

# CONICS - A POOR MAN'S ELLIPTIC CURVES

FRANZ LEMMERMEYER

## CONTENTS

Introduction	2
1. Dramatis Personae: Conics and Elliptic Curves	2
1.1. Elliptic Curves	2
1.2. Conics	2
2. Group Laws	3
2.1. Group Law on Elliptic curves	3
2.2. Group Law on Conics	4
3. Analytic Parametrization	4
3.1. Elliptic Curves	5
3.2. Pell Conics	5
4. The Group Structure	5
4.1. Elliptic Curves	5
4.2. Conics	6
5. Applications	7
5.1. Primality Tests	7
5.2. Factorization Methods	7
6. Mordell-Weil	8
6.1. Heights on Elliptic Curves	8
6.2. Heights on Pell Conics	9
6.3. 2-descent on Elliptic Curves	10
6.4. 2-descent on Pell Conics	10
6.5. Selmer and Tate-Shafarevich Group	11
7. Analytic Methods	12
7.1. Zeta Functions	12
7.2. L-Functions for Elliptic Curves	12
7.3. L-Functions for Conics	12
8. Coronidis Loco: The Conjecture of Birch and Swinnerton-Dyer	13
8.1. Birch and Swinnerton-Dyer for Elliptic Curves	13
8.2. Birch and Swinnerton-Dyer for Conics	14
9. Summary	15
10. Questions	15
Acknowledgments	16
References	16

## INTRODUCTION

It has been known for a long time that there is some form of analogy between elliptic curves and number fields; under this analogy, the group  $E(K)$  of  $K$ -rational points on an elliptic curve corresponds to the unit group of a number field, and the Tate-Shafarevich group  $\mathbf{III}(E/K)$  is the analog of the ideal class group of  $K$ . For popularizations of this point of view see e.g. [1, 2, 6, 15].

The aim of this article is to show that this analogy can be made much closer by looking at the units of quadratic number fields: geometrically these units are integral points on affine curves  $X^2 - dY^2 = 1$  called Pell conics; most concepts known from the arithmetic of elliptic curves, such as 2-descent, Selmer and Tate-Shafarevich groups, and even the conjecture of Birch and Swinnerton-Dyer, have an analog for Pell conics. We will not give any proofs here; the arithmetic of elliptic curves is well known, and for details in the case of conics as well as for historical comments we refer the interested reader to [7, 8, 9].

The extremely close analogy between the arithmetic of conics and of elliptic curves is quite surprising, in particular if one takes into account that we consider conics as groups of integral points in the affine plane, and elliptic curves as groups of rational points in the projective plane.

## 1. DRAMATIS PERSONAE: CONICS AND ELLIPTIC CURVES

Below we will discuss elliptic curves and Pell conics from a number theorists point of view. Both types of curves have a long history: Pythagorean triples correspond to rational points on the Pell conic  $X^2 + Y^2 = 1$ , solutions of the Pell equations have been studied by the Greeks (Archimedes used integral points on  $X^2 - 3Y^2 = 1$  and  $X^2 - 3Y^2 = -2$  to find an approximation for  $\sqrt{3}$  that he needed in his calculation of  $\pi$ ), 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, Sylvester and others before Poincaré laid down his program for studying diophantine equations given by curves according to their genus. While the history of the Pell equation has been studied in several books, a corresponding study of the history of elliptic curves is still lacking.

**1.1. Elliptic Curves.** An elliptic curve defined over  $\mathbb{Q}$  is an irreducible, nonsingular projective curve of genus 1 with a distinguished rational point. For us, elliptic curves will be given in Weierstrass form  $E : Y^2 = X^3 + aX + b$  with  $a, b \in \mathbb{Z}$  such that  $\Delta = -16(4a^2 + 27b^2) \neq 0$ , and the distinguished rational point is taken to be the point  $\mathcal{O} = [0 : 1 : 0]$  at infinity. The central problem in the arithmetic of elliptic curves is understanding the set  $E(\mathbb{Q})$  of rational points on  $E$ .

**1.2. Conics.** A conic is a plane affine curve of degree 2. Irreducible conics  $\mathcal{C}$  come in three types: we say that  $\mathcal{C}$  is a hyperbola, a parabola, or an ellipse according as the number of points at infinity on (the projective closure of)  $\mathcal{C}$  equals 2, 1, or 0. Over an algebraically closed field, every irreducible conic is a hyperbola.

Let  $d$  be a squarefree integer  $\neq 1$  and put

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

The conic  $\mathcal{P} : Q_0(X, Y) = 1$  associated to the principal quadratic form of discriminant  $\Delta$ ,

$$Q_0(X, Y) = \begin{cases} X^2 + XY + \frac{1-d}{4}Y^2 & \text{if } d \equiv 1 \pmod{4}, \\ X^2 - dY^2 & \text{if } d \equiv 2, 3 \pmod{4}, \end{cases}$$

is called the Pell conic of discriminant  $\Delta$ . Pell conics are irreducible nonsingular affine curves with a distinguished integral point  $N = (1, 0)$ . The problem corresponding to the determination of  $E(\mathbb{Q})$  is finding the integral points on a Pell conic.

## 2. GROUP LAWS

The idea that certain sets of points on curves can be given a group structure is relatively modern. For elliptic curves, the group structure became well known only in the 1920s; implicitly it can be found in the work of Clebsch, and Juel, in a rarely cited article, wrote down the group law for elliptic curves defined over  $\mathbb{R}$  and  $\mathbb{C}$  at the end of the 19th century.

### 2.1. Group Law on Elliptic curves.

*Geometric Group Law.* Given an elliptic curve  $E : y^2 = x^3 + ax + b$  defined over some 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. The group axioms are easily verified with the exception of associativity, which follows geometrically from a special case of Bézout's Theorem.

*Group Law via Divisors.* The problems with verifying associativity can be avoided by using the approach to the group law via function fields. To this end, let  $\mathcal{C}$  be the projective closure of the affine curve  $F(X, Y) = 0$ , where  $F \in K[X, Y]$ . For each point  $P$  on  $\mathcal{C}$ , the local ring  $\mathcal{O}_P(\mathcal{C})$  is a discrete valuation ring. Letting  $t_P$  denote a uniformizer, every element  $f \neq 0$  in the function field  $K(\mathcal{C})$  of  $\mathcal{C}$  can be written in the form  $f = t_P^r g$  for some  $g \in K(\mathcal{C})$  with  $g(P) \neq 0$ ; then we define  $\text{ord}_P(f) = r$ .

