LMS J. Comput. Math. 17 (Special issue A) (2014) 303–313
doi:10.1112/S1461157014000163

On the units generated by Weierstrass forms

Ömer Küçüksakallı

Abstract

There is an algorithm of Schoof for finding divisors of class numbers of real cyclotomic fields of prime conductor. In this paper we introduce an improvement of the elliptic analogue of this algorithm by using a subgroup of elliptic units given by Weierstrass forms. These elliptic units which can be expressed in terms of x-coordinates of points on elliptic curves enable us to use the fast arithmetic of elliptic curves over finite fields.

Introduction

The class numbers h_p of real cyclotomic fields $\mathbf{Q}_{(p)} = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$ are extremely hard to compute. General purpose algorithms are useless as the degree of the extension gets bigger. There is no practical method for computing the precise value of h_p and it is not known even for relatively small values of p. However, Schoof introduces an algorithm to find their divisors [9]. He achieves this by using the Jordan–Hölder filtration of the Galois module given by the quotient of the units of $\mathbf{Q}_{(p)}$ by the cyclotomic units.

There is an analogy between the real cyclotomic case and the elliptic case. Let K be an imaginary quadratic field with class number 1 and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree-one prime ideal of norm not dividing $6d_K$. Let $K_\mathfrak{p}$ be the ray class field of K of conductor $\mathfrak{p}$ and let $h_\mathfrak{p}$ be its class number. There is an explicit subgroup of special units in $K_\mathfrak{p}$, called elliptic units, whose index in the full unit group is precisely $h_\mathfrak{p}$ [12]. Moreover, if $N(\mathfrak{p})|h_\mathfrak{p}$ then $N(\mathfrak{p})$ divides the numerator of a nontrivial Hurwitz number [8]. This property is analogous to a property of cyclotomic extensions. A result of Herbrand states that if $p|h_p$ then p divides the numerator of an even Bernoulli number. This is the main property used by Buhler and Harvey in order to verify Vandiver's conjecture for primes up to 163 million [1].

We have generalized Schoof's algorithm to the elliptic case using the analogy between the cyclotomic and elliptic units [5]. We have encountered an interesting phenomenon, a counterexample to an elliptic analogue of Vandiver's conjecture. More precisely, we show that the class number of $K_\mathfrak{p}$, with $d_K = -163$ and $N(\mathfrak{p}) = 307$, is divisible by 307.

Basic algebraic properties of cyclotomic extensions enable Schoof to order cyclotomic units modulo a totally split prime according to the Galois action. Unlike the cyclotomic units, there is no closed formula giving algebraic relations between the conjugates of elliptic units. In order to overcome this drawback, we introduced an algorithm which does the same in the elliptic case [5]. However, we had to compute minimal polynomials of elliptic units by using complex numbers with high precision. This is feasible in the range $\mathfrak{p} < 700$. However, for extensions with larger conductor, such computations become impractical because of the growth of coefficients of minimal polynomials.

In this paper we introduce a faster algorithm which orders elliptic units modulo a totally split prime without computing their minimal polynomials. We achieve this by using a subgroup of elliptic units given by Weierstrass forms [4]. These elliptic units which are defined in terms

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11G16 (primary), 11R29, 11Y40 (secondary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

of values of Weierstrass $\wp$-function can also be expressed in terms of x-coordinates of points on an elliptic curve. Reducing this curve modulo a certain prime, we obtain an elliptic curve over a finite field. We need to find a $\mathfrak{p}$-torsion point there, but this can be achieved by using the fast arithmetic of elliptic curves over finite fields [**13**].

Using our improved algorithm, we have checked whether there is another counterexample for the elliptic analogue of Vandiver's conjecture within the range $-d_K \in \{7, 8, 11, 19, 43, 67, 163\}$ and $N(\mathfrak{p}) < 10\,000$. The first step of the generalized Schoof algorithm indicates that it is very likely that the class number of $K_{\mathfrak{p}}$, with $d_K = -43$ and $N(\mathfrak{p}) = 5521$, is divisible by 5521. We use the software PARI to do our computations on a computer with a quad-core CPU of 3.10 GHz with less than 1 gigabyte of memory allocated. Our computations take less than 12 hours. Vandiver's conjecture has been verified for primes up to 163 million [**1**]. Using the analogy between the Bernoulli and Hurwitz numbers [**8**], we hope to improve the range $N(\mathfrak{p}) < 10\,000$ in a future paper.

The organization of the paper is as follows. In § 1 we describe certain families of modular units. In § 2 we use the values of these modular units in order to obtain elliptic units in $K_{\mathfrak{p}}$. In § 3 we give a brief summary of Schoof's algorithm, focusing on its first step. Finally, in § 4, we explain how we improve the elliptic analogue of Schoof's algorithm and give an example to illustrate our computations.

1. *Modular units*

In this section, we describe certain families of units in the modular function field. Unless otherwise stated or proved, the assertions of this section can be found in [**4**]. We recall some elementary definitions from the theory of modular functions. A modular function of level N is defined as a meromorphic function on the extended upper half-plane $\mathcal{H}$, which is invariant under the congruence subgroup $\Gamma(N)$ of Γ.

We let $\mathcal{F}_N$ be the field of all modular functions of level N whose q-expansions at every cusp have coefficients in $\mathbf{Q}(\zeta_N)$. In particular, $\mathcal{F}_1$ is just $\mathbf{Q}(j)$. It is a well-known fact that $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ with

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\{\pm I_2\}$$

where I_2 denotes the 2×2 identity matrix. Let R_N be the integral closure of $\mathbf{Z}[j]$ in the function field $\mathcal{F}_N$. Elements of $R_N^{\times}$ are called modular units (over $\mathbf{Z}$). The units in $\mathcal{F}_N$ are precisely those modular functions in $\mathcal{F}_N$ which have zeros and poles only at the cusps.

