doi：103969/j. issn. 0490-6756. 2016. 01. 008

一类 Q 曲线的基本算术性质

任 远
(首都师范大学数学学院，北京 100037)

摘 要：本文对任意模 4 余 3 的正整数 D 构造了一类以判别式为 $-D$ 的虚二次域的整数环为复乘的椭圆曲线,并将考察其基本性质,如有理扭点,自同态环以及模性等.

关键词：椭圆曲线；复乘；Q 曲线
中图分类号：O156.2 **文献标识码**：A **文章编号**：0490-6756(2016)01-0042-05

Some basic arithmetic properties of a class of Q-curves

REN Yuan
(Department of Mathematics, Capital Normal University, Beijing 10037, China)

Abstract: In this paper, we construct elliptic curves with complex multiplications by the integer ring of $K = \mathbf{Q}(\sqrt{-D})$ for any positive integer D congruent to 3 modulo 4 and establish their basic properties. Our results generalize those of Gross.

Key words: Elliptic Curve; Complex multiplication; Q-curve
(2000 MSC 14H52)

1 Introduction

In number theory, the arithmetic of elliptic curves over a number field has been an area of great interests. To understand it, much effort have been devoted to the study of the congruent number elliptic curve $E: y^2 z = x^3 - xz^2$ (See, for example, Ref. [1,2]).

The congruent number elliptic curve is an elliptic curve with CM by the Gauss integer ring $\mathbf{Z}[i]$. In Ref. [3], Gross defined some elliptic curves with complex multiplications by the integer ring of $K = \mathbf{Q}(\sqrt{-p})$ for any prime p congruent to 3 modulo 4 (see also Ref. [4]). In that paper, Gross also established the basic properties of such curves, such as their rational torsion groups, ε-factors, endomorphism rings and modularity.

In this paper, we will generalize Gross' results to the case $K = \mathbf{Q}(\sqrt{-D})$ with D any positive integer congruent to 3 modulo 4, which will be called Gross curves. In the second section, we construct the Gross curves from the point of view of CM theory. Let E be any such curve and $F = \mathbf{Q}(j(E))$, then the main results can be summarized as the following

Theorem 1.1 (1) $E(F)_{\mathrm{tor}} \simeq \mathbf{Z}/2\mathbf{Z}$ or 0, according to whether $(\frac{2}{D}) = 1$ or -1;

(2) The ε-factor of $L(E,s)$ equals to $(\frac{2}{D})$;

(3) There is a nontrivial morphism $\pi: X_0(D^2) \to E$ over F, where $X_0(D^2)$ is the modular curve of level D^2.

It is hoped that the results here will be useful

收稿日期：2014-10-12
作者简介：任远(1986—)，男，四川成都人，博士，主要研究方向为数论及其应用. E-mail：ryl98628@163.com

for further study of the arithmetic properties of the Gross curves.

2 Construction of the Gross curves

Let D be a square free integer with $D > 3$ and $D \equiv 3 \pmod 4$.

Let $K = \mathbf{Q}(\sqrt{-D})$, O the integer ring of K, H = the Hilbert class field of K. For any ideal $a \subseteq O$, let $K(a)$ be the ray class field modulo a.

Consider the continuous homomorphism $\varphi_0 : K^\times(\prod_v O_v^\times) \to K^\times(O_\infty^\times := C^\times)$ satisfying

(1) $\varphi_0|_{K^\times} = \mathrm{id}_{K^\times}$;

(2)
$$\begin{array}{ccc} \prod_v O_v^\times & \longrightarrow & \{\pm 1\} \\ \downarrow & & \uparrow \delta \\ \prod_{v|(\sqrt{-D})} O_v^\times & \longrightarrow & (O/\sqrt{-D})^\times \end{array}$$

Here δ maps $x = a + b\dfrac{1+\sqrt{-D}}{2}$ $(a,b \in \mathbb{Z})$ to $\left(\dfrac{x \pmod{\sqrt{-D}}}{D}\right) = \left(\dfrac{a+\frac{b}{2}}{D}\right)$, where $\left(\dfrac{\cdot}{D}\right)$ is the Jacobi symbol. Note that $D \equiv 3 \pmod 4$ ensures this φ_0 is well defined.

