JOURNAL OF NUMBER THEORY 37, 100-121 (1991)

Computation of Iwasawa Lambda Invariants for Imaginary Quadratic Fields

D. S. DUMMIT,* D. FORD,[†] H. KISILEVSKY,[†] AND J. W. SANDS[‡]

Department of Mathematics and Statistics, University of Vermont,
Burlington, Vermont 05405

Communicated by W. Sinnott

Received October 1, 1989; revised February 6, 1990

A method for computing the Iwasawa lambda invariants of an imaginary quadratic field is developed and used to construct a table of these invariants for discriminants up to 1,000 and primes up to 20,000. © 1991 Academic Press, Inc.

INTRODUCTION

Iwasawa theory originated in the study of class numbers in the basic $\mathbb{Z}_p$-extension of a number field K, and this case still occupies a central place in the theory. After fixing a prime number p, begin with $\mathbb{Q}_\infty$, the Galois extension of the rational numbers $\mathbb{Q}$ having Galois group isomorphic to the additive group of the p-adic integers $\mathbb{Z}_p$. Then let K_n denote the unique field having degree p^n over K in $K \cdot \mathbb{Q}_\infty$. Iwasawa [11] proved that the exact power of p dividing the class number $h(K_n)$ is given by $\mu p^n + \lambda n + \nu$, for large n. The integer constants $\mu = \mu_p$, $\lambda = \lambda_p$, and $\nu = \nu_p$ are the Iwasawa invariants for K and p. The simplest nontrivial example occurs when K is a quadratic field. Then $\mu = 0$ [4] and when K is real, it is believed that $\lambda = 0$. Hence imaginary quadratic fields should provide a basis for the understanding of lambda invariants. However, even in this key situation, the values of lambda invariants have remained a mystery.

In this paper we describe a method of computation and provide a sizeable table of Iwasawa lambda invariants for imaginary quadratic fields. Our point of view is to consider λ_p as p varies and the base field K remains fixed. With our method (and also our access to extensive computer time), we are able to obtain λ_p for primes much larger than have been considered

* Research partially supported by NSF Vermont EPSCoR Grant RII-8610679.

[†] Research partially supported by grants from NSERC and FCAR.

[‡] Research partially supported by NSF Vermont EPSCoR Grant RII-8610679 and a University of Vermont Faculty Summer Research Fellowship.

0022-314X/91 $3.00

previously. For small primes, our results are seen to agree with those of Gold [7] and Ernvall–Metsänkylä [15]. The computations make use of p-adic L-functions, but are greatly accelerated by implementing a strictly algebraic criterion for triviality of Gold [6]. In implementing this criterion, we also describe a technique for obtaining generators of certain principal ideals in imaginary quadratic fields.

Our table of primes having a nontrivial lambda invariant is complete for discriminants up to 1,000 and primes up to 10,000,000. The actual value of the lambda invariant is computed for primes up to 20,000.

We thank Tauno Metsänkylä for his comments and Stephen J. Cavrak of the University of Vermont Academic Computing Center for his help with Pascal compilers.

I. Power Series for Leopoldt–Kubota P-Adic L-Functions

We first adapt the method of Ferrero and Greenberg [3] to compute the coefficients in the Iwasawa power series for a Leopoldt–Kubota p-adic L-function. In [3], the first coefficient was computed this way, and modifications of this approach also appear in [18, 15].

Fix an odd prime p and an embedding of the complex numbers $\mathbb{C}$ in the completion $\mathbb{C}_p$ of an algebraic closure of the p-adic field $\mathbb{Q}_p$. Let ω be the Teichmüller character modulo p. A nontrivial primitive Dirichlet character of the first kind with conductor $d \neq p$ may be written as $\psi\omega^{r+1}$, where ψ is a primitive Dirichlet character of conductor $d_0 \neq 1$ prime to p, and $r < p-1$ is a nonnegative integer. Let $\mathbb{Q}_p(\psi)$ denote the field obtained by adjoining all the values of ψ to $\mathbb{Q}_p$, and denote its ring of integers by $\mathcal{O}_\psi$. Note that $\mathcal{O}_{\psi\omega^{r+1}} = \mathcal{O}_\psi$, since $\mathbb{Q}_p(\omega) = \mathbb{Q}_p$. If ρ is a (possibly trivial) primitive character of the second kind, then we may fix $n \geqslant 0$ so that $\rho^{p^n} = 1$. Observe that the character $\psi\omega^{r+1}\rho$ is primitive with conductor dividing $d_0 p^{n+1}$. Set $u = \exp_p(p) = 1 + p + p^2/2! + \cdots$ in $\mathbb{Z}_p$. View ρ as a character on $\mathbb{Z}_p$ and put $\zeta_\rho = \rho(u)$, so that $\zeta_\rho^{p^n} = 1$.

Under these assumptions [16], the p-adic L-function $L_p(s, \psi\omega^{r+1})$ is associated with a power series

$$G(T, \psi\omega^{r+1}) = \sum_{m=0}^{\infty} a_m T^m$$

having coefficients in $\mathcal{O}_\psi$, such that

$$L_p(s, \psi\omega^{r+1}\rho) = G(\zeta_\rho^{-1} u^s - 1, \psi\omega^{r+1}).$$

The polynomial $\omega_n(T) = (1+T)^{p^n} - 1$ satisfies

$$\omega_n \equiv 0 \quad (\operatorname{mod}(T^p, p^n)) \quad \text{and} \quad \omega_n \equiv 0 \quad (\operatorname{mod}(T^{p^2}, p^{n-1})).$$

The fact that ω_n is distinguished allows one to write

$$G(T, \psi\omega^{r+1}) = F_n(T) + \omega_n(T)\, H_n(T),$$

where

$$F_n(T) = \sum_{k=0}^{p^n-1} b_k(1+T)^k$$

is a polynomial of degree less than p^n with coefficients b_k in $\mathcal{O}_\psi$. From the congruence

$$\begin{aligned}\sum_{m=0}^{\infty} a_m T^m = G(T, \psi\omega^{r+1}) &\equiv F_n(T)\\ &= \sum_{k=0}^{p^n-1} b_k(1+T)^k = \sum_{k=0}^{p^n-1} b_k\left(\sum_{m=0}^{k}\binom{k}{m} T^m\right)\\ &= \sum_{m=0}^{p^n-1}\left(\sum_{k=m}^{p^n-1} b_k\binom{k}{m}\right) T^m \qquad (\mathrm{mod}\ \omega_n(T)),\end{aligned}$$

we obtain

$$a_m \equiv \sum_{k=m}^{p^n-1} b_k\binom{k}{m} \qquad (\mathrm{mod}\ p^n) \quad (\text{when } m < p)$$

$$a_m \equiv \sum_{k=m}^{p^n-1} b_k\binom{k}{m} \qquad (\mathrm{mod}\ p^{n-1}) \quad (\text{when } m < p^2).$$

