# CONICS - A POOR MAN'S ELLIPTIC CURVES

FRANZ LEMMERMEYER

## Contents

## Introduction

The aim of this article is to show that the arithmetic of Pell conics admits a description which is completely analogous to that of elliptic curves: there is a theory of 2-descent with associated Selmer and Tate-Shafarevich groups, and there should be an analog of the conjecture of Birch and Swinnerton-Dyer. For the history and a theory of the first 2-descent, see [6, 7, 8]. The idea that unit groups of number fields and the group of rational points on elliptic curves are analogous is not new; see e.g. [1, 2, 5, 14] for some popularizations of this point of view. It is our goal here to show that, for the case of the unit group of real quadratic number fields, this analogy can be made much more precise.

## 1. The Group Law on Pell Conics and Elliptic Curves

Let $F \in \mathbb{Z}[X,Y]$ a polynomial. If $\deg F = 2$, the affine curve of genus 0 defined by $F = 0$ is called a conic. Let $d$ be a squarefree integer $\neq 1$ and define

$$\Delta = \begin{cases} d & \text{if } d \equiv 1 \bmod 4, \\ 4d & \text{if } d \equiv 2, 3 \bmod 4. \end{cases}$$

Then the curves $\mathcal{C} : X^2 - \Delta Y^2 = 4$ are called Pell conics; they are irreducible, nonsingular affine curves with a distinguished integral point $N = (2, 0)$.

If $\deg F = 3$, the projective curve $E$ described by $F$ has genus 1 if it is nonsingular; if in addition it has a rational point, then $E$ is called an elliptic curve defined over $\mathbb{Q}$. Elliptic curves given by a Weierstraß equation $Y^2 = X^3 + aX + b$ are irreducible, nonsingular projective curves with a distinguished integral point $\mathcal{O} = [0 : 1 : 0]$ at infinity.

Both types of curves have a long history: Pythagorean triples correspond to rational points on the Pell conic $X^4 + 4Y^2 = 4$, solutions of the Pell equations have been studied by the Greeks, the Indians, and the contemporaries of Fermat, such as Brouncker and Wallis. Problems leading to elliptic curves occur in the books of Diophantus and were studied by Bachet, Fermat, de Jonquières, Euler, Cauchy, Lucas, and Sylvester before Poincaré laid down his program for studying diophantine equations given by curves according to their genus.

### 1.1. Group Law on Conics.

The group law on non-degenerate conics $C$ defined over a field $F$ is quite simple: fix any rational point $N$ on $C$; for finding the sum of two rational points $A, B \in C(F)$, draw the line through $N$ parallel to $AB$, and denote its second point of intersection with $C$ by $A + B$. In the special case of Pell conics, the resulting formulas can be simplified to

**Proposition 1.** *Consider the conic $\mathcal{C} : Y^2 - \Delta X^2 = 4$, and put $N = (2, 0)$. Then the group law on $\mathcal{C}$ with neutral element $N$ is given by*

$$(r, s) + (t, u) = \Big(\frac{rt + \Delta su}{2}, \frac{ru + st}{2}\Big).$$

It is now easily checked that the map sending points $(r, s) \in \mathcal{C}(\mathbb{Z})$ to the unit $\frac{r+s\sqrt{d}}{2}$ with norm 1 in the quadratic number field $K = \mathbb{Q}(\sqrt{\Delta}\,)$ is a group homomorphism. Observe that the associativity of the geometric group law is equivalent to a special case of Pascal's theorem, which in turn is a very special case of Bezout's Theorem.

1.2. **Group Law on Elliptic curves.** Given an elliptic curve $E : y^2 = x^3 + ax + b$ defined over an algebraically closed field $K$, we define an addition law on $E$ by demanding that $A + B + C = 0$ for points $A, B, C \in E(K)$ if and only if $A, B, C$ are collinear. Since vertical lines intersect $E$ only in two affine points, we have to regard $E$ as a projective curve; then vertical lines intersect $E$ in two affine points as well as in the point at infinity. Associativity follows geometrically from a special case of Bezout's Theorem.

## 2. The Group Structure

Let us now compare the known results about the group structure of Pell conics over the most common rings and fields. Generally, we will study conics in the affine plane over integral domains, and elliptic curves in the projective plane over fields.