The divisor group  $\text{Div}(\mathcal{C})$  of  $\mathcal{C}$  is the free abelian group on the points of  $\mathcal{C}$  with coordinates in some algebraic closure  $\overline{K}$  of the base field  $K$ . Its elements can thus be written as  $\sum a_P(P)$  for  $P \in \mathcal{C}(\overline{K})$ , where only finitely many integers  $a_P$  are nonzero. The map  $\text{deg} : \text{Div}(\mathcal{C}) \rightarrow \mathbb{Z}; \sum a_P(P) \mapsto \sum a_P$  is called the degree map; the kernel of this map is the group  $\text{Div}^0(\mathcal{C})$  of divisors of degree 0.

To each  $f \in K(\mathcal{C})$  we associate the divisor

$$\text{div}(f) = \sum_{P \in \mathcal{C}(\overline{K})} \text{ord}_P(f)(P);$$

divisors of this form are called principal, and they form a subgroup  $\text{Pr}(\mathcal{C})$  of  $\text{Div}(\mathcal{C})$ . The quotient group  $\text{Pic}(\mathcal{C}) = \text{Div}(\mathcal{C})/\text{Pr}(\mathcal{C})$  is called the Picard group of  $\mathcal{C}$ , and the class of a divisor  $D$  will be denoted by  $[D]$ . Since principal divisors can be shown to have degree 0, we even have  $\text{Pr}(\mathcal{C}) \subset \text{Div}^0(\mathcal{C})$ ; the quotient  $\text{Pic}^0(\mathcal{C}) = \text{Div}^0(\mathcal{C})/\text{Pr}(\mathcal{C})$  is the Picard group of degree 0 of  $\mathcal{C}$ .

If  $E$  is an elliptic curve, then we have a homomorphism

$$\text{sum} : \text{Div}(E) \rightarrow E(\overline{K}); \sum a_P(P) \mapsto \sum a_P P.$$

**Proposition 1.** *Let  $E$  be an elliptic curve; then a divisor  $D \in \text{Div}(E)$  is principal if and only if  $\text{deg} D = 0$  and  $\text{sum}(D) = \mathcal{O}$ .*

This result easily implies that the map

$$\text{sum Pic}^0(E) \longrightarrow E(\overline{K})$$

is an isomorphism.

## 2.2. Group Law on Conics.

*Geometric Group Law.* The group law on Pell conics defined over a field  $F$  can be defined geometrically: for finding the sum of two rational points  $A, B \in \mathcal{P}(F)$ , draw the line through  $N$  parallel to  $AB$ , and denote its second point of intersection with  $C$  by  $A + B$ . 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 Bézout's Theorem. The addition formulas coming from the geometric definition can be simplified:

**Proposition 2.** *Consider the Pell conic  $\mathcal{P} : Q_0(X, Y) = 1$  with neutral element  $N = (1, 0)$ . Then the group law on  $\mathcal{P}$  is given by*

$$(r, s) + (t, u) = \begin{cases} (rt + \frac{d-1}{4}su, ru + st + su) & \text{if } d \equiv 1 \pmod{4}, \\ (rt + dsu, ru + st) & \text{if } d \equiv 2, 3 \pmod{4}. \end{cases}$$

Put

$$\omega_d = \begin{cases} \frac{1}{2}(1 + \sqrt{d}) & \text{if } d \equiv 1 \pmod{4}, \\ \sqrt{d} & \text{if } d \equiv 2, 3, \pmod{4}; \end{cases}$$

then it is easily checked that the map sending points  $(r, s) \in \mathcal{P}(\mathbb{Z})$  to the unit  $r + s\omega_d$  with norm 1 in the ring of integers  $\mathbb{Z}[\omega_d]$  of the quadratic number field  $K = \mathbb{Q}(\sqrt{d})$  is an isomorphism of groups.

*Group Law via Divisors.* (See Nekovar's lecture notes [11].)

Let  $\mathcal{C}$  be a smooth curve and  $S = \sum m_P(P) \geq 0$  some divisor in  $\text{Div}(\mathcal{C})$  with support  $S$  (this is the set of all places  $P$  with  $m_P \neq 0$ ). Then we define

$$\text{Div}_S(\mathcal{C}) = \{D \in \text{Div}(\mathcal{C}) : \text{supp}(D) \cap S = \emptyset\},$$

$$\text{Div}_S^0(\mathcal{C}) = \text{Div}_S(\mathcal{C}) \cap \text{Div}^0(\mathcal{C}),$$

$$P_m(\mathcal{C}) = \{\text{div}(f) : \text{ord}_P(f) \geq m_P\},$$

$$\text{Pic}_m(\mathcal{C}) = \text{Div}_S(\mathcal{C})/P_m(\mathcal{C}),$$

$$\text{Pic}_m^0(\mathcal{C}) = \text{Div}_S^0(\mathcal{C})/P_m(\mathcal{C}),$$

Consider the unit circle over  $\mathbb{C}$ . Its points at infinity are  $P_+ = [1 : i : 0]$  and  $P_- = [1 : -i : 0]$ . The map

$$\mathcal{C}(\mathbb{C}) \longrightarrow \text{Pic}_{(P_+)+(P_-)}^0; P \longmapsto [(P) - (N)],$$

where  $N = (1, 0)$ , is an isomorphism of groups.

Note that it is sufficient to give the group law for the unit circle  $\mathcal{C}$ , since every Pell conic is isomorphic to  $\mathcal{C}$  over the complex numbers.

## 3. ANALYTIC PARAMETRIZATION

In this section we briefly recall how to parametrize Pell conics and elliptic curves using trigonometric and Weierstrass  $\wp$ -functions.