From

$$0 \to K^\times(\Pi_v O_v^\times) \to A_{K^\times} \to Cl(K) \to 0$$

we get

$$0 \to \mathrm{Hom}(Cl(K), \bar{K}^\times) \to \mathrm{Hom}(A_{K^\times}, \bar{K}^\times) \to \mathrm{Hom}(K^\times(\prod_v O_v^\times), \bar{K}^\times) \to 0$$

because $\mathrm{Ext}^1(Cl(K), \bar{K}^\times) = 0$ as $\bar{K}^\times$ is divisible hence injective. From this, we have

Theorem 2.1 There is a continuous homomorphism $\varphi : A_K^\times \to \bar{K}^\times$ such that $\varphi|_{K^\times(\prod_v O_v^\times)} = \varphi_0$, in particular this character is of conductor $(\sqrt{-D})$. This character is unique up to a character of $Cl(K)$.

Let $\chi : A_H^\times \to K^\times$ be defined as $\chi = \varphi \circ N_K^H$, where N_K^H is the norm map. By the CM theory, there is a unique isogeny class of elliptic curves over H with CM by O and the associated character χ. We will call any elliptic curves in this isogeny class a Gross curve of level D.

From now on, we fix an elliptic curve E in this isogeny class and let $F = \mathbf{Q}(j(E))$. Then we have $\mathrm{Gal}(H/F) = <\tau> \cong \mathbf{Z}/(2)$ and $\mathrm{Gal}(H/Q) \cong Cl(K) \rtimes <\tau>$, with τ acts as inverse.

3 Rational torsion points and the ε − factors

Recall that (see Ref. [3], Chapter1) for any nonzero prime $\mathfrak{p}$ of O, the action of G_H on $E[\mathfrak{p}]$ is given by $\rho_\mathfrak{p} : G_H \to \mathrm{Aut}(E[\mathfrak{p}])$ which sending $x = (x_v)$ to $\chi(x) \cdot N_{K_\mathfrak{p}}^{H_\mathfrak{p}}(x)$ for any $x \in A_H^\times$. This allows us to determine the H − rational torsion points as following:

Proposition 3.1 Let $d \in \mathbf{Z}$ satisfying $(d, D) = 1$, $d \equiv 1 \pmod 4$ and $E^{(d)}$ the quadratic twist of E by d. Then we have

(1) If (2) splits in K, then $E(H)_{\mathrm{tor}} = E[2]$ and $E(F)_{\mathrm{tor}} \cong \mathbf{Z}/2\mathbf{Z}$;

(2) If (2) is inertia in K, then $E(H)_{\mathrm{tor}} = E(F)_{\mathrm{tor}} \cong \{1\}$.

Proof When D is a prime, this has been proved in Ref. [3], so we may assume D is not a prime. Note that as $(-d, D) = 1$ and $d \equiv 1 \pmod 4$, $E^{(D)}$ has good reduction at places of H over (2) and bad reduction at those dividing dD.

Let $\mathfrak{p}$ be a nonzero prime of O. We claim that if $(\mathfrak{p}) \geq 3$, then $E[\mathfrak{p}] \not\subseteq E(H)$ This is because if $(\mathfrak{p}, D) = 1$, then E has good reduction at the places of H over $\mathfrak{p}$. Then by the Lubin-Tate theory, we have $\mathrm{Gal}(H(E[\mathfrak{p}])/H) \cong (O/\mathfrak{p})^\times$ and so $E[\mathfrak{p}] \not\subseteq E(H)$. If $\mathfrak{p} \mid D$, we choose another prime $\mathfrak{q}$ of O which also divides D and w a place of H over $\mathfrak{q}$. By the construction of φ, there is some $x_\mathfrak{q} \in O_\mathfrak{q}^\times$ such that $\varphi(x_\mathfrak{q}) = -1$; as H over K is unramified everywhere, there is $y_w \in O_{H_w}^\times$ with $N_{K_\mathfrak{q}}^{H_w}(y_w) = x_\mathfrak{q}$. Then we have $\rho_\mathfrak{p}((\ldots, y_w, \ldots)) = \varphi(x_\mathfrak{q}) = -1$, so also $E[\mathfrak{p}] \not\subseteq E(H)$. This proves the claim.