Let $a = (a_1, a_2)$ be a pair of rational numbers such that $a \in (1/N)\mathbf{Z}^2$ but $a \notin \mathbf{Z}^2$. We say that a is primitive of level N if a has order N in $((1/N)\mathbf{Z}^2)/(\mathbf{Z}^2)$.

In order to obtain modular units, one can use the Siegel function. Kubert and Lang [**4**] use the notation g_a for this function. Since we reserve the letter g for a primitive root modulo p, we follow Stark's notation and denote the Siegel function by

$$\phi_a(z) = \phi(a_1, a_2, z).$$

This function has a q-expansion given by an explicit infinite product. It satisfies nice transformation properties, and it follows from these transformation properties that it is an element of $\mathcal{F}_{12N^2}$. Moreover, $\phi_a^{12N} \in \mathcal{F}_N$ and $\mathcal{F}_N = \mathcal{F}_1(\{\phi_a^{12N}\})$ [**12**].

The modular units in $\mathcal{F}_N$ consist of the power products $\prod \phi_a^{m(a)}$ such that the family $\{m(a)\}$ of integers satisfies certain quadratic relations. In particular,

$$u(a, c) := \left(\frac{\phi_{ca}}{\phi_a}\right)^{12N}$$

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

is a modular unit of level N if c is an integer relatively prime to N. The Galois action of $\alpha \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ on the unit $u(a,c)$ is given by the basic law

$$u(a,c)^{\sigma_\alpha} = u(a\alpha, c). \tag{1.1}$$

We will now consider another family of modular units of level N. Let $\wp(z;L)$ be the Weierstrass $\wp$-function. For $a = (a_1, a_2)$, we define

$$\wp_a(z) = \wp(a_1 z + a_2; \langle z, 1\rangle).$$

Let a be a primitive point of order N. Let r, r', s, s' be integers relatively prime to N such that $r \pm r'$ and $s \pm s'$ are also relatively prime to N. Then

$$\frac{\wp_{ra} - \wp_{r'a}}{\wp_{sa} - \wp_{s'a}}$$

is a modular unit over $\mathbf{Z}$ of level N. Its q-expansion has coefficients in $\mathbf{Z}[\zeta_N]$ and begins with a unit in $\mathbf{Z}[\zeta_N]$ times a fractional power of q.

Now we specialize to the case which will be considered in the following sections. Suppose that $N = p$ where p is prime. Let a be a primitive point of order p and let g be a primitive root modulo p. We define the modular unit

$$v(a,g) := \frac{\wp_{g^2 a} - \wp_{ga}}{\wp_{ga} - \wp_a}.$$

Similar to $u(a,g)$ (see equation (1.1)), the conjugates of $v(a,g)$ are given by a basic formula. For any $\alpha \in \mathrm{GL}_2(N)$, we have

$$v(a,g)^{\sigma_\alpha} = v(a\alpha, g).$$

There is an explicit relation between the units $u(a,g)$ and $v(a,g)$. To see this relation, we start with a standard elementary formula from the theory of elliptic functions,

$$\wp_a - \wp_b = -\frac{\sigma_{a+b}\sigma_{a-b}}{\sigma_a^2 \sigma_b^2},$$

where $\sigma(z;L)$ is the Weierstrass σ-function and $\sigma_a(z) = \sigma(a_1 z + a_2; \langle z, 1\rangle)$. Kubert and Lang call σ_a a Weierstrass form.

The Siegel ϕ-function and the Weierstrass σ-function are related to each other by an explicit equation [4, Chapter 2]. Combining this relation with the above formula, one can deduce that

$$\wp_a - \wp_b = \frac{\phi_{a+b}\phi_{a-b}}{\phi_a^2 \phi_b^2} \eta^{-4} \zeta_{12p}^*$$

where η is the Dedekind η-function and ζ_{12p}^* is a certain $12p$th root of unity depending on a and b. Applying the above identity to the modular unit $v(a,g)^{12p}$, we see that

$$v(a,g)^{12p} = \left(\frac{(\phi_{ga(g+1)}\phi_{ga(g-1)})/(\phi_{g^2 a}^2 \phi_{ga}^2)}{(\phi_{a(g+1)}\phi_{a(g-1)})/(\phi_{ga}^2 \phi_a^2)} \right)^{12p}.$$

Recall that $u(a,g) = (\phi_{ga}/\phi_a)^{12p}$. Let n be an integer not divisible by p. If $\alpha_n = nI_2$, then we have $u(a,g)^{\alpha_n} = u(na, g)$. We rewrite the equality above using this identity, and obtain

$$v(a,g)^{12p} = \frac{u(a,g)^{\alpha_g + I_2} \cdot u(a,g)^{\alpha_g - I_2}}{(u(a,g)^{\alpha_g} \cdot u(a,g))^2}. \tag{1.2}$$

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

Let us consider the discrete logarithm function which is defined by $\log_p(x) = k$ if $g^k = x \pmod p$. This function determines k uniquely modulo $p-1$. In order to express the above relation in a more compact way, we define the polynomial

$$\gamma_g(x) := x^{\log_p(g+1)} + x^{\log_p(g-1)} - 2x - 2.$$

Note that $\gamma_g(x)$ is uniquely determined in the ring $\mathbf{Z}[x]/(x^{p-1}-1)$. It follows by equation (1.2) that

$$v(a,g)^{12p} = u(a,g)^{\gamma_g(\alpha_g)}. \tag{1.3}$$

The polynomial γ_g will play an important role when we apply the first step of Schoof's algorithm specialized to the elliptic case.

2. *Elliptic units*

Let K be an imaginary quadratic field with $\mathcal{O}_K = \mathbf{Z}[\tau]$. In order to obtain elements in ramified abelian extensions of K, one can use the values $f(\tau)$ of modular functions. As a consequence of the main theorem of complex multiplication, we have the property that for every modular function $f \in \mathcal{F}_N$, the value $f(\tau)$, if finite, is contained in the ray class field $K_{(N)}$ of K with conductor (N) (see, for instance, [**12**, Theorem 3] or [**3**, p. 41]).