2.1. **Finite Fields.** Let $\mathcal{C} : x^2 - \Delta y^2 = 4$ be a Pell conic defined over a finite field $\mathbb{F}_q$ with $q = p^f$ elements, and assume that $\mathcal{C}$ is smooth, i.e. that $p \nmid \Delta$. Then

$$\mathcal{C}(\mathbb{F}_q) \simeq \mathbb{Z}/m\mathbb{Z}, \quad \text{where } m = q - \Big(\frac{\Delta}{p}\Big)^f .$$

If $\Delta$ is a square mod $p$ and $p$ is odd, this is immediately clear since there is an affine isomorphism between $\mathcal{C}$ and the hyperbolas $X^2 - Y^2 = 1$ and $XY = 1$; in particular, one has $\mathcal{C}(\mathbb{F}_q) \simeq \mathbb{F}_q^\times = \mathrm{GL}_1(\mathbb{F}_q)$ in this case.

On the elliptic curve side, we know that

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}, n_2 \mid n_1,$$

Moreover, we have $\#E(\mathbb{F}_p) = (p + 1) - a_p$, where $|a_p| \le 2\sqrt{p}$ by Hasse's theorem.

2.2. **$p$-adic Numbers.** If $p$ is an odd prime not dividing $\Delta$, then

$$\mathcal{C}(\mathbb{Z}_p) \simeq \begin{cases} \mathbb{Z}/(p-1) \oplus \mathbb{Z}_p & \text{if } (\frac{\Delta}{p}) = +1, \\ \mathbb{Z}/(p+1) \oplus \mathbb{Z}_p & \text{if } (\frac{\Delta}{p}) = -1, \\ \mathbb{Z}/2 \oplus \mathbb{Z}_p & \text{if } p \mid \Delta \neq -3, \\ \mathbb{Z}/6 \oplus \mathbb{Z}_p & \text{if } p = 3,\ \Delta = -3. \end{cases}$$

Reduction modulo $p^k$ then yields

$$\mathcal{C}(\mathbb{Z}/p^k) \simeq \begin{cases} \mathbb{Z}/(p-1) \oplus \mathbb{Z}/p^{k-1} & \text{if } (\frac{\Delta}{p}) = +1, \\ \mathbb{Z}/(p+1) \oplus \mathbb{Z}/p^{k-1} & \text{if } (\frac{\Delta}{p}) = -1, \\ \mathbb{Z}/2 \oplus \mathbb{Z}/p^k & \text{if } p \mid \Delta \neq -3, \\ \mathbb{Z}/6 \oplus \mathbb{Z}/3^{k-1} & \text{if } p = 3, \Delta = -3. \end{cases}$$

For elliptic curves $E/\mathbb{Q}_p$ we have a reduction map sending $\mathbb{Q}_p$-rational points to points defined over $\mathbb{F}_p$. The group $E_{ns}(\mathbb{F}_p)$ is the set of all nonsingular points of $E$ over $\mathbb{F}_p$. The subgroups $E_i(\mathbb{Q}_p)$ $(i = 0, 1)$ of $E(\mathbb{Q}_p)$ are defined as the inverse images of $E_{ns}(\mathbb{F}_p)$ and of the point of infinity of $E(\mathbb{F}_p)$ under the reduction map. These groups sit inside the exact sequence

$$0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{Q}_p) \longrightarrow E_{ns}(\mathbb{F}_p) \longrightarrow 0.$$

The structure of $E_{ns}(\mathbb{F}_p)$ is known: if $E/\mathbb{F}_p$ is nonsingular, it was discussed in Subsection 2.1; if $E/\mathbb{F}_p$ is singular, then $E_{ns}(\mathbb{F}_p)$ is isomorphic to $\mathcal{C}(\mathbb{F}_p)$ for a certain conic $\mathcal{C}$, and we say that $E$ has additive, multiplicative or split multiplicative reduction if the conic is a parabola ($\mathcal{C}(\mathbb{F}_p) \simeq \mathbb{F}_p$), a hyperbola ($\mathcal{C}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times$), or an ellipse ($\mathcal{C}(\mathbb{F}_p) \simeq \mathbb{F}_{p^2}[1]$, the group of elements with norm 1 in $\mathbb{F}_{p^2}$).