Substitution of $T = \zeta_p^{-1} - 1$ and $s = 0$ in the above formulas is valid. Combined with the interpolation property for p-adic L-functions and the evaluation of a Dirichlet L-function at zero via generalized Bernoulli numbers [18, Chaps. 4, 5], this yields

$$\begin{aligned}\sum_{k=0}^{p^n-1} b_k\zeta_p^{-k} &= F_n(\zeta_p^{-1} - 1) = G(\zeta_p^{-1} - 1, \psi\omega^{r+1})\\ &= L_p(0, \psi\omega^{r+1}\rho) = (1 - (\psi\omega^r\rho)(p))\, L(0, \psi\omega^r\rho)\\ &= \frac{-1}{d_0 p^{n+1}} \sum_{i=1,(i,p)=1}^{d_0 p^{n+1}} i\psi\omega^r\rho(i)\\ &= \frac{-1}{d_0 p^{n+1}} \sum_{i=1,(i,p)=1}^{p^{n+1}} \sum_{j=0}^{d_0-1} (i + jp^{n+1})\,\psi(i + jp^{n+1})\,\omega^r\rho(i)\\ &= \frac{-1}{d_0 p^{n+1}} \sum_{i=1,(i,p)=1}^{p^{n+1}} \sum_{j=0}^{d_0-1} jp^{n+1}\psi(i + jp^{n+1})\,\omega^r\rho(i)\\ &= \frac{-1}{d_0} \sum_{i=1,(i,p)=1}^{p^{n+1}} \sum_{j=0}^{d_0-1} j\psi\omega^r(i + jp^{n+1})\,\rho(i).\end{aligned}$$

We have made the assumption that ψ is primitive with conductor $d_0 \neq 1$ precisely so that the sum $\sum_{j=0}^{d_0-1} i\psi(i+jp^{n+1})\,\omega^r\rho(i)$ will vanish here.

For $(i, p)=1$ define $\langle i\rangle = i\omega^{-1}(i)$. Then $\log_p(i)=\log_p(\langle i\rangle)$, where the latter is defined by the usual p-adic power series. Also define $L(i)$ by $0 \geqslant L(i) > -p^n$, $L(i) \equiv \log_p(i)/p \pmod{p^n}$.

(1.1) LEMMA. *If $L(i) = -k$ then $\rho(i)=\zeta_\rho^{-k}$.*

Proof.

$$\begin{aligned} L(i) = -k &\Rightarrow \log_p(i) \equiv -kp \qquad \pmod{p^{n+1}} \\ &\Rightarrow \langle i\rangle \equiv \exp(-kp) = \exp(p)^{-k} = u^{-k} \qquad \pmod{p^{n+1}} \\ &\Rightarrow \rho(i) = \rho(\langle i\rangle) = \rho(u^{-k}) = \rho(u)^{-k} = \zeta_\rho^{-k}. \end{aligned}$$

The lemma allows us to rewrite the sum we have arrived at, and obtain

$$\sum_{k=0}^{p^n-1} b_k \zeta_\rho^{-k} = \frac{-1}{d_0} \sum_{k=0}^{p^n-1} \left(\sum_{i \leqslant i \leqslant p^{n+1}, (i,p)=1, L(i)=-k} \; \sum_{j=0}^{d_0-1} j\psi\omega^r(i+jp^{n+1}) \right) \zeta_\rho^{-k}.$$

This equation holds for each of the p^n distinct characters ρ of order dividing p^n, hence it holds whenever ζ_ρ is a p^nth root of unity. Thus we have a system of equations for the b_k. The coefficients form a Vandermonde matrix with nonzero determinant, and we conclude that

$$b_k = \frac{-1}{d_0} \sum_{1 \leqslant i \leqslant p^{n+1}, (i,p)=1, L(i)=-k} \; \sum_{j=0}^{d_0-1} j\psi\omega^r(i+jp^{n+1}).$$

Substituting this expression for b_k into the congruences for a_m results in the following. When $m > k$, we let $\binom{k}{m}=0$.

(1.2) THEOREM.

$$\begin{aligned} a_m \equiv \frac{-1}{d_0} &\sum_{i=1,(i,p)=1}^{p^{n+1}} \binom{-L(i)}{m} \\ &\times \sum_{j=0}^{d_0-1} j\psi\omega^r(i+jp^{n+1}) \qquad \pmod{p^n}(\text{for } m < p) \\ a_m \equiv \frac{-1}{d_0} &\sum_{i=1,(i,p)=1}^{p^{n+1}} \binom{-L(i)}{m} \\ &\times \sum_{j=0}^{d_0-1} j\psi\omega^r(i+jp^{n+1}) \qquad \pmod{p^{n-1}}(\text{for } m < p^2) \end{aligned}$$

II. The P-Adic Logarithm

We now compute $\log_p(i)$ (mod p^3).

Fix i with $(i, p) = 1$, and let $\langle i \rangle = 1 + jp$. Then $i^{p-1} = \langle i \rangle^{p-1} \equiv 1 - jp$ (mod p^2). Define l by $i^{p-1} = 1 - jp + lp^2$. Thus

$$i^{p-1} = \langle i \rangle^{p-1} = (1 + jp)^{p-1} = [1 + (1 - i^{p-1} + lp^2)]^{p-1},$$

and

$$i^{p-1} \equiv 1 + (p-1)(1 - i^{p-1}) - lp^2 + (1 - i^{p-1})^2 \qquad (\text{mod } p^3).$$

We conclude that

$$\begin{aligned} lp^2 &\equiv (1 - i^{p-1})(1 - i^{p-1} + p), \\ jp &\equiv (1 - i^{p-1})(2 - i^{p-1} + p) \qquad (\text{mod } p^3). \end{aligned}$$

In the last expression, note that $2 - i^{p-1} + p \equiv 1$ (mod p). So

$$\begin{aligned} \log_p(i) = \log_p(\langle i \rangle) = \log_p(1 + jp) &\equiv jp - \frac{(jp)^2}{2} \\ &\equiv (1 - i^{p-1})(2 - i^{p-1} + p) - \frac{(1 - i^{p-1})^2}{2} \\ &= (1 - i^{p-1})\left(2 - i^{p-1} + p - \frac{1}{2}(1 - i^{p-1})\right) \qquad (\text{mod } p^3). \end{aligned}$$

The computation is completed by combining terms. We replace the fraction $\frac{1}{2}$ by $(1 - p^2)/2$ to maintain integrality for computations; this suffices since $1 - i^{p-1} \equiv 0$ (mod p).

(2.1) Proposition. $\log_p(i) \equiv ((1 - p^2)/2)(1 - i^{p-1})(3 - i^{p-1} + 2p)$ (mod p^3).

III. The Iwasawa Lambda Invariant of a Power Series

Suppose K_P is a finite algebraic extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$, and let π be a uniformizing parameter for $\mathcal{O}$. A nonzero power series $H(T)$ with coefficients in $\mathcal{O}$ can be written in the form $\pi^\mu \sum_{m=0}^{\infty} c_m T^m$, with c_m

in $\mathcal{O}$ for each m and $c_m \not\equiv 0 \pmod{\pi}$ for some m. Then $\mu = \mu_p(H(T))$ is the Iwasawa μ-invariant of the power series. The Iwasawa λ-invariant $\lambda_p(H(T))$ of $H(T)$ is the smallest m such that $c_m \not\equiv 0 \pmod{\pi}$, i.e., such that c_m is a p-unit.