In analogy with the cyclotomic units, the ray class fields of imaginary quadratic fields have a subgroup of elliptic units whose index in the unit group is closely related to the class number. Stark shows that if the class number of K is 1 and if $\mathfrak{p} \subset K$ is a degree-one prime ideal of norm relatively prime to $6d_K$ then this index is precisely the class number [**12**]. Oukhaba provides a formula which is valid in a more general set-up [**7**]. This is analogous to the formula of Sinnott about the cyclotomic units [**11**].

In this paper we focus on the imaginary quadratic fields whose class number is 1. It is a well-known fact that the discriminant of such fields is given by

$$d_K \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

Let W be the number of roots of unity in $\mathcal{O}_K$. We have

$$W = \begin{cases} 6 & \text{if } d_K = -3, \\ 4 & \text{if } d_K = -4, \\ 2 & \text{otherwise.} \end{cases}$$

Let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree-one prime ideal of norm p not dividing $6d_K$. The ray class field $K_\mathfrak{p}$ is an abelian extension of K whose Galois group

$$G = \mathrm{Gal}(K_\mathfrak{p}/K)$$

is isomorphic to $I_K/P_{K,1}$ by class field theory [**2**]. We have $p \equiv 1 \pmod W$ and $G \cong \mathbf{F}_p^\times/\mu_W$ where μ_W is the group Wth roots of unity considered as a subgroup of $\mathbf{F}_p^\times$.

We denote by $\sigma_n \in G$ the automorphism of $K_\mathfrak{p}$ which corresponds to the class of ideals containing the ideal $n\mathcal{O}_K$. If g is a primitive root modulo p, then $G = \langle \sigma_g \rangle$. Note that the Galois group G is cyclic of order $(p-1)/W$.

We may choose $\tau = \sqrt{d_K}/2$ or $\tau = (\sqrt{d_K}+1)/2$ depending on the parity of the discriminant so that $\mathcal{O}_K = \mathbf{Z}[\tau]$. Let g be a primitive root modulo p. The elliptic units produced by Stark are of the form

$$\epsilon(a,g) := \frac{\phi_{ga}(\tau)}{\phi_a(\tau)} \cdot \zeta_{12p}^* \in \mathcal{O}_{K_\mathfrak{p}}^\times$$

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

for some $a = (a_1, a_2)$, a primitive pair of order p [12, p. 229]. If $\mathfrak{p} = (\pi_\mathfrak{p})$ then a can be found by the equation $\overline{\pi}_\mathfrak{p}/p = a_1\tau + a_2$. The conjugates of these elliptic units can be computed by Shimura's reciprocity law. More precisely, we have

$$\epsilon(a, g)^{\sigma_n} = \epsilon(an, g) \tag{2.1}$$

for $\sigma_n \in G$ by [12, Theorem 3]. Moreover, one can find the precise power of ζ_{12p} for each conjugate [5].

Let $\mathcal{E}(g)$ be the multiplicative $\mathbf{Z}[G]$-module generated by $\epsilon(a, g)$ together with roots of unity in $\mathcal{O}_K$. The group $\mathcal{E}(g)$ is independent of the primitive root chosen, so we put $\mathcal{E} = \mathcal{E}(g)$. Stark also shows that $[\mathcal{O}_{K_\mathfrak{p}}^\times : \mathcal{E}] = h_\mathfrak{p}$ where $h_\mathfrak{p}$ is the class number of the ray class field $K_\mathfrak{p}$ [12, p. 229].

We will now construct a special subgroup of $\mathcal{E}$ defined in terms of Weierstrass $\wp$-function values. This will allow us to use the arithmetic of elliptic curves within our algorithm. We define

$$\omega(a, g) := v(a, g)(\tau) = \frac{\wp_{g^2a}(\tau) - \wp_{ga}(\tau)}{\wp_{ga}(\tau) - \wp_a(\tau)}.$$

Recall that $v(a, g)$ is a modular unit. Evaluating this function at an imaginary quadratic value, we obtain an elliptic unit [12, Lemma 1]. Moreover, the special choice of a forces $\omega(a, g)$ to be in $K_\mathfrak{p}$ similar to $\epsilon(a, g)$. The unit $\omega(a, g)$ is related to $\epsilon(a, g)$ as follows:

$$\begin{aligned}\omega(a, g)^{12p} &= v(a, g)^{12p}|_{z=\tau} \\ &= u(a, g)^{\gamma_g(\alpha_g)}|_{z=\tau} \\ &= (\epsilon(a, g)^{\gamma_g(\sigma_g)})^{12p}.\end{aligned}$$

The first equality follows from the definition of $\omega(a, g)$. The second equality is by equation (1.3). The last equality holds because of the compatibility of Galois actions of $\mathrm{Gal}(\mathcal{F}_p/\mathcal{F}_1)$ and $\mathrm{Gal}(K_\mathfrak{p}/K)$. See equations (1.1) and (2.1).

One can show that $K_\mathfrak{p} \cap K(\zeta_{12p}) = K$ [5, Lemma 1.4]. In other words, the only roots of unity in $K_\mathfrak{p}$ are those in K. Therefore it is easy to see by the above equation that $\omega(a, g)$ and $\epsilon(a, g)^{\gamma_g(\sigma_g)}$ are equal up to a root of unity from $\mathcal{O}_K$. We write

$$\omega(a, g) \approx \epsilon(a, g)^{\gamma_g(\sigma_g)}.$$

Let $\mathcal{W}(g)$ be the multiplicative $\mathbf{Z}[G]$-module generated by $\omega(a, g)$. We want to determine the index of $\mathcal{W}(g)$ in $\mathcal{E}$. For a subgroup H of G, define the H-norm map by

$$N_H := \sum_{\sigma \in H} \sigma \in \mathbf{Z}[G].$$

If H is a proper subgroup and if $\gamma_g(\sigma_g)$ is divisible by N_H, then $\mathcal{W}(g)$ is a subset of $K_\mathfrak{p}^H$, the fixed field of H. In this case the unit rank of $K_\mathfrak{p}^H$ is smaller than that of $K_\mathfrak{p}$ and the subgroup $\mathcal{W}(g)$ is not of finite index in $\mathcal{E}$. For example, if $|G|$ is even then there is a unique subgroup H of G of order 2. In this case $N_H = \sigma_g^{|G|/2} + 1$ and it divides $\gamma_g(\sigma_g)$ if $\gamma_g(-1) = 0$. It follows that the index $[\mathcal{E} : \mathcal{W}(g)]$ is not finite. In general, the index $[\mathcal{E} : \mathcal{W}(g)]$ is not finite if $\gamma_g(\zeta) = 0$ for some $|G|$th root of unity ζ (not necessarily primitive). On the other hand, we have the following lemma.

