Advanced Studies in Pure Mathematics 17, 1989
Algebraic Number Theory — in honor of K. Iwasawa
pp. 261–265

Cyclotomic Z_p-extensions of $Q(\sqrt{-1})$ and $Q(\sqrt{-3})$

Yûji Kida

Dedicated to Professor Kenkichi Iwasawa on his 70th birthday

In the theory of Z_p-extensions of a number field, the λ-invariant has a special meaning that it is an analogue of the genus of an algebraic curve. In this point of view, one can naturally hope that there exists a uniform bound for λ_p independent of p when the base field is fixed, and this bound might be regarded as the genuine analogue of the genus for a number field. This question has been studied by Ferrero [1, 2] and Metsänkylä [5, 6].

In this paper, we refine Ferrero's results for some imaginary quadratic fields, in particular for $Q(\sqrt{-1})$ and $Q(\sqrt{-3})$.

§ 1.

We describe briefly how to get the exact values of a p-adic measure α defined below. We follow Sinnott [7] to construct a p-adic L-function. Let θ be an odd Dirichlet character with conductor d. We assume d is not a power of p. Define a rational function for θ by

$$F_\theta(X)=\sum_{a=1}^{d} \theta(a)(1+X)^a/\{(1+X)^d-1\}.$$

Let $\mathcal{O}$ be the integer ring of the field generated over Q_p by the values of θ, and let π be a prime element of $\mathcal{O}$. Then $F_\theta(X)$ can be expanded into a formal power series with $\mathcal{O}$-coefficients. Let α be the $\mathcal{O}$-valued p-adic measure corresponding to F_θ. Replace the period d in F_θ by dp^n. Then we get the following congruence from the fundamental correspondence between measures and power series:

$$\alpha(r+(p^n))(1+X)^r \equiv \{\sum{}' \theta(a)(1+X)^a\}/\{(1+X)^{dp^n}-1\} \pmod{(1+X)^{p^n}-1},$$

where r is an integer satisfying $0 \le r < p^n$, and the sum $\sum'$ is taken over all integers a with $1 \le a < dp^n$, $a \equiv r \pmod{p^n}$. Put $X=0$. Then we have

Received December 26, 1987.

$$\alpha(r+(p^n))=(\sum' \theta(a)a)/dp^n.$$

Assume further d is not divisible by p. Then we can easily get $\alpha(r+(p^n))=\theta(p)^n\{(1/d)\sum_{a=1}^{d}\theta(a)a+\sum_{a=1}^{s-1}\theta(a)\}$, where s is defined as the unique integer satisfying $1\leq s\leq d$, $sp^n\equiv r \pmod d$.

We denote by α^* the restriction of α to Z_p^*. That is, $\alpha^*(r+(p^n))=\alpha(r+(p^n))$ if $(r,p)=1$, and $\alpha^*(r+(p^n))=0$ if $(r,p)\neq 1$.

We choose the isomorphism from $1+pZ_p$ to Z_p which sends x to $(1/p)\log(x)$, where $\log(x)$ is the usual p-adic logarithm function. Put the resulting power series as $f(\theta, X)=\sum_{n=0}^{\infty}c_nX^n$. Then we have

$$c_0=\{1-\theta(p)\}(1/d)\left\{\sum_{a=1}^{d}\theta(a)a\right\},$$

$$c_1=\int\frac{1}{p}\log(x)d\alpha(x),$$

where $\log(x)$ is Iwasawa's p-adic logarithm function.

To calculate λ_p, it is sufficient to know the π-divisibility of c_n. Therefore, we can replace $(1/p)\log(x)$ by $l(x)=(1/p)(1-x^{p-1})$, and hence

$$c_1\equiv\sum' l(a)\alpha(a+(p^2)) \qquad \pmod p,$$

where the sum is taken over all a with $0\leq a<p^2$, $(a,p)=1$. This gives a criterion of the π-divisibility of c_1. But since this formula contains essentially p^2 terms, it is not convenient to calculate it for large p. If $p\equiv 1 \pmod d$, we can give a criterion containing essentially p terms.

Theorem 1. *If $p\equiv 1 \pmod d$, then $\lambda_p>1$ if and only if*

$$\sum_{x=1}^{d}\left\{\sum_{z=1}^{x-1}\alpha(z+(p^2))\right\}\{\sum' l(y)\}\equiv 0 \qquad \pmod \pi,$$

where the last sum is taken over all integers y satisfying $1\leq y<p$, $y\equiv x \pmod d$.