If (2) is inertia in K, then $\# k(\mathfrak{p}) \geq 3$ for any $\mathfrak{p}$, so proves the second assertion.

If (2) splits in K, say $(2) = \mathfrak{p} \cdot \bar{\mathfrak{p}}$. Then as $E[2] = E[\mathfrak{p}] \oplus E[\bar{\mathfrak{p}}]$, it is easy to see from the above argument that $E[2] \subseteq E(H)$. Because $\mathfrak{p}^\tau = \bar{\mathfrak{p}}$, we have $E(F) = E(H)^\tau \cong \mathbf{Z}/(2)$.

Let φ be the character as in Prop 3.1, which is determined up to $Cl(k)$.

Let ψ be the unitarization of the associated Hecke character of φ. So we have

$$\psi(x) = \left(\frac{x_\infty}{|x_\infty|_C}\right)^{-1} \cdot \prod_{v\mid D}\left(\frac{x_v(\mathrm{mod}\ \sqrt{-D})}{p_v}\right)$$

for any $x = (x_v) \in C^\times \cdot \prod O_v^\times$, where p_v means the prime below v. Now we want to determine the ε-factor of $L(s,\psi)$.

Fix an additive character a_v for any any place v of K as in Ref. [5]. Then for any unitary Hecke character ψ, define (Ref. [6])

(1) L- factor:

If $v < \infty$ and ψ_v is unramified, let $L_v(s,\psi_v) = [1-\psi_v(\mathfrak{p}_v)N(\mathfrak{p}_v)]^{-1}$;

If $v < \infty$ and ψ_v is ramified, let $L_v(s,\psi_v) = 1$;

If $v = \mathbb{R}$ and $\psi_v = (\mathrm{sgn})^\delta$ ($\delta = 0,1$), Let $L_v(s,\psi_v) = \pi^{-\frac{s+\delta}{2}}\Gamma(\frac{s+\delta}{2})$;

If $v = \mathbf{C}$ and $\psi_v(x_v) = |x_v|_v^\nu \cdot \left(\frac{x_v}{|x_v|_v^{\frac{1}{2}}}\right)^k$ for some $\nu \in \mathrm{i}\mathbb{R}$ and $k \in \mathbb{Z}$, let

$$L_v(s,\psi_v) = 2(2\pi)^{s+\nu+\frac{|k|}{2}} \cdot \Gamma(s+\nu+\frac{|k|}{2}).$$

(2) γ-factor:

$\gamma_v(s,\psi_v,a_v) = \zeta_v(1-s,\psi_v^{-1},\hat{\Phi}_v)\zeta_v(s,\psi_v,\Phi_v)$, for any $\varphi_v \in S(K_v)$.

(3) ε-factor:

$$\varepsilon_v(s,\psi_v) = \frac{\gamma_v(s,\psi_v,a_v)\cdot L_v(s,\psi_v)}{L_v(1-s,\psi_v^{-1})},$$ which is independent from the choice of a_v. Moreover, we know that $\varepsilon_v = 1$ for any finite place v such that both ψ_v and a_v are unramified. Let $\varepsilon(s,\psi) = \prod \varepsilon_v(s,\psi_v)$.

Our aim is to calculate $\varepsilon_v(\frac{1}{2},\psi_v)$ (for any v) and $\varepsilon(\frac{1}{2},\psi)$ for the unitary Hecke character ψ corresponding to E.