When $\psi\omega^{r+1}$ is odd (so $\psi\omega^r$ is even), one finds that $G(T, \psi\omega^{r+1}) = 0$. From now on, we assume that $\psi\omega^{r+1}$ is even. In this case, Ferrero and Washington [4] have shown that $\mu_p(G(T, \psi\omega^{r+1})) = 0$. We are interested in the invariant $\lambda_p(G(T, \psi\omega^{r+1}))$, also referred to as the λ-invariant of $L_p(s, \psi\omega^{r+1})$. Slightly modified definitions apply when one allows $d_0 = 1$. As usual, we extend the definition of the binomial coefficient $\binom{a}{m}$ to all $a \in \mathbb{Z}_p$ by $\binom{a}{m} = (a(a-1)\cdots(a-m+1)/m!)$.

(3.1) PROPOSITION. *If less than p^2, the Iwasawa λ-invariant of $L_p(s, \psi\omega^{r+1})$ is the smallest value of m such that the expression*

$$\sum_{l=1,(l,p)=1}^{p^2} \sum_{k=0}^{p-1} \binom{\left(\frac{p^2-1}{2}\right)\left(\frac{1-l^{p-2}(l-kp^2)}{p}\right)(3-l^{p-1}+2p)}{m}$$
$$\times \sum_{j=0}^{d_0-1} j\psi\omega^r(l+kp^2+jp^3)$$

is not congruent to $0 \pmod{\pi}$.

Proof. Let $n=2$ in Theorem 1.2. From Proposition 2.1, we have

$$-L(i) \equiv -\frac{\log_p(i)}{p} \equiv \left(\frac{p^2-1}{2}\right)\left(\frac{1-i^{p-1}}{p}\right)(3-i^{p-1}+2p) \pmod{p^2}.$$

Write each i uniquely as $i = l + kp^2$, with l and k in the ranges indicated and observe that $-L(l+kp^2) \equiv ((p^2-1)/2)((1-l^{p-2}(l-kp^2))/p)(3-l^{p-1}+2p) \pmod{p^2}$. Substitute this into the congruence of Theorem (1.2) for $m < p^2$, noting that the binomial coefficient is then unchanged modulo p. The result is that the expression in the statement of this proposition is congruent to $-d_0 a_m \pmod{p}$ when $m < p^2$. But $-d_0$ is a p-unit.

In our computations for imaginary quadratic fields, we have always found $m < p^2$. Indeed, usually $m < p$, so that the following proposition suffices.

(3.2) Proposition. *If less than p, the Iwasawa λ-invariant of $L_p(s, \psi\omega^{r+1})$ is the smallest value of m such that the expression*

$$\sum_{l=1}^{(p-1)/2} \sum_{k=0}^{p-1} \left(\frac{l^{p-2}(l-kp)-1}{p}\right)^{m} \sum_{j=0}^{d_0-1} j\psi\omega^r(l+kp+jp^2)$$

is not congruent to 0 (mod π).

Proof. This time we set $n=1$ in Theorem (1.2). When $m<p$, we can write $m!\binom{-L(i)}{m} = (-L(i))^m + \sum_{t=0}^{m-1} c_t(m)\binom{-L(i)}{t}$ with p-integral coefficients $c_t(m)$. Thus if $a_t \equiv 0 \pmod{p}$ for $0 \leqslant t < m$, we can replace $m!\binom{-L(i)}{m}$ by $(-L(i))^m$ in the computation of $m! a_m \pmod{p}$. Now use $-L(i) \equiv (i^{p-1}-1)/p \pmod{p}$. Write i uniquely as $i=l+kp$, and observe that $-L(l+kp) \equiv ((l^{p-2}(l-kp)-1)/p) \pmod{p}$. Replacing l by $p-l$, k by $p-1-k$, and j by $d-1-j$ and performing the sum over j makes no change (mod p) in the terms to be summed over l and k, due to the fact that $\psi\omega^r$ is odd and ψ is nontrivial. Hence twice the sum in the statement of the proposition is congruent to $-d_0 m!\, a_m \pmod{p}$, when $m<p$. The result follows.

IV. The Iwasawa Lambda Invariant of a Number Field

As in the introduction, let $\mathbb{Q}_\infty$ be the unique Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}_p$, let K be an algebraic number field (finite extension of $\mathbb{Q}$), and let K_n be the unique extension having degree p^n over K in $K \cdot \mathbb{Q}_\infty$. The Iwasawa invariants $\mu=\mu_p$, $\lambda=\lambda_p$, and $\nu=\nu_p$ of K are characterized by the property that $\mu p^n + \lambda n + \nu$ gives the exact power of p dividing the class number $h(K_n)$ for large n. A theorem of Iwasawa immediately identifies cases where $\mu=0=\lambda$.

(4.1) Theorem. *Suppose p does not divide $h(K)$ and L/K is a finite Galois p-extension, with at most one prime of K ramified in L. Then p does not divide $h(L)$.*

Proof. [18, p. 185]. Iwasawa's original proof [10] when L/K is cyclic also suffices for our applications.

(4.2) Corollary. *If only one prime of K divides p, and p does not divide $h(K)$, then $\mu_p = 0 = \lambda_p$ in K.*

Proof. Since p is the only prime of $\mathbb{Q}$ which ramifies in $\mathbb{Q}_\infty$, primes dividing p are the only ones which can ramify in K_n/K. (This is in fact true of any $\mathbb{Z}_p$-extension.) Thus the theorem applies and p does not divide $h(K_n)$. This implies that $\mu_p = 0 = \lambda_p$.

If K is a CM field with maximal real subfield K^+, we let $h^+(K) = h(K^+)$ and $h^-(K) = h(K)/h^+(K)$, which is an integer. Then each K_n is also CM and so we can define h_n^+ and h_n^- similarly. Iwasawa's theorem [11] then states that the power of p dividing h_n^+ is given by $\mu^+ p^n + \lambda^+ n + \nu^+$, while that dividing h_n^- is given by $\mu^- p^n + \lambda^- n + \nu^-$ for large n. So $\mu = \mu^+ + \mu^-$ and $\lambda = \lambda^+ + \lambda^-$. It is conjectured that $\mu^+ = \mu^- = \mu = 0$ [11] and that $\lambda^+ = 0$ [8].

Ferrero and Washington [4] investigated μ-invariants of Leopoldt–Kubota p-adic L-functions and proved that $\mu_p(K) = 0$ when K is an imaginary abelian field. Similarly, there is a connection between $\lambda_p(K)$ and the λ-invariants of Leopoldt–Kubota p-adic L-functions. We make the simplifying assumption that the conductor of K is not divisible by p^2, so that all associated Dirichlet characters are of the first kind.

(4.3) PROPOSITION. $\lambda_p^-(K) = \sum_{\text{odd}\,\chi \neq \omega^{-1}} \lambda(L_p(s, \chi\omega))$.

The sum runs over all odd primitive Dirichlet characters associated with K, with the exception of ω^{-1} in the case where ω^{-1} is an associated character.

