A quadratic reciprocity law for elliptic curves

Hugues Verdure
Institute of Mathematics and Statistics
University of Tromsø
9037 Tromsø
Norway
Hugues.Verdure@matnat.uit.no

August 18, 2008

Abstract

If E is an elliptic curve, then the Galois group of the extension generated by the n-torsion points acts on these points. We prove a quadratic reciprocity law involving this group action. This law is an extension of the usual quadratic reciprocity law.

Keywords : Elliptic curve – torsion – Galois group – quadratic reciprocity law

MSC[2000]: 14H52

This work was partially supported by Grant-in-Aid for Scientific Research (B)18340005, Japan Society for the Promotion of Science.

1 Introduction and notation

The quadratic reciprocity law is a well known theorem in number theory. It asserts that if p, q are two different odd prime numbers, then

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

where the Legendre symbol $\left(\frac{p}{q}\right)$ is 1 if p is a square modulo q, and -1 otherwise. It was first conjectured by Euler in 1782, and the first (incomplete) proof was given by Legendre [3] in 1788. In 1801, Gauss gave a complete proof by induction [2]. Since then, more than 220 different proofs have been published, among them at least 17 since year 2000.

We shall present in this article yet another proof of this law. To achieve this, we will study the cyclotomic character θ on the Galois group of the field extension generated by n-torsion points of an elliptic curve. We will prove that the image of this morphism is included in the kernel of the Jacobi symbol modulo

n if and only if $(-1)^{\frac{n-1}{2}}n$ is a square in the base field. Then taking an elliptic curve over a finite field with p elements, and $n = q$ gives us the usual quadratic reciprocity law.

Let $\mathbb{K}$ be a field of characteristic $\chi \neq 2, 3$ and let E be an elliptic curve defined over $\mathbb{K}$ by a Weierstrass equation

$$E : y^2 = x^3 + a_4x + a_6.$$

Let n be an odd integer, relatively prime to χ. The subgroup $E[n]$ of n-torsion points on E defined over an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$ generates a Galois extension $\mathbb{L} = \mathbb{K}(E[n]) \subset \overline{\mathbb{K}}$ of $\mathbb{K}$. The aim of this paper is to show the following quadratic reciprocity law (theorem 2):

$$Im(\theta) \subset Ker(J_n) \Leftrightarrow (-1)^{\frac{n-1}{2}}n \text{ is a square in } \mathbb{K}$$

where J_n is the Jacobi symbol modulo n. This reciprocity law is an extension of the usual quadratic reciprocity law (corollary 4).

We refer to [4, 5] for the theory of elliptic curves, and we will use its notation.

When studying torsion on elliptic curves, it is natural to look at division polynomials ψ_n. They have the property that a point $P = (x, y) \in E(\overline{\mathbb{K}})$ is n-torsion if and only if $\psi_n(x, y) = 0$. They are defined recursively in the following way:

$$\begin{aligned}
&\psi_1 = 1\\
&\psi_2 = 2y\\
&\psi_3 = 3x^4 + 6a_4x^2 + 12a_6x - a_4^2\\
&\psi_4 = 2y\left(x^6 + 5a_4x^4 + 20a_6x^3 - 5a_4^2x^2 - 4a_4a_6x - 8a_6^2 - a_4^3\right)\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \ (m \geqslant 2)\\
&2y\psi_{2m} = \psi_m\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right) \ (m \geqslant 3)
\end{aligned}$$

The interested reader will find an explanation of the recursive equations in [7]. Replacing y^2 by $x^3 + a_4x + a_6$, the polynomials ψ_{2m+1} and $\frac{\psi_{2m}}{2y}$ are in $\mathbb{K}[x]$, and actually in $\mathbb{Z}[a_4, a_6, x]$. Those are the polynomials we will consider in the sequel, and we denote them by $\widetilde{\psi}_m$. Note that the property of $\widetilde{\psi}_{2m+1}$ remains the same, while the zeroes of $\widetilde{\psi}_{2m}$ are just the x-coordinates of points of $2m$ torsion that are not 2-torsion. The leading coefficient of $\widetilde{\psi}_m$ is equal to m if m is odd, or $\frac{m}{2}$ if m is even.

If$(\alpha_1, \cdots, \alpha_s)$ is a s-tuple, we denote it by (α_i). By $(\alpha_i)'$, we mean the $(s-1)$-tuple $(\alpha_1, \cdots, \alpha_{s-1})$. Finally, if (α_i) and (β_i) are two s-tuples, then $\delta((\alpha_i), (\beta_i)) = \#\{i| \ \alpha_i \neq \beta_i\}$.

In the sequel, n is an odd integer relatively prime to χ. We prove the quadratic reciprocity law itself by looking at the action of $Gal(\mathbb{L}, \mathbb{K})$ on $E[n]$. More precisely, we show that there is a non-canonical group homorphism from $Gal(\mathbb{L}, \mathbb{K})$ into $GL_2(\mathbb{Z}/n\mathbb{Z})$, and if M_σ is the image of $\sigma \in Gal(\mathbb{L}, \mathbb{K})$, then the signature of the action of σ on $E[n]$ coincides with the Jacobi symbol of the determinant of M_σ. This enables us to describe the extension $\mathbb{K}(\sqrt{\delta_n})$, where δ_n is the discriminant of ψ_n.

As a corollary, we find the usual quadratic reciprocity law by considering elliptic curves over finite fields.

2 Relation between the discriminants of the elliptic curve and of the division polynomial

We will need several lemmas and propositions in order to prove theorem 1. We prove first that the discriminant of the division polynomial is a cusp form of the desired weight and without zeroes on the upper half plane. As a consequence, it has to be a constant multiplum of a power of the discriminant of the curve. It thus just remains to compute this constant. Throughout this section, the positive integer l is fixed.

