HIGHER DESCENT ON PELL CONICS. III. THE FIRST 2-DESCENT

FRANZ LEMMERMEYER

In [Lem2003b] we have sketched the historical development of problems related to Legendre's equations $ar^2 - bs^2 = 1$ and the associated Pell equation $x^2 - dy^2 = 1$ with $d = ab$. In [Lem2003c] we discussed certain "non-standard" ideas to solve the Pell equation. Now we move from the historical to the modern part: below we will describe the theory of the first 2-descent on Pell conics and explain its connections to some of the results described in [Lem2003b], leaving the theory of the second 2-descent and its relations to results from [Lem2003c] to another occasion.

As everyone familiar with the basic arithmetic of elliptic curves will notice, many of the results (e.g. those on heights) presented here are special cases of more general theorems.

1. Pell Conics

Since it is our ultimate goal to develop a theory of the Pell equation that is as close to the theory of elliptic curves as possible, we will first introduce a more geometric language.

We will work over a commutative ring R with a unit element, which most ofen is $\mathbb{Z}$, $\mathbb{Z}_p$, or a finite field of odd characteristic. Thus we may and will assume that R is an integral domain with a quotient field of characteristic $\neq 2$.

Working with the Pell equation $X^2 - dY^2 = 1$ leads to numerous problems (not insurmountable, but annoying). For this reason we will work exclusively with $X^2 - \Delta Y^2 = 4$, where

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

Here and in the rest of this article, d will always denote a squarefree integer; in particular, Δ is squarefree or 4 times a squarefree number. The equation $X^2 - \Delta Y^2 = 4$ with $\Delta \in R$ describes a plane algebraic affine curve $\mathcal{C}$, and the set

$$\mathcal{C}(R) = \{(x, y) \in R \times R : x^2 - dy^2 = 4\}$$

is called the set of R-integral points on the conic.

We now define a group law on the set $\mathcal{C}(\mathbb{Q})$ of rational points on $\mathcal{C}$ by fixing the neutral element $N = (2, 0)$ and defining $P + Q = R$ for points $P, Q, R \in \mathcal{C}(\mathbb{Z})$ by letting R denote the second point of intersection of the parallel to PQ through N (see Figure 1).

Proposition 1.1. *The sum of the two points $P = (r, s)$ and $Q = (t, u)$ in $\mathcal{C}(\mathbb{Q})$ is*

$$P + Q = \begin{cases} \left(\frac{r^2 + \Delta s^2}{2}, rs\right) = (r^2 - 2, rs) & \text{if } P = Q, \\ \left(2\frac{\Delta(s-u)^2 + (r-t)^2}{\Delta(s-u)^2 - (r-t)^2}\ ,\ 4\frac{(r-t)(s-u)}{\Delta(s-u)^2 - (r-t)^2}\right) & \text{if } P \neq Q. \end{cases} \tag{1}$$

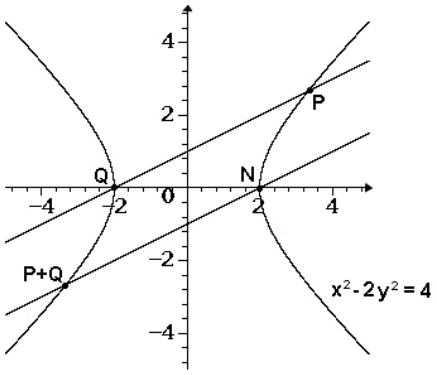

FIGURE 1. Addition Law on Pell Conics

Observe that these formulas work in any field in which Δ is not a square; this condition guarantees that the denominator $\Delta(s-u)^2-(r-t)^2$ is nonzero whenever $P \neq Q$.

Proof. For adding the points $P=(r,s)$ and $Q=(t,u)$, we have to draw a parallel to the line PQ through N and compute its second point of intersection with $\mathcal{C}$. Lines through $N=(2,0)$ have the equation $Y=m(X-1)$.