We also know hat $E_1(\mathbb{Q}_p) \simeq \mathbb{Z}_p$ and that the quotient group $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ is finite. Its order $c_p$ is called the Tamagawa number for the prime $p$, and clearly $c_p = 1$ we have for all primes $p \nmid \Delta$. More exactly it can be shown (albeit with some difficulty) that $c_p \le 4$ if $E$ has additive reduction, and that $c_p$ is the exact power of $p$ dividing $\Delta$ otherwise.

2.3. **Integral and Rational Points.** Now let us compare the structure of the groups of rational points: for elliptic curves, we have the famous theorem of Mordell-Weil that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\rm tors} \oplus \mathbb{Z}^r$, where $E(\mathbb{Q})_{\rm tors}$ is the finite group of points of finite order, and $r$ is the Mordell-Weil rank. For conics, on the other hand, we have two possibilities: either $C(\mathbb{Q}) = \varnothing$ (for example if $C : x^2 + y^2 = 3$) or $C(\mathbb{Q})$ is infinite, and in fact not finitely generated (see Tan [12]). The analogy can be saved, however, by looking at integers instead of rational numbers: if $K$ is a number field with ring of $S$-integers $\mathcal{O}_S$, then

$$C(\mathcal{O}_S) \simeq C(\mathcal{O}_S)_{\rm tors} \oplus \mathbb{Z}^r \qquad\qquad E(K) \simeq E(K)_{\rm tors} \oplus \mathbb{Z}^r$$

where $r \ge 0$ is called the Mordell-Weil rank. Shastri [10] computed the rank $r$ for the unit circle over number fields $K$ and $S = \varnothing$.

Note that the group of integral points on the hyperbola $XY = 1$ is isomorphic to $R^\times = \mathrm{GL}_1(R)$. Number theoretic algorithms working with the multiplicative group of $R = \mathbb{Z}/p\mathbb{Z}$ in general have an analog for conics, as we will see in the next section.

## 3. Applications

3.1. **Primality Tests.** The classical primality test due to Lucas is the following:

**Proposition 2.** *An odd integer $n$ is prime if and only if there exists an integer $a$ satisfying the following two conditions:*

i) $a^{n-1} \equiv 1 \bmod n$*;*
ii) $a^{(n-1)/r} \not\equiv 1 \bmod n$ *for every prime* $r \mid (n-1)$.

This primality test is based on the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, that is, on the group $\mathcal{H}(\mathbb{Z}/n\mathbb{Z})$ of $\mathbb{Z}/n\mathbb{Z}$-rational points on the hyperbola $\mathcal{H} : XY = 1$. Something similar works for any Pell conic:

**Proposition 3.** *Let $n \ge 5$ be an odd integer and $\mathcal{C} : X^2 - \Delta Y^2 = 4$ a nondegenerate Pell conic defined over $\mathbb{Z}/n\mathbb{Z}$ with neutral element $N = (2, 0)$, and assume that $(\Delta/n) = -1$. Then $n$ is a prime if and only if there exists a point $P \in \mathcal{C}(\mathbb{Z}/n\mathbb{Z})$ such that*

i) $(n+1)P = N$*;*
ii) $\frac{n+1}{r} P \ne N$ *for any prime $r$ dividing $n+1$.*

Of course, for both tests there are 'Proth-versions' in which only a part of $N \pm 1$ needs to be factored.

The following special case of Proposition 3 is well known: if $n = 2^p - 1$ is a Mersenne number, then $n \equiv 7 \bmod 12$ for $p \ge 3$, hence $(3/n) = -1$; if we choose the Pell conic $\mathcal{C} : X^2 - 12Y^2 = 4$ and and $P = (4, 1)$, then the test above is nothing but the Lucas-Lehmer test. We remark in passing that Gross [3] has come up with a primality test for Mersenne numbers based on elliptic curves.

3.2. **Factorization Methods.** The factorization method based on elliptic curves is very well known. Can we replace the elliptic curve by conics? Yes we can, and what we get is the $p-1$-factorization method for integers $N$ if we consider the conic $\mathcal{H} : xy = 1$, and some $p \pm 1$-factorization method for general Pell conics. The details are easy to work out for anyone familiar with Pollard's $p-1$-method.