2.1 The discriminant is a cusp form

Lemma 1. *Let $\tau \in \mathbb{H}$ and $(a,b) \in \mathbb{N}_{l-1}^2 \backslash \{(0,0)\}$. Then*

$$\wp_{a,b}\left(\frac{-1}{\tau}\right) = \tau^2 \wp_{l-b,a}(\tau).$$

Proof. We have

$$\wp_{a,b}(\tau) = \frac{1}{\left(\frac{a+b\tau}{l}\right)^2} + \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \left[\frac{1}{\left(\frac{a+b\tau}{l} - m - n\tau\right)^2} - \frac{1}{(m+n\tau)^2}\right]$$

so that

$$\begin{aligned}\wp_{a,b}\left(\frac{-1}{\tau}\right) &= \frac{\tau^2}{\left(\frac{a\tau-b}{l}\right)^2} + \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \left[\frac{\tau^2}{\left(\frac{a\tau-b}{l} - m\tau + n\right)^2} - \frac{\tau^2}{(m\tau-n)^2}\right] \\ &= \tau^2 \wp_{-b,a}(\tau) \\ &= \tau^2 \wp_{l-b,a}(\tau),\end{aligned}$$

the last equality coming from the periodicity of $\wp$ in the elements of the defining lattice. □ □

Corollary 1. *Let $\tau \in \mathbb{H}$. Then*

$$\delta_l\left(\frac{-1}{\tau}\right) = \tau^{2\#D(\#D-1)}\delta_l(\tau)$$

Proof. We know that the definition of $\delta_l(\tau)$ is independent of the choice of representatives (a,b) for the x-coordinates of points of l-torsion and of the order on this set. In this case, we choose

$$D = \{(a,0), a \in \mathbb{N}^*_{\frac{l-1}{2}}\} \cup \{(a,b), a \in \mathbb{N}_{l-1}, b \in \mathbb{N}^*_{\frac{l-1}{2}}\}$$

if l is odd, and

$$D = \{(a,b), a \in \mathbb{N}^*_{\frac{l}{2}-1}, b \in \{0, \frac{l}{2}\}\} \cup \{(a,b), a \in \mathbb{N}_{l-1}, b \in \mathbb{N}^*_{\frac{l}{2}}\}$$

if l is even, with any order (for example $(a,b) < (a',b') \Leftrightarrow al + b < a'l + b'$). Obviously, when (a,b) runs over D, then $(l-b,a)$ runs over another set of representatives for the x-coordinates of points of l-torsion. □

Lemma 2. *Let* $\tau \in \mathbb{H}$ *and* $(a,b) \in \mathbb{N}^2_{l-1} \backslash \{(0,0)\}$*. Then*

$$\wp_{a,b}(\tau+1) = \wp_{a+b,b}(\tau).$$

Proof. From the q-expansion of $\wp$, we can deduce a r-expansion of $\wp_{a,b}$, where $r = e^{\frac{2i\pi\tau}{l}}$ and $\zeta_l = e^{\frac{2i\pi}{l}}$. Namely, we have:

$$\frac{1}{(2i\pi)^2}\wp_{a,b}(\tau) \quad = \quad \sum_{n\in\mathbb{Z}} \frac{r^{ln+b}\zeta_l^a}{(1-r^{ln+b}\zeta_l^a)^2} + \frac{1}{12} - 2\sum_{n\geqslant 1}\frac{r^{ln}}{(1-r^{ln})^2}$$

But, under the transformation $\tau \mapsto \tau + 1$, we have $r \mapsto r\zeta_l$ and thus

$$\begin{aligned}
\frac{1}{(2i\pi)^2}\wp_{a,b}(\tau+1) &= \sum_{n\in\mathbb{Z}} \frac{r^{ln+b}\zeta_l^{ln+b}\zeta_l^a}{\left(1-r^{ln+b}\zeta_l^{ln+b}\zeta_l^a\right)^2} + \frac{1}{12} - 2\sum_{n\geqslant 1}\frac{r^{ln}\zeta^{ln}}{\left(1-r^{ln}\zeta_l^{ln}\right)^2} \\
&= \sum_{n\in\mathbb{Z}} \frac{r^{ln+b}\zeta_l^{a+b}}{\left(1-r^{ln+b}\zeta_l^{a+b}\right)^2} + \frac{1}{12} - 2\sum_{n\geqslant 1}\frac{r^{ln}}{(1-r^{ln})^2} \\
&= \frac{1}{(2i\pi)^2}\wp_{a+b,b}(\tau)
\end{aligned}$$

□

Corollary 2. *Let* $\tau \in \mathbb{H}$*. Then*

$$\delta_l(\tau+1) = \delta_l(\tau).$$

Proof. We choose the same D as in the previous corollary. Then when (a,b) runs over D, $(a+b,b)$ runs over another set of representatives for the x-coordinates of the points of l-torsion.We have therefore

$$\begin{aligned}
\delta_l(\tau+1) &= C \prod_{\substack{(a,b),(a',b') \in D \\ (a,b) < (a',b')}} \left(\wp_{a,b}(\tau+1) - \wp_{a',b'}(\tau+1)\right)^2 \\
&= C \prod_{\substack{(a,b),(a',b') \in D \\ (a,b) < (a',b')}} \left(\wp_{a+b,b}(\tau) - \wp_{a'+b',b'}(\tau)\right)^2 \\
&= \delta_l(\tau).
\end{aligned}$$

□ □

Proposition 1. *The function*

$$\begin{array}{rccc} \delta_l : & \overline{\mathbb{H}} & \longrightarrow & \mathbb{P}_1(\mathbb{C}) \\ & \tau & \longmapsto & \delta_l(\tau) \end{array}$$

is a cusp form of weight $2k = 2\#D(\#D-1)$ for $SL_2(\mathbb{Z})$. It has a unique zero in $i\infty$.