If $P=Q$, then the slope m of the the tangent at P can be computed by taking the derivative of the curve equation and solving for Y'; we find $Y'=\frac{x}{\Delta y}$, hence $m=\frac{r}{\Delta s}$ in $P=(r,s)$. A simple calculation yields $X=\frac{1}{2}(r^2+\Delta s^2)=r^2-2$ and $Y=rs$.

Now assume that $P \neq Q$; if $r=t$, then $P=(r,s)$ and $Q=(r,-s)$, and the line through N parallel to PQ is tangent to N, that is, we have $P+Q=N$; this agrees with the formulas above.

Thus we may assume that $r \neq t$; the line through PQ has slope $m=\frac{s-u}{r-t}$. Intersecting this line with $\mathcal{C}$ leads to

$$(X-2)\big[X+2-\Delta m^2(X-2)\big]=0;$$

since $X=2$ gives the point N, the X-coordinate of the second point of intersection is given by

$$X=2\frac{\Delta m^2+1}{\Delta m^2-1}.$$

Plugging in $m=\frac{s-u}{r-t}$, we find

$$P+Q=\Big(2\frac{\Delta(s-u)^2+(r-t)^2}{\Delta(s-u)^2-(r-t)^2}\ ,\ \frac{s-u}{r-t}(X-2)\Big).$$

Now observe that $\frac{s-u}{r-t}(X-2)=4\frac{(r-t)(s-u)}{\Delta(s-u)^2-(r-t)^2}$. □

Since we are interested in the integral and not the rational solutions of Pell equations, the geometric group law does not seem to be very helpful. Fortunately, all is not lost:

Proposition 1.2. *The addition formula (1) is valid over $\mathbb{Z}$: we have*

$$2\frac{\Delta(s-u)^2+(r-t)^2}{\Delta(s-u)^2-(r-t)^2}=\frac{rt+\Delta su}{2},\quad 4\frac{(r-t)(s-u)}{\Delta(s-u)^2-(r-t)^2}=\frac{ru+st}{2},$$

hence $P+Q=(\frac{rt+\Delta su}{2},\frac{ru+st}{2})\in\mathcal{C}(\mathbb{Z})$ for points $P=(r,s)$ and $Q=(t,u)$ in $\mathcal{C}(\mathbb{Z})$.

Proof. There is nothing to show if $P=Q$ since, in this case, the coordinates of $P+Q$ are obviously integral.

Thus we only have to consider the case $P\neq Q$. We have to show that the denominator $\Delta(s-u)^2-(r-t)^2$ divides the numerator. Now we can simplify this expression by observing

$$\Delta(s-u)^2-(r-t)^2=\Delta s^2-r^2+\Delta u^2-t^2+2rt-2\Delta su=2(rt-\Delta su-4).$$

Since $(rt-\Delta su-4)(ru+st)=4(r-t)(s-u)$, this gives

$$4\frac{(r-t)(s-u)}{\Delta(s-u)^2-(r-t)^2}=4\frac{(r-t)(s-u)}{2(rt-\Delta su-4)}=\frac{(rt-\Delta su-4)(ru+st)}{2(rt-\Delta su-4)}=\frac{ru+st}{2}.$$

Observe that if $\Delta\equiv 1 \bmod 4$, then $r\equiv s, t\equiv u \bmod 2$, hence $ru+st\equiv 0 \bmod 2$.

Now let us look at the numerator of the x-coordinate; since

$$\begin{aligned}4(r^2+\Delta s^2+t^2+\Delta u^2)&=(t^2-\Delta u^2)(r^2+\Delta s^2)+(r^2-\Delta s^2)(t^2+\Delta u^2)\\&=2(r^2t^2-\Delta^2s^2u^2)=2(rt+\Delta su)(rt-\Delta su),\end{aligned}$$

we find

$$\begin{aligned}2[\Delta(s-u)^2+(r-t)^2]&=2[r^2+\Delta s^2+t^2+\Delta u^2-2(rt+\Delta su)]\\&=(rt+\Delta su)(rt-\Delta su)-4(rt+\Delta su)]\\&=(rt+\Delta su)(rt-\Delta su-4).\end{aligned}$$