Proof. For any integer x prime to p, define $y_x\in Z/pZ$ by $x\equiv\omega+y_xp \pmod{p^2}$, where ω is a $(p-1)-st$ root of unity. Then we have $l(x)\equiv y_x/x \pmod p$. For simplicity, we denote $\alpha(x+p^2)$ by $\alpha(x)$ in the rest of this paper. Put

$$S(a)=\sum_{b=1}^{p-1}l(a+bp)\alpha(a+bp).$$

Then we have

$$S(a)\equiv\sum_{b=1}^{p-1}\{(y_a+b)/a\}\alpha(a+b) \qquad \pmod p$$

$$\equiv(1/a)\sum_{b=1}^{p-1}b\alpha(a+b) \qquad \pmod p.$$

We assume $p\equiv 1 \pmod{d}$. Divide the sum in the right hand side by every d terms. Then we have

$$\sum_{b=1}^{d} b\alpha(a+b)=\sum_{z=1}^{a}(d+z-a)\alpha(z)+\sum_{z=a+1}^{d}(z-a)\alpha(z)$$
$$=d\sum_{z=1}^{a}\alpha(z)+\sum_{z=1}^{d}z\alpha(z)-a\sum_{z=1}^{d}\alpha(z).$$

Since $\alpha(z)$ is a periodic function of period d and $c_0=\sum_{z=1}^{p^2}\alpha^*(z)$, the vanishing of c_0 implies the vanishing of the 3rd term. Denote the 2nd term by T. Since $\alpha(p^2-z)=\alpha(z)$, we have $\alpha(d+1-z)=\alpha(z)$. Therefore $T=\sum_{z=1}^{d}(d+1-z)\alpha(z)$. Hence $2T=(d+1)\sum_{z=1}^{d}\alpha(z)$, which is 0 by the above. Thus the 2nd term is also 0. Now we get

$$S(a)\equiv(1/a)\{(p-1)/d\}d\sum_{z=1}^{a}\alpha(z) \qquad (\mathrm{mod}\, p)$$
$$\equiv-(1/a)\sum_{z=1}^{a}\alpha(z) \qquad (\mathrm{mod}\, p).$$

Put

$$S=\sum_{a=1}^{p-1}\sum_{b=0}^{p-1}l(a+bp)\alpha(a+bp).$$

Then we have

$$S\equiv\sum_{a=1}^{p-1}l(a)\alpha(a)-\sum_{a=1}^{p-1}(1/a)\sum_{z=1}^{a}\alpha(z) \qquad (\mathrm{mod}\, p).$$

Since $1/a\equiv l(a)-l(p-a) \pmod{p}$, we get $S\equiv\sum l(a)\{\alpha(a)-\beta(a)+\beta(p-a)\}$ $(\mathrm{mod}\, p)$, where $\beta(a)=\sum_{z=0}^{a}\alpha(z)$. Since $\beta(p-a)=-\beta(a-1)$, we have

$$S\equiv-2\sum_{a=1}^{p-1}l(a)\beta(a-1) \qquad (\mathrm{mod}\, p).$$

Since $c_1\equiv S \pmod{p}$, Theorem 1 is proved. Q.E.D.

For $Q(\sqrt{-1})$ and $Q(\sqrt{-3})$, clearly $c_0\equiv 0 \pmod{p}$ if and only if $\theta(p)\equiv 1 \pmod{p}$, which is equivalent to $p\equiv 1 \pmod{d}$. Therefore we obtain the following criterion for $\lambda_p>1$. Since the coefficients of $l(x)$ are rational integers, we can write it in the product form.

Corollary (cf. Ferrero [2, p. 19]).

(1) *For $Q(\sqrt{-1})$, $\lambda_p>0$ if and only if $p\equiv 1$ (mod 4). Further, $\lambda_p>1$ if and only if $p\equiv 1$ (mod 4) and $(\prod_1 y/\prod_2 y)^{p-1}\equiv 1$ (mod p^2), where the 1st product $\prod_1$ is taken over all y with $1\leq y<p$, $y\equiv 2$ (mod 4), and the 2nd product $\prod_2$ is taken over all y with $1\leq y<p$, $y\equiv 0$ (mod 4).*

(2) *For* $Q(\sqrt{-3})$, $\lambda_p>0$ *if and only if* $p\equiv 1 \pmod 3$. *Further*, $\lambda_p>1$ *if and only if* $p\equiv 1 \pmod 3$ *and* $(\prod_1 y/\prod_2 y)^{p-1}\equiv 1 \pmod{p^2}$, *where the 1st product* $\prod_1$ *is taken over all* y *with* $1\leq y<p$, $y\equiv 0 \pmod 3$, *and the 2nd product* $\prod_2$ *is taken over all* y *with* $1\leq y<p$, $y\equiv 2 \pmod 3$.