LEMMA 2.1. *Let g be a primitive root modulo p and let ζ_m be a primitive mth root of unity where $m = [K_\mathfrak{p} : K]$. If $\gamma_g(\zeta_m^j) \neq 0$ for $j = 1, \ldots, m-1$, then the index $[\mathcal{E} : \mathcal{W}(g)]$ is finite and is given by*

$$[\mathcal{E} : \mathcal{W}(g)] = \prod_{j=1}^{m-1} \gamma_g(\zeta_m^j).$$

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

Proof. Any elliptic unit in $\epsilon_0 \in \mathcal{E}$ can be written in the form

$$\epsilon_0 = \zeta_W^* \prod_{i=0}^{m-2} \sigma_g^i(\epsilon(a,g))^{c_i}.$$

We need to compare the regulator of the unit groups $\mathcal{E}$ and $\mathcal{W}(g)$. Note that

$$\log|\epsilon_0| = \mathbf{e}\cdot\mathbf{c}^T$$

where $\mathbf{e} = (\log|\epsilon(a,g)|, \ldots, \log|\sigma_g^{m-2}(\epsilon(a,g))|)$ and $\mathbf{c} = (c_0, \ldots, c_{m-2})$. We need to express the value of $\log|\sigma(\epsilon_0)|$ in terms of $\mathbf{e}$ and $\mathbf{c}^T$ for a given $\sigma \in G$. Observe that

$$\log|\sigma_g(\epsilon_0)| = \mathbf{e}\cdot E\cdot\mathbf{c}^T$$

where E is the following $(m-1)\times(m-1)$ matrix:

$$E = \left[\begin{array}{c|ccc} 0 & & & \\ \vdots & & I_{m-2} & \\ 0 & & & \\ \hline -1 & -1 & \ldots & -1 \end{array}\right]_{(m-1)\times(m-1)}$$

in which I_{m-2} is the identity matrix of dimension $(m-2)\times(m-2)$. Since $\sigma_g^m = \mathrm{id}$, we also have $E^m = I_{m-1}$. It is obvious that the eigenvalues of E are mth roots of unity except 1.

The regulator of $\mathcal{W}(g)$ is given by the determinant

$$\mathrm{Reg}(\mathcal{W}(g)) = \det[2\log(|\sigma_g^{i+j}(\omega)|)].$$

Since $\omega(a,g) \approx \epsilon(a,g)^{\gamma_g(\sigma_g)}$, we have $\mathrm{Reg}(\mathcal{W}(g)) = \mathrm{Reg}(\mathcal{E})\cdot\gamma_g(E)$. It follows that $[\mathcal{E}:\mathcal{W}(g)] = \det(\gamma_g(E))$. The eigenvalues of the matrix $\gamma_g(E)$ are given by $\gamma_g(\zeta_m^j)$ where j runs through $\{1,\ldots,m-1\}$. This finishes the proof. □

3. *Schoof's algorithm*

In this section we give a brief summary of Schoof's algorithm which investigates the class numbers h_p of real cyclotomic fields $\mathbf{Q}_{(p)} = \mathbf{Q}(\zeta_p+\zeta_p^{-1})$ of prime conductors p [9]. We specialize on its first step. The computations in the elliptic case are in complete analogy with the real cyclotomic case. For details of the elliptic analogue, see [5].

Throughout this section, let G be the Galois group of the extension $\mathbf{Q}_{(p)}/\mathbf{Q}$. A finite $\mathbf{Z}[G]$-module A is a product of its l-parts $A\otimes\mathbf{Z}_l$. We write $x^{(p-1)/2}-1 = \prod\varphi(x)$ as a product of distinct irreducible polynomials $\varphi(x)\in\mathbf{F}_l[x]$. Each l-part of A can be decomposed as a product of eigenspaces A_φ, each of which admits a filtration with simple subquotients isomorphic to the residue field $\mathbf{F}_q \cong \mathbf{F}_l[x]/(\varphi(x))$. The order of a simple Jordan–Hölder factor is the order $q = l^f$ where f is the degree of φ and its degree d is the order of x modulo $\varphi(x)$.

For any $\mathbf{Z}[G]$-module A, the additive group $A^\perp = \mathrm{Hom}_{\mathbf{Z}[G]}(A,\mathbf{Z}[G])$ is a $\mathbf{Z}[G]$-module via $(\lambda f)(a) = \lambda f(a) = f(\lambda a)$ for $\lambda\in\mathbf{Z}[G]$ and $a\in A$. Let U be the unit group of $\mathbf{Q}_{(p)}$ and let $\mathcal{C}$ be its subgroup of cyclotomic units. It is a well-known fact that $h_p = [U:\mathcal{C}]$. Consider the $\mathbf{Z}[G]$-module $B = U/\mathcal{C}$. Let l be a prime number. Note that h_p is divisible by l if and only if $B[l]$, the subgroup of l-torsion elements of B, admits a nontrivial Jordan–Hölder factor.

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

It turns out that $B[l]^{\perp}$ is Jordan–Hölder isomorphic to $B[l]$. As a result one can alternatively work with the Galois module $B[l]^{\perp}$ in order to decide if h_p is divisible by l or not.

