

A REMARK ON ELLIPTIC UNITS

BY AKIRA AIBA

§ 0. Introduction

Let p be a prime number such that $p \equiv 3 \pmod{4}$ and $p > 3$. Put $K = \mathbf{Q}(\sqrt{-p})$ and let H be the absolute class field of K . In [5], Gross defined units u_σ ($\sigma \in \text{Gal}(H/K)$) in a class field of HT of a CM -field T containing K . He gave a question about a property of these units. In this paper, following Robert [8], we give the explicit method to calculate u_σ . In particular when $p=23$ we calculate them concretely to show that Gross' question is correct.

I would like to thank Prof. T. Kanno for encouragement and suggestion.

§ 1.

First we define the notations and recall the problem of Gross [5]. Let p be a prime number such that $p \equiv 3 \pmod{4}$ and $p > 3$. Let $K = \mathbf{Q}(\sqrt{-p})$ with the integer ring $O = O(K)$. Let H be the absolute class field of K with the integer ring $O(H)$. Let I_K (resp. I_H) be the idele group of K (resp. H). Let E be an elliptic curve defined over H with complex multiplication by O . We fix a Weierstrass model for E , $y^2 = 4x^3 - g_2x - g_3$ where $g_2, g_3 \in O$. Let j_E be the absolute invariant of E

i. e.
$$j_E = \frac{1728g_2^3}{g_2^3 - 27g_3^2}.$$

Let v be a finite place of H where E has good reduction. Let H_v be the completion at v , and let k_v be the residue field of H_v . Let \tilde{E}_v be the reduction of E at v . The reduction of endomorphisms gives an injection:

$$\theta_v: K \xrightarrow{\sim} \text{End}_H(E) \otimes \mathbf{Q} \longrightarrow \text{End}_{k_v}(E_v) \otimes \mathbf{Q}$$

whose image contains the Frobenius endomorphism π_v . Let α_v be the unique element of K with $\theta_v(\alpha_v) = \pi_v$.

Let χ_E be the Grössen character of E . This is a continuous homomorphism of I_H to the multiplicative group K^\times , which is the uniquely characterized by the following conditions:

- 1) If $a = (\alpha)$ is a principal idele, $\chi_E(a) = N_{H/K}(\alpha)$.

Received March 22, 1989

2) If $a=(a_v)$ is an idele with $a_v=1$ at all infinite places of H and at those places where E has bad reduction,

$$\chi_E(a)=\prod \alpha_v^{v(a_v)}$$

where the product is taken over the places of H at which E has good reduction.

Let h be the class number of K . It is known that the absolute invariant is H -isomorphism invariant and there are just h absolute invariants of elliptic curves whose endomorphism rings are isomorphic to O . We denote this set of absolute invariants by J . The character χ_E is H -isogeny invariant.

We say a curve E over H with complex multiplication by O is a \mathbf{Q} -curve if it is isogenous over H to all of its Galois conjugates E^τ ($\tau \in \text{Aut}(H)$).

Recall the \mathbf{Q} -curve $A=A(p)$ which was studied in [2][4][5].

Let χ_p be the unique continuous homomorphism of I_H to K which satisfies

- 1) If $a=(\alpha)$ is a principal idele, $\chi_p(a)=N_{H/K}(\alpha)$.
- 2) If $a=(a_v)$ is an idele with $a_v=1$ for all $v|\infty, p$ and p_v is prime at v , then

$$\chi_p(a)=\prod_{v|\infty, p} \alpha_v^{v(a_v)}$$

where ε is the composition of the natural isomorphism from $(O/\sqrt{-p}O)^\times$ to $(\mathbf{Z}/p\mathbf{Z})^\times$ and quadratic residue homomorphism from $(\mathbf{Z}/p\mathbf{Z})^\times$ to $\{\pm 1\}$, and α_v is the element of O such that $N_{H/K}p_v=(\alpha_v)$ and $\varepsilon(\alpha_v)=1$. (In this case this determines α_v uniquely.)

There exists an elliptic curve with complex multiplication by O defined over $F=\mathbf{Q}(j)$ ($j \in J$) with the absolute value j , the Grössen character χ_p and the minimal discriminant $(-p^3)$ over F . It is determined uniquely up to F -isomorphism and we denote this curve by $A=A(p)$. (In fact $A(p)$ is F -isomorphic to the following elliptic curve.