This finally shows

$$2\frac{\Delta(s-u)^2+(r-t)^2}{\Delta(s-u)^2-(r-t)^2}=\frac{(rt+\Delta su)(rt-\Delta su-4)}{2(rt-\Delta su-4)}=\frac{rt+\Delta su}{2},$$

and now it follows as before that the x-coordinate of $P+Q$ is integral. □

These addition formulas also show that we have a group law over any ring in which 2 is a unit or a prime, such as $\mathbb{F}_q$ for odd prime powers q, the ring $\mathbb{Z}_p$ of p-adic integers and its quotient field $\mathbb{Q}_p$, or the rings $\mathbb{Z}_S$ of S-integers.

The group law on Pell conics has a well known algebraic interpretation: consider the maximal order $\mathcal{O}_K=\mathbb{Z}[\frac{1}{2}(\Delta+\sqrt{\Delta})]$ of the quadratic number field K with discriminant Δ; sending $(x,y)\in\mathcal{C}(\mathbb{Z})$ to the unit $\frac{1}{2}(x+y\sqrt{d})\in\mathcal{O}_K^\times$ induces a bijection $\phi:\mathcal{C}(\mathbb{Z})\longrightarrow\mathcal{O}_K^\times$.

Corollary 1.3. *The map ϕ defined above is an isomorphism of groups.*

Proof. Since ϕ is bijective, it is sufficient to show that it is a homomorphism; but this is clear from

$$\Big(\frac{r+s\sqrt{\Delta}}{2}\Big)\Big(\frac{t+u\sqrt{\Delta}}{2}\Big)=\frac{1}{2}\Big(\frac{rt+\Delta su}{2}+\frac{ru+st}{2}\sqrt{\Delta}\Big)$$

and Proposition 1.2. □

2. History of Group Laws

Describing the history of group laws, whether on elliptic curves or on conics, is a difficult task for various reasons: first, because the concept of abstract groups developed very slowly; in fact, the axioms for abstract groups did not become common knowledge until the 1890s. The second reason is that the group laws were first discovered in a complex environment: the fact that the points on the unit circle S^1 form a group had been known implicitly since Gauss identified S^1 with the set of complex numbers with absolute value 1; these form a group with respect to multiplication, as is evident from the relation $e^{is}e^{it} = e^{i(s+t)}$ known to Euler. But who first realized that the set of *rational* points on S^1 also form a group?

It is somewhat surprising that the algebraic group structure on the unit circle $\mathcal{C}$ was first defined not over $\mathbb{Q}$ but over the finite rings $R = \mathbb{Z}/n\mathbb{Z}$: Schönemann [Sch1839] showed that the set $\mathcal{C}(\mathbb{Z}/n\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/n\mathbb{Z} : x^2 + y^2 \equiv 1 \bmod n\}$ is closed with respect to the addition $(x, y) + (x', y') = (xx' - yy', xy' + x'y)$. He also showed that $\#\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) = p - (\frac{-1}{p})$ annihilates the group $\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$. Schönemann's language was algebraic; the geometric definition of a group law on conics was given by Juel [Jue1896, p. 101][1] who stated it only for circles and hyperbolas. In a review for the Fortschritte der Mathematik, Stäckel [Sta1896] writes about Juel's parametrization of conics (see Figure 2):

> [Die Parameterdarstellung] beruht auf einer eigentümlichen Art geometrischer Addition, die sich übrigens unter anderem Namen schon bei v. Staudt findet. Ist nämlich E ein fester Curvenpunkt, so stehen die drei Curvenpunkte A, B, C in der Beziehung $A+B = C$, wenn die Geraden AB und EC sich auf einer festen Geraden OU schneiden.[2]

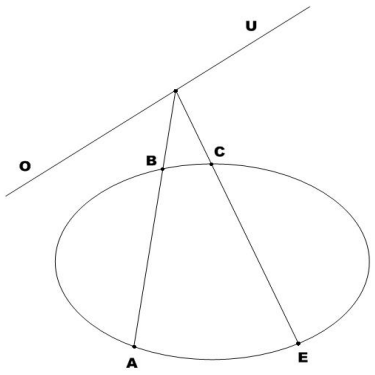

Figure 2. Addition Law on Conics

By taking OU to be the line at infinity we recover the geometric group law defined above.