Proof. The proof is based on the analytic class number formula.

V. IMAGINARY QUADRATIC FIELDS AND THE CRITERION OF GOLD

Now let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field of discriminant $-d$, and let χ be the associated nontrivial quadratic Dirichlet character of conductor d. Thus $\chi(i) = (-d/i)$ is given by the Jacobi symbol.

(5.1) PROPOSITION. $\lambda_p(K) = \lambda_p^-(K) = \lambda(L_p(s, \chi\omega))$.

Proof. Now $K^+ = \mathbb{Q}$, so $\lambda_p^+(K) = 0$ by Corollary (4.2). Thus $\lambda_p(K) = \lambda_p^-(K)$. The second equality is a special case of Proposition (4.3).

The following theorem of Gold greatly facilitates the computation of lambda invariants of imaginary quadratic fields.

(5.2) THEOREM (Gold [6]). *Assume that* $\chi(p) = 1$, *so that p splits in K,* $(p) = \mathscr{P}\bar{\mathscr{P}}$. *Then* $\lambda_p(K) \geqslant 1$. *Suppose furthermore that* $\mathscr{P}^r = (\pi)$ *is principal* *for some integer r not divisible by p. Then $\lambda_p(K) > 1$ if and only if $\pi^{p-1} \equiv 1$* (mod $\mathscr{P}^2$).

(5.3) *Remark.* A generalization of this theorem to arbitrary CM fields K follows from a result of Federer–Gross–Sinnott [1]. A corollary (for which more direct proofs and stronger statements are available) is that $\lambda_p(K) > 0$ if p divides $h(K)$.

In the case of $p = 2$, Kida [12] and Ferrero [2] independently found a simple formula for $\lambda_2(K)$ when K is imaginary quadratic. Let $D > 3$ be a square-free odd integer, and for any positive integer M, let $(M)_2$ denote the largest factor of M which is a power of 2. Then

$$\lambda_2(\mathbb{Q}(\sqrt{-D})) = \lambda_2(\mathbb{Q}(\sqrt{-2D})) = -1 + \sum_{l \mid D} \left(\frac{l^2-1}{8}\right)_2,$$

where the sum is over all prime divisors l of D. In the remaining cases of $D = 1$, 2, or 3, observe that $\lambda_2 = 0$ by (4.1). For the sake of completeness, we will also include the values of $\lambda_2(K)$ in our table.

We now prove a proposition to be used in the implementation of Gold's criterion, after briefly recalling the relation between quadratic forms of discriminant $-d$ and ideals in $K = \mathbb{Q}(\sqrt{-d})$.

For any (fractional) ideal $\mathscr{A}$ of K with $\mathbb{Z}$-basis $\mathscr{A} = [\alpha, \beta]$ (assumed ordered; i.e. $\operatorname{Im}(\alpha/\beta) > 0$) there is an associated norm form

$$Q(x, y) = ax^2 + bxy + cy^2 = \frac{\mathbb{N}(\alpha x + \beta y)}{\mathbb{N}\mathscr{A}}.$$

The form $Q(x, y)$ has integer coefficients and is a positive definite quadratic form of discriminant $b^2 - 4ac = -d$. Any change of basis for $\mathscr{A}$ by an element of $SL_2(\mathbb{Z})$ gives a quadratic form $SL_2(\mathbb{Z})$-equivalent to $Q(x, y)$. Any ideal $\gamma\mathscr{A}$ principally equivalent to $\mathscr{A}$ gives the same collection of quadratic forms since the norm form for $[\alpha, \beta]$ is the same quadratic form as the norm form for $[\gamma\alpha, \gamma\beta]$.

Conversely, to the positive definite quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = -d$ we can associate an ideal

$$\mathscr{A} = \left[a, \frac{b - \sqrt{-d}}{2}\right]$$

of norm a. Then the quadratic form associated to $\mathscr{A}$ with respect to this basis is $Q(x, y)$.

The association

$$Q(x, y) = ax^2 + bxy + cy^2 \leftrightarrow \mathscr{A} = \left[a, \frac{b - \sqrt{-d}}{2}\right] \tag{1}$$

associates to the quadratic form $Q(x, y)$ a specific basis for a particular ideal whose associated norm form is $Q(x, y)$. We now see how these ideals are related under an $SL_2(\mathbb{Z})$ transformation of the quadratic form.

Let

$$A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \tag{2}$$

so that

$$Q(x, y) = (x \;\; y)\, A \begin{pmatrix} x \\ y \end{pmatrix}.$$

Let $P \in SL_2(\mathbb{Z})$ and suppose

$$\begin{pmatrix} x \\ y \end{pmatrix} = P \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Then

$$Q(x, y) = ax^2 + bxy + cy^2 = a'x'^2 + b'x'y' + cy'^2 = Q'(x', y'),$$

where

$$Q'(x', y') = (x' \;\; y')\, A' \begin{pmatrix} x' \\ y' \end{pmatrix}$$

with

$$A' = \begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix} = P^t A P \tag{3}$$

(P^t the transpose of P).

The association in (1) defines an ideal (even with a chosen basis) to each of the ($SL_2(\mathbb{Z})$-equivalent) forms $Q(x, y)$ and $Q'(x', y')$. Since these ideals have the same associated norm forms, the ideals are principally equivalent. The following result in particular specifically identifies the relation between these ideals.

(5.4) PROPOSITION. *Suppose $P \in SL_2(\mathbb{Z})$ and A and A' are defined by* (2) *and* (3) *above. Then for any integers x_0, y_0 and x_0', y_0' related by $\binom{x_0}{y_0} = P\binom{x_0'}{y_0'}$ we have*

$$\left(x_0 a + y_0 \frac{b+\sqrt{-d}}{2}\right)\left[1, \frac{b-\sqrt{-d}}{2a}\right]$$

$$= \left(x_0' a' + y_0' \frac{b'+\sqrt{-d}}{2}\right)\left[1, \frac{b'-\sqrt{-d}}{2a'}\right]$$

as fractional ideals of k. More precisely, if

$$\omega_1 = x_0 a + y_0 \frac{b+\sqrt{-d}}{2}$$

$$\omega_2 = \left(x_0 a + y_0 \frac{b+\sqrt{-d}}{2}\right)\frac{b-\sqrt{-d}}{2a} = x_0 \frac{b-\sqrt{-d}}{2} + y_0 c$$

are the basis for the first ideal above and similarly for ω_1', ω_2', then

$$\begin{pmatrix}\omega_1' \\ \omega_2'\end{pmatrix} = P^{\mathrm{t}} \begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix}.$$