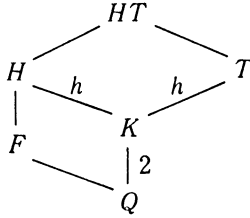
$$y^2=x^3+\frac{mp}{2^4 \cdot 3}x-\frac{np^2}{2^5 \cdot 3^3}$$

where $m^3=j_{A(p)}$

$$n^2=\frac{j-1728}{-p} \quad \text{sign } n=\left(\frac{2}{p}\right) \quad (\text{c. f. Gross [5]})$$

Let $B=B(p)=\text{Res}_{H/K}A(p)=\prod_{\sigma \in \text{Gal}(H/K)} A(p)^\sigma$ be the Weil restriction of $A(p)$

which is an abelian variety of dimension h . Then $T=\text{End}_K(B) \otimes \mathbf{Q}$ is CM -field of degree $2h$ and



Here we can define the Grössen character of B , $\chi_B: I_K \rightarrow T^\times$: continuous homomorphism

- s. t. 1) If $a=(\alpha)$ is a principal idele, $\chi_B(a)=\alpha$
- 2) If $a=(a_v)$ is an idele with $a_v=1$ when $v|\infty$ or B is bad reduction at v , then

$$\chi_B(a)=\prod \alpha_v^{v(a_v)}$$

where the product is taken over the places of K at which B has good reduction and α_v is the inverse image of the Frobenius endomorphism as in the elliptic case.

From now on in this section, we write $\mathfrak{a}, \mathfrak{b}$ for integral ideals of K which are prime to p and write α for an integer of K which is prime to p .

By the definition of χ_B , we get an integer $\chi_B(\mathfrak{a})$ of T . If we write $O(T)$ for the integer ring of T , a principal ideal $\chi_B(\mathfrak{a})O(T)$ is $\alpha O(T)$ and the following identities hold:

- (1) $\chi_B(\alpha)=\alpha$
- (2) $\chi_B(\mathfrak{a}\mathfrak{b})=\chi_B(\mathfrak{a})\chi_B(\mathfrak{b})$.

The restriction $f=\chi_B(\mathfrak{a})|_A$ is an isogeny from A to A^{σ_α} , where σ_α is $(\alpha, H/K)$. Let f_α be an element of H s. t. $f^*(\omega^{\sigma_\alpha})=f_\alpha\omega$, where f^* is the pull back of f . Then the principal idele $f_\alpha O(H)$ is $\alpha O(H)$ and the following identities hold:

- (1) $f_{(\alpha)}=\alpha$
- (2) $f_{\mathfrak{a}\mathfrak{b}}=f_\mathfrak{a}f_\mathfrak{b}$.

By the above we get units $u_\mathfrak{a} \stackrel{\text{def}}{=} \chi_B(\mathfrak{a})/f_\mathfrak{a}$ of HT and $u_{\mathfrak{a}\mathfrak{b}}=u_\mathfrak{a}u_\mathfrak{b}^{\sigma_\alpha}$.

Since $u_\mathfrak{a}$ depends only on the ideal class of \mathfrak{a} , we denote $u_{\sigma_\alpha}=u_\mathfrak{a}$. Let U_{HT} be the unit group of HT . By the above

$$\begin{array}{ccc} u : \text{Gal}(HT/T) \cong \text{Gal}(H/K) & \longrightarrow & U_{HT} \\ \Downarrow & & \Downarrow \\ \sigma & \longrightarrow & u_\sigma|_H \end{array}$$

is 1-cocycle. Gross gave the following two questions.

- Q 1 Is the cocycle u a coboundary? i. e. $u \in B^1(\text{Gal}(HT/T), U_{HT})$?
- Q 2 Does the summation of $u(\sigma)$ over $\text{Gal}(HT/T)$ belong to U_{HT} ?

i. e.
$$\sum_{\sigma \in \text{Gal}(HT/T)} u(\sigma) \in U_{HT}?$$

§ 2. The explicit algorithm for u

For a prime p we have h different $A(p)$ (so do $\{u_\sigma\}$) followed by the choice of j , where h is the class number of $K=Q(\sqrt{-p})$. But from the definition they are conjugate and we may only examine the case when $j \in \mathbf{R}$, and we may suppose the coefficients of the defining equation of $A(p)$ are integers.