## 4. 2-Descent

Consider the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$. Define a map $\alpha : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ by

$$\alpha(x,y) = \begin{cases} (x+2)\mathbb{Q}^{\times\,2} & \text{if } x \neq -2, \\ -\Delta\mathbb{Q}^{\times\,2} & \text{if } x = -2. \end{cases}$$

If $P = (x,y) \in \mathcal{C}(\mathbb{Z})$ with $x > 0$, then $P$ gives rise to an integral point on the descendant $\mathcal{T}_a(\mathcal{C}) : aX^2 - bY2 = 4$, where $a$ is a positive squarefree integer determined by $\alpha(P) = a\mathbb{Q}^{\times\,2}$, and $ab = \Delta$. Conversely, any integral point on some $\mathcal{T}_a(\mathcal{C})$ gives rise to an integral point with positive $x$-coordinate on the Pell conic $\mathcal{C}$.

It can be shown that $\alpha$ is a group homomorphism, and that we have an exact sequence

$$0 \longrightarrow 2\mathcal{C}(\mathbb{Z}) \longrightarrow \mathcal{C}(\mathbb{Z}) \xrightarrow{\alpha} \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}.$$

Moreover, we have $\#\mathrm{im}\,\alpha = 2^r$, where $r$ is the Mordell-Weil-rank of $C(\mathbb{Z})$, and the elements of $\mathrm{im}\,\alpha$ are represented by the first descendants $\mathcal{T}_a$ with $\mathcal{T}_a(\mathbb{Z}) \neq \varnothing$. Thus computing the Mordell-Weil rank is equivalent to counting the number of first descendants $\mathcal{T}_a$ with an integral point (see [8]).

The situation is completely analogous for elliptic curves $E : Y^2 = X(X^2+aX+b)$ with a rational point $(0,0)$ of order 2, except that here we also have to consider the 2-isogenous curve $\widehat{E} : Y^2 = X(X^2 + \widehat{a}\,X + \widehat{b})$, where $\widehat{a} = -2a$ and $\widehat{b} = a^2 - 4b$. We have two Weil maps $\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ and $\widehat{\alpha} : \widehat{E}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$, and the Mordell-Weil rank is given by Tate's formula $2^{r+2} = \#\mathrm{im}\,\alpha \cdot \#\mathrm{im}\,\widehat{\alpha}$. For more information on the descent via 2-isogenies we refer to Silverman & Tate [11].

4.1. **Selmer and Tate-Shafarevich Group.** The subset of descendants $\mathcal{T}_a$ : $ar^2 - bs^2 = 4$ with a rational point form a subgroup $\mathrm{Sel}_2(C)$ of $\mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ called the 2-Selmer group of $C$. Next we define the Tate-Shafarevich group $\text{Ш}_2(C)$ by the exact sequence

$$1 \longrightarrow \mathrm{im}\,\alpha \longrightarrow \mathrm{Sel}_2(C) \longrightarrow \text{Ш}_2(C) \longrightarrow 1.$$

In [8] we have shown that the 2-part of the Tate-Shafarevich group of the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$ is $\text{Ш}_2(\mathbb{Z}) \simeq \mathrm{Cl}^+(k)^2[2]$.

For a cohomological definition of Selmer and Tate-Shafarevich groups, we need to interpret conics as principal homogeneous spaces. Every conic $X^2 - \Delta Y2 = 4c$ is a principal homogeneous space for $\mathcal{C}(\mathbb{Q})$; this is to say that the map

$$\mu : \mathcal{D}(\mathbb{Z}) \times \mathcal{C}(\mathbb{Z}) \longrightarrow \mathcal{D}(\mathbb{Z}) : \mu((u,v),(x,y)) = (\tfrac{ux+\Delta vy}{2}, \tfrac{vx+uy}{2}).$$

has the following properties:

(1) $\mu(p,N) = p$ for all $p \in \mathcal{D}(\overline{\mathbb{Q}})$, where $N = (2,0)$ is the neutral element of $\mathcal{C}$.
(2) $\mu(\mu(p,P),Q) = \mu(p,P+Q)$ for all $p \in \mathcal{D}(\overline{\mathbb{Q}})$ and all $P,Q \in \mathcal{C}(\overline{\mathbb{Q}})$.

(3) For all $p, q \in \mathcal{D}(\mathbb{Q})$ there is a unique $P \in \mathcal{C}(\mathbb{Q})$ with $\mu(p, P) = q$.

Here $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$.

Note, however, that only those $\mathcal{D}$ with $c \mid \Delta$ are principal homogeneous space for $\mathcal{C}(\mathbb{Z})$, i.e., satisfy the property that for all $p, q \in \mathcal{D}(\mathbb{Z})$ there is a $P \in \mathcal{C}(\mathbb{Z})$ with $\mu(p, P) = q$. Also observe that the conics $\mathcal{D}$ with $c \mid \Delta$ can be written in the form $aX^2 - bY^2 = 4$ with $ab = \Delta$, that is, these are exactly the first descendants.