[1] This paper also contains the first explicit statement of the group law on elliptic curves.

[2] [The parametrization] is based on a remarkable way of geometric addition, which can be found in a different guise already in the work of v. Staudt. In fact, if E is some fixed point on the curve, then the three points A, B, C on the curve satisfy $A + B = C$ if and only if the lines AB and EC intersect on some fixed line OU.

Veblen & Young [VY1910] gave a simplified account of von Staudt's theory of throws, describing the geometric group law on affine lines and on certain conics.

The article [Nie1908] by Niewenglowski (mentioned by Dickson [Dic1920, vol II, p. 396]) also contained a hint at the geometric group law on conics. Niewenglowski considers the hyperbola $x^2 - ay^2 = 1$ and writes

> Soient $A(1,0)$ le sommet, $A_1(x_1, y_1)$ le premier point entier à coordonnées positives; la parallèle menée par A à la tangente an A_1 donnera le point $A_2(x_2, y_2)$; la corde A_1A_3 sera parallèle à la tangente en A_2, etc., et l'on obtiendra ainsi tous les points à coordonnées entières et positives.[3]

The fact that certain arithmetic techniques concerning curves of genus 1 admit a geometric interpretation became common knowledge at the end of the 19th century through the work of Lucas and Sylvester (see Schappacher [Sch1990]). The algebraic geometer E. Turrière [Tur1915] became interested in number theoretic problems in 1915, when he discussed Fibonacci's question whether 5 is a congruent number using the hyperbolas $y^2 - x^2 = a$ and $z^2 - x^2 = b$, as well as the cubic $uv(u - v) = av - bu$. In a series of articles [Tur1916, Tur1917, Tur1918] he then put forward his 'arithmogeometry', a geometric investigation of rational points on algebraic curves. His plead for a new 'arithmetic geometry' seems to have fallen on deaf ears; I am not aware of a single reference to these articles.

Now consider Pythagorean triples (a, b, c), that is, integral solutions of $a^2 + b^2 = c^2$. We call (a, b, c) primitive if $\gcd(a, b) = 1$; every Pythagorean triple can be written in the form $(\lambda a, \lambda b, \lambda c)$ for some nonzero integer λ and a primitive triple (a, b, c), and Pythagorean triples that are multiples of the same primitive triple are called equivalent.

Idenitfying the equivalence class of the Pythagorean triple (a, b, c) with the rational point $(\frac{a}{c}, \frac{b}{c})$ on the unit circle gives a group structure to equivalence classes of Pythagorean triples. Olga Taussky [Tau1970] also identified the triples (a, b, c), $(-a, b, c)$, $(-b, -a, c)$ and $(a, -b, c)$ coming from multiplication by i on S^1; thus Taussky's group of Pythagorean triples is isomorphic to $\mathcal{C}(\mathbb{Q})/\mathcal{C}(\mathbb{Q})_{\text{tors}}$, where $\mathcal{C}(\mathbb{Q})_{\text{tors}} = \langle(0, 1)\rangle$ is the torsion group of $\mathcal{C}(\mathbb{Q})$. Eckert [Eck1984] proved that this group is free abelian, and in fact is a direct sum of infinitely many copies of $\mathbb{Z}$, one for each prime $p \equiv 1 \bmod 4$. This was rediscovered by Tan [Tan1996], who worked with the group $\mathcal{C}(\mathbb{Q})$ instead. Shastri [Sha2001] determined the group of integral points on the unit circle over number fields.