**3.1. Elliptic Curves.** An important tool for studying elliptic curves  $E$  over the complex numbers is the isomorphism  $\mathbb{C}/\Lambda \simeq E$  provided by Weierstrass  $\wp$ -functions: for every elliptic curves there is a lattice  $\Lambda$  in  $\mathbb{C}$  such that the Weierstrass  $\wp$ -function with period lattice  $\Lambda$  parametrizes  $E$ ; in fact, we have an isomorphism  $\mathbb{C}/\Lambda \longrightarrow E : z + \Lambda \longmapsto (\wp(z), \wp'(z))$  of groups.

**3.2. Pell Conics.** Consider the Pell conic  $X^2 - dY^2 = 1$  (something analogous works for the Pell conics with discriminant  $\Delta \equiv 1 \pmod{4}$ ); then it is well known that  $\mathcal{P}$  is parametrized by

$$(X, Y) = \begin{cases} (\cos \alpha, \frac{\sin \alpha}{\sqrt{-d}}) & \text{if } \Delta < 0, \\ (\cosh \alpha, \frac{\sinh \alpha}{\sqrt{d}}) & \text{if } \Delta > 0. \end{cases}$$

This parametrization induces a group isomorphism

$$\mathcal{P}(\mathbb{R}) \simeq \begin{cases} \mathbb{R}/2\pi\mathbb{Z} & \text{if } \Delta < 0, \\ \mathbb{R} & \text{if } \Delta > 0. \end{cases}$$

The periodicity of the hyperbolic functions becomes visible only over the complex numbers.

Note that the parametrization

$$X = \frac{(1-d)\cos\alpha + 1 + d}{(1+d)\cos\alpha + 1 - d}, \quad Y = \frac{2\sin\alpha}{(1+d)\cos\alpha + 1 - d}$$

gives a bijection  $\mathbb{R}/2\pi\mathbb{Z} \longrightarrow \overline{\mathcal{P}}(\mathbb{R})$  between the circle  $\mathbb{R}/2\pi\mathbb{Z}$  and the projective closure  $\overline{\mathcal{P}}(\mathbb{R})$  of the Pell conic  $\mathcal{P}(\mathbb{R})$  over the reals. In general, however, it does not induce a group isomorphism.

#### 4. THE GROUP STRUCTURE

Let us now compare the known results about the group structure of the group of rational points on elliptic curves and the group of integral points on Pell conics over finite fields and the  $p$ -adic numbers.

##### 4.1. Elliptic Curves.

*Finite Fields.* The number of points on elliptic curves over a finite field  $\mathbb{F}_q$  satisfy the Hasse bound: we have  $\#E(\mathbb{F}_p) = (p + 1) - a_p$ , where  $|a_p| \leq 2\sqrt{p}$ . Moreover it is known that

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

*$p$ -adic Numbers.* 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 set  $E_{\text{ns}}(\mathbb{F}_p)$  of all nonsingular points of  $E$  over  $\mathbb{F}_p$  forms a group with respect to the geometric addition law given above. The subgroups  $E_i(\mathbb{Q}_p)$  ( $i = 0, 1$ ) of  $E(\mathbb{Q}_p)$  are defined as the inverse images of  $E_{\text{ns}}(\mathbb{F}_p)$  and of the point of infinity of  $E(\mathbb{F}_p)$  under the reduction map. These groups sit inside the exact sequence

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

following directly from the definitions and Hensel's Lemma. The structure of  $E_{\text{ns}}(\mathbb{F}_p)$  is known: for nonsingular curves  $E/\mathbb{F}_p$  it was discussed above; if  $E/\mathbb{F}_p$

is singular, then  $E_{\text{ns}}(\mathbb{F}_p)$  is isomorphic to  $\mathcal{C}(\mathbb{F}_p)$  for an irreducible conic  $\mathcal{C}$ , and we say that  $E$  has

$$\begin{cases} \text{additive} \\ \text{split multiplicative} \\ \text{nonsplit multiplicative} \end{cases} \quad \text{reduction if } \mathcal{C} \text{ is } \begin{cases} \text{a parabola} & (\mathcal{C}(\mathbb{F}_p) \simeq \mathbb{F}_p), \\ \text{a hyperbola} & (\mathcal{C}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times), \\ \text{an ellipse} & (\mathcal{C}(\mathbb{F}_p) \simeq \mathbb{F}_{p^2}[N]), \end{cases}$$

where  $\mathbb{F}_{p^2}[N]$  is the group of elements with norm 1 in  $\mathbb{F}_{p^2}$ .

We also know that  $E_1(\mathbb{Q}_p) \simeq \mathbb{Z}_p$  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  $c_p \leq 4$  if  $E$  has additive reduction, and that  $c_p$  is the exact power of  $p$  dividing  $\Delta$  otherwise.

#### 4.2. Conics.

*Finite Fields.* Let  $\mathcal{P} : Q_0(X, Y) = 1$  be a Pell conic defined over a finite field  $\mathbb{F}_q$  with  $q = p^f$  elements, and assume that  $\mathcal{P}$  is smooth, i.e. that  $p \nmid \Delta$ . Then

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

If  $\Delta$  is a square mod  $p$  and  $p$  is odd, this is immediately clear since there is an affine isomorphism between  $\mathcal{P}$  and the hyperbolas  $X^2 - Y^2 = 1$  and  $XY = 1$ ; in particular, one has  $\mathcal{P}(\mathbb{F}_q) \simeq \mathbb{F}_q^\times = \text{GL}_1(\mathbb{F}_q)$  in this case. If  $\Delta$  is a nonsquare modulo  $p$ , it turns out that  $\mathcal{P}(\mathbb{F}_q) \simeq \mathbb{F}_{q^2}^\times[N]$ , where  $\mathbb{F}_{q^2}^\times[N]$  denotes the kernel of the norm map from  $\mathbb{F}_q(\sqrt{\Delta})^\times$  to  $\mathbb{F}_q^\times$ .