From now on $j \in \mathbf{R}$

$$A(p): y^2=4x^3-g_2x-g_3 \quad g_2, g_3 \in O \quad \omega=dx/y$$

It is easy to calculate $\chi_B(\mathfrak{a})$ from the definition of χ_B and χ_p . We give the algorithm for $f_{\mathfrak{a}}$, followed by Robert [8].

First we give a few notations.

$$L = \left\{ \omega \mid \gamma \in H_1(A(\mathbf{C}), \mathbf{Z}) \right\} \quad L_\sigma = \left\{ \omega^\sigma \mid \gamma \in H_1(A^\sigma(\mathbf{C}), \mathbf{Z}) \right\} \quad (\sigma \in \text{Gal}(H/K))$$

$$G_2(\mathcal{L}) = \lim_{\substack{s \rightarrow 0 \\ s > 0}} \sum_{\lambda \in \mathcal{L} - \{0\}} \frac{1}{\lambda^2 \cdot |\lambda|^{2s}} \quad G_k(\mathcal{L}) = \sum_{\lambda \in \mathcal{L} - \{0\}} \frac{1}{\lambda^k} \quad (k > 2)$$

(\mathcal{L} : a lattice)

Then $G_k(L) \in H$ ($k \geq 2$)

$$\mathcal{P}(z, \mathcal{L}) = \frac{1}{z^2} + \sum_{\lambda \in \mathcal{L} - \{0\}} \left\{ \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right\} : \text{the Weierstrass } \mathcal{P}\text{-function}$$

Then

$$\mathcal{P}(z, \mathcal{L}) = \frac{1}{z^2} + \sum_{k \geq 1} (2k+1) G_{2k+2}(\mathcal{L}) z^{2k} \quad (0 < |z| < \text{Min}_{\omega \in \mathcal{L} - \{0\}} |\omega|)$$

(\mathcal{L} : a lattice)

$$\mathcal{P}_{\mathfrak{a}, L} = \sum_{0 \neq \lambda \in \mathfrak{a}^{-1}L/L} \mathcal{P}(\lambda, L) \in H.$$

We use the q -expansions and the integral conditions to calculate u explicitly as follows.

1. the determination of $G_2(L)$

1. approximate value of $G_2(L)$

$$(1) \quad \left(\frac{w_1}{2\pi}\right)^2 G_2(\mathfrak{a}^{-1}) = \frac{1}{12} \left(1 - 24 \sum_{n \geq 1} \frac{nq^n}{1-q^n} \frac{3}{\pi \text{Im}(w_2/w_1)} \right),$$

$$(2) \quad \left(\frac{w_1}{2\pi}\right)^2 G_4(\mathfrak{a}^{-1}) = \frac{1}{720} \left(1 + 240 \sum_{n \geq 1} \frac{n^3 q^n}{1-q^n} \right),$$

$$(3) \quad \left(\frac{w_1}{2\pi}\right)^2 G_6(\alpha^{-1}) = \frac{1}{30240} \left(1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1-q^n}\right),$$

where α is an integral ideal of K s. t. $\alpha^{-1} = (w_1, w_2)$ $\text{Im}(w_1/w_2) > 0$
 $q = \exp(2\pi i(w_2/w_1))$.

From the complex multiplication theory, there exists

$$\rho(\alpha) = \rho(\alpha, L) \in C \quad \text{s. t. } L_{\sigma_\alpha} = \rho(\alpha)\alpha^{-1}$$

$$(4) \quad \rho(\alpha)^2 = \frac{140}{60} \cdot \frac{g_2}{g_3} \cdot \frac{G_6(\alpha^{-1})}{G_4(\alpha^{-1})},$$

$$(5) \quad G_2(L)^{\sigma_\alpha} = G_2(L_{\sigma_\alpha}) = \rho(\alpha)^{-2} G_2(\alpha^{-1}).$$

2. the integral condition of $G_2(L)$

$$(6) \quad 2\sqrt{-p} G_2(L) \in O(H).$$

In general it is difficult to determine the integer ring when the degree is high, but in this case when j is real we can do it slightly more easily.