Proof. Note that

$$\begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix} = \begin{pmatrix} a & b/2 \\ b/2 & c\end{pmatrix}\begin{pmatrix}x_0 \\ y_0\end{pmatrix} + \frac{\sqrt{-d}}{2}\begin{pmatrix} y_0 \\ -x_0\end{pmatrix}$$

$$= A\begin{pmatrix}x_0 \\ y_0\end{pmatrix} + \frac{\sqrt{-d}}{2}\begin{pmatrix} y_0 \\ -x_0\end{pmatrix}$$

and similarly for ω_1', ω_2'. Then

$$\begin{pmatrix}\omega_1' \\ \omega_2'\end{pmatrix} = A'\begin{pmatrix}x_0' \\ y_0'\end{pmatrix} + \frac{\sqrt{-d}}{2}\begin{pmatrix} y_0' \\ -x_0'\end{pmatrix}$$

$$= A'P^{-1}\begin{pmatrix}x_0 \\ y_0\end{pmatrix} + \frac{\sqrt{-d}}{2}P^{\mathrm{t}}\begin{pmatrix} y_0 \\ -x_0\end{pmatrix}$$

$$= P^{\mathrm{t}}A\begin{pmatrix}x_0 \\ y_0\end{pmatrix} + \frac{\sqrt{-d}}{2}P^{\mathrm{t}}\begin{pmatrix} y_0 \\ -x_0\end{pmatrix}$$

$$= P^{\mathrm{t}}\left[A\begin{pmatrix}x_0 \\ y_0\end{pmatrix} + \frac{\sqrt{-d}}{2}\begin{pmatrix} y_0 \\ -x_0\end{pmatrix}\right]$$

$$= P^{\mathrm{t}}\begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix}.$$

VI. Computational Methods

The computation of $\lambda_p(K)$ for $K = \mathbb{Q}(\sqrt{-d})$ proceeds as follows. Again let χ be the nontrivial character associated with K, that is, the odd quadratic Dirichlet character of conductor d. If $(p, h(K)) = 1$ and $\chi(p) \neq 1$, then $\lambda_p(K) = 0$ by Corollary (4.2). If $(p, h(K)) = 1$ and $\chi(p) = 1$, then $\lambda_p(K) \geqslant 1$ and Gold's criterion (with $r = h(K)$) quickly determines whether $\lambda_p = 1$. In the remaining cases (empirically very few), the exact value of $\lambda_p(K) = \lambda(L_p(s, \chi\omega))$ is determined by means of Propositions (3.1) and (3.2), usually only requiring the consideration of a single value of m. Note that the conductor d of K is not divisible by p^2, since K is imaginary quadratic. Also we may assume that $d \neq p$ since otherwise we would have $K = \mathbb{Q}(\sqrt{-p})$ and $h(K) < p$; this is the case where $\lambda_p(K) = 0$. Thus $d_0 > 1$ and the hypotheses of (3.1) and (3.2) are satisfied. If Proposition (3.2) indicates that $\lambda_p(K) \geqslant p$, then Proposition (3.1) is employed, beginning with $m = p$.

We now describe our algorithm in more detail. See [13] for a discussion of the facts which we state without proof. All main programs were run on a VAX 8550 computer at the Computer Centre of Concordia University, Montreal. Programs for the special cases of p dividing the class number or the norm of a reduced ideal (defined below), and of $\lambda_p \geqslant p$ were run on a VAX 8600 at the Academic Computing Center of the University of Vermont, as well as a check of all programs for $p < 10{,}000$ and $d < 500$.

Precomputation

(1) Given d, first find all reduced positive definite quadratic forms $ax^2 + bxy + cy^2$ with nonnegative coefficients and discriminant $b^2 - 4ac = -d$. This is a finite search since all the coefficients are less than $\sqrt{d/3}$. Such a quadratic form corresponds to the ideal written in terms of its ordered integral basis as $\mathscr{A} = [a, (b - \sqrt{-d})/2]$. The ideal $\mathscr{A}$ has norm a, which is the minimum norm for integral ideals in the ideal class of $\mathscr{A}$, by virtue of the form being reduced. We also say that such an ideal is reduced. Given an ideal class of $K = \mathbb{Q}(\sqrt{-d})$, there is a unique form on our list corresponding to this class or its inverse (conjugate). Hence the class number $h(K)$ is found by counting ambiguous forms (those corresponding to an ideal class which is its own inverse) once and all others twice.

(2) Raise each representative ideal $\mathscr{A} = [a, (b - \sqrt{-d})/2]$ to the $h(K)$ power by the method of Hellegouarch [9]. Specifically, when $(a, d) = 1$, first use Newton's method to solve for b' such that $(b')^2 \equiv -d \pmod{4a^{h(K)}}$ and $b' \equiv b \pmod{2a}$. Then $\mathscr{A}^{h(K)} = [a^{k(K)}, (b' - \sqrt{-d})/2]$. It is easy to reduce to the case of $(a, d) = 1$ by first removing the ramified prime factors from $\mathscr{A}$, and using the fact that their squares are principal

ideals, generated by rational primes. This solves the problem when $h(K)$ is even. But when $h(K)$ is odd, there is only one ramified prime, and it is principal. Thus it will never occur in the factorization of a reduced ideal.

(3) Determine a generator $\gamma = (A + B\sqrt{-d})/2$ for the resulting principal ideal $\mathscr{A}^{h(K)}$ as follows. Again we may assume that the ramified prime factors have been removed from $\mathscr{A}$ as above. The principal ideal $\mathscr{A}^{h(K)} = [a^{h(K)}, (b' - \sqrt{-d})/2]$ corresponds to the quadratic form $Q(x, y) = a^{h(K)}x^2 + b'xy + c'y^2$; therefore this quadratic form reduces to the quadratic form representing the principal class; i.e.,

$$\begin{cases} x'^2 + \dfrac{d}{4}y'^2 & \text{if } d \equiv 0 \bmod 4 \\[2ex] x'^2 + x'y' + \dfrac{1+d}{4}y'^2 & \text{if } d \equiv 3 \bmod 4. \end{cases}$$

Find the transformation $P \in SL_2(\mathbb{Z})$ reducing $Q(x, y)$ to the principal class [13]. Then

$$P^{t}\begin{pmatrix} a^{h(K)} & b'/2 \\ b'/2 & c' \end{pmatrix} P = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & d/4 \end{pmatrix} & \text{if } d \equiv 0 \bmod 4 \\ \begin{pmatrix} 1 & 1/2 \\ 1/2 & (1+d)/4 \end{pmatrix} & \text{if } d \equiv 3 \bmod 4. \end{cases}$$

Define the integers r, s by

$$P^{-1}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} r \\ s \end{pmatrix}$$

Then by Proposition (5.4) we have

$$(a^{h(K)})\left[1, \frac{b' - \sqrt{-d}}{2a^{h(K)}}\right] = (r + s\bar{\omega})[1, \omega],$$

where

$$\omega = \begin{cases} \dfrac{-\sqrt{-d}}{2} & \text{if } d \equiv 0 \bmod 4 \\[2ex] \dfrac{1 - \sqrt{-d}}{2} & \text{if } d \equiv 3 \bmod 4 \end{cases}$$

defines an integral basis for the ring of integers of K. It follows that

$$\mathscr{A}^{h(K)} = (r + s\bar{\omega})$$

as ideals; i.e., we have determined a principal generator for $\mathscr{A}^{h(K)}$.