*p-adic Numbers.* It is easy to see that  $\mathcal{P}(\mathbb{Z}_p) \simeq S^\times[N]$  for odd primes  $p$ , where  $S = \mathbb{Z}_p[\sqrt{\Delta}]$  and  $N$  is the norm in the (possibly trivial) extension  $\mathbb{Q}_p(\sqrt{\Delta})/\mathbb{Q}_p$ . Standard results on the structure of the unit group of  $\mathbb{Z}_p[\sqrt{\Delta}]$  now imply the following:

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

Now consider the Pell conic  $\mathcal{P}$  over  $\mathbb{Z}_p$  for odd primes  $p \mid \Delta$ . Reduction modulo  $p$  gives a map  $\mathcal{P}(\mathbb{Z}_p) \rightarrow \mathcal{P}(\mathbb{Z}/p\mathbb{Z})$ , where

$$\mathcal{P}(\mathbb{Z}/p\mathbb{Z}) : \begin{cases} X^2 - 1 = 0 & \text{if } p \mid d, d \equiv 2, 3 \pmod{4}, \\ (X + \frac{1}{2}Y)^2 - 1 = 0 & \text{if } p \mid d, d \equiv 1 \pmod{4}. \end{cases}$$

These conics over  $\mathbb{F}_p$  are degenerate and describe pairs of lines. We now call

$$\mathcal{P}^0(\mathbb{Z}/p\mathbb{Z}) : \begin{cases} Q_0(X, Y) = 1 & \text{if } p \nmid \Delta, \\ X = 1 & \text{if } p \mid d, d \equiv 2, 3 \pmod{4}, \\ X + \frac{1}{2}Y = 1 & \text{if } p \mid d, d \equiv 1 \pmod{4}. \end{cases}$$

the nonsingular part of  $\mathcal{P}(\mathbb{Z}/p\mathbb{Z})$ . Let  $\mathcal{P}_0$  denote the preimage of  $\mathcal{P}^0(\mathbb{Z}/p\mathbb{Z})$  under the reduction map; for odd primes  $p$ , the index

$$c_p = (\mathcal{P}(\mathbb{Z}_p) : \mathcal{P}_0)$$

is called the Tamagawa number for  $p$ . Since, for odd primes  $p$ , every point on  $\mathcal{P}^0(\mathbb{Z}/p\mathbb{Z})$  lifts to a point on  $\mathcal{P}(\mathbb{Z}_p)$ , we find

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

in this case. If  $p = 2$ , we simply define  $c_p$  by this property.

## 5. APPLICATIONS

Note that the group of integral points on the hyperbola  $XY = 1$  defined over some ring  $R$  is isomorphic to  $R^\times = \text{GL}_1(R)$ . 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 below. The corresponding algorithms based on elliptic curves are so well known that we do not bother to discuss them here.

**5.1. Primality Tests.** A classical primality test due to Lucas is the following:

**Proposition 3.** *An odd integer  $n$  is prime if and only if there exists an integer  $a$  satisfying the following two conditions:*

- i)  $a^{n-1} \equiv 1 \pmod{n}$ ;
- ii)  $a^{(n-1)/r} \not\equiv 1 \pmod{n}$  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 4.** *Let  $n \geq 5$  be an odd integer and  $\mathcal{P} : Q_0(X, Y) = 1$  a nondegenerate Pell conic defined over  $\mathbb{Z}/n\mathbb{Z}$  with neutral element  $N = (1, 0)$ , and assume that  $(\Delta/n) = -1$ . Then  $n$  is a prime if and only if there exists a point  $P \in \mathcal{P}(\mathbb{Z}/n\mathbb{Z})$  such that*

- i)  $(n+1)P = N$ ;
- ii)  $\frac{n+1}{r}P \neq N$  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 4 is well known: if  $n = 2^p - 1$  is a Mersenne number, then  $n \equiv 7 \pmod{12}$  for  $p \geq 3$ , hence  $(3/n) = -1$ ; if we choose the Pell conic  $\mathcal{P} : X^2 - 3Y^2 = 1$  and  $P = (2, 1)$ , 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.

**5.2. Factorization Methods.** The factorization method based on elliptic curves is very well known. Replacing the elliptic curve by conics we get the  $p-1$ -factorization method for the conic  $\mathcal{H} : XY - 1 = 0$ , 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.

## 6. MORDELL-WEIL

The original theorem of Mordell says that the group  $E(\mathbb{Q})$  is finitely generated. The simple proof given shortly thereafter by Weil proceeds in two steps: first it is shown that  $E(\mathbb{Q})/2E(\mathbb{Q})$  is finite, and then a height function compatible with the group structure is used to complete the proof. It is easy to see that  $\mathcal{P}(\mathbb{Q})$  is not finitely generated (see e.g. Tan [13]); on the other hand, imitating the proof above will show that  $\mathcal{P}(\mathbb{Z})$  is indeed a finitely generated abelian group. This last result is quite trivial, but remains true for the ring  $\mathbb{Z}_S$  of  $S$ -integers, where a little bit more work is required. Thus the theorem of Mordell-Weil states

$$C(\mathbb{Z}_S) \simeq C(\mathbb{Z}_S)_{\text{tors}} \oplus \mathbb{Z}^r \qquad E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

where  $r \geq 0$  is called the Mordell-Weil rank. Shastri [12] computed the rank  $r$  for the unit circle over number fields  $K$  and  $S = \emptyset$ . In this article we only deal with the case of ordinary integers ( $S = \emptyset$ ); the modifications that need to be made for general sets  $S$  of primes are worked out in [5].

The height functions for rational points on conics and elliptic curves are based on the notion of the height of a rational number. For  $q = \frac{m}{n}$  in lowest terms we define its height  $H(q) = \log \max\{|m|, |n|\}$ ; note that  $H(0) = 0$  and  $H(q) \geq 0$  for all  $q \in \mathbb{Q}$ .