Proof. The r-expansion of $\wp_{a,b}(\tau)$ shows that it is a meromorphic function on $\overline{\mathbb{H}}$. Actually, this is a holomorphic function since the only poles of the function $\wp$ are at the points of the lattice, and we always evaluate the functions outside of these points. Since δ_l is a combination of finite sums and products of these functions, it is also a meromorphic function on $\overline{\mathbb{H}}$. The corollaries 1 and 2 show that δ_l is then a modular function of weight $2k$. Using the r-expansion of $\wp_{a,b}$ again, we see that $\delta_l(i\infty) = 0$ so that δ_l is a cusp form. Finally, we have for $\tau \in \mathbb{H}$ and $(a,b),(a',b') \in \mathbb{N}^2_{l-1}\backslash\{(0,0)\}$,

$$\wp_{a,b}(\tau) = \wp_{a',b'}(\tau) \Leftrightarrow (a,b) = \pm(a',b') \mod l.$$

This shows that δ_l has no zeroes on $\mathbb{H}$. □ □

Corollary 3. *There exists a constant k_l (depending on l) such that*

$$\delta_l = k_l \Delta^{k/6}.$$

Proof. We know ([5], cor. I.3.8) that

$$\frac{1}{2}\mathrm{ord}_i(\delta_l) + \frac{1}{3}\mathrm{ord}_\rho(\delta_l) + \mathrm{ord}_{i\infty}(\delta_l) + \sum_{\substack{\tau\,\in\,X(1)\\ \tau\,\neq\,i,\,\rho,\,i\infty}} \mathrm{ord}_\tau(\delta_l) = \frac{k}{6}.$$

We also know that the only possible zero or pole of δ_l is at $i\infty$ so that

$$\mathrm{ord}_{i\infty}(\delta_l) = \frac{k}{6}.$$

The function $\Delta^{k/6}$ is also a cusp form of weight $2k$ with the same zeroes and poles, so that they have to differ by a multiplicative constant. □ □

We shall now make this constant explicit.

2.2 Computation of the constant k_l

We will compute d_l, the term of lowest degree of the r-expansion of δ_l, and compare it to the term of lowest degree of $\Delta^{k/6}$. The latter one is known to be $(2\pi)^{2k}q^{k/6}$. Let us denote $f_{a,b,a',b'}$ the term of lowest degree of the r-expansion of $\wp_{a,b} - \wp_{a',b'}$. We will then have

$$d_l = \prod_{(a,b)<(a',b')} f^2_{a,b,a',b'}.$$

We have

$$\begin{aligned}\frac{1}{(2i\pi)^2}\left(\wp_{a,b}(\tau)-\wp_{a',b'}(\tau)\right) &= \sum_{n=0}^{\infty}\left(\frac{r^{ln+b}\zeta_l^{a}}{(1-r^{ln+b}\zeta_l^{a})^2}-\frac{r^{ln+b'}\zeta_l^{a'}}{\left(1-r^{ln+b'}\zeta_l^{a'}\right)^2}\right)\\ &\quad+\sum_{n=0}^{\infty}\left(\frac{r^{ln-b}\zeta_l^{-a}}{\left(1-r^{ln-b}\zeta_l^{-a}\right)^2}-\frac{r^{ln-b'}\zeta_l^{-a'}}{\left(1-r^{ln-b'}\zeta_l^{-a'}\right)^2}\right)\end{aligned}$$

and since

$$\frac{r^{ln\pm b}\zeta_l^{\pm a}}{\left(1-r^{ln\pm b}\zeta_l^{\pm a}\right)^2}=\begin{cases} r^{ln\pm b}\zeta_l^{\pm a}+\mathcal{O}\left(r^{ln\pm b}\right) & \text{if } ln\pm b\neq 0\\ \frac{\zeta_l^{\pm a}}{\left(1-\zeta_l^{\pm a}\right)^2}+\mathcal{O}(1) & \text{otherwise,}\end{cases}$$

looking carefully at the terms of lowest degree, we find that

Lemma 3. *Keeping the same notation,*

$$\frac{1}{(2i\pi)^2}f_{a,b,a',b'}=\begin{cases} \frac{\zeta_l^a}{\left(1-\zeta_l^a\right)^2}-\frac{\zeta_l^{a'}}{\left(1-\zeta_l^{a'}\right)^2} & \textit{if } b=b'=0\\ \frac{\zeta_l^a}{\left(1-\zeta_l^a\right)^2} & \textit{if } 0=b<b'\\ \left(\zeta_l^a-\zeta_l^{a'}\right)r^b & \textit{if } 0<b=b'<\frac{l}{2}\\ \zeta_l^a r^b & \textit{if } 0<b<b'\\ \left(\zeta_l^a+\zeta_l^{-a}-\zeta_l^{a'}-\zeta_l^{-a'}\right)r^{\frac{l}{2}} & \textit{if } b=b'=\frac{l}{2}.\end{cases}$$

To ease the computation, we introduce the following notation:

$$g_{a,b}=\prod_{(a'b')>(a,b)}f^2_{a,b,a',b'}$$

so that

$$d_l=\prod_{(a,b)\in D}g_{a,b}.$$

We have to distinguish two cases, namely l odd and l even. As we are just interested in the case l odd in the sequel, this is the case we will develop. We will mention the result when l is even, without proof. The interested reader may find it on [6]. From now on, l is odd.

Recall that in this case, we choose the set D to be

$$D=\left\{(a,0),a\in\mathbb{N}^*_{\lfloor\frac{l}{2}\rfloor}\right\}\cup\left\{(a,b),a\in\mathbb{N}_{l-1},\ b\in\mathbb{N}^*_{\lfloor\frac{l}{2}\rfloor}\right\}$$

We first compute the $g_{a,b}$, and we distinguish two cases, namely $b=0$ and $b>0$.