4.2. **Heights.** For a rational number $q = \frac{m}{n}$ in lowest terms, define its height $H(q) = \log \max\{|m|, |n|\}$; note that $H(0) = 0$ and $H(q) \geq 0$ for all $q \in \mathbb{Q}$. For rational points $P = (x, y) \in C(\mathbb{Q})$ on a conic $C : X^2 - \Delta Y^2 = 4$ put $H(P) = H(x)$.

Define the canonical height $\widehat{h}(P)$ by

$$\widehat{h}(P) = \lim_{n \to \infty} \frac{H(2^n P)}{2^n}.$$

The canonical height $\widehat{h}$ on the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$ has all the suspected properties (and more):

(1) $|\widehat{h}(P) - H(P)| < \log 4$;
(2) $\widehat{h}(T) = 0$ if and only if $T \in \mathcal{C}(\mathbb{Q})_{\rm tors}$;
(3) $\widehat{h}(mP) = m\widehat{h}(P)$ for all integers $m \geq 1$;
(4) $\widehat{h}(P + Q) \leq \widehat{h}(P) + \widehat{h}(Q)$;
(5) the square of the canonical height satisfies the parallelogram equality

$$\widehat{h}(P - Q)^2 + \widehat{h}(P + Q)^2 = 2\widehat{h}(P)^2 + 2\widehat{h}(Q)^2$$

for all $P, Q \in \mathcal{C}(\mathbb{Q})$.

In addition, there are explicit formulas for the canonical height. It is an easy exercise to show that every rational point on a Pell conic has the form $P = (x, y)$ with $x = \frac{r}{n}$, $y = \frac{s}{n}$, and $(r, n) = (s, n) = 1$. In this case we have

$$\widehat{h}(P) = \begin{cases} \log \frac{|r| + |s|\sqrt{\Delta}}{2} & \text{if } \Delta > 0, \\ \log |n| & \text{if } \Delta < 0. \end{cases}$$

The finiteness of $\mathcal{C}(\mathbb{Z}_S)/2\mathcal{C}(\mathbb{Z}_S)$ and the existence of a height function implies the theorem of Mordell-Weil.

## 5. Analytic Methods

5.1. **Zeta Functions.** Both for conics and elliptic curves over $\mathbb{Q}$ there is an analytic method that sometimes provides us with a generator for the group of integral or rational points on the curve. Before we can describe this method, we have to talk about zeta functions of curves.

Take a conic $C$ or an elliptic curve $E$ defined over the finite field $\mathbb{F}_p$; let $N_r$ denote the cardinalities of the groups of $\mathbb{F}_{p^r}$-rational points on $C$ and $E$ respectively, where we count solutions in the affine plane for $C$ and in the projective plane for $E$. Then

$$Z_p(T) = \exp\Big(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\Big)$$

is called the zeta function of $C$ or $E$ over $\mathbb{F}_p$.

For the parabola $C : y = x^2$, we clearly have $C(\mathbb{F}_q) \simeq \mathbb{F}_q$, hence $N_r = p^r$, and we find

$$Z_p(T) = \exp\Big(\sum_{r=1}^{\infty} p^r \frac{T^r}{r}\Big) = \exp(-\log(1-pT)) = \frac{1}{1-pT}.$$

For the conic $X^2 - \Delta Y^2 = 4$ we find after a little calculation

$$Z_p(T) = \frac{1}{(1-pT)(1-\chi(p)T)},$$

where $\chi$ is the Dirichlet character defined by $\chi(p) = (\Delta/p)$. The substitution $T = p^{-s}$ turns this into

$$\zeta_p(s;\mathcal{C}) = \frac{1}{(1-p^{1-s})(1-\chi(p)p^{-s})}.$$

For nonsingular elliptic curves over $\mathbb{F}_p$ we similarly get

$$Z_p(T) = \frac{P(T)}{(1-T)(1-pT)},$$

where $P(T) = qT^2 - a_pT + 1$ and $a_p$ is defined by $\#E(\mathbb{F}_p) = p + 1 - a_p$.