**6.1. Heights on Elliptic Curves.** We can define a naive height on elliptic curves by putting  $H(\mathcal{O}) = 1$  and  $H(P) = H(x)$  for  $P = (x, y) \in E(\mathbb{Q})$ . This height function has the following properties:

**Proposition 5.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ .*

- (1) *for each  $\kappa > 0$ , the set  $\{P \in E(\mathbb{Q}) : H(P) < \kappa\}$  of rational points with bounded height is finite;*
- (2) *there exist constants  $C_1, C_2 > 0$  such that  $C_1 H(P)^4 \leq H(2P) \leq C_2 H(P)^4$  for all  $P \in E(\mathbb{Q})$ ;*
- (3) *there are constants  $c_1, c_2 > 0$  such that  $c_1 H(P)^2 H(Q)^2 \leq H(P+Q)H(P-Q) \leq c_2 H(P)^2 H(Q)^2$  for all  $P, Q \in E(\mathbb{Q})$ .*

The next step is the construction of the canonical height. First we introduce the logarithmic height  $h_0(P) = \log H(P)$ ; then we show

**Proposition 6.** *There is a unique function  $\widehat{h} : E(\mathbb{Q}) \rightarrow \mathbb{R}_{\geq 0}$  with the properties*

- (1) *there is some  $C > 0$  such that  $|\widehat{h}(P) - h_0(P)| < C$  for all  $P \in E(\mathbb{Q})$ ,*
- (2)  *$\widehat{h}(2P) = 4\widehat{h}(P)$  for all  $P \in E(\mathbb{Q})$ ;*

*it is given by*

$$\widehat{h}(P) = \lim_{n \rightarrow \infty} \frac{h_0(2^n P)}{4^n}.$$

The function  $\widehat{h}$  defined above is called the canonical height on  $E$ .

**Theorem 7.** *We have*

- (1)  *$\widehat{h}(T) = 0$  for  $T \in E(\mathbb{Q})$  if and only if  $T \in E(\mathbb{Q})_{\text{tors}}$ ;*
- (2)  *$\widehat{h}(mP) = m^2 \widehat{h}(P)$  for all  $m \in \mathbb{N}$  and all  $P \in E(\mathbb{Q})$ ;*

(3) *the canonical height satisfies the parallelogram equality:*

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

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

Had we defined a height  $H'$  by  $H'(P) = H(y)$ , the height function  $H'$  would differ only slightly from  $H$ . In fact since for points with large coordinates we have  $H(y^2) \approx H(x^3)$ , a simple calculation shows that  $H'(P)^2 \approx H(P)^3$ , and therefore  $2\widehat{h}'(P) = 3\widehat{h}(P)$ . This suggests putting  $h(P) = \frac{1}{2}\widehat{h}(P)$ ; then  $\widehat{h}(P) = 2h(P)$  and  $\widehat{h}'(P) = 3h(P)$ .

The height function  $h$  still has the properties of Theorem 7. The fact that  $h$  satisfies the parallelogram equality implies that the pairing

$$\langle P, Q \rangle = h(P + Q) - h(P) - h(Q)$$

for  $P, Q \in E(\mathbb{Q})$  is bilinear. If  $P_1, \dots, P_r$  are points in  $E(\mathbb{Q})$ , then  $\det(\langle P_i, P_j \rangle) = 0$  if and only if the  $P_i$  are dependent, i.e., if and only if there is a nontrivial relation  $a_1P_1 + \dots + a_rP_r = \mathcal{O}$  for integers  $a_i$ .

If the  $P_i$  are a basis of the free part of  $E(\mathbb{Q})$ , then the nonzero determinant

$$R(E) = \det(\langle P_i, P_j \rangle)$$

is independent of the choice of a basis and is called the regulator of  $E$ .

**6.2. Heights on Pell Conics.** Let  $\mathcal{P}$  denote the Pell conic of discriminant  $\Delta$ . We define the naive height of a rational point  $P = (x, y)$  on  $\mathcal{P}$  by  $H(P) = H(x)$ . This height function has the expected properties:

**Proposition 8.** *Let  $\mathcal{P}$  be the Pell conic of discriminant  $\Delta$ .*

- (1) *For each  $\kappa > 0$ , the set  $\{P \in \mathcal{P}(\mathbb{Q}) : H(P) < \kappa\}$  of rational points with bounded height is finite;*
- (2) *We have  $\frac{1}{4}H(P)^2 \leq H(2P) \leq 4H(P)^2$  for all  $P \in \mathcal{P}(\mathbb{Q})$ ;*
- (3) *We have  $H(P + Q)H(P - Q) \leq H(P)^2H(Q)^2$  for all  $P, Q \in E(\mathbb{Q})$ .*

As above, the naive height gives rise to the canonical height defined by

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

We find

**Theorem 9.** *The canonical height on Pell conics has the following properties:*

- (1)  $|\widehat{h}(P) - H(P)| < \log 2$  for all  $P \in \mathcal{P}(\mathbb{Q})$ ;
- (2)  $\widehat{h}(T) = 0$  if and only if  $T \in \mathcal{P}(\mathbb{Q})_{\text{tors}}$ ;
- (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  $P, Q \in \mathcal{P}(\mathbb{Q})$ .

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

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

Our definition of the canonical height has to be modified slightly; in fact, the analog of the conjecture of Birch and Swinnerton-Dyer only holds if we replace  $\widehat{h}$  by  $h = \frac{1}{2}\widehat{h}$ . This modification can be motivated as follows.

Let  $\phi : \mathbb{P}^1\mathbb{Q} \rightarrow C(\mathbb{Q}); t = [r : s] \mapsto P_t = (x_t, y_t)$  denote the parametrization of  $C : X^2 - dY^2 = 1$  given by

$$\phi([r : s]) = \left( \frac{s^2 + dr^2}{s^2 - dr^2}, \frac{2rs}{s^2 - dr^2} \right).$$

Then we define the naive height of  $P_t = (x_t, y_t) = \phi(t)$  with respect to  $\phi$  as  $H_\phi(P_t) = H(t) = \max\{|r|, |s|\}$  for  $t = [r : s]$ . The associated canonical height  $h$  is then equal to  $\frac{1}{2}\widehat{h}$ .

The fact that the square of the height satisfies the parallelogram equality means that we can define an associated pairing just as for elliptic curves.