In the first case, we have

$$\begin{aligned}
g_{a,0} &= \prod_{a'=a+1}^{\frac{l-1}{2}} f^2_{a_0,a',0} \prod_{b'=1}^{\frac{l-1}{2}} \prod_{a'=0}^{l-1} f^2_{a,0,a',b'} \\
&= \prod_{a'=a+1}^{\frac{l-1}{2}} (2i\pi)^4 \left[\frac{\zeta_l^a}{(1-\zeta_l^a)^2} - \frac{\zeta_l^{a'}}{\left(1-\zeta_l^{a'}\right)^2} \right]^2 \prod_{b'=1}^{\frac{l-1}{2}} \prod_{a'=0}^{l-1} (2i\pi)^4 \frac{\zeta_l^{2a}}{(1-\zeta_l^a)^4} \\
&= \frac{(2\pi)^{2l^2-2-4a}}{(1-\zeta_l^a)^{2l^2-2-4a}} \zeta_l^{-a-2a^2} \prod_{a'=a+1}^{\frac{l-1}{2}} \frac{\left(1-\zeta_l^{a'-a}\right)^2 \left(1-\zeta_l^{a'+a}\right)^2}{\left(1-\zeta_l^{a'}\right)^4}
\end{aligned}$$

and in the latter

$$\begin{aligned}
g_{a,b} &= \prod_{a'=a+1}^{l-1} f^2_{a,b,a',b} \prod_{b'=b+1}^{\frac{l-1}{2}} \prod_{a'=0}^{l-1} f^2_{a,b,a',b'} \\
&= \prod_{a'=a+1}^{l-1} (2i\pi)^4 \left(\zeta_l^a - \zeta_l^{a'}\right)^2 r^{2b} \prod_{b'=b+1}^{\frac{l-1}{2}} \prod_{a'=0}^{l-1} (2i\pi)^4 \zeta_l^{2a} r^{2b} \\
&= (2\pi)^{2l^2+2l-4bl-4-4a} \, r^{bl^2-2b^2l+bl-2b-2ab} \prod_{a'=a+1}^{l-1} \left(\zeta_l^a - \zeta_l^{a'}\right)^2
\end{aligned}$$

We now compute the product of all the $g_{a,b}$ when (a,b) runs through D. We then get:

$$\begin{aligned}
\frac{d_l}{r^{lk/6}(2\pi)^{2k}} &= \frac{\prod_{a=1}^{\frac{l-1}{2}} g_{a,0} \prod_{b=1}^{\frac{l-1}{2}} g_{a,b}}{r^{lk/6}(2\pi)^{2k}} \\
&= \left(\prod_{a=1}^{\frac{l-1}{2}} \frac{\zeta_l^{-2a-2a^2}}{(1-\zeta_l^a)^{2l^2-2-4a}} \prod_{a'=a+1}^{\frac{l-1}{2}} \frac{\left(1-\zeta_l^{a'-a}\right)^2 \left(1-\zeta_l^{a'+a}\right)^2}{\left(1-\zeta_l^{a'}\right)^4} \right) \\
&\quad \left(\prod_{b=1}^{\frac{l-1}{2}} \prod_{a=0}^{l-1} \prod_{a'=a+1}^{l-1} \left(\zeta_l^a - \zeta_l^{a'}\right)^2 \right)
\end{aligned}$$

After a little bit of combinatorics, we find that

$$\prod_{a=1}^{\frac{l-1}{2}} \prod_{a'=a+1}^{\frac{l-1}{2}} \left(1-\zeta_l^{a'}\right)^4 = \prod_{a=1}^{\frac{l-1}{2}} (1-\zeta_l^a)^{4a-4}$$

while

$$\prod_{a=1}^{\frac{l-1}{2}} \prod_{a'=a+1}^{\frac{l-1}{2}} \left(1-\zeta_l^{a'-a}\right)^2 = \prod_{a=1}^{\frac{l-1}{2}} (1-\zeta_l^a)^{l-1-2a} .$$

Let us now look at the quantity

$$\prod_{a=1}^{\frac{l-1}{2}} \prod_{a'=a+1}^{\frac{l-1}{2}} \left(1-\zeta_l^{a'+a}\right)^2 .$$

Given a $1 \leqslant c \leqslant \frac{l-1}{2}$, how many couples (a, a') in the product are such that $a + a' = c$ or $a + a' = l - c$? It actually depends on the parity of c: if c is even, then there exists respectively $\frac{c}{2} - 1$ and $\frac{c}{2}$ such couples, while if c is odd, then the numbers are both equal to $\frac{c-1}{2}$. When c is even,

$$\begin{aligned}
\prod_{a+a' \equiv \pm c\ [l]} \left(1-\zeta_l^{a+a'}\right)^2 &= \prod_{a+a'=c} \left(1-\zeta_l^{c}\right)^2 \prod_{a+a'=l-c} \left(1-\zeta_l^{-c}\right)^2 \\
&= \left(1-\zeta_l^{c}\right)^{c-2} \left(-\zeta_l^{-c}\right)^{c} \left(1-\zeta_l^{c}\right)^{c} \\
&= \frac{\left(1-\zeta_l^{c}\right)^{2c-2}}{\zeta_l^{c^2}},
\end{aligned}$$

while the same computation shows that when c is odd,

$$\prod_{a+a' \equiv \pm c\ [l]} \left(1-\zeta_l^{a+a'}\right)^2 = \frac{\left(1-\zeta_l^{c}\right)^{2c-2}}{\zeta_l^{c^2-c}}.$$