The software for this precomputation was written in the ALGEB language (see [5]), and was performed for all $d < 1{,}000$. The maximum coefficient among the generators of the principal ideals was 23 45980 63128 02816 37826. This precomputation required 1 min, 58 sec of CPU time to complete.

Applying the Criterion of Gold

Having completed the precomputation, begin to apply the criterion of Gold (5.2) to those primes p which split in K and do not divide $h(K)$.

(1) Find $g > 0$ such that $g^2 \equiv -d \pmod{4p}$ by the algorithm of Shanks [17]. The form $((g^2 + d)/4p)x^2 + gxy + py^2$ has discriminant $-d$ and represents p when $(x, y) = (0, 1)$.

(2) Reduce this form by the standard procedure [13] to obtain a reduced form $ax^2 + bxy + cy^2$, and also modify (x, y) correspondingly at each step to obtain (X, Y) so that $aX^2 + bXY + cY^2 = p$. The reduced form appears on the list derived in our precomputation and corresponds to some ideal $\mathscr{A} = [a, (b - \sqrt{-d})/2]$ with norm a. Obtain the generator $\gamma = (A + B\sqrt{-d})/2$ for $\mathscr{A}^{h(K)}$ from the list. The element $\delta = aX + [(b - \sqrt{-d})/2]\,Y$ is in $\mathscr{A}$ and has norm pa. Thus $(\delta) = \mathscr{P}\mathscr{A}$, where $\mathscr{P}$ is one of the primes above p in K (and $\mathscr{A}$ is a representative ideal of the class of $\bar{\mathscr{P}}$). Set $r = h(K)$ in (5.2), and note that p does not divide r, by assumption. Then the element $\pi = \delta^{h(K)}/\gamma$ generates $\mathscr{P}^{h(K)}$, as required.

(3) When $\mathscr{A} \not\subset \bar{\mathscr{P}}$, the criteria $\pi^{p-1} \equiv 1 \pmod{\bar{\mathscr{P}}^2}$ for $\lambda_p(K) > 1$ of (5.2) may be rewritten as $\gamma^{p-1} \equiv (\delta^{p-1})^{h(K)} \pmod{\bar{\mathscr{P}}^2}$. This reduces to a congruence between rational integers $(\mathrm{mod}\ p^2)$, as follows.

Since $\delta^2 \equiv \delta^2 + \bar{\delta}^2 \pmod{\bar{\mathscr{P}}^2}$, the right hand side being a rational integer, one has

$$\delta^{p-1} \equiv (-dY^2)^{(p-3)/2}\,(-dY^2 - ap) \qquad \pmod{\bar{\mathscr{P}}^2}.$$

The fact that $\bar{\delta}^2 \in \bar{\mathscr{P}}^2$ also shows that

$$(2aX + bY)\,Y\sqrt{-d} \equiv (dY^2 - 2ap) \qquad \pmod{\bar{\mathscr{P}}^2}.$$

Hence

$$[2(2aX+bY)\,Y]\gamma \equiv (2aX+bY)\,YA + (dY^2-2ap)B \pmod{\mathscr{P}^2}.$$

Upon multiplication by $(2aX+bY)\,Y$ (which is not divisible by p since δ is not), the criterion becomes

$$\begin{aligned}&[(2aX+bY)\,YA+(dY^2-2ap)B]^{p-1}\\&\quad\equiv[2(2aX+bY)\,Y]^{p-1}\\&\qquad\times[(-dY^2)^{(p-3)/2}(-dY^2-ap)]^{h(K)}\pmod{p^2}.\end{aligned}$$

Determine whether $\lambda_p(K)>1$ by checking this congruence.

If $\mathscr{A}\subset\bar{\mathscr{P}}$ then in fact $\mathscr{A}=\bar{\mathscr{P}}$, because $\mathscr{A}$ is the integral ideal of smallest norm in the ideal class of $\bar{\mathscr{P}}$. Hence $p=a$ and the criterion in this case is simply $A^{p-1}\equiv 1 \pmod{p^2}$. Determine whether $\lambda_p(K)>1$ by checking this congruence.

The software for this step was written in PASCAL, with assembler routines for arithmetic mod p and arithmetic mod p^2. To do all $d<1{,}000$ and $p<10^7$ required 149 hr, 30 min of CPU time.

Computation of Iwasawa Coefficients Modulo p

Once it has been determined that $\lambda_p(K)\geqslant 1$ because p divides $h(K)$, or that $\lambda_p(K)\geqslant 2$ by the criterion of Gold, proceed with the computation of $\lambda_p(K)$ based on (3.2) and (3.1) as follows. First tabulate the values of $\chi(i)=(-d/i)$ for $1\leqslant i\leqslant d-1$ by repeated use of reduction and quadratic reciprocity. Then evaluate the expression in (3.2) modulo p, beginning with $m=1$ when p divides $h(K)$ and with $m=2$ when the criterion of Gold has already been applied. Repeated use of a procedure to multiply modulo p^2 ensures that all integers remain less than p^2. For each value of $l\leqslant(p-1)/2$, compute $l^{(p-2)}$ by repeated squaring modulo p^2. For each value of $k\leqslant(p-1)$, obtain $((l^{p-2}(l-kp)-1)/p)^m$ modulo p. Finally, compute $i=l+kp+jp^2$ modulo d, and obtain $\chi(i)$ by referring to the tabulated values. Compute the sums over j, k, and l modulo p. If the result is nonzero modulo p, then $\lambda_p(K)=m$. Otherwise increase m and begin the computation again; this is rarely necessary, especially with larger primes, as the tables show. Eventually either $\lambda_p(K)$ is determined or $m=p-1$ is reached. In the latter case, begin computing the expression in (3.1) with $m=p$ in much the same way. This has only been required for a few cases where $p=3$, and has always succeeded in determining $\lambda_3(K)$.

The software for this step was written in PASCAL, with assembler routines for arithmetic mod p, arithmetic mod p^2, and character value sums. For $d<1{,}000$ and $p<20{,}000$ this step required 516 hr, 48 min of CPU time.

VII. Heuristics

In a fixed imaginary quadratic field K, we have seen that $\lambda_p = 0$ for any prime p which is inert in K and does not divide the class number h_K. Also since $\lambda_p \geqslant 1$ for every prime which splits in K, it follows that the density of prime numbers for which $\lambda_p = 0$ is one half, as is the density of primes for which $\lambda_p \geqslant 1$.

Again let χ be the quadratic Dirichlet character associated with K and

$$G(T, \chi\omega) = \sum_{m=0}^{\infty} a_m T^m$$

be the corresponding Iwasawa power series. Then $\lambda_p > n$ if and only if a_m is divisible by p for all $m \leqslant n$. For a prime p which splits in K, we have $a_0 = 0$ and $a_1 \neq 0$ by [3]. If one assumes that the coefficients a_m are uniformly distributed modulo p, then the probability that $\lambda_p > 1$ is just the probability that p divides a_1, namely $1/p$. Since the sum $\sum 1/p$ diverges when taken over all primes p which split in K, it follows from the Borel–Cantelli lemma that "with probability 1," there are an infinite number of primes p for which $\lambda_p > 1$. Indeed, one would expect the cardinality of $\{p\colon \lambda_p > 1,\ p < x\}$ to be asymptotic to $c \log(\log(x))$ for some $c > 0$. On the other hand the probability that p divides both a_1 and a_2 is $1/p^2$ under this assumption, and as $\sum 1/p^2$ converges, it follows that the expected number of p such that $\lambda_p > 2$ is finite.