**6.3. 2-descent on Elliptic Curves.** Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  with three rational points of order 2. Such an elliptic curve can be written in the form  $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$  for pairwise distinct integers  $e_i$ . The Weil homomorphism is a map  $E(\mathbb{Q}) \rightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$  defined by

$$\alpha(P) = \begin{cases} (1, 1) & \text{if } P = \mathcal{O}, \\ ((e_1 - e_2)(e_1 - e_3)) & \text{if } P = (e_1, 0), \\ ((e_2 - e_1)(e_2 - e_3)) & \text{if } P = (e_2, 0), \\ (x - e_1, x - e_2) & \text{if } P = (x, y), P \neq \{\mathcal{O}, (e_1, 0), (e_2, 0)\}. \end{cases}$$

The Weil homomorphism induces an exact sequence

$$0 \longrightarrow 2E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}) \xrightarrow{\alpha} \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2},$$

and the Mordell-Weil rank of  $E$  is determined by  $\#\text{im } \alpha = 2^{r+2}$ .

**6.4. 2-descent on Pell Conics.** Consider the Pell conic  $\mathcal{P} : Q_0(X, Y) = 1$ . In order to construct a Weil homomorphism  $\alpha : \mathcal{P}(\mathbb{Z}) \rightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$  with kernel  $2\mathcal{P}(\mathbb{Z})$ , we observe that for  $\mathcal{P} : X^2 - dY^2 = 1$  we have  $2(r, s) = (r^2 + ds^2, 2rs) = (2r^2 - 1, 2rs)$ ; since  $2(2r^2 - 1) + 2 = 4r^2$  is a square, we are led to define

$$\alpha(x, y) = \begin{cases} 2(x+1)\mathbb{Q}^{\times 2} & \text{if } x \neq -1, d \equiv 2, 3 \pmod{4} \\ (2(x+1) + y)\mathbb{Q}^{\times 2} & \text{if } x \neq -1, d \equiv 1 \pmod{4} \\ -\Delta\mathbb{Q}^{\times 2} & \text{if } x = -1. \end{cases}$$

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

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

Now consider factorizations  $d = ab$ ; for each such factorization put

$$Q_a(X, Y) = \begin{cases} aX^2 + aXY + \frac{a-b}{4}Y^2 & \text{if } d \equiv 1 \pmod{4}, \\ aX^2 - bY^2 & \text{if } d \equiv 2 \pmod{4}, \\ aX^2 - bY^2, 2aX^2 + 2aXY + \frac{a-b}{2}Y^2 & \text{if } d \equiv 3 \pmod{4}. \end{cases}$$

Then  $Q_a$  is a binary quadratic form whose square in the class group of forms with discriminant  $\Delta$  is the principal class:  $2[Q_a] = [Q_0]$ . Next define conics

$$\mathcal{T}_a : Q_a(X, Y) = 1.$$

These conics are principal homogeneous spaces under the natural action of  $\mathcal{P}$ . Every point  $P = (x, y) \in \mathcal{P}(\mathbb{Z})$  with  $x > 0$  gives rise to an integral point on some  $\mathcal{T}_a(\mathcal{P})$ .

Moreover, we have  $\#\text{im } \alpha = 2^{r+1}$ , where  $r$  is the Mordell-Weil-rank of  $\mathcal{P}(\mathbb{Z})$ , and the elements of  $\text{im } \alpha$  are represented by the conics  $\mathcal{T}_a$  with  $\mathcal{T}_a(\mathbb{Z}) \neq \emptyset$ . Thus computing the Mordell-Weil rank is equivalent to counting the number of  $\mathcal{T}_a$  with an integral point (see [9]).

Note that if e.g.  $ab = d \equiv 3 \pmod{4}$ , then the principal homogeneous space  $\mathcal{T} : 2aX^2 + 2aXY + \frac{a-b}{2}Y^2 = 1$  can be written in the form  $ax^2 - by^2 = 2$  for  $x = 2X + Y$  and  $y = Y$ , hence indeed gives first descendants of the Pell conic as we know them from [7, 9].

**6.5. Selmer and Tate-Shafarevich Group.** The integral points on a Pell conic  $\mathcal{P}$  of discriminant  $\Delta$  act on a conic  $\mathcal{T} = \mathcal{T}_Q : Q(X, Y) = 1$ , where  $Q$  also has discriminant  $\Delta$ , in a natural way: interpreting rational points on  $\mathcal{T}$  as elements of a certain norm in  $\mathbb{Q}(\sqrt{\Delta})$ , the action of a point on the Pell conic is given by multiplication by the corresponding unit.

This action makes  $\mathcal{T}$  into a principal homogeneous space for  $\mathcal{P}$ , i.e., the map  $\mu : \mathcal{T} \times \mathcal{P}(\mathbb{Z}) \longrightarrow \mathcal{T}$  has the following properties:

- (1)  $\mu(p, N) = p$  for all  $p \in \mathcal{T}(\mathbb{A})$ , where  $N$  is the neutral element of  $\mathcal{P}$ .
- (2)  $\mu(\mu(p, P), Q) = \mu(p, P + Q)$  for all  $p \in \mathcal{T}(\mathbb{A})$  and all  $P, Q \in \mathcal{P}(\mathbb{Z})$ .
- (3) For all  $p, q \in \mathcal{T}(\mathbb{Z})$  there is a unique  $P \in \mathcal{P}(\mathbb{Z})$  with  $\mu(p, P) = q$ .

Here  $\mathbb{A}$  denotes the ring of algebraic integers.

Recall that two quadratic forms  $Q, Q'$  of discriminant  $\Delta$  are called equivalent over  $\mathbb{Z}$  ( $\mathbb{Z}_p$ ) if there exists a unimodular matrix  $T$  with coefficients in  $\mathbb{Z}$  ( $\mathbb{Z}_p$ ) such that  $Q' = Q|_T$ ; if  $T = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$  and  $Q = (a, b, c)$ , then  $Q' = (a', b', c')$  is given by

$$a'X^2 + b'XY + c'Y^2 = a(rX + tY)^2 + b(rX + tY)(sX + uY) + c(sX + uY)^2.$$

Two torsors  $\mathcal{T}, \mathcal{T}'$  are called equivalent over  $\mathbb{Z}$  ( $\mathbb{Z}_p$ ) if the corresponding quadratic forms  $Q, Q'$  are equivalent.