Computing the product of all these quantities when $1 \leqslant c \leqslant \frac{l-1}{2}$ shows that

$$\prod_{a=1}^{\frac{l-1}{2}} \prod_{a'=a+1}^{\frac{l-1}{2}} \left(1-\zeta_l^{a+a'}\right)^2 = \frac{\mu(l) \prod_{c=1}^{\frac{l-1}{2}} (1-\zeta_l^{c})^{2c-2}}{\zeta_l^{\frac{l(l^2-1)}{24}}},$$

where

$$\mu(l) = \begin{cases} \zeta_l^{\frac{(l-1)^2}{16}} & \text{if } l \equiv 1 \pmod 4 \\ \zeta_l^{\frac{(l+1)^2}{16}} & \text{if } l \equiv 3 \pmod 4 \end{cases}.$$

If we gather everything in our original formula, we obtain

$$\begin{aligned}
d_l &= \frac{(2\pi)^{2k} \mu(l) \left(\prod_{1 \leqslant a < a' \leqslant \frac{l-1}{2}} \left(\zeta_l^{a} - \zeta_l^{a'}\right)^2\right)^{\frac{l-1}{2}} r^{lk/6}}{\zeta_l^{\frac{(l-1)(l+1)(l+2)}{8}} \prod_{a=1}^{\frac{l-1}{2}} \left(1-\zeta_l^{a}\right)^{2l^2-l-3}} \\
&= \frac{(-1)^{\frac{l-1}{2}} (2\pi)^{2k} \, l^{\frac{l(l-1)}{2}} \mu(l) r^{lk/6}}{\zeta_l^{\frac{(l-1)(l+1)(l+2)}{8}} \prod_{a=1}^{\frac{l-1}{2}} \left(1-\zeta_l^{a}\right)^{2l^2-l-3}}
\end{aligned}$$

Finally

$$\begin{aligned}
\prod_{a=1}^{\frac{l-1}{2}} \left(1-\zeta_l^a\right)^2 &= \prod_{a=1}^{\frac{l-1}{2}} \left(1-\zeta_l^a\right) \prod_{a=1}^{\frac{l-1}{2}} \left(-\zeta_l^a\right)\left(1-\zeta_l^{-a}\right) \\
&= (-1)^{\frac{l-1}{2}} \zeta_l^{\frac{l^2-1}{8}} \prod_{a=1}^{l-1} \left(1-\zeta_l^a\right) \\
&= (-1)^{\frac{l-1}{2}} \zeta_l^{\frac{l^2-1}{8}} l,
\end{aligned}$$

and putting everything together, we get

$$d_l \quad = \quad \frac{(-1)^{\frac{l-1}{2}} (2\pi)^{2k} \mu(l) l^{\frac{l-1}{2}} r^{lk/6}}{\zeta_l^{\frac{(l-1)(l+1)^2(2l-1)}{16}} l^{\frac{(l+1)(2l-3)}{2}}} = \frac{(-1)^{\frac{l-1}{2}} (2\pi)^{2k} \mu(l) \zeta_l^{\frac{(l-1)(l+1)^2}{16}} r^{lk/6}}{l^{\frac{l^2-3}{2}}}.$$

Considering the two cases $l \equiv 1 \pmod 4$ and $l \equiv 3 \pmod 4$, it is then easy to see that

$$\mu(l)\zeta_l^{\frac{(l-1)(l+1)^2}{16}} = 1$$

and thus

$$d_l = (-1)^{\frac{l-1}{2}} r^{\frac{l(l^4-4l^2+3)}{24}} (2\pi)^{\frac{l(l^4-4l^2+3)}{2}} l^{\frac{3-l^2}{2}}.$$

Theorem 1. *Keeping the same notation, we have*

$$\delta_l = \begin{cases} (-1)^{\frac{l-1}{2}} l^{\frac{l^2-3}{2}} \Delta^{\frac{l^4-4l^2+3}{24}} & \text{if } l \text{ is odd} \\ (-1)^{\frac{l}{2}-1} 16 l^{\frac{l^2-6}{2}} \Delta^{\frac{l^4-10l^2+24}{24}} & \text{if } l \text{ is even} \end{cases}.$$

Proof. This is a direct consequence of the above computations, corollary 3 and the fact that

$$disc(\lambda P) = \lambda^{2\deg(P)-2} disc(P)$$

□ □

3 Main result

Let n be an odd integer such that $(n,d)=1$. Let $T_n = (\mathbb{Z}/n\mathbb{Z})^2 \setminus \left\{\begin{bmatrix}0\\0\end{bmatrix}\right\}$ and V_n is obtained from T_n by identifying v with $-v$. There are obvious actions of $GL_2(\mathbb{Z}/n\mathbb{Z})$ on T_n and V_n that we denote by τ and $\overline{\tau}$ respectively. Let σ and $\overline{\sigma}$ be the signature on $Sym(V_n)$ and $Sym(T_n)$ respectively.

Proposition 2. *With the previous notation, we have:*

$$\forall M \in GL_2(\mathbb{Z}/n\mathbb{Z}),\ \sigma \circ \tau(M) = \overline{\sigma} \circ \overline{\tau}(M) = \left(\frac{det(M)}{n}\right)$$

where $\left(\frac{\cdot}{\cdot}\right)$ *is the Jacobi symbol.*

Proof. Since $GL_2(\mathbb{Z}/n\mathbb{Z})$ is generated by $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and for $d \in (\mathbb{Z}/n\mathbb{Z})^*$, $U_d = \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}$, it suffices to show the equalities for these matrices. Moreover, if we write $n = \prod_{i=1}^m p_i^{\alpha_i}$, then $(\mathbb{Z}/n\mathbb{Z})^*$ is generated by m elements d_i such that $d_i \equiv 1 \pmod{p_j}$ if $i \neq j$, and d_i is a generator of $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$. It is then sufficient to show the equalities for $d = d_i$, and since the argument will be similar for all i, one may assume without loss of generality that $i = m$, and that $d = d_m$.