5.2. **L-Functions for Conics.** Now we take the zeta function for each $p$ and multiply them together to get a global zeta function. The first factor $1/(1-p^{1-s})$ gives us the product

$$\prod_{p \,\text{odd prime}} \frac{1}{1-p^{1-s}} = \zeta(s-1)(1-2^{1-s}),$$

that is, essentially the Riemann zeta function.

The other factor, on the other hand, is more interesting:

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}}$$

is a Dirichlet $L$-function for the quadratic character $\chi = (\Delta/\cdot)$. This function converges on the right half plane $\operatorname{Re} s > 1$ and can be extended to a holomorphic function on the complex plane.

Now the nice thing discovered by Dirichlet (in his proof that every arithmetic progression $ax+b$ with $(a,b) = 1$ contains infinitely many primes) is that, for every nontrivial (quadratic) character $\chi$, $L(s,\chi)$ has a nonzero value at $s = 1$. In fact, he was able to compute this value:

$$L(1,\chi) = \begin{cases} h \cdot \frac{2\pi}{w\sqrt{|\Delta|}} & \text{if } \Delta < 0, \\ h \cdot \frac{2\log\varepsilon}{\sqrt{\Delta}} & \text{if } \Delta > 0 \end{cases}$$

where $\chi(p) = (\Delta/p)$, and where $w$, $\Delta$, $h$ and $\varepsilon > 1$ are the number of roots of unity, the discriminant, the class number and the fundamental unit of $\mathbb{Q}(\sqrt{\Delta}\,)$.

The upshot is this: if $\Delta > 0$, the group $\mathcal{C}(\mathbb{Z})$ has rank 1; by using only local information (numbers of $\mathbb{F}_{p^r}$-rational points on $\mathcal{C}$) we have constructed a function whose value at 1 gives, up to well understood constants, a power of a generator of $\mathcal{C}(\mathbb{Z})$, namely the $h$-th power of the fundamental unit.

The functional equation of Dirichlet's $L$-function allows us to rewrite Dirichlet's formula as

$$\lim_{s\to 0} s^{-r} L(s,\chi) = \frac{2hR}{w},$$

where $r = 0$ and $R = 1$ for $\Delta < 0$, and $r = 1$ and $R = \log\varepsilon$ for $\Delta > 0$.

Observe that the evaluation of the $L$-funtion (which was defined using purely local data) at $s = 0$ yields a generator of the free part of the group $\mathcal{C}(\mathbb{Z})$ (which is a global object)!

### 5.3. L-Functions for Elliptic Curves.

The really amazing thing is that exactly the same thing works for elliptic curves of rank 1: by counting the number $N_r$ of $\mathbb{F}_{p^r}$-rational points on $E$, we get a zeta function $Z_p(T)$ that can be shown to have the form

$$Z_p(T) = \frac{P(T)}{(1-T)(1-pT)}$$

for some polynomial $P(T) \in \mathbb{Z}[T]$ of degree 2 (if $p$ does not divide the discriminant of $E$). In fact, if $p \nmid E$ we have $P(T) = 1 - a_p t + pt^2$, where $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Put $L_p(s) = 1/P(p^{-s})$ and define the $L$-function

$$L(s,E) = \prod_p L_p(s).$$

Hasse conjectured that this $L$-function can be extended analytically to the whole complex plane; moreover, there exists an $N \in \mathbb{N}$ such that

$$\Lambda(s,E) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s,E)$$

satisfies the functional equation $\Lambda(s-2,E) = \pm\Lambda(s,E)$ for some choice of signs. For curves with complex multiplication, this was proved by Deuring; the general conjecture is a consequence of the now proved Taniyama-Shimura conjecture.

## 6. Birch–Swinnerton-Dyer

### 6.1. Birch and Swinnerton-Dyer for Elliptic Curves.

The conjecture of Birch and Swinnerton-Dyer for elliptic curves predicts that $L(s,E)$ has a zero of order $r$ at $s = 1$, where $r$ is the rank of the Mordell-Weil group. More exactly, it is believed that

$$\lim_{s\to 1} \ (s-1)^r L(s;E) = \frac{\Omega \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot R(E/\mathbb{Q}) \cdot \prod c_p}{(\#E(\mathbb{Q})_{\text{tors}})^2},$$

where $r$ is the Mordell-Weil rank of $E(\mathbb{Q})$, $\Omega = c_\infty$ the real period, $\text{Ш}(E/\mathbb{Q})$ the Tate-Shafarevich group, $R(E/\mathbb{Q})$ the regulator of $E$ (some matrix whose entries are canonical heights of basis elements of the free part of $E(\mathbb{Q})$), $c_p$ the Tamagawa number for the prime $p$ (trivial for all primes not dividing the discriminant), and $E(\mathbb{Q})_{\text{tors}}$ the torsion group of $E$.