Let η be a cyclotomic unit generating $\mathcal{C}$ as a $\mathbf{Z}[G]$-module and let $\mathcal{S}$ be the set of unramified prime ideals of $\mathbf{Q}_{(p)}(\zeta_{2l})$. Each prime ideal $\mathfrak{R} \in \mathcal{S}$ lies over a rational prime $r \in \mathbf{Z}$ such that $r \equiv 1 \pmod{2l}$ and $r \equiv \pm 1 \pmod{p}$ by class field theory. To each $\mathfrak{R} \in \mathcal{S}$ we attach an element $f_{\mathfrak{R}}(\eta) = \sum_{\sigma \in G} c_\sigma(\eta)\sigma$ whose coefficients $c_\sigma(\eta)$ are uniquely determined modulo l by the equation $(\sigma^{-1}(\eta))^{(r-1)/l} \equiv \zeta_l^{c_\sigma(\eta)} \pmod{\mathfrak{R}}$ for some fixed choice of ζ_l. Let I be the augmentation ideal of the group ring $\mathbf{F}_l[G]$. There is an isomorphism of $\mathbf{Z}[G]$-modules

$$B[l]^{\perp} \cong I/\{f_{\mathfrak{R}}(\eta) | \mathfrak{R} \in \mathcal{S}\}. \tag{3.1}$$

This isomorphism can be obtained by using Kummer theory and Chebotarev's density theorem. The idea is to attach $\mathbf{Z}[G]$-homomorphisms to certain Frobenius automorphisms (see [9, Theorem 2.2] for details). For simplicity, this isomorphism can also be formulated in terms of polynomials. Replacing a generator σ of the cyclic group G with x, we can consider elements $f_{\mathfrak{R}}(\eta)$ in the ring $\mathbf{F}_l[x]/(x^m - 1)$ where $m = [\mathbf{Q}_{(p)} : \mathbf{Q}]$.

The first step of Schoof's algorithm checks if $B^{\perp}$, equivalently B, admits any Jordan–Hölder factor of order $q = l^f$. Set $\delta = \gcd(m, q-1)$. The first step of the algorithm is trivial if $\delta = 1$ since Jordan–Hölder factors of degree $d = 1$ do not occur. If $\delta > 1$, then we construct elements $f_{\mathfrak{R}}(\eta)$ in the ring $\mathbf{F}_l[x]/(x^m - 1)$ and then reduce them to $\mathbf{F}_l[x]/(x^\delta - 1)$. The algorithm will be faster if we directly construct elements $f_{\mathfrak{R}}(\eta)$ in the latter ring. Being in the augmentation ideal, each $f_{\mathfrak{R}}(\eta)$ is divisible by $x-1$. If the greatest common divisor of several $f_{\mathfrak{R}}(\eta)$ is trivial, namely $x-1$, at some point, then we conclude that there is no contribution from the factor(s) φ of degree f by using the isomorphism (3.1). This is what happens most of the time, and this part of the algorithm must be as efficient as possible.

If $f_{\mathfrak{R}}(\eta)$ is divisible by some specific φ for several attempts, for example 10, then we suspect that $B_{\varphi}^{\perp}$ is nontrivial. In that case, we proceed to the second step of the algorithm in which we lift elements $f_{\mathfrak{R}}(\eta)$ to certain rings in order to determine the possible structure of $B_{\varphi}^{\perp}$. In the third and last step it is proved that $B_{\varphi}^{\perp}$ is isomorphic to the module found in the second part. This last step requires the computation of certain cyclotomic units with high precision and taking their lth roots uniquely.

4. *Improvement of the algorithm*

In this section we explain how we improve the elliptic analogue of Schoof's algorithm by using $\mathcal{W}(g)$ instead of $\mathcal{E}$. The reader is warned not to confuse the use of same symbols for analogous objects in this section and the previous section.

Let K be an imaginary quadratic field of class number 1, and let $\mathfrak{p}$ be a prime ideal of norm relatively prime to $6d_K$. Let $K_{\mathfrak{p}}$ be the ray class field of K of conductor $\mathfrak{p}$. Stark shows that the Galois module

$$B = \mathcal{O}_{K_{\mathfrak{p}}}^{\times}/\mathcal{E}$$

is of order precisely the class number of $K_{\mathfrak{p}}$ [12]. Moreover, we have generalized Schoof's algorithm to these fields. We find all Jordan–Hölder factors of order less than 2000 in this module for conductors $\mathfrak{p}$ with $N(\mathfrak{p}) < 700$ [5].

Let l be a prime number and let $F = K_{\mathfrak{p}}(\zeta_{lW})$ where W is the number of roots of units in $\mathcal{O}_K$. Let $\mathcal{S}$ be the set of unramified degree-one prime ideals of F. In other words, $\mathcal{S}$ is the set of prime ideals lying over a rational prime $r \in \mathbf{Z}$ which totally splits in the extension $F/\mathbf{Q}$. Each such prime ideal $\mathfrak{R} \subset F$ must be lying over a degree-one prime ideal $\mathfrak{r} = (\pi_{\mathfrak{r}})$ of K such that its generator $\pi_{\mathfrak{r}}$ is congruent to a root of unity of $\mathcal{O}_K$ modulo $\mathfrak{p}$. Note that $r = N(\pi_{\mathfrak{r}})$ and we have $r \equiv 1 \pmod{l}$ by class field theory as well. Let G be the Galois group of the