$$(7) \quad 2p G_2(L) \in O(F): \text{ the integer ring of } F = \mathbf{Q}(j).$$

2. the determination of $\mathcal{P}_{\alpha, L}$

1. approximate value of $(\mathcal{P}_{\alpha, L})^{\sigma_\mathfrak{b}}$

$$(8) \quad \left(\frac{w_3}{2\pi i}\right) \mathcal{P}(z, \mathfrak{b}) = \frac{1}{12} \sum_{m \in \mathbf{Z}} \frac{q^m q_z}{(1 - q^m q_z)^2} - 2 \sum_{n=1}^{\infty} \frac{n q^n}{1 - q^n}$$

where \mathfrak{b} is an integral ideal s. t. $\mathfrak{b} = (w_3, w_4)$ $\text{Im}(w_3/w_4) > 0$
 $q = \exp(2\pi i(w_4/w_3)) \quad q_z = \exp(2\pi i(z/w_3))$

$$(9) \quad (\mathcal{P}_{\alpha, L})^{\sigma_\mathfrak{b}} = \mathcal{P}_{\alpha, L \sigma_\mathfrak{b}} = \rho(\mathfrak{b})^{-2},$$

2. the integral condition of $\mathcal{P}_{\alpha, L}$

$$(10) \quad 2\mathcal{P}_{\alpha, L} \in O(H)$$

Especially when $N\alpha = 2$

$$(11) \quad 4\mathcal{P}_{\alpha, L}^3 - g_2 \mathcal{P}_{\alpha, L} - g_3 = 0$$

3.1. the determination of $G_2(\alpha^{-1}L)$

$$(12) \quad G_2(\alpha^{-1}L) - N\alpha G_2(L) = \mathcal{P}_{\alpha, L}$$

From 1, 2 and (12) we can determine $G_2(\alpha^{-1}L)$

2. the determination of f_α

$$(13) \quad G_2(\alpha^{-1}L) = f_\alpha^2 G_2(L)$$

From 1 and (13) we can determine f_a .

Proof of (1)~(13)

(1) (3), (8) See Lang [7] Chap. 4 and Kubert and Lang [6] Chap. 10

(12) Define

$$\sigma(z, L) = z \prod_{\lambda \in L - \{0\}} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right): \text{ the Weierstrass } \sigma\text{-function.}$$

Then

$$\mathcal{P}(z, L) = -\frac{\partial^2}{\partial z^2} \log \sigma(z, L)$$

Define

$$\theta(z, L) = \Delta(L) \sigma^{12}(z, L) \exp(-6G_2(L)z^2)$$

where $\Delta(L) = (2\pi)^{12}((60G_4(L))^3 - 27(140G_6(L))^2)$.

Then

$$\begin{aligned} z \frac{\partial}{\partial z} \log \theta(z, L) &= -12G_2(L)z^2 + 12 \frac{\sigma'(z, L)}{\sigma(z, L)} z \\ &= 12\left(1 - \sum_{\substack{k>0 \\ 2 \nmid k}} G_k(L)z^k\right) \end{aligned}$$

Let α be an integral ideal of K .

Define

$$\theta(z, L; \alpha) = \theta(z, L)^{N\alpha} / \theta(z, \alpha^{-1}L).$$

Then

$$z \frac{\partial}{\partial z} \log(z, L; \alpha) = 12(N\alpha - 1 + \sum_{\substack{k>0 \\ 2 \nmid k}} (G_k(\alpha^{-1}L) - N\alpha G_k(L))z^k)$$

On the other hand, $\theta(z, L; \alpha)$ is an elliptic function *w.r.* to L and an even function. Comparing zeros, poles and the first coefficient of power series expansion at $z=0$, we get the next equation:

$$\theta(z, L; \alpha) = \frac{\Delta(L)}{\Delta(\alpha^{-1}L)} \prod_{\lambda \in \alpha^{-1}L/L - \{0\}} \frac{\Delta(L)}{(\mathcal{P}(z, L) - \mathcal{P}(\lambda, L))^6}$$

We compare two expression of z^2 -coefficient of $z(\partial/\partial z) \log \theta(z, L; \alpha)$ and we get the result.

(5), (9) From the definition and (12).

