k = 1$) is intimately related to the Birch and Swinnerton-Dyer conjecture. The vanishing of other values $L^*(k, \bar{\psi}^{k+j})$ should fit in the framework of the Bloch-Kato and Beilinson-Bloch Conjectures. In particular, Guo [11] has given an explanation of their vanishing in terms of generalized Selmer groups. Our interest in these values resides in the following statement:

Proposition 4 *Let K be a quadratic imaginary field of class number $h_K = 1$ and let k be an integer divisible by e, the number of roots of unity in K. Then $L(k, \psi^k)/\Omega^k$ is rational and:*
$$e \cdot L^*(k, \psi^k) = \frac{e \cdot L(k, \psi^k)}{\Omega^k} = G_k(L).$$

PROOF. As we pointed out after Theorem 22, if $k \equiv 0 \mod e$ then $\psi^k(\mathfrak{A}) = \alpha^k$ where α is any generator of $\mathfrak{A}$. Also recall that $L = \Omega\mathcal{O}_K$ and $\mathcal{O}_K$ is assumed to be a PID, so every non-zero ideal has exactly e generators. Then, for $k \geq 4$ with $e|k$, one has:
$$\begin{aligned} G_k(L) &= \sum_{w \in L \setminus \{0\}} \frac{1}{w^k} = \sum_{\alpha \in \mathcal{O}_K \setminus \{0\}} \frac{1}{(\Omega\alpha)^k} \\ &= \frac{e}{\Omega^k} \sum_{\mathfrak{A} = (\alpha) \neq (0)} \frac{\alpha^k}{N(\mathfrak{A})^k} = \frac{e}{\Omega^k} L(k, \psi^k). \quad \blacksquare \end{aligned}$$

Since $e = 2$, 4 or 6 and $p \geq 5$, the Hurwitz numbers $G_k(L)$ may be replaced by $L^*(k, \psi^k)$ in the statement of Theorem 18.

5.2 Saito's improvement

As we have mentioned, Robert's work [36] is quite a bit more general than Theorem 18. In particular, his work is valid for arbitrary h_K and, moreover, his criterion applies to any subfield $M \subseteq K(\wp)$. More concretely, his methods give sufficient conditions for the quotient h_M/h_{H_0} to be relatively prime to p, where H_0 is the Hilbert class field of K. On the other hand, there are two drawbacks: the criterion does not provide a necessary condition (in the inert case, at least) and the required hypothesis is written in terms of $\mathcal{O}_K/\wp$-linear independence of Hurwitz numbers $G_k(\mathfrak{A}^{-1}L)$.

In 1985, Saito published in [38] an improved version of Robert's methods which overcomes, in some sense, the disadvantages of Robert's earlier work. In particular, the criterion is an if-and-only-if statement written solely in terms of the divisibility of special values of Hecke L-functions attached to certain Grössencharacters. The reader should be warned, the rest of this section is fairly technical in order to state the theorem in its outmost generality.

Let A be an elliptic curve with complex multiplication by $\mathcal{O}_K$, let p be a prime which does not divide $6h_K$ and let $\wp$ be a prime of K lying above p, as before. Let $\mathfrak{f}_0$ be an ideal prime to p and let $K(\mathfrak{f}_0)$ be the ray class field of K of conductor $\mathfrak{f}_0$. Let $A[\wp]$ be the group of $\wp$-division points of A and let $K(\mathfrak{f}_0)(A[\wp])$ be the field which results by adjoining to $K(\mathfrak{f}_0)$ the coordinates of points in $A[\wp]$. Fix a subfield $F \subseteq K(\mathfrak{f}_0)$ and let M be an abelian extension of F, such that $F \subsetneq M \subseteq K(\mathfrak{f}_0)(A[\wp])$, $m = [M : K]$ is prime to p, and M is not strictly contained in $K(\mathfrak{f}_0)$. Let N be another number field such that $F \subseteq N \subseteq M$.

Let X_M be the group of all $\overline{\mathbb{Q}}$-valued characters of $G = \mathrm{Gal}(M/K)$ and let $X_{M/N}$ be the subset of all $\chi \in X_M$ such that $\mathrm{Gal}(M/N)$ is not included in $\mathrm{Ker}\,\chi$. A character $\chi \in X_M$ with conductor $\mathfrak{f}(\chi)$ will also be regarded as a character of the ray class group $\mathrm{Cl}(K, \mathfrak{f}(\chi))$ via the Artin map. We denote the maximal ideal of the valuation ring of $\mathbb{C}_p$ by P. The following proposition specifies the Grössencharacter that we need.

Proposition 5 ([38, Prop. 3.4]) *Assume $\chi \in X_{M/N}$ satisfies $\chi(C_{(\alpha)}) \equiv \alpha^k \mod P$ for α such that $(\alpha, \mathfrak{f}(\chi)) = 1$ and $\alpha \equiv 1 \mod \mathfrak{f}(\chi)/\wp$, where $C_{(\alpha)}$ is the class of (α) in $\mathrm{Cl}(K, \mathfrak{f}(\chi))$. Then there exists a unique Grössencharacter $\widetilde{\chi}$ of K with the properties:*

1. *The conductor of $\widetilde{\chi}$ equals $\mathfrak{f}(\widetilde{\chi}) = \mathfrak{f}(\chi)/\wp$;*
2. *$\widetilde{\chi}((\alpha)) = \bar{\alpha}^k$ if $\alpha \equiv 1 \mod \mathfrak{f}(\widetilde{\chi})$;*
3. *$\widetilde{\chi}(\mathfrak{A}) \equiv \chi(C_{\mathfrak{A}})^{-1} N\mathfrak{A}^k \mod P$ for any ideal $\mathfrak{A}$ prime to $\mathfrak{f}(\chi)$.*

The following constants will also be needed. Let L be the lattice attached to the elliptic curve A. Since A has complex multiplication by $\mathcal{O}_K$, there is $\Omega \in \mathbb{C}$ and $\mathfrak{f} \in \mathcal{O}_K$ such that $L = \mathfrak{f}\Omega$. Moreover, by Lemma 2.3 in [38], there exist τ_1 and τ_2 such that $\Omega = \tau_1 + \tau_2$ and $\tau_1^{-1}L \cap \mathcal{O}_K = \wp$ and $\tau_2^{-1}L \cap \mathcal{O}_K = \mathfrak{f}_0$.