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

extension $K_{\mathfrak{p}}/K$. To each $\mathfrak{R} \in \mathcal{S}$ and $\varepsilon \in \mathcal{O}_{K_{\mathfrak{p}}}^{\times}$ we attach an element

$$f_{\mathfrak{R}}(\varepsilon) = \sum_{\sigma \in G} c_{\sigma}(\varepsilon)\sigma$$

in the group ring $\mathbf{F}_l[G]$. The coefficients $c_{\sigma}(\varepsilon)$ are uniquely determined modulo l by the equation $(\sigma^{-1}(\varepsilon))^{(r-1)/l} \equiv \zeta_l^{c_{\sigma}(\varepsilon)} \pmod{\mathfrak{R}}$ for some fixed choice of ζ_l. In complete analogy with the real cyclotomic case (see equation (3.1)), there is an isomorphism of $\mathbf{Z}[G]$-modules in the elliptic case [**5**, Theorem 2.4]

$$B[l]^{\perp} \cong I/\{f_{\mathfrak{R}}(\epsilon(a,g))|\mathfrak{R} \in \mathcal{S}\}.$$

The major difficulty we have previously encountered is to find the congruence values $\sigma(\epsilon(a,g)) \pmod{\mathfrak{R}}$ for each $\sigma \in G$. In order to apply our previous algorithm, we need to evaluate minimal polynomials of several elliptic units using high precision complex numbers and then order their roots modulo a totally split prime according to the Galois action. This is a task feasible in the range $\mathfrak{p} < 700$. However, for extensions with larger conductor, such computations become impractical because of the growth of coefficients of minimal polynomials.

We overcome this difficulty in this paper by using units obtained by the special values of the Weierstrass $\wp$-function, namely the units $\omega(a,g)$, instead of the units $\epsilon(a,g)$. These elliptic units can also be expressed in terms of x-coordinates of points on an elliptic curve. For this purpose, we work with an elliptic curve E with complex multiplication by $\mathcal{O}_K$.

There is a well-known formula which produces elliptic curves with designated complex multiplication. More precisely, we have [**13**]

$$E : y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}. \tag{4.1}$$

Here $j = j(\mathcal{O}_K)$ is the classical j-invariant. Note that this formula is valid in the generic case, i.e. $d_K < -4$. A quick verification shows that all these curves have good reduction at any degree-one prime ideal of norm not dividing $6d_K$ for imaginary quadratic fields with $-d_K \in \{7, 8, 11, 19, 43, 67, 163\}$.

There is a natural group structure on E. Let O be the zero point on the elliptic curve E. Then the group of $\mathfrak{p}$-torsion points of E is defined by

$$E[\mathfrak{p}] = \{P \in E : [\alpha]P = O \ \forall \alpha \in \mathfrak{p}\}.$$

The uniformization theorem for elliptic curves says that there exists a unique lattice $\Lambda \subset \mathbf{C}$ such that E is parametrized by the Weierstrass $\wp$-function $\wp(z,\Lambda)$ and its derivative [**10**, I.4.3]. Since E has complex multiplication by $\mathcal{O}_K = \langle \tau, 1 \rangle$, we must have $\Lambda = \langle c\tau, c \rangle$ for some constant c. Recall that a is given by $\overline{\pi}_{\mathfrak{p}}/p = a_1\tau + a_2$, so we have

$$P_a = (c^{-2}\wp_a(\tau), c^{-3}\wp_a'(\tau)) \in E[\mathfrak{p}].$$

Moreover, we have the following equality which is independent of the constant c, and therefore the chosen elliptic curve:

$$\omega(a,g) = \frac{x([g^2]P_a) - x([g]P_a)}{x([g]P_a) - x(P_a)} \in \mathcal{O}_{K_{\mathfrak{p}}}^{\times}.$$

In order to generate abelian extensions of K, the values of Weber function at torsion points can be used. As a consequence of the main theorem of complex multiplication, we have $K_{\mathfrak{p}} = K(x(E[\mathfrak{p}])^{W/2})$. See [**10**, II.5.6], for instance. In order to express the units $\omega(a,g)$ in terms of x-coordinates of $\mathfrak{p}$-torsion points of E, we restrict ourselves to the case where $W = 2$.

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

The isogeny $[g] : E \to E$ is explicit and enables us to relate conjugates in the set $x(E[\mathfrak{p}])$ algebraically. Moreover, this action is compatible with the Galois action of $\sigma_g \in G$ (see [6, Chapter 10]). For each integer $i \geqslant 0$, we have

$$x([g^i]P_a)^{\sigma_g} = x([g^{i+1}]P_a).$$

Consider a degree-one prime ideal $\mathfrak{r} = (\pi_\mathfrak{r})$ of K which totally splits in $K_\mathfrak{p}$. The isogeny $[\pi_\mathfrak{r}] : E \to E$ is a rational function with coefficients from the Hilbert class field H. In our case we have simply $H = K$. Reducing $[\pi_\mathfrak{r}]$ modulo $\mathfrak{r}$ we obtain a map on $E/\mathbf{F}_r$ where $r = N(\mathfrak{r})$. Without loss of generality we have $\overline{[\pi_\mathfrak{r}]} = \mathrm{Frob}_r$ [10, II.5.4]. If the reduced map is not the Frobenius map than we can twist E by a quadratic nonresidue modulo r. See the example at the end of this section for an illustration of this phenomenon.

The prime ideal $\mathfrak{r} \subset \mathcal{O}_K$ splits completely in $K_\mathfrak{p}$, thus we may assume $\pi_\mathfrak{r} = \alpha\pi_\mathfrak{p} + 1$ for some $\alpha \in \mathcal{O}_K$ by class field theory. It follows that $E(\mathbf{F}_r) = \mathrm{Ker}(\overline{[\alpha\pi_\mathfrak{p}]})$. Thus if we start with an arbitrary point P_0 of $E(\mathbf{F}_r)$ and compute $[\alpha]P_0$, we must obtain a point of $E[\mathfrak{p}]$ modulo r. For simplicity suppose that $\pi_\mathfrak{r} = k\pi_\mathfrak{p} + 1$ for some positive integer k so that we can apply the isogeny $[k]$ to the point P_0 easily. If the resulting point $[k]P_0$ is trivial then we can repeat our computation until we find a nontrivial $\mathfrak{p}$-torsion point. Observe that we do not need to know the minimal polynomial of elements generating the ray class field $K_\mathfrak{p}$ for this computation.