It is a well known fact that a permutation on a finite set has signature $(-1)^{q-o}$ where q is the set's cardinality, while o is the number of orbits.

Let $M \in GL_2(\mathbb{Z}/n\mathbb{Z})$. If $< t >$ is the orbit of $t \in T_n$ under the action of M, let

$$\Omega_1 = \{< t > \mid -t \in < t >, t \in T_n\}$$

and

$$\Omega_2 = \{< t > \mid -t \notin < t >, t \in T_n\}$$

Let $\omega_i = \#\Omega_i$ for $i = 1, 2$. Obvioulsy, ω_2 is even. The obvious map from the orbits of M acting on T_n onto the orbits of M acting on V_n is $1-1$ on Ω_1, while it is $2-1$ on Ω_2. Then

$$\sigma(\tau(M)) = (-1)^{(n^2-1)-(\omega_1+\omega_2)} = (-1)^{\omega_1}$$

while

$$\overline{\sigma}(\overline{\tau}(M)) = (-1)^{\frac{n^2-1}{2}-(\omega_1+\frac{\omega_2}{2})} = (-1)^{\omega_1+\frac{\omega_2}{2}}.$$

The first equality in the proposition holds if $\omega_2 \equiv 0 \pmod 4$.

If $M = S$, then it is easy to see that $\omega_1 = \frac{n^2-1}{4}$, $\omega_2 = 0$, and since $det(M) = 1$, the proposition holds in this case.

If $M = T$, then for $r \in \mathbb{Z}$, $M^r \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + ry \\ y \end{bmatrix}$, and once again, $\omega_1 = 0$. This shows also that if $y \neq 0$, the length l of the orbit of $\begin{bmatrix} x \\ y \end{bmatrix}$ is the smallest positive integer r such that $ry = 0$. If we write $y = y' \prod_{i=1}^m p_i^{\beta_i}$ with $(y', n) = 1$, then

$$ry = 0 \Leftrightarrow r \prod_{i=1}^m p_i^{\beta_i} = 0 \text{ in } \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists \lambda \in \mathbb{N},\ r = \lambda \prod_{i=1}^m p_i^{\alpha_i - \beta_i}$$

and therefore $l = \prod_{i=1}^m p_i^{\alpha_i-\beta_i}$. Given $y \neq 0$, there are exactly n points of the form $\begin{bmatrix} x \\ y \end{bmatrix}$, and each of them lie in an orbit of length $\prod_{i=1}^m p_i^{\alpha_i-\beta_i}$. This gives $\prod_{i=1}^m p_i^{\beta_i}$ such orbits. Given a m-tuple (β_i), there are exactly $\phi(\prod_{i=1}^m p_i^{\alpha_i-\beta_i})$ elements y that are of the form $y = y' \prod_{i=1}^m p_i^{\beta_i}$ with $(y', n) = 1$. If we add to this the $n - 1$ fixed points coming from $y = 0$, we get

$$\omega_2 = n - 1 + \sum_{\substack{(\beta_i)=(0) \\ (\beta_i)\neq(\alpha_i)}}^{(\alpha_i)} \left(\prod_{i=1}^m p_i^{\beta_i} \phi \left(\prod_{i=1}^m p_i^{\alpha_i-\beta_i} \right) \right).$$

If $\delta((\alpha_i),(\beta_i)) \geqslant 2$, then a factor $(p_i-1)(p_j-1)$ appears in $\phi(\prod_{i=1}^m p_i^{\alpha_i-\beta_i})$, which makes the corresponding term congruent to 0 modulo 4. We just need to consider terms with $\delta((\alpha_i),(\beta_i))=1$, which gives, modulo 4,

$$\begin{aligned}
\omega_2 &\equiv n-1+\sum_{k=1}^{m}\sum_{\beta_k=0}^{\alpha_k-1}\left(\prod_{\substack{i=1\\ i\neq k}}^{m} p_i^{\alpha_i}\right)p_k^{\alpha_k}\phi(p_k^{\alpha_k-\beta_k})\\
&\equiv n-1+\sum_{k=1}^{m}\sum_{\beta_k=0}^{\alpha_k-1}\left(\prod_{\substack{i=1\\ i\neq k}}^{m} p_i^{\alpha_i}\right)p_k^{\alpha_k}(p_k-1)p_k^{\alpha_k-\beta_k-1}\\
&\equiv n-1+\sum_{k=1}^{m}\alpha_k\frac{n}{p_k}(p_k-1)\\
&\equiv n-1+\sum_{\substack{k=1\\ p_k\equiv 3 \pmod 4}}^{m} 2\alpha_k\frac{n}{p_k}\\
&\equiv n-1+2\sum_{\substack{k=1\\ p_k\equiv 3 \pmod 4\\ \alpha_k\equiv 1 \pmod 2}}^{m} \frac{n}{p_k}
\end{aligned}$$

Let $E=\{k|\ p_k\equiv 3 \pmod 4,\ \alpha_k\equiv 1 \pmod 2\}$ and $e=\#E$. Then

$$n=\prod_{i=1}^{m}p_i^{\alpha_i}\equiv 3^e \pmod 4 \text{ and } \frac{n}{p_k}\equiv 3^{e-1} \pmod 4.$$

This sums up to

$$\omega_2\equiv 3^e-1+2e3^{e-1}\equiv 0 \pmod 4$$

independently on the parity of e, and the first equality is proved. Since $det(M)=1$, once again, the proposition holds for $M=T$.