VIII. Table

For each $d < 1{,}000$, Table I lists all primes p for which $\lambda_p > 1$ in the imaginary quadratic field of discriminant $-d$. When $p < 20{,}000$, the computed value is $\lambda_p = 2$ unless a larger computed value appears in parentheses. When a prime $p > 20{,}000$ appears, it is always followed by an asterisk; this is to denote that $\lambda_p > 1$ but the exact value of λ_p has not been computed. In these cases it is highly probable that $\lambda_p = 2$. The first number in parentheses in each row is the value of λ_2, determined from the formula of Kida and Ferrero.

For primes which are not listed, it is easy to determine whether $\lambda_p = 1$ or $\lambda_p = 0$ from the class number h_K, also given in the table, and the Jacobi symbol $(-d/p)$, which can be computed rapidly by repeated reduction and quadratic reciprocity. Specifically, as described earlier, $\lambda_p = 0$ when $(p, h_K) = 1$ and $(-d/p) \neq 1$; otherwise $\lambda_p > 0$.

TABLE I

Complete Table of All $\lambda_p > 1$, $p < 10,000,000$ in Imaginary Quadratic Fields $|\mathrm{DISC}| = d < 1,000$

D	H	P=2	ODD PRIMES					
3	1	(0)	13	181	2521	76543*	489061*	6811741*
4	1	(0)	29789					
7	1	(1)	19531					
8	1	(0)						
11	1	(0)	5	1769069*				
15	2	(1)	1741					
19	1	(0)	11					
20	2	(0)	5881					
23	3	(1)						
24	2	(0)	131	5237693*				
31	3	(7)	227	727				
35	2	(2)	3	13				
39	4	(1)						
40	2	(0)						
43	1	(0)	1741					
47	5	(3)	3	17	157	1193	1493	1511
51	2	(4)	5					
52	2	(0)	113					
55	4	(1)	8447					
56	4	(1)	3					
59	3	(0)	1771183					
67	1	(0)	24421	880301*				
68	4	(3)	8521					
71	7	(1)	29	2497867*				
79	5	(3)						
83	3	(0)	17	41	89431*			
84	4	(2)	107	173	3635459*			
87	6	(1)	1187					
88	2	(0)	23	29				
91	2	(2)	761	787				
95	8	(1)	94531*	2298209*				
103	5	(1)						
104	6	(0)	5					
107	3	(0)	3	11	79			
111	8	(1)	7					
115	2	(2)	563					
116	6	(0)	5741					
119	10	(5)						
120	4	(1)						
123	2	(2)	47	61				
127	5	(31)	5	11				
131	5	(0)	7057					
132	4	(1)	281581*					
136	4	(3)	5	7	709			
139	3	(0)						
143	10	(1)	7(3)					
148	2	(0)	23	1051				
151	7	(1)	7(3)	13627				
152	6	(0)	211(3)	6947				
155	4	(8)						
159	10	(1)						
163	1	(0)	1523	108529*				
164	8	(1)	3(3)	5				
167	11	(1)	61	392149*				
168	4	(2)	251	4856903*				
179	5	(0)	13	383				
183	8	(1)	1201	4049	29851*	99623*		
184	6	(1)						
187	2	(4)	29					
191	13	(15)	17					
195	4	(2)	7					
199	9	(1)	509	382693*				
203	4	(2)						

TABLE I—*Continued*

D	H	P=2	ODD PRIMES			
211	3	(0)	3			
212	6	(0)	81439*	7597823*		
215	14	(1)	113	5824723*		
219	4	(2)	37	2556193*		
223	7	(7)				
227	5	(0)	3	11	113	
228	4	(1)	79	13729		
231	12	(3)	3	13		
232	2	(0)	3037			
235	2	(4)	23			
239	15	(3)	3(6)			
244	6	(0)	11			
247	6	(1)	1949			
248	8	(7)	1283897*			
251	7	(0)	773	79867*		
255	12	(5)	131	172867*		
259	4	(2)				
260	8	(1)	3	19	103	1663
263	13	(1)	17	137		
264	8	(1)	1248571*	3019109*		
267	2	(2)	1201	534329*		
271	11	(3)	7			
276	8	(2)				
280	4	(2)				
283	3	(0)	4100849			
287	14	(3)	3			
291	4	(8)	7369			
292	4	(1)	7			
295	8	(1)	5657			
296	10	(1)	3	641	5711	
299	8	(2)	1013			
303	10	(1)				
307	3	(0)				
308	8	(2)				
311	19	(1)	3(4)	21859*	5(4)	
312	4	(1)	3307	1562567*		
319	10	(1)				
323	4	(4)	3	278563*		
327	12	(1)	12323			
328	4	(1)	43			
331	3	(0)	31			
335	18	(1)	36383*			
339	6	(4)				
340	4	(4)				
344	10	(0)	3(3)			
347	5	(0)	15277			
355	4	(2)				
356	12	(1)	7			
359	19	(1)				
367	9	(3)				
371	8	(2)	1231			
372	4	(8)	677			
376	8	(3)	11	13		
379	3	(0)	3	191		
383	17	(31)	17	27239*	38653*	229601*
388	4	(7)	241			
391	14	(5)				
395	8	(4)				
399	16	(3)				
403	2	(8)	11			
404	14	(0)	3	634331*		
407	16	(1)	167			
408	4	(4)	163	63709*		
411	6	(2)	7	47	54011*	282851*
415	10	(1)				
419	9	(0)	3			

TABLE I—*Continued*

D	H	P=2	ODD PRIMES				
420	8	(3)	101287*				
424	6	(0)	17				
427	2	(2)	31				
431	21	(3)	29				
435	4	(2)	73	173			
436	6	(0)					
439	15	(1)	5				
440	12	(1)					
443	5	(0)	13(3)				
447	14	(1)					
451	6	(2)	5				
452	8	(3)	3	3037			
455	20	(3)	363149*				
456	8	(1)	5	37	19333		
463	7	(3)	63691*				
467	7	(0)	3				
471	16	(1)	5				
472	6	(0)	7	17			
479	25	(7)	5				
483	4	(4)	11	47	31013*		
487	7	(1)					
488	10	(0)	73				
491	9	(0)					
499	3	(0)	5				
503	21	(1)	3				
511	14	(3)					
515	6	(2)	47				
516	12	(1)					
519	18	(1)	5(3)	13	17		
520	4	(1)					
523	5	(0)	5				
527	18	(11)					
532	4	(2)					
535	14	(1)	11	61			
536	14	(0)	23	33563*			
543	12	(1)	3	419	37811*		
547	3	(0)	157				
548	8	(1)					
551	26	(1)	23	18311			
552	8	(2)	7247	5021773*			
555	4	(2)	163	907			
559	16	(1)	17	16657			
563	9	(0)	34061*				
564	8	(4)	133319*				
568	4	(1)	13567				
571	5	(0)	13				
579	8	(16)	17	70853*			
580	8	(1)	7(3)				
583	8	(1)	79				
584	16	(1)	19				
587	7	(0)	3(3)	167	193		
591	22	(1)					
595	4	(6)	1319	9257			
596	14	(0)	3	23			
599	25	(1)	3	5(3)			
607	13	(7)	389	749429*			
611	10	(4)	3	5	11	17	118463*
615	20	(3)	5(3)				
616	8	(2)					
619	5	(0)	127	889069*	1408349*		
623	22	(3)	101				
627	4	(2)	313				
628	6	(0)					
631	13	(1)	41				
632	8	(3)	3				
635	10	(32)	3	197753*			