As we have seen above, we can obtain a nontrivial $\mathfrak{p}$-torsion point (x_0, y_0) in $E(\mathbf{F}_r)$. Moreover, using the fast arithmetic of elliptic curves, we can also compute

$$(x_i, y_i) \equiv [g^i](x_0, y_0) \pmod{r}.$$

Let $\mathfrak{R}$ be a prime ideal of $K_\mathfrak{p}$ lying over $\mathfrak{r} \subset \mathcal{O}_K$ such that $\omega(a, g) \equiv (x_2 - x_1)/(x_1 - x_0) \pmod{\mathfrak{R}}$. In general, we have

$$\omega(a, g)^{\sigma_g^i} \equiv \frac{x_{2+i} - x_{1+i}}{x_{1+i} - x_i} \pmod{\mathfrak{R}}$$

for all integers $i \geqslant 0$. In other words, for each $\sigma \in G$, we can find the congruences $\sigma(\omega(a, g)) \pmod{\mathfrak{R}}$. This enables us to obtain $f_\mathfrak{R}(\omega(a, g))$ in the ring $\mathbf{F}_l[x]/(x^m - 1)$. Unfortunately this is a multiple of the element $f_\mathfrak{R}(\epsilon(a, g))$. We have

$$f_\mathfrak{R}(\omega(a, g)) = \gamma_g \cdot f_\mathfrak{R}(\epsilon(a, g)).$$

However, this is not a big problem. When we perform the first step of the algorithm with the elements $f_\mathfrak{R}(\omega(a, g))$ instead of $f_\mathfrak{R}(\epsilon(a, g))$, all we need to do is to disregard those factors coming from γ_g. We can possibly fail to detect some factors appearing in the Jordan–Hölder filtration of $B[l]^\perp$. Thus we shall repeat our computations for different values of g so that all possible factors φ are checked.

In practice, it is not hard to find a suitable primitive root g modulo p to check if $B_\varphi^\perp$ is trivial or not. It is sufficient to choose g such that $\gcd(\gamma_g, \varphi) = 1$ in the ring $\mathbf{F}_l[x]$. We have encountered no example in which φ divides every γ_g in $\mathbf{F}_l[x]$. Even in the worst cases, such as small values of $\deg(\varphi)$ and l, there is a big majority of primitive roots g which give γ_g relatively prime to φ in $\mathbf{F}_l[x]$.

We now give an example to illustrate what happens when the algorithm is run. We focus on the case $l = p$.

EXAMPLE 1. Let $K = \mathbf{Q}(\sqrt{-43})$ and let $\mathfrak{p}$ be a prime ideal of norm $p = 11$. In this example we will show that $h_\mathfrak{p}$ is not divisible by p. Since $[K_\mathfrak{p} : \mathbf{Q}] = 10$, a relatively small degree, one can find that the class number $h_\mathfrak{p}$ is trivial in a reasonable amount of time with PARI/GP [14]. However, this is not the case if p is large, for example if $p > 50$.

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

The Jordan–Hölder factors of $B[p]^\perp$ come only from the irreducible factors φ of x^m-1 in $\mathbf{F}_p[x]$ where $m=[K_\mathfrak{p}:K]=5$. Recall that Jordan–Hölder factors of degree 1 do not appear, so we can exclude $\varphi=x-1$. Let $g=2$, a primitive root modulo p. We find by Lemma 2.1 that $[\mathcal{E}:\mathcal{W}(g)]=11$. Note that $\gamma_g=x^{10}+x^8-2x-2$ and $\gcd(x^m-1,\gamma_g)=x+7$ in $\mathbf{F}_p[x]$. Now we check whether $B[p]^\perp$ admits any Jordan–Hölder factors coming from the divisors of

$$\frac{x^m-1}{(x-1)(x+7)}\in\mathbf{F}_p[x].$$

In this case every irreducible factor of x^m-1 is linear. As a result we can fix $\delta=m$ and check for all φ, except $x+7$, simultaneously.

Fix $\pi_\mathfrak{p}=(\sqrt{-43}-1)/2$ such that $N(\pi_\mathfrak{p})=p$. Consider the ideal $\mathfrak{r}\subset\mathcal{O}_K$ generated by $\pi_\mathfrak{r}=k\pi_\mathfrak{p}+1$ with $k=11$. This turns out to be a prime ideal of norm $r=1321$. Note that $r\equiv 1 \pmod p$. We will work with the elliptic curve $E:y^2=x^3+Ax+B$ where A and B are as in equation (4.1). This curve has complex multiplication by $\mathcal{O}_K$. Let $\bar{E}$ be the reduction of E modulo r. Over $\mathbf{F}_r$, we have $A\equiv 1190$ and $B\equiv 353$. Consider the point $P_0=(2,182)\in\bar{E}(\mathbf{F}_r)$. We find that $[k]P_0$ is not in $\bar{E}[\mathfrak{p}]$ since $[pk]P_0\neq O$. This means that the trace of the Frobenius map is of opposite sign. Since 7 is a quadratic nonresidue modulo r, the following elliptic curve gives a suitable quadratic twist of $\bar{E}$:

$$\bar{E}':y^2=x^3+7^2Ax+7^3B.$$

Now we consider the point $P_0'=(1,475)$ in $\bar{E}'(\mathbf{F}_r)$. In this case $[k]P_0'=(914,1129)$ is obviously in $\bar{E}'[\mathfrak{p}]$. One can verify this also by computing $[pk]P_0'=O$. If we had obtained $[k]P_0'=O$ then we would change the x-coordinate and try again.