We also define a set of indices $\mathcal{K}$ as follows. Let $m = [M : K]$, $q = (N\wp - 1)/m$ and, for every $k \in \mathbb{Z}$, let $k(p)$ be a positive integer $1 \leq k(p) \leq N(\wp) - 1$ such that $k(p) \equiv kp \mod (N(\wp) - 1)$. Define

$$\mathcal{K} = \{k \in \mathbb{Z} : q|k,\ (k, p) = 1,\ q \leq k \leq N(\wp) - 2\}$$

and a partition $\mathcal{K} = \mathcal{K}_1 \cup \mathcal{K}_2$ where $\mathcal{K}_2$ is the subset of $k \in \mathcal{K}$ such that $k(p) = kp$ and $\mathcal{K}_1 = \mathcal{K} \setminus \mathcal{K}_2$. Let c_k be the character of the inertia subgroup $I(M/K) \subset \mathrm{Gal}(M/K)$ defined in [38, Prop. 1.2]. Let $X^1_{M/N}$ be the set of $\chi \in X_{M/N}$ such that $\bar{\chi} = c_k$ when restricted to $I(M/K)$ for some $k \in \mathcal{K}_1$ and $\chi \neq \omega \circ N^K_{\mathbb{Q}}$, where ω is the Teichmüller character. Similarly, let $X^2_{M/N}$ be the set of all $\chi \in X_{M/N}$ such that $\bar{\chi} = c_k$ when restricted to $I(M/K)$ for $k \in \mathcal{K}_2$ or $k(p) \in \mathcal{K}_2$.

For a number field T, with $K \subset T$, let $\mathcal{M}_T$ be the maximal p-abelian extension of T which is unramified at all primes of T not dividing $\wp$. We put $\mathcal{X}_T = \mathrm{Gal}(\mathcal{M}_T/M)$ and let $\mathcal{X}_{M/N}$ be the kernel of the restriction map from $\mathcal{X}_M$ to $\mathcal{X}_N$. The natural injection between the idele groups $\mathcal{A}^*_N \to \mathcal{A}^*_M$ induces a map $j : \mathcal{X}_N \to \mathcal{X}_M$. Let $\mathcal{M}_{M/N}$ be the subfield of $\mathcal{M}_M$ which corresponds to $j(\mathcal{X}_N)$, thus $\mathcal{X}_{M/N} \cong \mathrm{Gal}(\mathcal{M}_{M/N}/M)$. Let $\wp = \mathfrak{P}_1 \dots \mathfrak{P}_s$ be the decomposition into prime ideals in F and let $\widetilde{\mathfrak{P}}_i$ be the unique prime ideal of M

lying above $\mathfrak{P}_i$. Suppose $l = [M : F]$. We define the extension $\mathcal{F}(l)/M$ to be the composite of all cyclic extensions of M of degree p inside $\mathcal{M}_{M/N}$ whose conductor divide $\wp = (\widetilde{\mathfrak{P}}_1 \dots \widetilde{\mathfrak{P}}_s)^l$.

Finally, we are ready to state Saito's theorem:

Theorem 24 (Saito, [38, Thm. 4.1]) *With notation as above, consider the following conditions:*

1. $\left(L(k, \widetilde{\chi})\tau_2^{-k}, L(k(p), \widetilde{\chi}')\tau_2^{-k(p)}\right) \equiv 0 \mod P$ *for some* $\chi \in X^1_{M/N}$*;*
2. $L(k, \widetilde{\chi})\tau_2^{-k} \equiv 0 \mod P$ *for some* $\chi \in X^2_{M/N}$*;*
3. h_M/h_N *is divisible by* p*;*
4. $(h_M/h_N, p) = 1$ *and* $\mathcal{X}_{M/N}$ *has a torsion;*
5. $(h_M/h_N, p) = 1$*,* $\mathcal{X}_{M/N}$ *is torsion free and* $\dim_{\mathbb{F}_p}(\mathrm{Gal}(\mathcal{F}(l)/M))$ *is larger than the cardinality of* $X^1_{M/N}$*.*

Then conditions 1 *or* 2 *occurs if and only if conditions* 3*,* 4 *or* 5 *occurs. Moreover, condition* 5 *implies that* p *remains prime and condition* 2 *or* p *ramifies and condition* 1*.*

The strategy followed by Saito is the one used by Robert, namely the method of proof exploits the index of a suitable group of elliptic units together with logarithmic derivatives for elliptic units (essentially as outlined in Section 4.4), although the techniques are greatly refined.

5.3 The work of Coates-Wiles

Recall that Kummer's criterion may be extended as in Theorem 10. In particular, conditions (1) and (4) are equivalent: at least one of the numbers $\zeta^*(k)$ is divisible by p, for some even $k = 2, 4, \dots, p-3$ if and only if there exists a $\mathbb{Z}/p\mathbb{Z}$-extension of $\mathbb{Q}(\zeta_p)^+$ which is unramified outside the prime above p and which is distinct from $\mathbb{Q}(\zeta_{p^2})^+$. In the case of $\mathbb{Q}(\zeta_p)$ these two conditions are also equivalent to the class number $h(\mathbb{Q}(\zeta_p))$ being divisible by p. However, as we have seen (see Remark 6), in the case of a quadratic imaginary field K, the divisibility by p of a number $L^*(k, \psi^k)$ is not sufficient to conclude that $h(K(\wp))$ is divisible by p. On the other hand, Saito's theorem 24 indicates that the p-divisibility of the numbers $L^*(k, \psi^k)$ is related to the existence of $\mathbb{Z}/p\mathbb{Z}$-extensions of $K(\wp)$ which are unramified outside the primes not dividing $\wp$. Robert had already proved results in this direction in the split case. We state his theorem in the particular case $h_K = 1$ for simplicity. For arbitrary h_K the interested reader should consult [36].

Theorem 25 (Robert, [36, Thm. 2]) *Let* K *be a quadratic imaginary field of class number* 1 *and let* $p \geq 5$ *be a split prime in* K *(such that* $A/\mathbb{Q}$ *is of good reduction at* p*). Then* $G_k(L)$ *is not divisible by* p *for all* k *divisible by* e *and* $e \leq k \leq p-1$ *if and only if the maximal abelian* p*-extension of* $K(\wp)$ *unramified outside the prime above* $\wp$ *is abelian over* K*.*

Let $K(\wp^n)$ be the ray class field of K of conductor $\wp^n$. Then $K(\wp^2)/K(\wp)$ is an abelian p-extension, totally ramified above $\wp$, unramified elsewhere and $K(\wp^2)/K$ is abelian. Hence, if $G_k(L)$ is divisible by p for some k then, by Robert's theorem, there must exist an abelian p-extension $F/K(\wp)$, unramified outside primes above $\wp$ but non-abelian over K, so F must differ from $K(\wp^2)$.