If $M=U_d$, then for $r\in\mathbb{Z}$, $M^r\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}d^rx\\y\end{bmatrix}$. Then if $t=\begin{bmatrix}x\\y\end{bmatrix}$,

$$-t\in<t>\Leftrightarrow y=0 \text{ and } \exists r, d^rx=-x.$$

Write $x=x'\prod_{i=1}^m p_i^{\gamma_i}$ with $(x',n)=1$. Then $d^rx=-x \Leftrightarrow d^r=-1$ in $\mathbb{Z}/(\prod_{i=1}^m p_i^{\alpha_i-\gamma_i})\mathbb{Z}$. The choice of d implies $\gamma_i=\alpha_i$ for $i<m$. Thus

$$-t\in<t>\Leftrightarrow t=\begin{bmatrix}x'p_m^{\gamma_m}\prod_{i=1}^{m-1}p_i^{\alpha_i}\\0\end{bmatrix}$$

for $(x',n)=1$ and $0\leqslant\gamma_m<\alpha_m$. If t is of this kind then the length of the orbit $<t>$ is equal to the order of d in $\mathbb{Z}/(p_m^{\alpha_m-\gamma_m})\mathbb{Z}$, that is $\phi(p_m^{\alpha_m-\gamma_m})$. On the other hand, there are exactly $\phi(p_m^{\alpha_m-\gamma_m})$ many x of that kind, which means that for every $0 \leqslant \gamma_m < \alpha_m$, there is exactly one orbit of length $\phi(p_m^{\alpha_m-\gamma_m})$ in Ω_1. We have thus proved that $\omega_1 = \alpha_m$.

Now, if $x = x' \prod_{i=1}^m p_i^{\gamma_i}$, $(x', n) = 1$, the same argument shows that the length of the orbit generated by $\begin{bmatrix} x \\ y \end{bmatrix}$ is $\phi(\prod_{i=1}^m p_i^{\alpha_i-\gamma_i})$. But, this is equal to $\phi(p_m^{\alpha_m-\gamma_m})$ by the choice of $d = d_m$. Given an m-tuple (γ_i), there are exactly $\phi(\prod_{i=1}^m p_i^{\alpha_i-\gamma_i})$ many x of the form $x = x' \prod_{i=1}^m p_i^{\gamma_i}$, $(x', n) = 1$. In order to find ω_2, we have to be careful to eliminate all the m-tuples $(\alpha_1, \ldots, \alpha_{m-1}, \gamma_m)$ which give an orbit in Ω_1, and not to forget the fixed points of the form $\begin{bmatrix} 0 \\ y \end{bmatrix}$. This gives, modulo 4:

$$
\begin{aligned}
\omega_2 &\equiv n - 1 + n \sum_{\substack{(\gamma_i)=(0) \\ (\gamma_i)\neq(\alpha_i)}}^{(\alpha_i)} \frac{\phi(\prod_{i=1}^m p_i^{\alpha_i-\gamma_i})}{\phi(p_m^{\alpha_m-\gamma_m})} - \#\omega_1 \\
&\equiv n - 1 + n \sum_{\substack{(\gamma_i)=(0) \\ (\gamma_i)\neq(\alpha_i)}}^{(\alpha_i)} \phi\left(\prod_{i=1}^{m-1} p_i^{\alpha_i-\gamma_i}\right) - \#\omega_1 \\
&\equiv n - 1 - \alpha_m + n \left(\sum_{\substack{(\gamma_i)'=(0) \\ (\gamma_i)'\neq(\alpha_i)'}}^{(\alpha_i)'} \sum_{\gamma_m=0}^{\alpha_m} \phi\left(\prod_{i=1}^{m-1} p_i^{\alpha_i-\gamma_i}\right) + \sum_{\gamma_m=0}^{\alpha_m-1} \phi(1) \right) \\
&\equiv (n-1)(\alpha_m+1) + n(\alpha_m+1) \sum_{\substack{(\gamma_i)'=(0) \\ (\gamma_i)'\neq(\alpha_i)'}}^{(\alpha_i)'} \phi\left(\prod_{i=1}^{m-1} p_i^{\alpha_i-\gamma_i}\right) \\
&\equiv (n-1)(\alpha_m+1) + n(\alpha_m+1) \sum_{\substack{k=1 \\ p_k \equiv 3 \pmod 4}}^{m-1} \sum_{\gamma_k=0}^{\alpha_k-1} \phi(p_k^{\alpha_k-\gamma_k}) \\
&\equiv (n-1)(\alpha_m+1) + n(\alpha_m+1) \sum_{\substack{k=1 \\ p_k \equiv 3 \pmod 4}}^{m-1} 2 \sum_{\gamma_k=0}^{\alpha_k-1} p_k^{\alpha_k-\gamma_k-1} \\
&\equiv (n-1)(\alpha_m+1) + n(\alpha_m+1) \sum_{\substack{k=1 \\ p_k \equiv 3 \pmod 4}}^{m-1} (3^{\alpha_k} - 1) \\
&\equiv (n-1)(\alpha_m+1) + n(\alpha_m+1) \sum_{\substack{k=1 \\ p_k \equiv 3 \pmod 4 \\ \alpha_k \equiv 1 \pmod 2}}^{m-1} 2
\end{aligned}
$$

If $\alpha_m \equiv 0 \pmod 2$, then obviously, $\omega_2 \equiv 0 \pmod 4$. If not, then let

$$\begin{array}{rcl} e & = & \#\{k|\ 1 \leqslant k \leqslant m,\ p_k \equiv 3 \pmod 4,\ \alpha_k \equiv 1 \pmod 2\} \\ & = & \#\{k|\ 1 \leqslant k \leqslant m-1,\ p_k \equiv 3 \pmod 4,\ \alpha_k \equiv 1 \pmod 2\}. \end{array}$$