Numerical examples.

For $Q(\sqrt{-1})$, the only value $p<150000$ with $\lambda_p>1$ is $p=29789$.

For $Q(\sqrt{-3})$, the only values $p<150000$ with $\lambda_p>1$ are $p=13$, 181, 2521, 76543.

Remark. If there were only a finite number of p with $\lambda_p>1$, we could give an affirmative answer to the question stated in the introduction.

§ 2.

We shall use standard notation in the theory of Z_p-extensions. Let k_∞ be the cyclotomic Z_p-extension of k and k_n its unique subfield of degree p^n over k. Let L_∞ be the maximal unramified abelian p-extension over k_∞, and $X(k)$ the Galois group $\mathrm{Gal}(L_\infty/k_\infty)$ with the action of $\mathrm{Gal}(k_\infty/k)$.

Theorem 2. *Let* $k=Q(\sqrt{-m})$ *be an imaginary quadratic field with* $m=1, 2, 3, 5, 6, 7, 10, 11, 15$ *or* 19. *Then for each prime number p, we have* $\lambda_p<p$.

Proof. Let θ be the nontrivial Dirichlet character attached to k. Ferrero proved ([1, p. 407]) for these fields that if $\lambda_p\geq p$ the power series $f(\theta, X)$ corresponding to the p-adic L-function for θ (cf. § 1) is divisible by $(1+X)^p-1$. Then, the theorem of Mazur-Wiles tells that the characteristic polynomial of the Iwasawa module $X(k)$ is also divisible by $(1+X)^p-1$. This means that the p-rank of the $\mathrm{Gal}(k_\infty/k_1)$-invariant submodule of $X(k)$ is at least p. On the other hand, formula for ambiguous class numbers (cf. [4, Lemma 1]) tells the number of the invariant classes in k_n/k_1 is equal to the product of the class number of k_1 and $p^{(n-1)}$. Therefore the p-rank of this submodule is 1. This contradiction proves Theorem 2. Q.E.D.

Theorem 3. *Let k be as in Theorem* 2. *Then for any* $p>2$, *we have* $e_{p,n}=\lambda_p\cdot n$ *for all* $n\geq 0$, *where* $e_{p,n}$ *is the exponent of the maximal power of p dividing the class number of* k_n.

Proof. If p does not split in k/Q, then $e_{p,n}=0$ for all $n\geq 0$. Thus the theorem holds in this case. If p splits in k/Q, then $c_0=0$ (cf. § 1). Therefore $f(\theta, X)$ is a product of X and a power series whose λ_p is less than $p-1$ by Theorem 2. Applying Iwasawa's argument [3, p. 93] to each power series, we get $e_{p,n+1}-e_{p,n}=\lambda_p$ for all $n\geq 0$. Since $e_{p,0}=0$, we have Theorem 3. Q.E.D.

Remark. For $Q(\sqrt{-1})$ and $Q(\sqrt{-3})$, Theorem 3 holds also for $p=2$. In fact, $e_{2,n}=0$ for all $n\geq 0$.

References

[1] Ferrero, B., An explicit bound for Iwasawa's λ-invariant, Acta Arith., **33** (1977), 405–408.

[2] ——, Iwasawa invariants of abelian number fields, Math. Ann., **234** (1978), 9–24.

[3] Iwasawa, K., Lectures on p-adic L-functions, Ann. of Math. Studies, **74,** Princeton University Press 1972.

[4] Kida, Y., l-Extensions of CM-Fields and Cyclotomic Invariants, J. Number Theory, **12** (1980), 519–528.

[5] Metsänkylä, T., An upper bound for the λ-invariant of Imaginary abelian fields, Math. Ann., **264** (1983), 5–8.

[6] ——, A simple method for estimating the Iwasawa λ-invariant, J. Number Theory, **27** (1987), 1–6.

[7] Sinnott, W., On the μ-invariant of the Γ-transform of a rational function, Invent. math., **75** (1984), 273–282.

Department of Mathematics
Faculty of Science
Kanazawa University
Kanazawa 920, Japan