Around the same time that Robert's work was conceived, Coates and Wiles produced a different proof of the previous theorem, which works only for the case $h_K = 1$.

Theorem 26 (Coates, Wiles, [4, Thm. 1]) *Let* K *and* $p \geq 5$ *be as in the preceding theorem (in particular* p *is assumed to split in* K *and* $h_K = 1$*). Then* p *divides at least one of the numbers* $L^*(k, \psi^k)$ *for some* k *divisible by* e *and* $e \leq k \leq p-1$ *if and only if there exists a* $\mathbb{Z}/p\mathbb{Z}$*-extension of* $K(\wp)$*, which is unramified outside the prime above* $\wp$ *and which is distinct from* $K(\wp^2)$*, the ray class field of* K *of conductor* $\wp^2$*.*

At this point in the survey, the approach of Coates and Wiles should feel very natural: first they use class field theory to obtain p-adic residue class number formulas for arbitrary finite extensions of K, which are combined with p-adic analytic functions for $K(\wp)/K$ due to Katz and Lichtenbaum.

5.3.1 Sketch of the proof of the Coates-Wiles theorem

Let $p \geq 5$ be a prime which splits in K. Let $K_\infty = \bigcup_{n\geq 1} K(\wp^n)$ be the compositum of all ray class fields of K of conductor $\wp^n$ for $n \geq 1$. The field K_∞ is a $\mathbb{Z}_p$-extension of $K(\wp)$, in particular $\mathrm{Gal}(K_\infty/K(\wp)) \cong \mathbb{Z}_p$ has no torsion. Let M be the maximal abelian p-extension of $K(\wp)$ unramified outside the prime of $K(\wp)$ dividing $\wp$. Clearly $\mathrm{Gal}(M/K_\infty) = 0$ if and only if there is no cyclic extension of $K(\wp)$ of degree p, unramified outside the prime above $\wp$ and distinct from $K(\wp^2)$, the first layer of $K_\infty/K(\wp)$. Moreover, it can be shown using class field theory that $\mathrm{Gal}(M/K_\infty)$ is always finite in our setting (due to the fact that the $\wp$-adic regulator is non-vanishing). The strategy is to relate the numbers $L^*(k, \psi^k)$ to the order of $\mathrm{Gal}(M/K_\infty)$. The first step is the following theorem.

Theorem 27 ([4, Thm. 11]) *Let $\mathcal{O}_\wp$ be the ring of integers in $K_\wp$ and let $D_{K(\wp)/K}$ be the relative discriminant of the extension. Let $R_\wp$ be the $\wp$-adic regulator of $K(\wp)/K$ (as defined in* [4, p. 13]*). Then the order of $\mathrm{Gal}(M/K_\infty)$ is equal to the inverse of the p-adic valuation of*

$$\frac{h_p \cdot R_\wp}{\sqrt{\Delta_\wp}}$$

where h_p is the class number of $K(\wp)$ and the quantity $\Delta_\wp$ is a generator of the ideal $D_{K(\wp)/K}\mathcal{O}_\wp$.

The previous theorem is obtained using techniques from class field theory. We will not go into the proof. The reader should be aware that Coates and Wiles prove the theorem more generally for any arbitrary finite extension F of K. The following step towards the proof of Kummer's criterion for K consists of relating the valuation of $h_p R_\wp/\sqrt{\Delta_\wp}$ to the values of Hecke L-functions. This is accomplished using the p-adic L-functions constructed by Katz and Lichtenbaum, which we describe next.

Let X be the set of all non-trivial $\mathbb{Z}_p^\times$-valued characters of the Galois group $\mathrm{Gal}(K(\wp)/K)$. Let $A[\wp]$ be the kernel of the multiplication by π map, where $\wp = (\pi)$, and put $\mathcal{F} = K(A[\wp])$. The extension $\mathcal{F}/K(\wp)$ is an extension of degree e. Let $\theta : \mathrm{Gal}(\mathcal{F}/K) \to \mathbb{Z}_p^\times$ be the character which describes the action of Galois on the $\wp$-torsion points (i.e. on $A[\wp]$), so that $P^\sigma = \theta(\sigma)P$ for all $P \in A[\wp]$ and $\sigma \in \mathrm{Gal}(\mathcal{F}/K)$. Then $X = \{\theta^k : e|k \text{ and } e \leq k \leq p-2\}$. Finally, let R be the ring of integers in $\overline{\mathbb{Q}_p^{\mathrm{unr}}}$, the completion of the maximal unramified extension of $\mathbb{Q}_p$.

Theorem 28 (Katz [15], [16]; Lichtenbaum [24]) *Let $\chi \in X$. There exists a p-adic holomorphic function $L_p(s, \chi)$ which satisfies the following properties:*

1. *For each $\chi \in X$ there exists a power series $H_\chi(T) \in R[[T]]$ such that $L_p(s, \chi) = H_\chi((1+p)^s - 1)$.*
2. *Let j be an integer divisible by e and $e \leq j \leq p-2$ (so that $\theta^j \in X$). Then, for each integer $k \geq 1$ with $k \equiv j \mod (p-1)$ there exists a unit α_k in the ring of integers R of $\overline{\mathbb{Q}_p^{unr}}$ such that*

$$L_p(1-k, \theta^j) = \alpha_k L^*(k, \psi^k).$$

3. *There exists a unit β in R such that:*

$$\prod_{\chi \in X} L_p(1, \chi) = \frac{\beta \cdot h_p \cdot R_\wp}{\sqrt{\Delta_\wp}}.$$

The reader should compare the previous theorem with Theorems 5 and 16 which we have stated in preceding sections. The first p-adic L-functions for elliptic curves with complex multiplication were introduced by Manin and Vishik [26]. Many others have constructed L-functions in this setting: Katz ([15, 16]), Lichtenbaum [24], Coates-Wiles [6], Coates-Goldstein [3], Yager ([45, 46]), de Shalit [9], Boxall [1], among others. Part 3 of Theorem 28 is proved by establishing a p-adic analogue of the Kronecker limit formulas as in Theorem 20, part 2.