Other articles dealing with group (or ring) structures on the set of Pythagorean triples are Baldisserri [Bal1999], Beauregard & Suryanarayan [BS1996, BS1997, BS1999], Dawson [Daw1994], Grytczuk [Gry1997], Hlawka [Hla2000], Wojtowicz [Woi2001], and Zanardo & Zannier [ZZ1991], whereas Mariani [Mar1962] and Morita [Mor1986] study groups acting on Pythagorean triples.

In the modern mathematical literature, the group law on conics is hardly ever discussed; an exception is the book [PS1997] by Prasolov & Solovyev, or the web site

`http://www-cabri.imag.fr/abracadabri/Algebre/Groupes/FoliumD.html`,

[3]Let $A(1,0)$ be the vertex, $A_1(x_1, y_1)$ the first integral point with positive coordinates; the parallel through A to the tangent at A_1 will give the point $A_2(x_2, y_2)$; the secant A_1A_3 will be parallel to the tangent at A_2, etc., and in this way we obtain all the integral points with positive coordinates.

which contains a detailed exposition of the group law on conics.

3. The First 2-Descent

The conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$ comes attached with an isomorphism

$$\psi : \mathcal{C}(\mathbb{Q}) \longrightarrow K^\times[N] : (x,y) \longmapsto \frac{x + y\sqrt{\Delta}}{2}$$

from the group of rational points on $\mathcal{C}$ to the elements of norm 1 in $K^\times$, where $K = \mathbb{Q}(\sqrt{\Delta}\,)$ is the quadratic number field with discriminant Δ. We know that ψ restricts to an isomorphism $\mathcal{C}(\mathbb{Z}) \longrightarrow \mathcal{O}_K^\times$.

3.1. **The Set of First Descendants.** Now consider any integral point $(x,y) \in \mathcal{C}(\mathbb{Q})$ on the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$. Write $\Delta y^2 = x^2 - 4 = (x-2)(x+2)$. Since $\gcd(x+2, x-2) \mid 4$, there are three possible cases:

(1) $x \equiv 1 \bmod 2$: then $\Delta \equiv 5 \bmod 8$, $\gcd(x-2, x+2) = 1$, hence $x + 2 = ar^2$ and $x - 2 = bs^2$, where $ab = \Delta$. Thus $ar^2 - bs^2 = 4$.
(2) $x \equiv 2 \bmod 4$: then we find $\gcd(x-2, x+2) = 4$, hence $x + 2 = ar^2$, $x - 2 = bs^2$, and again $ar^2 - bs^2 = 4$.
(3) $x \equiv 0 \bmod 4$: then $\Delta = 4d$ with $d \equiv 3 \bmod 4$ and $\gcd(x-2, x+2) = 2$, so $x + 2 = 2Ar^2$, $x - 2 = 2Bs^2$ with $ab = d$, hence $ar^2 - bs^2 = 4$ for $a = 2A$, $b = 2B$ and $ab = \Delta$.

The curves $\mathcal{T}_a : ar^2 - bs^2 = 4$ are called the first descendants of $X^2 - \Delta Y^2 = 4$. Every integral point on $\mathcal{C}$ comes from an integral point on one of the descendants.

If $\Delta < 0$, then $x^2 + |\Delta| y^2 = 4$ implies that $x^2 \le 4$, which in turn shows that $x + 2 > 0$ unless $x = -2$. Thus the descendants all have the form $\mathcal{T}_a$ for positive integers a.

If $\Delta > 0$, then $x \ge 2$ or $x \le -2$. The points with $x > 0$ come from descendants $\mathcal{T}_a : ar^2 - bs^2 = 4$ with $a > 0$. If (x,y) is such a point, then the points $(-x, \pm y)$ will come from the descendant $\mathcal{T}_{-\Delta/a} : -br^2 + as^2 = 4$ (or, if $4 \mid \Delta$, from $\mathcal{T}_{-\Delta/4b}$) describing the same curve (up to a change of variables) as $\mathcal{T}_a$. It is therefore sufficient to consider descendants $\mathcal{T}_a$ for $a > 0$ squarefree.