### 6.2. Birch and Swinnerton-Dyer for Conics.

We now want to interpret Dirichlet's class number formula in a similar way. Let $k = \mathbb{Q}(\sqrt{\Delta}\,)$ denote the quadratic number field associated to the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$. Then we conjecture that there is a cohomological definition of the Tate-Shafarevich group $\text{Ш}(\mathcal{C})$ whose 2-torsion coincides with the group $\text{Ш}_2(\mathcal{C})$ defined above, and that we have

$$\text{Ш}(\mathcal{C}) \simeq \text{Cl}^+(k)^2.$$

If we (preliminarily) define the Tamagawa numbers by

$$c_p = \begin{cases} 2 & \text{if } p \mid \Delta, \\ 1 & \text{otherwise,} \end{cases}$$

then Gauss's genus theory implies that

$$\prod c_p = 2(\mathrm{Cl}^+(k) : \mathrm{Cl}^+(k)^2).$$

Thus if we put $\Omega = \frac{1}{2}$, then $\Omega \cdot \#\text{Ш}(\mathcal{C}) \cdot \prod c_p = h^+$ equals the class number of $k$ in the strict sense, hence is equal to $2^u \cdot h$, where $u = 1$ if $N\varepsilon = +1$, and $u = 0$ otherwise.

If $\Delta > 0$, let $\eta > 1$ denote a generator of the free part of $\mathcal{C}(\mathbb{Z})$; then the regulator of $\mathcal{C}$ equals $\widehat{h}(\eta) = \log \eta$. Now we find $R(\mathcal{C}) = 2^{1-u}R$, hence $\Omega \cdot \#\text{Ш}(\mathcal{C}) \cdot R(\mathcal{C}) \cdot \prod c_p = h^+ \log \eta = 2hR$; this also holds for $\Delta < 0$ if we put $R = 1$.

Finally, $\mathcal{C}(\mathbb{Z})_{\mathrm{tors}}$ is the group of roots of unity contained in $k$, and we find

$$\frac{2hR}{w} = \frac{\Omega \cdot \#\text{Ш}(\mathcal{C}) \cdot R(\mathcal{C}) \cdot \prod c_p}{\#\mathcal{C}(\mathbb{Z})_{\mathrm{tors}}}$$

in (almost) perfect analogy to the Birch–Swinnerton-Dyer conjecture for elliptic curves.

In fact, the analogy would be even closer if we would replace $\#\mathcal{C}(\mathbb{Z})_{\mathrm{tors}}$ by $(\#\mathcal{C}(\mathbb{Z})_{\mathrm{tors}})^2$ and adjust the formulas for $c_2$ and $c_3$ for the two Pell conics with nontrivial torsion; this would also allow us to put $\Omega = 1$.

## 7. Summary

The analogy between Pell conics and elliptic curves is summarized in the following table:

| | $\mathrm{GL}_1$ | Pell conics | elliptic curves |
|---|---|---|---|
| group structure on | affine line | affine plane | projective plane |
| defined over | rings | rings | fields |
| group elements | $S$-units | $S$-integral points | rational points |
| group structure | $\mathbb{Z}/2 \oplus \mathbb{Z}^{\#S}$ | $C(\mathbb{Z}_S)_{\mathrm{tors}} \oplus \mathbb{Z}^r$ | $E(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r$ |
| associativity | clear | Pascal's Theorem | Bezout's Theorem |
| factorization alg. | $p-1$ | $p \pm 1$ | ECM |
| primality tests | Lucas-Proth | Lucas-Lehmer | ECPP |
| **Ш** | 1 | $\mathrm{Cl}^+(k)^2$ | ? |
| L-series | $\mathbb{Z}$ | quadratic field | modular form |

Moreover, cyclotomic fields are for Pell conics what modular curves are for elliptic curves, and cyclotomic units correspond to Heegner points. The analog of Heegner's Lemma (if a curve of genus 1 of the form $Y^2 = f_4(X)$, where $f_4$ is a quartic polynomial with rational coefficients, has a $K$-rational point for some number field $K$ of odd degree, then the curve has a rational point; cf. [4]) is due to Nagell [9], who proved the same result with $f_4$ replaced by a quadratic polynomial $f_2$.