(4) From the homogeneity of G_4 and G_6 ,

$$\rho(\alpha)^2 = \left(\frac{G_6(\alpha^{-1})}{G_6(L)}\right) \left(\frac{G_4(\alpha^{-1})}{G_4(L)}\right)^{-1} = \frac{140}{60} \cdot \frac{g_2}{g_3} \cdot \frac{G_6(\alpha^{-1})}{G_4(\alpha^{-1})}$$

(6) In (12) we take $\alpha = (\alpha)$. $\alpha \in \mathcal{O}$

$$\mathcal{O} \ni 2\mathcal{P}_{\alpha, L} = 2(G_2(\alpha^{-1}L) - N\alpha G_2(L)) = \alpha(\alpha - \bar{\alpha})G_2(L).$$

Since the greatest common ideal of $\alpha(\alpha - \bar{\alpha})$ is $(\sqrt{-p})$, $2\sqrt{-p}G_2(L) \in \mathcal{O}$

(7) Since $H=Q(j, \sqrt{-p})$,

$$2\sqrt{-p}G_2(L)=x_0+x_1\sqrt{-p}+x_2j+x_3j\sqrt{-p}+x_4j^2+x_5j^2\sqrt{-p} \quad x_i \in Q$$

Since j is real, $G_2(L)$ is also real and

$$2\sqrt{-p}G_2(L)=x_1\sqrt{-p}+x_3j\sqrt{-p}+x_5j^2\sqrt{-p}$$

From (6)

$$O(F) \ni N_{H/K}(2\sqrt{-p}G_2(L))=p(x_1+x_3j+x_5j^2)^2$$

$$O(F) \ni p(x_1+x_3j+x_5j^2)=2pG_2(L)$$

(10) See Cassels [3]

(11) From

$$A(p): y^2=4x^3-g_2x-g_3$$

(13) From $f_aL=aL$ and (5).

§ 3. Calculation example when $p=23$.

If the class number of $K=Q(\sqrt{-p})$ is 1, then $u_\sigma=1$ and Q_1 and Q_2 are trivially correct. There doesn't exist K of the class number 2 under the assumption of p . Under the condition that the class number of K is 3, $p=23$ is minimal. In this case we calculate u_σ concretely by the method of § 2, and show that Q_1 and Q_2 are correct.

Let $p=23$ and $K=Q(\sqrt{-23})$, then we have the absolute class field $H=K(\alpha)$ for $\alpha \in R$ such that $\alpha^3-\alpha-1=0$.

Set

$$O = Z + ((1 + \sqrt{-23})/2)Z,$$

$$\alpha = 2Z + ((1 + \sqrt{-23})/2)Z$$

and

$$\tilde{\alpha} = 2Z + ((1 - \sqrt{-23})/2)Z.$$

Then $\text{Gal}(H/K) = \{\sigma_0, \sigma_\alpha, \sigma_{\tilde{\alpha}}\}$ and since $N\alpha = N\tilde{\alpha} = 2$, in this case we can use (11). And

$$j = -\alpha^{125^3}(2\alpha-1)^3(3\alpha+2)^3$$

$$A(23): y^2 = 4x^3 - 2^2 3^3 c_4 x - 2^3 3^3 c_6$$

$$\text{where } c_4 = 5 \cdot 23^2 \alpha^4 (2\alpha - 1)(3\alpha + 2)$$

$$c_6 = \frac{7 \cdot 23^3 \alpha^8 (4\alpha^2 + 2\alpha - 3)(3\alpha + 1)}{2\alpha + 3}.$$

As for the numerical value above, see Berwick [1] or Gross [4]. From the

algorithm of § 2

$$G_2(L)=33\alpha^2+30\alpha+9$$

$$\mathcal{P}_{\alpha,L}=-\frac{3}{2}(13\alpha^2+38\alpha+45-3(\alpha^2-2\alpha+1)\sqrt{-23})$$

$$f_{\alpha}=-\frac{1}{2}\alpha^2+\frac{1}{2}\alpha-\frac{1}{2}-\frac{7}{46}\alpha^2\sqrt{-23}-\frac{1}{46}\alpha\sqrt{-23}-\frac{3}{46}\sqrt{-23}$$