The proof of Theorem 26 can now be completed. As explained at the beginning of this subsection, it suffices to show that $\mathrm{Gal}(M/K_\infty) = 0$ if and only if p divides $L^*(k, \psi^k)$ for some k divisible by e and $e \leq k \leq p-1$. By Theorem 27 the order of $\mathrm{Gal}(M/K_\infty)$ equals the inverse of the p-adic valuation of $h_p R_\wp / \sqrt{\Delta_\wp}$. By Theorem 28, part 3, we have $h_p R_\wp / \sqrt{\Delta_\wp} = \prod_k L_p(1, \theta^k)$, where the product is over all k divisible by e and $e \leq k \leq p-1$. Moreover, by part 1 of the theorem, $L_p(1, \theta^k)$ is a unit if and only if $L_p(1-k, \theta^k)$ is a unit, and by part 2 the latter equals $\alpha_k L^*(k, \psi^k)$, with $\alpha_k \in R^\times$. Hence, the theorem follows.

5.4 A generalization by Yager

In this final section we will describe a generalization of Theorem 26 due to Yager, in 1982, which essentially follows the approach of Coates and Wiles.

Let K be a quadratic imaginary field of class number 1 and let A/K be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Let Ω be chosen so that the period lattice of A is $L = \Omega \mathcal{O}_K$. Let $p \geq 5$ be a split prime in K, $p\mathcal{O}_K = \wp\overline{\wp}$, such that A has good reduction at $\wp$ and $\overline{\wp}$. Let $\mathcal{F} = K(A[p])$, where $A[p]$ denotes the p-torsion of A. Let $\psi = \psi_{A/K}$ be the Grössencharacter associated to A/K. Recall that by Damerell's Theorem 23, the values

$$L^*(k, \bar{\psi}^{k+j}) := \left(\frac{2\pi}{\sqrt{D_K}}\right)^j \frac{L(k, \bar{\psi}^{k+j})}{\Omega^{k+j}}, \quad k \geq 1,\ j \geq 0$$

are algebraic and they belong to K when $0 \leq j < k$. Further, Yager has shown in [45] that $L^*(k, \bar{\psi}^{k+j})$ belongs to $K_\wp$ and is $\wp$-integral if $0 \leq j < p-1$ and $1 < k \leq p$. Finally, let χ_1 and χ_2 be the canonical characters with values in $\mathbb{Z}_p^\times$ giving the action of $\mathrm{Gal}(\overline{K}/K)$ on $A[\wp]$ and $A[\overline{\wp}]$ respectively (here $A[\wp]$ are the $\wp$-torsion points on A). Notice that the characters χ_1 and χ_2 generate $\mathrm{Hom}(\mathrm{Gal}(\mathcal{F}/K), \mathbb{Z}_p^\times)$. If F is a subfield of $\mathcal{F}$ we shall say that a character $\chi \in \mathrm{Gal}(\mathcal{F}/K)$ belongs to F if $\mathrm{Gal}(\mathcal{F}/F)$ is included in the kernel of χ.

Theorem 29 (Yager, [44, Thm. 3]) *Let F/K be a Galois extension with $F \subseteq \mathcal{F} = K(A[p])$. Then the following are equivalent conditions:*

1. *There exists a $\mathbb{Z}/p\mathbb{Z}$-extension of F which is unramified outside the primes above $\wp$ and which is distinct from the compositum of F and $K(\wp^2)$;*

2. *There exist integers k and j with $0 \leq j < p-1$ and $1 < k \leq p$ such that $\chi_1^k \chi_2^{-j}$ is a non-trivial character belonging to F (i.e. $\mathrm{Gal}(\mathcal{F}/F) \subset \mathrm{Ker}\, \chi_1^k \chi_2^{-j}$) and $L^*(k, \bar{\psi}^{k+j})$ is not a unit in $K_\wp$.*

The strategy of the proof is analogous to that of the criterion of Coates and Wiles. Let F_∞ denote the compositum of F and K_∞, the unique $\mathbb{Z}_p$-extension of K unramified outside $\wp$. Let M be the maximal abelian p-extension of F unramified outside the primes of F dividing $\wp$. Then $\mathrm{Gal}(M/F_\infty)$ is finite and it is trivial if and only if there exists a $\mathbb{Z}/p\mathbb{Z}$-extension of F which is unramified outside the primes above $\wp$ and which is distinct from the compositum of F and $K(\wp^2)$. The proof follows by extending the results of Katz and Lichtenbaum in this more general case and by making use of Theorem 27.

6 Arithmetic Applications

In this section we provide examples of some of the known arithmetic applications of Kummer's criterion and its generalizations.

6.1 The classical case and Fermat's last theorem

Kummer's motivation for finding a criterion regarding the regularity of prime numbers was Fermat's last theorem since, if we assume the regularity of p, it is possible to show that $x^p + y^p = z^p$ has no non-trivial solutions in $\mathbb{Q}$. The proof of this fact usually considers two distinct cases: in the first (and easier) case we assume that $\gcd(xyz, p) = 1$ and in the second case one deals with $\gcd(xyz, p) \neq 1$, which requires a more careful study of the units in $\mathbb{Q}(\zeta_p)$.

In this section we will show that the first case of Fermat's last theorem is true in a much more general setting: it holds for totally real number fields under certain conditions, and regular primes in the sense of Greenberg. In particular, we may use Theorem 15 to find examples of fields and primes where the (sufficient) conditions are satisfied. The proof is a straightforward generalization of the rational case, as can be found in [47]. Since we have not been able to find a reference to the result in this generality, we include the proof here.

Before we describe the proof, we mention that there has been some progress on Fermat's last theorem ($x^n + y^n = z^n$) over quadratic number fields by Alexander Aigner (for $n = 3, 6, 9$), Daniel Christy ($n = 4$) and Paul Rivoire (for certain prime values of n and quadratic imaginary number fields) among others.

6.1.1 Preliminary lemmas

In this section p will be a prime number greater than 2.