TABLE I—*Continued*

D	H	P=2	ODD PRIMES		
643	3	(0)	307		
644	16	(3)	223		
647	23	(1)	2383	197009*	
651	8	(10)	5	11	16451
655	12	(1)	301751*		
659	11	(0)	3(3)	13	
660	8	(2)	19	181	
663	16	(5)			
664	10	(0)	5(3)		
667	4	(2)	547	395111*	973283*
671	30	(1)			
679	18	(9)	5393		
680	12	(4)	14071		
683	5	(0)	3(3)		
687	12	(1)	541*	4955417*	
691	5	(0)			
692	14	(0)	3	661	
695	24	(1)			
696	12	(1)	7829		
699	10	(2)			
703	14	(1)	29		
707	6	(2)	71	24623*	
708	4	(1)	2552009*		
712	8	(1)			
715	4	(2)	633161*		
719	31	(3)			
723	4	(4)	11(3)	58027*	
724	10	(0)	761		
727	13	(1)	1051		
728	12	(2)	11	41	
731	12	(4)	1031		
739	5	(0)	5		
740	16	(1)	112939*		
743	21	(1)	3	71(3)	263
744	12	(8)	3		
751	15	(3)	3	13	347(3)
755	12	(2)			
759	24	(3)	5	7	
760	4	(1)			
763	4	(2)	167		
767	22	(1)	37		
771	6	(64)	5	2741	333857*
772	4	(15)	103	274871*	
776	20	(7)	7(3)	839	8543
779	10	(2)			
787	5	(0)	107		
788	10	(0)	31	225697*	
791	32	(5)	5098237*		
795	4	(2)	3313	1531331*	
799	16	(7)	5(3)	139	
803	10	(2)	5	3613	
804	12	(1)	325607*	477977*	
807	14	(1)	167	1831	
808	6	(0)	127		
811	7	(0)	11		
815	30	(1)	3(3)	103	5813
820	8	(2)	163	317	
823	9	(1)			
824	20	(1)	56113*	4124357*	
827	7	(0)	3(3)	19	450301*
831	28	(1)	5	7	11
835	6	(2)			
836	20	(1)	13	1987	
839	33	(1)	23		
840	8	(3)			
843	6	(2)	3(3)	421	13757
851	10	(2)	173		

TABLE I—*Continued*

D	H	P=2	ODD PRIMES			
852	8	(2)	5779	371343*		
856	6	(0)	3(4)	2213		
859	7	(0)	5	7	61	16573
863	21	(7)	3	17		
868	8	(9)	773			
871	22	(1)				
872	10	(0)	3	401		
879	22	(1)	5			
883	3	(0)	79	91757*		
884	16	(4)	59	8574767*		
887	29	(1)	29	457	4079	
888	12	(1)	17	271753*		
895	16	(1)				
899	14	(8)	3	190669*		
903	16	(3)	17	311		
904	8	(3)				
907	3	(0)	3(3)	19	1229	
911	31	(3)	5			
915	8	(2)	11777			
916	10	(0)	9839	596611*		
919	19	(1)	23(3)			
920	20	(2)	3	5	1277	305497*
923	10	(2)				
932	12	(1)	44131*			
935	28	(5)	3(3)			
939	8	(2)	367	192013*		
943	16	(3)	173			
947	5	(0)	41			
948	12	(4)	17	113	127	
951	26	(1)	509	797	1549	
952	8	(5)	37			
955	4	(16)	167			
959	36	(3)				
964	12	(3)	5(3)	61	103	
967	11	(1)	139	1291		
971	15	(0)	3	3361		
979	8	(2)	7			
983	27	(1)				
984	12	(2)				
987	8	(6)				
991	17	(7)				
995	8	(2)	3			
996	12	(1)	3			

Note. $\lambda_p = 2$ unless otherwise indicated in parentheses. p^* denotes $p > 20{,}000$ for which $\lambda_p > 1$ and probably equals 2 (but this is unconfirmed).

References

1. L. J. Federer and B. H. Gross, (Appendix by W. Sinnott), Regulators and Iwasawa modules, *Invent. Math.* **62** (1981), 443–457.
2. B. Ferrero, The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields, *Amer. J. Math.* **102**, No. 3 (1980), 447–459.
3. B. Ferrero and R. Greenberg, On the behaviour of p-adic L-functions at $s = 0$, *Invent. Math.* **50** (1978), 91–102.
4. B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395.
5. D. Ford, "On the Computation of the Maximal Order in a Dedekind Domain," Ph.D. Dissertation, Ohio State University, 1978.
6. R. Gold, The nontriviality of certain $\mathbb{Z}_l$-extensions, *J. Number Theory* **6** (1974), 369–373.
7. R. Gold, Examples of Iwasawa invariants, II, *Acta Arith.* **26** (1975), 233–240.
8. R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263–284.

9. Y. Hellegouarch, Algorithme pour calculer les puissances successives d'une classe d'idéaux dans uns corps quadratique. Application aux courbes elliptiques, *C. R. Acad. Sci. Paris Sér. I* **305** (1987), 573–576.
10. K. Iwasawa, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258.
11. K. Iwasawa, On Γ-extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183–226.
12. Y. Kida, On cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields, *Tôhoku Math. J.* **31** (1979), 91–96.
13. H. W. Lenstra, Jr., On the calculation of class numbers and regulators of quadratic fields, *in* "London Math. Soc. Lecture Note Ser.," Vol. 56, pp. 123–150, Cambridge Univ. Press, Cambridge, 1982.
14. H. W. Leopoldt, Eine p-adische Theorie der Zetawerte. II. Die p-adische Γ-Transformation, *J. Reine Angew. Math.* **274/275** (1975), 224–239.
15. R. Ernvall and T. Metsänkylä, A method for computing the Iwasawa λ-invariant, *Math. Comp.* **49**, No. 179 (1987), 281–294.
16. K. Ribet, "Fonctions L p-adiques et Théorie d'Iwasawa (Notes de P. Satgé d'après un cours de K. Ribet)," Publ. Math. d'Orsay 79.01, Département de Mathématique, Bâtiment 425, Université de Paris-Sud, 91405 Orsay, France, 1979.
17. D. Shanks, Five number theoretic algorithms, *in* "Proceedings of the Second Manitoba Conference on Numerical Mathematics (1972)," pp. 51–70.
18. L. C. Washington, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1982.