**Proposition 10.** *A torsor  $\mathcal{T}_Q$  is equivalent to the torsor  $\mathcal{P}$  over  $\mathbb{Z}$  ( $\mathbb{Z}_p$ ) if and only if  $\mathcal{T}_Q(\mathbb{Z}) \neq \emptyset$  ( $\mathcal{T}_Q(\mathbb{Z}_p) \neq \emptyset$ ).*

The set of equivalence classes of torsors of the Pell conic  $\mathcal{P}$  form a group: the product of  $\mathcal{T}_Q$  and  $\mathcal{T}_{Q'}$  is the class of the torsor  $\mathcal{T}_{QQ'}$ , where  $QQ'$  denotes the composition of the (classes of) quadratic forms  $Q$  and  $Q'$ .

**Theorem 11.** *The Weil-Châtelet group  $WC(\mathcal{P})$  of all torsors of  $\mathcal{P}$  is isomorphic to  $\text{Cl}^+(\Delta)$ , the class group in the strict sense of binary quadratic forms with discriminant  $\Delta$ . The Tate-Shafarevich group  $\mathbf{III}(\mathcal{P})$  is the subgroup of classes of everywhere locally solvable torsors (those with a point in  $\mathbb{Z}_p$  for every prime  $p$ ), and is isomorphic to  $\text{Cl}^+(\Delta)^2$ , the group of squares of ideal classes in the strict sense.*

The definition of the Weil-Châtelet group for conics that we have given possibly has to be modified, and a more intrinsic definition might give rise to a group that contains the  $WC(\mathcal{P})$  given above as a proper subgroup. Our definition is good enough to capture the torsors occurring in the various 2-descents; in particular, the 2-torsion  $\mathbf{III}(\mathcal{P})[2]$  coincides with the group  $\mathbf{III}_2(\mathcal{P})$  defined above.

## 7. ANALYTIC METHODS

**7.1. 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

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

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

**7.2. L-Functions for Elliptic Curves.** For nonsingular elliptic curves over  $\mathbb{F}_p$ , the zeta function has the form

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

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

Now put  $L_p(s) = 1/P(p^{-s})$  with

$$P(T) = \begin{cases} 1 - a_pT + pT^2 \\ 1 - T \\ 1 + T \\ 1 \end{cases} \quad \text{if the reduction of } E \text{ is } \begin{cases} \text{good,} \\ \text{split multiplicative,} \\ \text{non-split multiplicative,} \\ \text{additive,} \end{cases}$$

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 should exist an integer  $N \in \mathbb{N}$  such that

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

satisfies the functional equation  $\Lambda(2-s, E) = \pm \Lambda(s, E)$  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.

**7.3. L-Functions for Conics.** The zeta function of the parabola  $Z = X^2$  is easily seen to be

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

For the Pell conic  $Q_0(X, Y) = 1$  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  $\chi(p) = (\Delta/p)$ . In particular, we have

$$Z_p(T) = \begin{cases} \frac{1}{(1-pT)(1-T)} & \text{if } \mathcal{C} \text{ is a hyperbola,} \\ \frac{1}{(1-pT)(1+T)} & \text{if } \mathcal{C} \text{ is an ellipse.} \end{cases}$$

We regard the factor  $\frac{1}{1-pT}$  as trivial; the nontrivial factors of the zeta function is then

$$P(T) = \begin{cases} 1 & \text{if } \mathcal{C} \text{ is a parabola,} \\ \frac{1}{1-T} & \text{if } \mathcal{C} \text{ is a hyperbola,} \\ \frac{1}{1+T} & \text{if } \mathcal{C} \text{ is an ellipse.} \end{cases}$$

(Compare this with the zeta functions of elliptic curves with bad reduction at  $p$ .)

We now make the substitution  $T = p^{-s}$  and multiply the nontrivial factors together to get a global zeta function. The trivial factor  $1/(1 - p^{1-s})$  gives us the product

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

that is, just a shift of the Riemann zeta function.

The other factor is more interesting:

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

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

For stating the functional equation, let  $\chi$  be a quadratic Dirichlet character with conductor  $N > 0$ , let  $\tau(\chi)$  be the associated Gauss sum, and set

$$\varepsilon = \begin{cases} 0 & \text{if } \chi(-1) = +1, \\ 1 & \text{if } \chi(-1) = -1; \end{cases}$$

note that  $\chi(-1) = +1$  is equivalent to  $\Delta > 0$ . Now define the completed  $L$ -series

$$\Lambda(\chi, s) = N^{s/2} \pi^{-(s+\varepsilon)/2} \Gamma\left(\frac{s+\varepsilon}{2}\right) L(s, \chi).$$

Then the functional equation is

$$\Lambda(s, \chi) = \Lambda(1 - s, \chi).$$

For Dirichlet characters that are not necessarily quadratic, the functional equation reads  $\Lambda(s, \chi) = W_\chi \Lambda(1 - s, \bar{\chi})$ , where  $W_\chi = \frac{(-i)^\varepsilon}{\sqrt{N}} \tau(\chi)$  is a constant of absolute value 1.

Note that the functional equation coupled with the fact that  $\Gamma(s)$  has a simple pole at  $s = 0$  implies that  $L(s, \chi)$  has a simple zero if  $\chi(-1) = 1$ , and that  $L(0, \chi) \neq 0$  if  $\chi(-1) = -1$ .

## 8. CORONIDIS LOCO: THE CONJECTURE OF BIRCH AND SWINNERTON-DYER

**8.1. 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

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

where  $r$  is the Mordell-Weil rank of  $E(\mathbb{Q})$ ,  $\Omega = c_\infty$  the real period,  $\mathbf{III}(E/\mathbb{Q})$  the Tate-Shafarevich group,  $R(E/\mathbb{Q})$  the regulator of  $E$  (some matrix whose entries measure the 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  $E$ .