Lemma 6 *Let K be a number field with ring of integers $\mathcal{O}_K$ and discriminant D_K. If $\gcd(p, D_K) = 1$ then the ring of integers of $L = K(\zeta_p)$ is the ring $\mathcal{O}_L = \mathcal{O}_K[\zeta_p]$.*

PROOF. The result is a corollary of [22, Ch. III, Prop. 17], which says that if F and M are two number fields such that their (absolute) discriminants are relatively prime then $\mathcal{O}_{FM} = \mathcal{O}_F\mathcal{O}_M$. Since the discriminant of $\mathbb{Q}(\zeta_p)$ is a power of p (in absolute value), the ring of integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$ and by assumption $\gcd(p, D_K) = 1$, it follows that $\mathcal{O}_L = \mathcal{O}_K \cdot \mathbb{Z}[\zeta_p] = \mathcal{O}_K[\zeta_p]$, as claimed. ■

Lemma 7 *Let K be a totally real field. Then the only roots of unity in $K(\zeta_p)$ are of the form $\pm\zeta_p^a$ for some $0 \leq a < p$.*

PROOF. Let K, p and ζ_p be as in the statement of the lemma and put $L = K(\zeta_p)$. Suppose that q is prime and $F = K(\zeta_q) \subseteq K(\zeta_p) = L$. Notice that since K is totally real then the only roots of unity already in K are ± 1, thus $K \subsetneq F$ and $[F : K] = n > 1$. Moreover, the extension F/K is totally ramified at the primes of K above q. However, L/K is also totally ramified at the primes of K above p and by assumption $K \subsetneq F \subseteq L$. Therefore $p = q$ which concludes the proof. ■

Lemma 8 ([47, p. 4, 39]) *If α is an algebraic integer all of whose conjugates have absolute value 1, then α is a root of unity. In particular, if K is a totally real number field and ϵ is an algebraic unit in $K(\zeta_p)$ then $\epsilon/\bar{\epsilon}$ is an algebraic integer of absolute value 1, hence a root of unity.*

Theorem 30 ([47, p. 40]) *Let L be a CM-field and let E be its unit group. Let E^+ be the unit group of L^+ and let W be the group of roots of unity in L. Then $Q = [E : WE^+] = 1$ or 2.*

Notice that if K is totally real then, for all primes $p > 2$, the field $L = K(\zeta_p)$ is a CM-field.

Lemma 9 (cf. [47, Prop. 1.5]) *Let K be a totally real number field such that $\gcd(p, D_K) = 1$. Let $L = K(\zeta_p)$ and also denote the maximal real subfield of L by $L^+ = K(\zeta_p + \zeta_p^{-1})$. Let E and E^+ be the unit groups of L and L^+ respectively. Then $[E : \mu_p E^+] = 1$.*

PROOF. Let $\epsilon \in E$ be a unit of L. By Lemma 8, the quotient $\alpha = \epsilon/\bar{\epsilon}$ is a root of unity of L and, by Lemma 7, $\alpha = \pm\zeta_p^a$ for some $a \in \mathbb{Z}$.

Suppose first that $\alpha = \epsilon/\bar{\epsilon} = -\zeta_p^a$. By Lemma 6 we can write

$$\epsilon = b_0 + b_1\zeta_p + \cdots + b_{p-2}\zeta_p^{p-2}, \quad \bar{\epsilon} = b_0 + b_1\zeta_p^{-1} + \cdots + b_{p-2}\zeta_p^{-(p-2)}$$

with $b_i \in \mathcal{O}_K$ (notice that the expression for $\bar{\epsilon}$ is valid because K is totally real, therefore $\bar{b} = b$ for all $b \in K$). Thus $\epsilon \equiv \bar{\epsilon} \equiv b_0 + b_1 + \cdots + b_{p-2} \mod (1-\zeta_p)$. On the other hand $\epsilon = -\zeta_p^a\bar{\epsilon} \equiv -\bar{\epsilon} \mod (1-\zeta_p)$. Thus $2\bar{\epsilon} \equiv 0 \mod (1-\zeta_p)$, or equivalently, $2\bar{\epsilon} \in (1-\zeta_p)$. However, since $\bar{\epsilon}$ is a unit the latter inclusion implies that 2 is in the ideal $(1-\zeta_p)$ but this is impossible because $p > 2$ and the only prime ideals dividing $(1-\zeta_p)$ lay above the prime $p \neq 2$.

Therefore $\epsilon/\bar{\epsilon} = +\zeta_p^a$. Let $2r \equiv a \mod p$ and put $\epsilon_1 = \zeta_p^{-r}\epsilon$. Thus $\epsilon = \zeta_p^r\epsilon_1$ and $\bar{\epsilon_1} = \epsilon_1$. ■

Lemma 10 *Let K be a totally real number field with $\gcd(D_K, p) = 1$, $L = K(\zeta_p)$ and let $\alpha \in \mathcal{O}_L$. Then α^p is congruent modulo p to an integer in $\mathcal{O}_K$.*

PROOF. By Lemma 6, we can write $\alpha = b_0 + b_1\zeta_p + \cdots + b_{p-2}\zeta_p^{p-2}$. Then $\alpha^p \equiv b_0^p + b_1^p + \cdots + b_{p-2}^p \mod p$, which proves the lemma. ■

Lemma 11 *Let $p \geq 5$ be prime, let K be a totally real number field of class number 1 and let x, y, z be pairwise relatively prime elements of $\mathcal{O}_K$ such that $x^p + y^p = z^p$ and $\gcd(xyz, p) = 1$. Then the ideals $(x + \zeta_p^i y) \subsetneq \mathcal{O}_K[\zeta_p]$, $i = 0, 1, \ldots, p-1$, are pairwise relatively prime.*

PROOF. Suppose $\wp$ is a prime ideal of $\mathcal{O}_L = \mathcal{O}_K[\zeta_p]$ such that $\wp$ divides the ideals $(x+\zeta_p^i y)$ and $(x+\zeta_p^j y)$ where $i \neq j$. Then $\wp$ divides $(\zeta_p^i y - \zeta_p^j y) = (\text{unit})(1-\zeta_p)y$, thus $\wp$ divides $(1-\zeta_p)$ or y. The prime ideal $\wp$ also divides $\zeta_p^j x - \zeta_p^i x = (\text{unit})(1-\zeta_p)x$ so $\wp$ divides $(1-\zeta_p)$ or x. If $\wp$ does not divide $(1-\zeta_p)$ then, if $\widehat{\wp} = (\omega)$ is the prime of K lying below $\wp$ (we assumed that the field K is a PID) then ω divides both x and y, in contradiction with the assumption that x and y are relatively prime.