• $v = \infty$:

We have $K_v = C$ and $\nu = 0, k = -1$, so

$$L_v(s,\psi_v) = 2(2\pi)^{s+\frac{1}{2}} \cdot \Gamma(s+\frac{1}{2})$$

and then

$$L_v(1-s,\psi_v^{-1}) = 2(2\pi)^{1-s+\frac{1}{2}} \cdot \Gamma(1-s+\frac{1}{2}).$$

Then by the calculation in Ref. [5], we get

$$\varepsilon_v(\frac{1}{2},\psi_v) = \gamma_v(\frac{1}{2},\psi_v,a_v) = \mathrm{i}.$$

• $v \times \infty \cdot D$:

In this case, both a_v and ψ_v are unramified, so $\varepsilon_v(\frac{1}{2},\psi_v) = 1$.

• $v \mid D$:

Notations as in Ref. [5], we have the conductor f_v of ψ_v is $(\sqrt{-D})$ and $\delta_v = (\sqrt{-D})$. Moreover, $\sqrt{-D}$ is a uniformizer at v.

Let $p_v^{-t_v} = \psi_v(\sqrt{-D})$ and $\psi_v' = \psi_v \cdot \|_v^{-t_v}$ so that $\psi_v'(\sqrt{-D}) = 1$ and $\varepsilon_v(s,\psi_v) = \varepsilon_v(s+t_v,\psi_v')$.

By Ref. [5], we have

$$\varepsilon_v(s,\psi_v)^{-1} = N(\delta_v f_v)^{s+t_v-\frac{1}{2}} \cdot N(f_v)^{-\frac{1}{2}} \cdot \sum_{a\in(O_v^\times/1+\mathfrak{p})} \psi'(a)\mathrm{e}^{2\pi\mathrm{i}(-\frac{tra}{D})} = p_v^{2s+2t_v-\frac{3}{2}} \cdot \sum_{a\in(\mathbf{Z}/p_v)^\times}\left(\frac{a}{p_v}\right)\mathrm{e}^{2\pi\mathrm{i}(-\frac{2a}{D})}.$$

So that we get

$$\varepsilon_v(\frac{1}{2},\psi_v)^{-1} = p_v^{2t_v} \cdot \frac{1}{\sqrt{p_v}} \cdot \left(\frac{(-2D/p_v)}{p_v}\right) \cdot \sum_{a\in(\mathbf{Z}/p_v)^\times}\frac{a}{p_v}\mathrm{e}^{2\pi\mathrm{i}\frac{a}{p_v}}.$$

By the well known result about the signature of Gauss sum (Ref. [7]), we find that:

$$\varepsilon_v(\frac{1}{2},\psi_v) = \psi_v(-D)\cdot\left(\frac{-2D/p_v}{p_v}\right), \text{ if } p_v \equiv 1 \pmod 4;$$

$$\varepsilon_v(\frac{1}{2},\psi_v) = -\mathrm{i}\cdot\psi_v(-D)\cdot\left(\frac{-2D/p_v}{p_v}\right), \text{ if } p_v \equiv 3 \pmod 4.$$

$$\varepsilon(\frac{1}{2},\psi) = \left(\frac{2}{D}\right).$$

Because $1 = \psi(-D) = \psi_\infty(-D)\cdot\prod_{v\mid D}\psi_v(-D)$ and $\psi_\infty(-D) = -1$, we have $\prod_{v\mid D}\psi_v(-D) = -1$. Then the result is easily verified.

4 Endomorphism rings and the modularity

In this section, we will determine the endomorphism rings of $A^{(d)} = Res_{F/\mathbf{Q}}(E^{(d)})$ for any d

$\in \mathbf{Q}^{\times}$.