We set $(x_0,y_0)=[k]P_0'$ and compute $(x_i,y_i)=[g^i](x_0,y_0)$ for $0\leqslant i<m$:

i	0	1	2	3	4
x_i	914	943	765	1220	35
y_i	1129	139	395	112	302

Now we are ready to find $f_\mathfrak{R}(\omega(a,g))$. A pth root of unity in $\mathbf{F}_r$ is obtained by raising a primitive root in $\mathbf{F}_r$, say 13, to its $(r-1)/p$th power. Let $\mathfrak{R}$ be the unique ideal of $F=K_\mathfrak{p}(\zeta_p)$ lying over $\mathfrak{r}$ such that $x(P_a)\equiv x_0$ and $\zeta_p\equiv 13^{(r-1)/p}$ modulo $\mathfrak{R}$. One can choose $\mathfrak{R}$ differently, but this only changes $f_\mathfrak{R}$ up to a unit. See Schoof for details [9, Theorem 3.2].

The constant term of $f_\mathfrak{R}(\omega(a,g))$ is obtained by

$$\left(\frac{x_2-x_1}{x_1-x_0}\right)^{(r-1)/p}\equiv\zeta_p^5 \pmod{\mathfrak{R}}.$$

Similarly other coefficients can be found and we have $f_\mathfrak{R}(\omega(a,g))=6x^4+4x^3+x^2+6x+5$. In the ring $\mathbf{F}_p[x]/(x^m-1)$, we have

$$\gcd\left(\frac{x^m-1}{(x-1)(x+7)},f_\mathfrak{R}(\omega(a,g))\right)=1.$$

Thus we conclude that there is no contribution to $B[p]^\perp$ from the factors of x^m-1 except $x+7$.

We have to check for $\varphi=x+7$ separately. For this purpose, we choose $g=6$. In this case $\gamma_g(x)$ is relatively prime to $x+7$ in $\mathbf{F}_p[x]$. We can similarly find an element $f_\mathfrak{R}(\omega(a,g))$ as we have done above. If the resulting element is coprime to $x+7$, we can conclude that there is no contribution from this factor either. This is what happens if we repeat our algorithm with the same underlying prime ideal $\mathfrak{r}$ but with this different g. As a result we find that the order of $B[p]^\perp$ is not divisible by p and therefore $h_\mathfrak{p}$ is not divisible by p.

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press

Previously, we have found all Jordan–Hölder factors of order less than 2000 in the Galois module B for conductors $\mathfrak{p}$ with $N(\mathfrak{p}) < 700$. In particular, we show that the class number of $K_{\mathfrak{p}}$, with $d_K = -163$ and $N(\mathfrak{p}) = 307$, is divisible by 307 [5]. Using our improved algorithm, we have checked for another counterexample of the elliptic analogue of Vandiver's conjecture within the range $-d_K \in \{7, 8, 11, 19, 43, 67, 163\}$ and $700 < N(\mathfrak{p}) < 10\,000$. We use the software PARI to do our computations on a computer with a quad-core CPU of 3.10 GHz with less than 1 gigabyte of memory allocated. Our computations take less than 12 hours.

The first step of the algorithm indicates that it is very likely that the class number of $K_{\mathfrak{p}}$, with $d_K = -43$ and $N(\mathfrak{p}) = 5521$, is divisible by 5521. In order to prove this one may attempt to use the method given in our previous paper [5, Example 2.9]. For this, we need to obtain certain elliptic units with high r-adic precision, take their 5521st roots uniquely and verify that the resulting polynomial is integral. Those computations rely on the PARI command `factorpadic` and it is not feasible to use the same method in this example which requires a much higher precision.

Vandiver's conjecture has been verified for primes up to 163 million [1]. Using the analogy between the Bernoulli and Hurwitz numbers [8], we hope to improve the range $N(\mathfrak{p}) < 10\,000$ in a future paper.

Acknowledgement. We would like to thank the referee for carefully reading our manuscript and making useful comments which helped improve the quality of the paper.

References

1. J. P. Buhler and D. Harvey, 'Irregular primes to 163 million', *Math. Comp.* 80 (2011) no. 276, 2435–2444.
2. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication* (Wiley, New York, 1989).
3. A. Gee, 'Class fields by Shimura reciprocity', PhD Thesis, Universiteit Leiden, 2001.
4. D. Kubert and S. Lang, *Modular units*, Grundlehren der mathematischen Wissenschaften 244 (Spinger, Berlin, 1981).
5. O. Kucuksakalli, 'Class numbers of ray class fields of imaginary quadratic fields', *Math. Comp.* 80 (2011) no. 274, 1099–1122.
6. S. Lang, *Elliptic functions*, 2nd edn, Graduate Texts in Mathematics 112 (Springer, New York, 1987).
7. H. Oukhaba, 'Index formulas for ramified elliptic units', *Compos. Math.* 137 (2003) no. 1, 1–22.
8. G. Robert, 'Nombres de Hurwitz et unités elliptiques. Un critère de régularité pour les extensions abéliennes d'un corps quadratique imaginaire', *Ann. Sci. Éc. Norm. Supér.* (4) 11 (1978) no. 3, 297–389.
9. R. Schoof, 'Class numbers of real cyclotomic fields of prime conductor', *Math. Comp.* 72 (2003) no. 242, 913–937.
10. J. S. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151 (Springer, New York, 1994).
11. W. Sinnott, 'On the Stickelberger ideal and the circular units of a cyclotomic field', *Ann. of Math.* (2) 108 (1978) no. 1, 107–134.
12. H. M. Stark, 'L-functions at $s = 1$. IV. First derivatives at $s = 0$', *Adv. Math.* 35 (1980) no. 3, 197–235.
13. L. Washington, *Elliptic curves. Number theory and cryptography*, 2nd edn, Discrete Mathematics and its Applications (Chapman & Hall/CRC, Boca Raton, FL, 2008).
14. PARI/GP, version 2.3.5, http://pari.math.u-bordeaux.fr/, Bordeaux, 2010.

Ömer Küçüksakallı
Department of Mathematics
Middle East Technical University
06800 Ankara
Turkey

komer@metu.edu.tr

https://doi.org/10.1112/S1461157014000163 Published online by Cambridge University Press