Therefore $\wp$ divides the ideal $(1-\zeta_p)$ and the rational prime below $\wp$ is p. Notice that $x + y \equiv x + \zeta_p^i y \mod (1-\zeta_p)$ implies the same congruence modulo $\wp$. Also, by assumption, $x + \zeta_p^i y \equiv 0 \mod \wp$. Moreover, since $x + y \in \mathcal{O}_K$ then $x + y \equiv 0 \mod \widehat{\wp}$. But $z^p = x^p + y^p \equiv x + y \mod p$, together with the fact that the rational prime below $\wp$ must be p, implies that $z^p \equiv 0 \mod \widehat{\wp}$ and so $\widehat{\wp}$ divides z, which contradicts $\gcd(xyz, p) = 1$. ■

Lemma 12 *Let K be totally real and of class number 1 such that $\gcd(p, D_K) = 1$. Let $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$ with $a_i \in \mathcal{O}_K$ and at least one $a_i = 0$. Let $\wp = (\omega)$ be a prime of K lying above p. If ω divides α then ω divides each a_j.*

PROOF. By Lemma 6, the ring of integers of $L = K(\zeta_p)$ is $\mathcal{O}_K[\zeta_p]$. Since $1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$ any subset of $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$ with $p-1$ distinct elements is a basis of the $\mathcal{O}_K$-module $\mathcal{O}_K[\zeta_p]$. Since at least one a_j is zero, the other a_j's give the coefficients with respect to a basis. The statement follows. ■

6.1.2 The proof of the first case

Theorem 31 *Let K be a totally real number field of class number 1 and such that $\gcd(D_K, p) = 1$. Let $p \geq 5$ be a prime which does not divide the class number of $L = K(\zeta_p)$. Then:*

$$x^p + y^p = z^p, \quad \gcd(xyz, p) = 1$$

has no solutions in $\mathcal{O}_K$.

PROOF. Let p, K be as in the statement of the theorem and suppose for a contradiction that there exist $x, y, z \in \mathcal{O}_K$ such that $x^p + y^p = z^p$ and $\gcd(xyz, p) = 1$. Notice that $x \equiv y \equiv -z \mod p\mathcal{O}_K$ is impossible (because $3z^p \equiv 0 \mod p\mathcal{O}_K$ and $p > 3$ implies that $\gcd(z, p) \neq 1$). Thus, by renaming the variables if necessary, we may assume $x \neq y \mod p\mathcal{O}_K$.

From the equation $x^p + y^p = z^p$ follows that there is an equality of ideals of L:

$$\prod_{i=0}^{p-1}(x + \zeta_p^i y) = (z)^p.$$

By Lemma 11 the ideals $(x + \zeta_p^i y)$ are pairwise relatively prime, thus, each one must be the pth power of an ideal $(x + \zeta_p^i y) = A_i^p$. Since A_i^p is principal and p does not divide the class number of L it follows that $A_i = (\alpha_i)$ is principal. Consequently $x + \zeta_p^i y = (\text{unit})\alpha_i^p$. In particular, $x + \zeta_p y = \epsilon\alpha^p$ for some unit ϵ. By Lemma 9, there exists ϵ_1 such that $\epsilon = \zeta_p^r \epsilon_1$ and $\bar{\epsilon_1} = \epsilon_1$. By Lemma 10 there is an algebraic integer $a \in \mathcal{O}_K$ such that $\alpha^p \equiv a \mod p$. Thus:

$$x + \zeta_p y = \zeta_p^r \epsilon_1 \alpha^p \equiv \zeta_p^r \epsilon_1 a^p \mod p \quad \text{and} \quad x + \zeta_p^{-1} y = \zeta_p^{-r} \bar{\epsilon_1} \bar{\alpha}^p \equiv \zeta_p^{-r} \epsilon_1 a^p \mod p$$

since x, y, a, p are equal to their complex conjugates. Hence $\zeta_p^{-r}(x + \zeta_p y) \equiv \zeta_p^r(x + \zeta_p^{-1} y) \mod p$ or $x + \zeta_p y - \zeta_p^{2r-1} y - \zeta_p^{2r} x \equiv 0 \mod p$. Let $\wp$ be a prime of K lying above p. Then $x + \zeta_p y - \zeta_p^{2r-1} y - \zeta_p^{2r} x \equiv 0 \mod \wp$. If $1, \zeta_p, \zeta_p^{2r-1}, \zeta_p^{2r}$ are all distinct then Lemma 12 implies that $\wp$ divides x and y, in direct contradiction with $\gcd(xyz, p) = 1$. Thus, they are not distinct. Clearly $1 \neq \zeta_p$ and $\zeta_p^{2r-1} \neq \zeta_p^{2r}$. All other three cases ($1 = \zeta_p^{2r}$, $1 = \zeta_p^{2r-1}$ and $\zeta_p = \zeta_p^{2r-1}$) yield contradictions with Lemma 12 and $\gcd(xyz, p) = 1$ (see [47, p. 6]). ■

In section 6.2 we will provide some examples of real quadratic number fields where the hypothesis of the theorem (and those of Greenberg's theorem 15) are satisfied.

6.1.3 The second case

As we mentioned earlier, the second case of Fermat's last theorem (over $\mathbb{Q}$), i.e. the case $\gcd(xyz, p) \neq 1$, is much more difficult than the first case (the full proof can be found in [47, Chapter 9]). A more refined use of the units in cyclotomic extensions is needed. Moreover, the proof also requires the following famous theorem, due to Kummer:

Theorem 32 (Kummer's Lemma, [47]) *Let p be a regular prime and let η be a unit in $\mathbb{Q}(\zeta_p)$. If η is congruent to an integer $n \in \mathbb{Z}$ modulo p then η is the pth power of a unit of $\mathbb{Q}(\zeta_p)$.*

It does not seem to be known whether the second case of Fermat's last theorem holds for totally real number fields of class number 1. Kummer's Lemma has been generalized to totally real number fields by Ozaki [30]. However, Ozaki's theorem does not seem strong enough in order to provide a direct generalization of the argument given in the the proof of Fermat's last theorem over $\mathbb{Q}$.

6.2 Examples of regular primes for totally real number fields

In this section we intend to illustrate the theory with several examples of regular (and irregular) primes, which provide examples for Theorem 15 and Theorem 31.

An extensive list of irregular primes over $\mathbb{Q}$ can be found, for example, in [47] (where one can find all irregular primes $p \leq 4001$). The first few irregular primes are: 37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293, ... Examples of regular and irregular primes for quadratic imaginary number fields, in the sense of Robert (Theorem 18) can be found in [36, Appendix B].