Firstly, one observes that

$$\mathrm{End}\,(A^{(d)} = \prod_{\sigma,\sigma' \in \mathrm{Gal}(H/K)} \mathrm{Hom}((E^{(d)})^{\sigma},(E^{(d)})^{\sigma}{}'),$$

as

$A^{(d)} = \prod_{\sigma\in \mathrm{Gal}(H/K)} (E^{(d)})^{\sigma}$ over H. In particular, an element of End $(A^{(d)}$ can be represented by a matrix $\alpha = (\varphi_{\sigma,\sigma'})$. For any $\rho \in \mathrm{Gal}(H/K)$, we have $\rho(\alpha) = (\rho(\varphi_{\sigma,\sigma'})) = (\varphi_{\rho\sigma,\rho\sigma'})$.

Let $R_K = \sum_{\sigma\in \mathrm{Gal}(H/K)} \mathrm{Hom}((E^{(d)})^{\sigma},E^{(d)})\cdot\sigma$, be the ring such that $(\varphi\cdot\sigma)\cdot(\varphi'\cdot\sigma') = (\varphi\circ(\varphi')^{\sigma})\sigma\sigma'$.

Lemma 4.1 $R_K \otimes \mathbf{Q} = \mathrm{End}_K(A^{(d)}) \otimes \mathbf{Q}$. Immediate from the above arguments.

Lemma 4.2 $R_K \otimes \mathbf{Q}$ is commutative.

Choose a set of ideals $\{a\}$ in O relatively prime to D, such that $\{\sigma_a\} = \mathrm{Gal}(H/K)$. By Ref. [8], page 42, Proposition 1.5, there is a $\varphi_a \in \mathrm{Hom}((E^{(d)})^{\sigma_a},E^{(d)})$ for each a satisfying $\varphi_a \circ (\varphi_b)^{\sigma_a} = \varphi_b\circ(\varphi_a)^{\sigma_b}$. This is what we want for $R_K \otimes \mathbf{Q}$ to be commutative.

Proposition 4.3 $\mathrm{End}_{\mathbf{Q}}(A^{(d)}) \otimes \mathbf{Q}$ is a totally real field.

Proof As $A^{(d)} = \prod_{\sigma\in \mathrm{Gal}(H/K)} (E^{(d)})^{\sigma}$ over H, so $A^{(d)}$ is a simple abelian variety over K. Hence the center of $\mathrm{End}_K(A^{(d)})_{\mathbf{Q}}$ is a CM field (note as $K \subseteq \mathrm{End}_K(A^{(d)})_{\mathbf{Q}}$, it can not be totally real). By Lemma 4.2, $\mathrm{End}_K(A^{(d)})_{\mathbf{Q}}$ is commutative, so it is a CM field itself. Then

$$\mathrm{End}_{\mathbf{Q}}(A^{(d)}) \otimes Q = (\mathrm{End}_K(A^{(d)})_{\mathbf{Q}})^{Gal(K/\mathbf{Q})}$$

is totally real.

Now we come back to the elliptic curve E over F and the original character φ. Recall that E is just an arbitrarily fixed elliptic curve in isogeny class as in Prop 3.1 and $F = \mathbf{Q}(j(E))$. In the following, we always let $A = Res_{F/\mathbf{Q}}E$ be the corresponding abelian variety defined over $\mathbf{Q}$. It is well known that $L(s,A/\mathbf{Q}) = L(s,E/F) = \prod_{\sigma\in \mathrm{Gal}(H/K)} L(s,\varphi^{\sigma})$.

Lemma 4.4 Let $f_{\varphi}(z) = \sum_{(a,D)=1}\varphi(a)\cdot e^{2\pi i\cdot N_{K/\mathbf{Q}}(a)\cdot z}$ ($z\in\mathbb{C}$ with $\mathbf{I_m}(z) > 0$), then $f_{\varphi}(z)$ is an eigenform in $S_2(\Gamma_0(D^2))$.

Proof This is just Lemma 3 of Ref. [9]. Note that $f_{\varphi}(z)$ is an eigenform because $L(s,f_{\varphi}) = L(s,\varphi)$ has Eulerian product.