And from the definition of χ_B

$$\chi_B(\alpha)=\left(\frac{3-\sqrt{-23}}{2}\right)^{1/3} \quad (\text{Fix a cubic root of unity.})$$

Therefore

$$u_{\sigma_0}=1$$

$$u_{\sigma_{\alpha}}=\left(\frac{1}{2}\alpha^2-\frac{1}{4}\alpha-\frac{3}{4}-\frac{1}{46}\alpha^2\sqrt{-23}+\frac{3}{92}\alpha\sqrt{-23}+\frac{9}{92}\sqrt{-23}\right)\left(\frac{3-\sqrt{-23}}{2}\right)^{1/3}$$

$$u_{\sigma_{\bar{\alpha}}}=\bar{u}_{\sigma_{\alpha}}.$$

To see that $u_{\sigma_0}+u_{\sigma_{\alpha}}+u_{\sigma_{\bar{\alpha}}}$ is unit, we examine

$$\begin{aligned} & \frac{1}{u_{\sigma_0}+u_{\sigma_{\alpha}}+u_{\sigma_{\bar{\alpha}}}} \\ & =(-\alpha^2+1)+\frac{1}{92}(23\alpha+12\alpha^2\sqrt{-23}+5\alpha\sqrt{-23}-8\sqrt{-23})\left(\frac{3-\sqrt{-23}}{2}\right)^{1/3} \\ & \quad +\frac{1}{92}(23\alpha-12\alpha^2\sqrt{-23}-5\alpha\sqrt{-23}+8\sqrt{-23})\left(\frac{3-\sqrt{-23}}{2}\right)^{1/3} \end{aligned}$$

is an integer.

To do so, we may examine that the elementary symmetric polynomials of the conjugates of $1/\sum u_{\sigma}$ over T . They all are in T^+ (the maximal real subfield of T). Since $[T^+:\mathbf{Q}]=3$, the integer ring of T^+ is determined by Tornheim [9], for example. In this case the integer ring of T^+ is $\mathbf{Z}[\chi_B(\alpha)+\chi_B(\alpha)^{-1}]$ and they all are integers and Q 1, 2 are correct.

Thus we have

PROPOSITION. *Let $K=\mathbf{Q}(\sqrt{-23})$ and let H be the absolute class field of K . Let $A(23)$ be the \mathbf{Q} -curve as in § 1. Let $B=\prod_{\sigma\in\text{Gal}(H/K)} A(23)^{\sigma}$ be the Weil restriction of $A(23)$. Let $T=\text{End}_K(B)\otimes\mathbf{Q}$. Let U_{HT} be the unit group of HT . Let u be the 1-cocycle of $\text{Gal}(HT/T)$ to U_{HT} as in § 1.*

Then u is contained in $B^1(\text{Gal}(HT/T), U_{HT})$ and $\sum_{\sigma\in\text{Gal}(HT/T)} u(\sigma)$ is contained in U_{HT} .

REFERENCES

- [1] W. E. H. BERWICK, Modular invariants expressible in terms of quadratic and cubic irrationalities, *Proc. London Math. Soc.* (1927), 53-69.
- [2] J. P. BUHLER AND B. GROSS, Arithmetic on elliptic curves with complex multiplication, *Invent. Math.* (1985), 11-29.
- [3] J. W. S. CASSELS, A note on the division values of $\mathcal{P}(u)$, *Proc. Cambridge Philos. Soc.* (1949), 167-172.
- [4] B. GROSS, Arithmetic on elliptic curves with complex multiplication, *SLN 776* (1980).
- [5] B. GROSS, Minimal models for elliptic curves with complex multiplication, *Composito Math.* (1982), 155-164.
- [6] D. S. KUBERT AND S. LANG, *Modular units*, Springer (1981).
- [7] S. LANG, *Elliptic functions*, Addison Wesley (1973).
- [8] G. ROBERT, Nombre de Hurwitz et unités elliptiques, *Ann. Sci. E. N. S.* (1978), 297-389.
- [9] L. TORNHEIM, Minimal basis and inessential discriminant divisors for a cubic field, *Pacific Journal of Math.* (1955), 623-631.

DEPARTMENT OF MATHEMATICS
IBARAKI UNIVERSITY
BUNKYOH, MITO
IBARAKI, JAPAN