Let K be a real quadratic number field of discriminant D_K and let $\zeta_K(s)$ be the Dedekind zeta function of K. As long as $\gcd(p, D_K) = 1$ one has $[K(\zeta_p) : K] = p - 1$. In Table 2 we list 18 discriminants

Table 2. Examples of irregular primes

D_K	h_K	Primes $p \leq 150$, p divides numerator of $p \cdot \prod_{\substack{i=2 \\ i \text{ even}}}^{p-1} \zeta_K(1-i)$
5	1	17, 19, 37, 41, 59, 61, 67, 73, 101, 103, 107, 127, 131, 137, 139, 149
8	1	11, 13, 19, 37, 59, 67, 71, 79, 89, 101, 103, 107, 127, 131, 149
12	1	11, 13, 23, 37, 41, 43, 47, 59, 61, 67, 83, 101, 103, 113, 127, 131, 137, 139, 149
13	1	29, 31, 37, 43, 47, 53, 59, 61, 67, 79, 83, 97, 101, 103, 107, 109, 127, 131, 149
17	1	19, 23, 37, 41, 47, 59, 61, 67, 71, 97, 101, 103, 109, 131, 139, 149
21	1	7, 11, 31, 37, 59, 67, 73, 79, 83, 101, 103, 107, 109, 113, 127, 131, 149
40	2	7, 19, 37, 53, 59, 61, 67, 71, 73, 79, 83, 101, 103, 127, 131, 149
60	2	19, 23, 37, 47, 59, 61, 67, 71, 73, 83, 97, 101, 103, 127, 131, 137, 149
65	2	19, 37, 43, 59, 67, 79, 83, 89, 101, 103, 107, 131, 137, 149
85	2	3, 17, 31, 37, 41, 59, 61, 67, 79, 101, 103, 109, 127, 131, 149
104	2	5, 13, 19, 31, 37, 53, 59, 67, 73, 101, 103, 107, 109, 113, 131, 149
105	2	3, 11, 31, 37, 41, 59, 67, 73, 83, 97, 101, 103, 107, 127, 131, 137, 149
229	3	3, 13, 29, 37, 59, 67, 101, 103, 107, 127, 131, 137, 139, 149
257	3	5, 17, 19, 37, 59, 67, 89, 101, 103, 107, 113, 131, 139, 149
316	3	7, 17, 23, 37, 47, 59, 61, 67, 73, 79, 89, 97, 101, 103, 109, 127, 131, 137, 149
321	3	3, 11, 37, 41, 59, 67, 79, 97, 101, 103, 109, 131, 137, 149
469	3	5, 11, 17, 37, 59, 67, 71, 89, 97, 101, 103, 113, 131, 137, 149
473	3	3, 11, 17, 31, 37, 43, 47, 59, 67, 73, 79, 83, 101, 103, 107, 113, 127, 131, 139, 149.

(the first 6 discriminants of class number h for $h = 1, 2, 3$), the class number h_K of K and primes p which divide the numerator of

$$p \cdot \prod_{\substack{i=2 \\ i \text{ even}}}^{p-1} \zeta_K(1-i).$$

Notice that the values of $\zeta_K(s)$ at negative integers can be easily computed in this case using Theorem 3 and Theorem 7 in this article.

6.3 Applications of elliptic units

The theory of elliptic units has proved to be an essential tool in number theory, being one of the fundamental ingredients in some major developments of the last decades. Some of the most important conjectures in arithmetic geometry have been solved in the particular case of quadratic imaginary fields and CM curves using the theory briefly described above. Here we will only mention two important results which rely on elliptic units: the Birch and Swinnerton-Dyer conjecture for CM elliptic curves and the "main conjectures" of Iwasawa theory.

Extending their methods (which allowed them to prove Theorem 26), Coates and Wiles were able to show in [5] a particular case of the Birch and Swinnerton-Dyer conjecture: if an elliptic curve $A/\mathbb{Q}$ has complex multiplication and $A(\mathbb{Q})$ is infinite then the Hasse-Weil L-function of $A/\mathbb{Q}$ vanishes at $s = 1$, i.e. $L(1, A/\mathbb{Q}) = 0$. Moreover, their methods also led to a precise statement of the so-called one-variable "main conjecture" for imaginary quadratic fields.

Later on, Rubin proved in [37] the one-variable and two-variable "main conjectures" of Iwasawa theory for quadratic imaginary fields, again relying on the theory of elliptic units and complex multiplication. More recently, Pollack and Rubin [31], building on Rubin's work, have been able to show the "main conjecture" for CM elliptic curves at supersingular primes. In particular, as a corollary it follows another piece of the

Birch and Swinnerton-Dyer conjecture: if $A/\mathbb{Q}$ is a CM elliptic curve and $L(1, A/\mathbb{Q}) \neq 0$ then $A(\mathbb{Q})$ is finite and the Tate-Shafarevich group of A is also finite, and of order as predicted by the BS-D conjecture.

Finally, we would like to point out that in a very recent article Darmon and Dasgupta [8] have been able to construct elliptic units over real quadratic number fields, which may have many interesting arithmetic applications similar to those of the elliptic units in the imaginary case.

Acknowledgement. The author would like to thank the participants of the number theory seminar at Cornell University, especially Henri Johnston, Jason Martin and Damiano Testa, for helping to shape this survey into what it is. I am also thankful to Pilar Bayer, Ravi Ramakrishna, David Rohrlich and Larry Washington for several interesting suggestions, comments and corrections.

References

[1] Boxall, J. L., (1986). A new construction of p-adic L-functions attached to certain elliptic curves with complex multiplication, *Ann. Inst. Fourier*, (Grenoble) **36**, 4,31–68.

[2] Carlitz, L., (1968), Bernoulli Numbers, *Fib. Quart.*, **6**, 71–85.

[3] Coates, J. and Goldstein, C., (1983). Some remarks on the main conjecture for elliptic curves with complex multiplication, *Amer. J. Math.*, **105**, 337–366.

[4] Coates, J. and Wiles, A., (1977). Kummer's criterion for Hurwitz numbers, *Algebraic number theory*, (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto), S. Iyanaga (Ed.), 9–23.

[5] Coates, J. and Wiles, A., (1977). On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.*, **39**, 3, 223–251.

[6] Coates, J. and Wiles, A., (1978). On p-adic L-functions and Elliptic Units, *J. Austral. Math. Soc., ser. A*, **26**, 1–25.