Theorem 3.1. *Every integral solution (x,y) of the Pell equation $X^2 - \Delta Y^2 = 4$ gives rise to an integral solution of one of the equations $\mathcal{T}_a : ar^2 - bs^2 = 4$, where a and b are integers such that $ab = \Delta$, and where a is squarefree.*

Conversely, any integral solution (r,s) of $\mathcal{T}_a$ gives rise to an integral solution (x,y) of the Pell equation, where $x = ar^2 - 2$ and $y = rs$.

Remark 1. If $\Delta = 4d$ with $d \equiv 3 \bmod 4$, the descendants $\mathcal{T}_{2a} : 2ar^2 - 2bs^2 = 4$ with $4ab = \Delta$ coincide with the curves $ar^2 - bs^2 = 2$ occurring in the theory of Legendre (see [Lem2003b, Section 2]).

Remark 2. Assume that $ar^2 - bs^2 = 4$, where $ab = \Delta$. If $s = 1$ is a solution, then $b = ar^2 - 4$, hence $\Delta = ab = a(ar^2 - 4) = a^2r^2 - 4a$. A solution $s = 2$ implies that $r = 2m$ and leads to $\Delta = a^2m^2 - a$. Similarly, solutions $r = 1, 2$ leads to values of Δ that are of Richaud-Degert type $\Delta = n^2 + r$ with $r \mid 4n$.

Example. Consider $\mathcal{C}(\mathbb{Z})$ for $\mathcal{C} : x^2 - 205y^2 = 4$. The associated descendants with an integral point (r, s) and the corresponding point (x, y) on $\mathcal{C}$ are given below:

a	$\mathcal{T}_a(\mathcal{C})$	(r, s)	(x, y)
1	$r^2 - 205s^2 = 4$	$(2, 0)$	$(2, 0)$
5	$5r^2 - 41s^2 = 4$	$(3, 1)$	$(43, 3)$
41	$41r^2 - 5s^2 = 4$	$(\frac{1}{3}, \frac{1}{3})$	$(\frac{23}{9}, \frac{1}{9})$
205	$205r^2 - s^2 = 4$	$(\frac{2}{3}, \frac{28}{3})$	$(\frac{802}{9}, \frac{56}{9})$

The existence of integral points on the last two descendants cannot be excluded via congruences alone; this is a case where a second 2-descent would help.

3.2. **The Group Structure.** The number of descendants we have to consider is always a power of 2, as is the number of descendants with an integral point. This could be explained by giving this set of descendants the structure of an elementary abelian 2-group. How can we accomplish this?

1. The Naive Construction. The naive idea is to make the first descendants into an elementary abelian group by defining $\mathcal{T}_a \cdot \mathcal{T}_b = \mathcal{T}_c$, where $ab = cm^2$ for integers c, m with c squarefree. This is easily seen to coincide with the group structure defined by Dickson [Dic1930, §25] (see also [Lem2003b]).

2. Using the Group Structure on the Pell conic. The set of descendants with a rational point can be given a group structure as follows: given $(r, s) \in \mathcal{T}_a(\mathbb{Q})$ and $(t, u) \in \mathcal{T}_b(\mathbb{Q})$, compute the corresponding rational points (x, y) and (z, w) on the Pell conic; the sum $(x, y) + (v, w)$ on $\mathcal{C}(\mathbb{Q})$ will then come from a rational point on some descendant $\mathcal{T}_c$, and we put $\mathcal{T}_a \oplus \mathcal{T}_b = \mathcal{T}_c$.