Then

$$\omega_2 \equiv (3^e - 1)(\alpha_m + 1) + 2e3^e(\alpha_m + 1) \equiv 0 \pmod 4$$

idependently on the parity of e. This shows once again the first equality. Since d generates $(\mathbb{Z}/p_m\mathbb{Z})^*$, it can not be a square there, and $\left(\frac{d}{p_m}\right) = -1$. We also have that $\left(\frac{d}{p_i}\right) = 1$ for $i < m$. Then,

$$\left(\frac{det(M)}{n}\right) = \prod_{i=1}^{m} \left(\frac{d}{p_i}\right)^{\alpha_i} = \left(\frac{d}{p_m}\right)^{\alpha_m} = (-1)^{\alpha_m} = \sigma \circ \tau(M),$$

and the proposition holds in this case too. □

We can now prove our quadratic reciprocity law. Let E be an elliptic curve defined over a field $\mathbb{K}$ and $n \geqslant 3$ be an odd integer prime to the characteristic of $\mathbb{K}$. Let δ_n be the discriminant of the n-th division polynomial ψ_n. Let $\mathbb{L}$ be the extension of $\mathbb{K}$ generated by $E[n]$. This is a Galois extension of $\mathbb{K}$ with Galois group G. This group acts canonically on $E[n]$. If $< P, Q >$ is a basis of $E[n]$, then we have a natural embedding

$$\varphi_{P,Q} : G \hookrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}).$$

We also have

$$det : GL_2(\mathbb{Z}/n\mathbb{Z}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$

The morphism $\theta = det \circ \varphi_{P,Q}$ is independent of P and Q. Let $H = Im(\theta)$, and $S \subset (\mathbb{Z}/n\mathbb{Z})^*$ be the kernel of the Jacobi symbol $J_n = \left(\frac{\cdot}{n}\right)$. We have the following quadratic reciprocity law:

Theorem 2. *The following assertions are equivalent:*

$H \subset S$,

δ_n is a square in $\mathbb{K}$,

$(-1)^{\frac{n-1}{2}} n$ is a square in $\mathbb{K}$.

Proof. Let $w \in \mathbb{L}$ be a square root of δ_n. It is given by

$$w = \pm \prod (x(P) - x(P'))$$

where P, P' in $E[n]\backslash\{0\}$ run over ordered pairs modulo the action of $\{\pm Id\}$. Let $\lambda \in G$. Then λ induces a permutation on $\{x(P)|\ P \in E[n]\}$, and thus

$\lambda(w) = \pm w$. By proposition 2, we have, for $< P, Q >$ any basis of $E[n]$,

$$\begin{aligned} \lambda(w) = w \quad &\Leftrightarrow \quad \overline{\sigma} \circ \overline{\tau}(\varphi_{P,Q}(\lambda)) = 1 \\ &\Leftrightarrow \quad \left(\frac{\theta(\lambda)}{n}\right) = \left(\frac{det \circ \varphi_{P,Q}(\lambda)}{n}\right) = 1 \\ &\Leftrightarrow \quad \theta(\lambda) \in S. \end{aligned}$$

Then we have

$$\delta_n \text{ is a square in } \mathbb{K} \Leftrightarrow w \in \mathbb{K} \Leftrightarrow \forall \lambda \in G,\ \theta(\lambda) \in S \Leftrightarrow H \subset S.$$

From theorem 1, we know that $\delta_n = (-1)^{\frac{n-1}{2}} n^{\frac{n^2-3}{2}} \Delta^{\frac{n^4-4n^2+3}{24}}$. This is a square if and only if $(-1)^{\frac{n-1}{2}} n$ is a square. For a detail proof of [1], see [6] □

4 The standard quadratic reciprocity law

As a corollary, we can prove the usual quadratic reciprocity law:

Corollary 4. *Let p, q be two odd primes. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Proof. Let E be any elliptic curve defined over $\mathbb{F}_p$. Take $n = q$. As we are dealing with finite fields, the Galois group G is generated by the Frobenius endomorphism Fr. Let $< P, Q >$ be any basis of $E[q]$, and write $\varphi_{P,Q}(Fr) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Since $< P, Q >$ is a basis of $E[q]$, the root of unity $\zeta_q = e_q(P, Q)$, where e_q is the Weil pairing, is primitive. By the properties of the Weil pairing, we have:

$$\begin{aligned} Fr(e_q(P, Q)) &= Fr(\zeta_q) = \zeta_q^p \\ &= e_q(Fr(P), Fr(Q)) = e_q(aP + bQ, cP + dQ) \\ &= e_q(P, Q)^{ad-bc} = \zeta_q^{det \circ \varphi_{P,Q}(Fr)}. \end{aligned}$$

By the primitivity of ζ_q, we have then

$$\theta(Fr) \equiv p \pmod{q}.$$

This gives us

$$H =< \theta(Fr) >=< p > .$$

By the previous theorem, p is a square in $\mathbb{Z}/q\mathbb{Z}$ if and only if $(-1)^{\frac{q-1}{2}} q$ is a square in $\mathbb{F}_p$.

□

References

[1] I.A. Burhanuddin, and M.-D. Huang, *Elliptic curve torsion points and division polynomials*, in *Computational aspects of algebraic curves*, Lecture Notes Ser. Comput., **13** (2005), 13–37.

[2] C.F. Gauss, *Disquisitiones Arithmeticae*, Werke 1, Art 125-145.

[3] A.M. Legendre, *Recherches d'analyse indtermine*, Histoire de l'Académie Royale des Sciences de Paris (1785), 465-559, Paris 1788

[4] J.H. Silverman, *The arithmetic of elliptic curves.* Number 106 in Graduate texts in mathematics, Springer-Verlag, 1986.

[5] J.H. Silverman, *Advanced topics in the arithmetics of elliptic curves.* Number 151 in Graduate texts in mathematics, Springer-Verlag, 1994.

[6] http://www.math.uit.no/users/verdure/reciprocity-law.html

[7] H. Weber, *Lehrbuch der Algebra.* Braunschweig: Vieweg und Son, 1895.