[7] Damerell, R. M., (1970-71). L-functions of elliptic curves with complex multiplication, I and II, *Acta Arith.*, **XVII** and **XIX**.

[8] Darmon, H. and Dasgupta, S., (2006). Elliptic units for real quadratic fields, *Ann. of Math.* (2), **163**, 1, 301–346.

[9] De Shalit, E., (1984), Ph. D. Thesis, Princeton University.

[10] Greenberg, R., (1973). A Generalization of Kummer's Criterion, *Invent. Math.*, **21**, 247–254.

[11] Guo, L., (1993). General Selmer Groups and Critical Values of Hecke L-functions, *Math. Ann.*, **197**, 221–233.

[12] Herbrand, J., (1932). Sur les classes des corps circulaires, *J. Math. Pures et Appliquées*, 9^e série **11**, 417–441.

[13] Hurwitz, A., (1899). Über die Entwicklungskoeffitizienten der lemniscatischen Functionen, *Math. Ann.*, **51**, 196–226.

[14] Katz, N., (1975). The Congruences of Clausen - von Staudt and Kummer for Bernoulli-Hurwitz numbers, *Math. Ann.*, **216**, 1–4.

[15] Katz, N., (1977), The Eisenstein measure and p-adic interpolation, *Amer. J. of Math.*, **99**, 238–311.

[16] Katz, N., (1976). p-adic interpolation of real analytic Eisenstein series, *Ann. of Math.*, **104**, 459–571.

[17] Kida, M., (1991). Kummer's criterion for totally real number fields, *Tokyo J. Math.*, **14**, 2, 309–317.

[18] Klingen, H., (1961/1962). Über die Werte der Dedekindschen Zetafunktion, *Math. Ann.*, **145**, 265–272.

[19] Kubota, T. and Leopoldt, H. W., (1964). Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-funktionen, *J. reine angew. Math.*, **214/215**, 328–339.

[20] Kubert, D. S. and Lang, S., (1981). *Modular Units*, Grundlehren der Mathematischen Wissenschaften, **244**, Springer-Verlag, New York.

[21] Lang, S., (1987). *Elliptic Functions*, 2nd Edition, Springer-Verlag, New York.

[22] Lang, S., (1994). *Algebraic Number Theory*, 2nd Edition Springer-Verlag, New York.

[23] Lehmer, D. H., (1935). Lacunary Recurrences for the Bernoulli Numbers, *Ann. Math.*, **36**, 637–649.

[24] Lichtenbaum, S., (1980). On p-adic L-functions Associated to Elliptic Curves, *Invent. Math.*, **56**, 19–55.

[25] Lozano-Robledo, A., (2006). On elliptic units and p-adic Galois representations attached to elliptic curves, *J. Number Theory*, **117**, issue 2, 439–470.

[26] Manin, J. and Vishik, M. M., (1974). p-adic Hecke series of imaginary quadratic fields, *Math. USSR Sbornik*, **24**, 345–371.

[27] Meyer, C., (1957). *Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkörpern*, Akademie-Verlag, Berlin.

[28] Novikov, A. P., (1969). Sur la régularité des idéaux premiers de degré un d'un corps quadratique imaginaire, *Isv. Akad. Nauk S.S.S.R.*, **33**, 1059–1079; *Math. of U.S.S.R. Isv.*, **3**, 1001–1018.

[29] Odlyzko, A. M., (1990). Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results, *Sém. Théor. Nombres Bordeaux (2)*, **2**,1, 119–141.

[30] Ozaki, M., (1997). Kummer's lemma for $\mathbb{Z}_p$-extensions over totally real number fields, *Acta Arith.*, **LXXXI**, 1.

[31] Pollack, R. and Rubin, K., (2004). The main conjecture for CM elliptic curves at supersingular primes, *Ann. of Math. (2)*, **159**, Issue 1, 447–464.

[32] Ramachandra, K., (1964). Some Applications of Kronecker's Limit Formulas, *Ann. of Math. (2)*, **80**, Issue 1, 104–148.

[33] Ribet, K., (1976). A Modular Construction of Unramified p-Extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.*, **334**, 151–162.

[34] Robert, G., (1973). Unités Elliptiques, *Bull. Soc. Math. France*, Mém. No. **36**, Tome 101. Société Mathématique de France, Paris.

[35] Robert, G., (1974). Régularité des idéaux premiers d'un corps quadratique imaginaire de nombre de classes un, Astérisque, t. 24–25; *J. Arith. de Bordeaux*, 75–80.

[36] Robert, G., (1978). Nombres de Hurwitz et Unités Elliptiques, *Ann. scient. Éc. Norm. Sup., 4^e série*, **11**, 297–389.

[37] Rubin, K., (1991). The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.*, **103**, 1, 25–68.

[38] Saito, H., (1987). Elliptic Units and a Kummer's Criterion for Imaginary Quadratic Fields, *J. Number Theory*, **25**, 53–71.

[39] Serre, J-P., (1973). Formes modulaires et fonctions zeta p-adiques, *Modular functions of one variable, III*, (Proc. Internat. Summer School, Univ. Antwerp, 1972), 191–268. Lecture Notes in Math., **350**, Springer, Berlin.

[40] Siegel, C. L., (1961). *Lectures on Advanced Analytic Number Theory*, Tata Institute Lecture Notes.

[41] Siegel, C. L., (1937). Über die analytische Theorie der quadratischen Formen. III, *Ann. of Math. (2)*, **38**, 1, 212–291.

[42] Silverman, J. H., (1985). *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York.

[43] Silverman, J. H., (1994). *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York.

[44] Yager, R. I., (1982). A Kummer criterion for imaginary quadratic fields, *Compositio Math.*, **47**, 1, 31–42.

[45] Yager, R. I., (1982). On two variable p-adic L-functions, *Ann. of Math.*, **115**, 411–449.

[46] Yager, R. I., (1984). p-adic measures on Galois groups, *Invent. Math.*, **76**, 331–343.

[47] Washington, L. C., (1983). *Introduction to Cyclotomic Fields*, Second Edition, Springer-Verlag, New York.

[48] Washington, L. C., (1976). A note on p-adic L-functions, *J. Number Theory*, **8**, 245–250.

Álvaro Lozano-Robledo
Dept. of Mathematics,
584 Malott Hall,
Cornell University, Ithaca,
NY 14853.