In order to decide whether these group laws coincide (on the subset of descendants with a rational point) or not, we need a better way of finding the descendant $\mathcal{T}_a$ to which an $(x, y) \in \mathcal{C}(\mathbb{Q})$ gives rise. Observe that since $x = ar^2 - 2$, we can recover a by mapping $(x, y) \in \mathcal{C}(\mathbb{Z})$ to the coset $(x + 2)\mathbb{Q}^{\times 2} = a\mathbb{Q}^{\times 2}$. Actually, we get a mapping $\alpha : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ by putting $\alpha(x, y) = (x + 2)\mathbb{Q}^{\times 2}$ for all $(x, y) \neq (-2, 0)$; using the equation $x^2 - 4 = \Delta y^2$, we see that we have $(x + 2)\mathbb{Q}^{\times 2} = (x - 2)\Delta\mathbb{Q}^{\times 2}$ whenever both sides are defined, and this suggests we define $\alpha(-2, 0) = -\Delta\mathbb{Q}^{\times 2}$.

Proposition 3.2. *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* $\mathcal{T}_a(\mathcal{C})$*, where* a *is a positive squarefree integer determined by* $\alpha(P) = a\mathbb{Q}^{\times 2}$.

3.3. **The Weil Homomorphism.** The map $\alpha : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is a map between two abelian groups; is it a homomorphism? Before we show that the answer is yes, we will give another way to motivate the definition of α.

Consider the Pell conic $X^2 - \Delta Y^2 = 4$. We want to define a 'Weil homomorphism' $\alpha : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ with kernel $\ker\alpha = 2\mathcal{C}(\mathbb{Q})$. Since $2(r, s) = (r^2 - 2, rs)$, we could try to map (x, y) to the coset $(x + 2)\mathbb{Q}^{\times 2}$; this defines a map annihilating $2\mathcal{C}(\mathbb{Q})$, but is not defined for $P = (-2, 0)$. On the other hand, we also have

$2(x,y) = (2+\Delta y^2, xy)$; the map $(x,y) \longmapsto \Delta(x-2)\mathbb{Q}^{\times 2}$ is defined except for $(x,y) = (2,0)$, and it agrees with the map defined before for all points $\neq (\pm 2, 0)$.

Now we claim

Theorem 3.3. *The map $\alpha : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is a group homomorphism.*

This will be proved using Galois cohomology below. Before we do this, let us derive a few consequences.

Corollary 3.4. *The group laws defined on the set of first descendants coincide.*

Proof. Assume that the points P and Q on $\mathcal{C}(\mathbb{Q})$ give rise to points on the descendants $\mathcal{T}_a$ and $\mathcal{T}_b$; then $\alpha(P) = a\mathbb{Q}^{\times 2}$, $\alpha(Q) = b\mathbb{Q}^{\times 2}$, and since α is a group homomorphism, $\alpha(P+Q) = ab\mathbb{Q}^{\times 2}$, hence $P+Q$ gives rise to a point on the descendant $\mathcal{T}_c$ with $ab = cm^2$ and c squarefree. □

Proposition 3.5. *The image of $\alpha : \mathcal{C}(\mathbb{Z}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ consists of all square classes $a\mathbb{Q}^{\times 2}$ for which $ab = \Delta$ for $a, b \in \mathbb{Z}$ and $ar^2 - bs^2 = 4$ has an integral solution.*

Proof. If $a\mathbb{Q}^{\times 2} \in \operatorname{im}\alpha$, then there is a $P = (x,y) \in \mathcal{C}(\mathbb{Z})$ such that $\alpha(P) = a\mathbb{Q}^{\times 2}$, and by our construction above the point P comes from an integral point on $ar^2 - bs^2 = 4$. Conversely, if $ar^2 - bs^2 = 4$ has an integral solution, then it gives rise to the integral point $P = (ar^2 - 2, rs)$ on the associated Pell conic, and $\alpha(P) = (x+2)\mathbb{Q}^{\times 2} = a\mathbb{Q}^{\times 2}$. □

This shows

Corollary 3.6. *The image of $\alpha : \mathcal{C}(\mathbb{Z}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is finite.*

Proof. This follows at once from the observation that there are only finitely many classes $a\mathbb{Q}^{\times 2}$ with $ab = \Delta$ and $a, b \in \mathbb{Z}$. □

Now we claim

Theorem 3.7. *We have an exact sequence*

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

Proof. We claim that the kernel of the homomorphism $\alpha : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is $\ker\alpha = 2\mathcal{C}(\mathbb{Q})$. Moreover, the kernel of the induced map $\mathcal{C}(\mathbb{Z}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is $2\mathcal{C}(\mathbb{Z})$.