**8.2. Birch and Swinnerton-Dyer for Conics.** Dirichlet, in his proof that every arithmetic progression  $ax + b$  with  $(a, b) = 1$  contains infinitely many primes, discovered 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:

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

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

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

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

We now would like to interpret Dirichlet's class number formula in a way that resembles the conjecture of Birch and Swinnerton-Dyer. Let  $k = \mathbb{Q}(\sqrt{\Delta})$  denote the quadratic number field associated to the Pell conic  $\mathcal{P} : Q_0(X, Y) = 1$ . Recall that

$$\mathbf{III}(\mathcal{P}) \simeq \text{Cl}^+(k)^2,$$

and that the Tamagawa numbers are given by

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

Now Gauss's genus theory implies that

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

Thus  $\#\mathbf{III}(\mathcal{P}) \cdot \prod c_p = 2h^+$  equals twice the class number of  $k$  in the strict sense, hence is equal to  $2^{1+u} \cdot h$ , 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  $\mathcal{P}(\mathbb{Z})$ ; then the regulator of  $\mathcal{P}$  equals  $h(\eta) = \frac{1}{2} \log \eta$ . Thus  $R(\mathcal{P}) = 2^{-u} R$ , hence  $\#\mathbf{III}(\mathcal{P}) \cdot R(\mathcal{P}) \cdot \prod c_p = 2hR$ ; this also holds for  $\Delta < 0$  if we put  $R = 1$ .

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

$$\frac{2hR}{w} = \frac{\#\mathbf{III}(\mathcal{P}) \cdot R(\mathcal{P}) \cdot \prod c_p}{\#\mathcal{P}(\mathbb{Z})_{\text{tors}}}$$

in perfect analogy to the Birch–Swinnerton-Dyer conjecture for elliptic curves. The fact that the integral defining  $\Omega$  does not converge for conics explains the absence

of  $\Omega$ ; the reason why the denominator is  $\#\mathcal{P}(\mathbb{Z})_{\text{tors}}$  and not its square is explained by Zagier [15].

9. SUMMARY

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

	GL <sub>1</sub>	Pell conics	elliptic curves
group structure on	affine line	affine plane	projective plane
defined over	rings	rings	fields
group elements	units	integral points	rational points
group structure	$\mathbb{Z}/2 \oplus \mathbb{Z}$	$\mathcal{P}(\mathbb{Z})_{\text{tors}} \oplus \mathbb{Z}^r$	$E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$
associativity	clear	Pascal's Theorem	Bézout's Theorem
factorization alg.	$p - 1$	$p \pm 1$	ECM
primality tests	Lucas-Proth	Lucas-Lehmer	ECPP
<b>III</b>	1	$\text{Cl}^+(k)^2$	finite ?
L-series	$\zeta(s)$	$L(s, \chi)$	$L(s, f)$

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 [10], who proved the same result with  $f_4$  replaced by a quadratic polynomial  $f_2$ .

10. QUESTIONS

It is rather obvious that other concepts from the arithmetic of elliptic curves also can be transferred to Pell conics; this is true in particular for division polynomials, Tate modules, Galois representations, Euler systems, . . .

There are also many questions whose investigation seems promising. First we can ask 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? For which rings  $R$  is  $\mathcal{P}(R)$  finitely generated? Is it true for rings of finite type over  $\mathbb{Z}$ , i.e. for quotient rings of  $\mathbb{Z}[X_1, \dots, X_n]$ ? Computing the rank is a nontrivial problem even for "Pell surfaces" ( $n = 1$ ), where the existence of a nontrivial solution can be linked to problems in the Jacobian of hyperelliptic curves (see Yu [14]); it certainly would be interesting to link the obstruction to the existence of solutions to the Tate-Shafarevich group of the Pell conic over  $\mathbb{Z}[T]$ .

We can also think of generalizing the approach described here: the groups GL<sub>1</sub> and the Pell conics are special norm tori in the theory of algebraic groups, and we can ask 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?

There are good reasons of studying the norm-1 torus for pure cubic fields over the field  $\mathbb{Q}(\rho)$  of cube roots of unity. In fact, an important tool in working with the Tate-Shafarevich group of conics is the parametrization of the Pell conic, which can be done algebraically as follows: the rational points  $(x, y)$  on  $X^2 - \Delta Y^2 = 1$  are solutions of the equation  $N\alpha = 1$  with  $\alpha = x + y\sqrt{\Delta}$ . By Hilbert's Theorem 90, these can be written in the form  $\alpha = \beta^{1-\sigma}$ , and setting  $\beta = r + s\sqrt{\Delta}$  gives the parametrization  $x = \frac{r^2 + \Delta s^2}{r^2 - \Delta s^2}$ ,  $y = \frac{2rs}{r^2 - \Delta s^2}$ . The same approach works for pure cubic fields over  $\mathbb{Q}(\rho)$ .

Recently, analogs of the Pell conics have been studied in connection with torus-based cryptography. It remains to be seen whether the program outlined here can also be adapted to this more general situation.

#### 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. I also exchanged emails with Jeff Lagarias; in particular the idea of using binary quadratic forms to construct principal homogeneous spaces for Pell conics is due to him.

#### 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. 7
- [4] K. Heegner, *Diophantische Analysis und Modulfunktionen*, *Math. Z.* **56** (1952), 227–253; cf. p. 15
- [5] J. Lagarias, private communication 8
- [6] F. Lemmermeyer, *Kreise und Quadrate modulo  $p$* , *Math. Sem. Ber.* **47** (2000), 51–73; cf. p. 2
- [7] F. Lemmermeyer, *Higher Descent on Pell Conics. I. From Legendre to Selmer*, preprint 2003; cf. p. 2, 11
- [8] F. Lemmermeyer, *Higher Descent on Pell Conics. II. Two Centuries of Missed Opportunities*, preprint 2003; cf. p. 2
- [9] F. Lemmermeyer, *Higher Descent on Pell Conics. III. The First 2-Descent*, preprint 2003; cf. p. 2, 11
- [10] T. Nagell, *Un théorème arithmétique sur les coniques*, *Arkiv f. Mat.* **2** (1952), 247–250; cf. p. 15
- [11] J. Nekovar, *Elliptic curves and modular forms*, lecture notes DEA 2003/04, Paris VI; cf. p. 4
- [12] P. Shastri, *Integral Points on the Unit Circle*, *J. Number Theory* **91** (2001), 67–70; cf. p. 8
- [13] L. Tan, *The group of rational points on the unit circle*, *Math. Mag.* **69** (1996), no. 3, 163–171; cf. p. 8
- [14] J. Yu, *On arithmetic of hyperelliptic curves*, *Aspects of Mathematics*, HKU 2001, 395–415 15
- [15] 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, 15