Let T be the field generated by the image of φ. Then T is a CM field with $T^{+} = \mathbf{Q}(\{a_n\})$.

By Theorem 7.14 and Theorem 7.15 of Ref. [10], there is a sub-abelian variety $i: A \to J_0(D^2)$ over $\mathbf{Q}$ and an embedding $\theta: T^{+} \to \mathrm{End}_{\mathbf{Q}}(A)$, such that $T_n|_A = \theta(a_n)$ for any n, where T_n is the Hecke operator.

Proposition 4.5 There is a $\mathbf{Q}$-curve E/F with character χ such that $Res_{F/\mathbf{Q}}E \cong A$, where $F = \mathbf{Q}(j(E))$.

Proof By Theorem 1 of Ref. [9], A is isogenous to $E^{\oplus h}$ for some elliptic curve with CM by O. Then we have also A isogenous to $(E^{\sigma})^{\oplus h}$ for any $\sigma \in \mathrm{Gal}(H/\mathbf{Q})$. So E' is isogenous to E^{σ} for any $\sigma \in \mathrm{Gal}(H/\mathbf{Q})$, i.e. E' is a $\mathbf{Q}$-curve (note that $\bar{\mathbf{Q}}$-isogeny is automatically H-isogeny).

It is clear that there is a $\mathbf{Q}$-morphism between $\prod_{\sigma}(E')^{\sigma}$ and A. Because $\prod_{\sigma}(E')^{\sigma}$ is simple over $\mathbf{Q}$, this morphism must be an isogeny. Then, modulo the kernel, we find an E such that $Res_{F/\mathbf{Q}}E = \prod_{\sigma}(E)^{\sigma} \cong A$.

As $L(E/F,s) = L(s,\chi) = L(s,A/Q) = \prod \tau L(s,f^{\tau}) = L(s,\chi)$ (up to finite Euler factors), we have $\chi_E = \chi$.

Consider the dual $\pi: J_0(D^2)^{\vee} \to A$ of i, composed with the canonical $X_0(D^2) \to J_0(D^2)^{\vee}$ and an isomorphism $A^{\vee} \cong A$ (as A is a product of elliptic curves), we get a $\mathbf{Q}$-morphism (also denoted by π) $\pi: X_0(p^2) \to A$. Thus we get the following corollary:

Corollary 4.6 There is a non-trivial F-morphism $\pi: X_0(D^2) \to E$.

References:

[1] Han D C. On the BSD conjecture of elliptic curves $E_{D^2}: y^2 - x^3 - d_2 x$ [J]. J Sichuan Univ: Nat Sci Ed, 2013, 50(3): 470.

[2] She D M. On the computing of the Artin root number of the elliptic curve $E_{d^2}: y^2 = x^3 - d^2 x$ over the Gaussian integers[J]. J Sichuan Univ: Nat Sci Ed, 2013, 50(4): 668.

[3] Gross B, Atithmetic of elliptic curves with complex

multiplication[M]. Lecture Notes in Mathematics 776. Berlin: Springer Verlag, 1980.

[4] Ren Y, On the construction of a class of Q-curve [J]. J Sichuan Univ: Nat Sci Ed, 2013, 50 (3): 455.

[5] Tate J, Fourier analysis in number fields and Hecke ′s Zeta-functions [J]. Algebraic Number Theory, 1967: 305.

[6] Bump D, Automorphic forms and automorphic representations[M]. Cambridge: Cambridge University Press, 1998

[7] Lang S, Cyclotomic field[M]. Berlin/New York: Springer-Verlag, 1978.

[8] de Shalit E, The Iwasawa theory of elliptic curves with complex multiplication: *P*-adic *L*-functions [M]. Salt Lake City: Acadmic Press, 1987.

[9] Shimura G, Elliptic curves with CM as factors of Jacobians of modular fuctions[J]. Nagoya Math J, 1971, 43, 199.

[10] Shimura G, Introduction to the artithmetic theory of automorphic functions[M]. Princeton: Princeton University Press, 1971.