## 8. Questions

Although the arithmetic of conics is generally regarded as being almost trivial, there are a lot of questions that are still open. The main problem is a good definition of the Tamagawa numbers in the case of conics, a cohomological description of the Selmer and Tate-Shafarevich groups, and the proof of $\text{Ш}(\mathcal{C}) \simeq \text{Cl}^+(k)^2$.

The next problem is the analytic construction of generators of $\mathcal{C}(\mathbb{Z}_S)$ if $S \neq \varnothing$. This suggests looking at the Stark conjectures, which predict that we can construct certain units (actually $S$-units) in number fields. It seems, however, that we cannot hope to find "independent" elements (see [13]).

On a simpler level there's the question whether iterated 2-descents on Pell conics provide an algorithm for computing the fundamental unit that is faster than current methods. And how does 3-descent on Pell conics work?

We can also think of generalizing the approach described here: the groups $\text{GL}_1$ and the Pell conics are special norm tori in the theory of algebraic groups, and there's the question of how much of the above carries over to the more general situation. The norm-1 tori associated to pure cubic fields can be described geometrically as cubic surfaces $\mathcal{S}$; do the groups of integral points on $\mathcal{S}$ admit a geometric group law? It is known that the groups of rational points on cubic surfaces coming from norm forms satisfy the Hasse principle; is there a connection between the 3-class groups of these fields and the Tate-Shafarevich groups on $\mathcal{S}$ defined as above as the obstruction to lifting the Hasse principle from rational to integral points?

On the elliptic curve side, there are a few questions suggested by the analogy worked out in this article. For example, is there a natural group whose order equals $\#\text{Ш}(E) \cdot \prod c_p$? Recall that $\exp(\widehat{h}(P))$ is algebraic for rational points on Pell conics; are there meromorphic functions $F$ such that $F(\widehat{h}(P))$ is algebraic for rational points $P$ on elliptic curves, at least for curves with complex multiplication?

## Acknowledgments

This article owes a lot to work done while I was at the University of Seoul in August 2002; I would like to thank Soun-Hi Kwon for the invitation and the hospitality.

## References

[1] H. Darmon, *Wiles' theorem and the arithmetic of elliptic curves*, in: Modular Forms and Fermat's Last Theorem, G. Cornell et al. (eds.), Springer Verlag 1997, 549–569; cf. p. 2

[2] H. Darmon, C. Levesque, *Sommes infinies, équations diophantiennes et le dernier théorème de Fermat*, Gazette des Sciences Mathématiques du Québec, Vol. XVIII, Avril 1996; cf. p. 2

[3] B. Gross, *An elliptic curve test for Mersenne primes*, preprint 2003; cf. p. 5

[4] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253; cf. p. 9

[5] F. Lemmermeyer, *Kreise und Quadrate modulo p*, Math. Sem. Ber. **47** (2000), 51–73; cf. p. 2

[6] F. Lemmermeyer, *Higher Descent on Pell Conics. I. From Legendre to Selmer*, preprint 2003; cf. p. 2

[7] F. Lemmermeyer, *Higher Descent on Pell Conics. II. Two Centuries of Missed Opportunities*, preprint 2003; cf. p. 2

[8] F. Lemmermeyer, *Higher Descent on Pell Conics. III. The First* 2*-Descent*, preprint 2003; cf. p. 2, 5

[9] T. Nagell, *Un théorème arithmétique sur les coniques*, Arkiv f. Mat. **2** (1952), 247–250 9

[10] P. Shastri, *Integral Points on the Unit Circle*, J. Number Theory **91** (2001), 67–70; cf. p. 4

[11] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag 1992; cf. p. 5

[12] Lin Tan, *The group of rational points on the unit circle*, Math. Mag. **69** (1996), no. 3, 163–171; cf. p. 4

[13] B. Tangedal, *A question of Stark*, Pac. J. Math. **180** (1997), 187–199; cf. p. 10

[14] D. Zagier, *The Birch-Swinnerton-Dyer conjecture from a naive point of view*, Arithmetic algebraic geometry (Texel, 1989), 377–389, Progr. Math., **89** 1991; cf. p. 2