One direction is clear: if $(x,y) = 2(r,s)$ for some $(r,s) \in \mathcal{C}(\mathbb{Q})$, then $x = r^2 - 2$, hence $x + 2 = r^2$ is a square, and this means that $(x,y) \in \ker\alpha$.

For the converse, observe that $(x,y) \in \ker\alpha$ if and only if $x + 2 = r^2$ for some $r \in \mathbb{Q}$. Next, $\Delta y^2 = x^2 - 4 = (x-2)(x+2)$, hence $\Delta y^2 = (x-2)r^2$, and thus $x - 2 = \Delta s^2$ for some $s \in \mathbb{Q}$. On the other hand, $x - 2 = x + 2 - 4 = r^2 - 4$, hence $r^2 - \Delta s^2 = 4$. Thus $(r,s) \in \mathcal{C}(\mathbb{Q})$, and it is easily checked that $2(r,s) = (x,y)$.

Now consider the restriction of α to $\mathcal{C}(\mathbb{Z})$. If $x \in \mathbb{Z}$ in the above proof, then clearly $r \in \mathbb{Z}$, and $r^2 - \Delta s^2 = 4$ then implies that we also have $s \in \mathbb{Z}$ if $(x,y) \in \mathcal{C}(\mathbb{Z})$. □

This immediately implies

Corollary 3.8 (Weak Theorem of Mordell-Weil)**.** *The group $\mathcal{C}(\mathbb{Z})/2\mathcal{C}(\mathbb{Z})$ is finite.*

In the next section, we will use the theory of heights to prove that $\mathcal{C}(\mathbb{Z})$ is finitely generated. This implies that $\mathcal{C}(\mathbb{Z}) \simeq \mathcal{C}(\mathbb{Z})_{\mathrm{tors}} \oplus \mathbb{Z}^r$ for some $r \geq 0$, and the fact that the torsion group $\mathcal{C}(\mathbb{Q})_{\mathrm{tors}}$ is cyclic shows that $\mathcal{C}(\mathbb{Z})/2\mathcal{C}(\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^{r+1}$. This is the analog of Tate's formula for the 2-rank of an elliptic curve with rational 2-torsion:

Proposition 3.9. *We have $\mathcal{C}(\mathbb{Z}) \simeq \mathcal{C}(\mathbb{Z})_{\mathrm{tors}} \oplus \mathbb{Z}^r$, where $r \geq 0$ is determined by $\operatorname{im}\alpha = 2^{r+1}$.*

This also implies

Theorem 3.10. *Consider the Weil map $\alpha > \mathcal{C}(\mathbb{Z}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ for the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$, where $\Delta > 0$. The following assertions are equivalent:*

1. *$\mathcal{C}(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$;*
2. *$\#\operatorname{im}\alpha = 4$.*

The implication (1) $\Longrightarrow$ (2) of Theorem 3.10 is a modern formulation of Dirichlet's Theorem [Lem2003b, Thm. 3.3.].

Proof of Theorem 3.3. Let $\mathcal{C} : X^2 - dY^2 = 4$ denote the Pell conic, and $[2] : \mathcal{C}(K) \longrightarrow \mathcal{C}(K)$ multiplication by 2.

Proposition 3.11. *We have an exact sequence*

$$0 \longrightarrow \mathcal{C}(\overline{\mathbb{Q}})[2] \longrightarrow \mathcal{C}(\overline{\mathbb{Q}}) \xrightarrow{[2]} \mathcal{C}(\overline{\mathbb{Q}}) \longrightarrow 0, \tag{2}$$

where $\mathcal{C}(\overline{\mathbb{Q}})[2] = \{(-2,0),(2,0)\} = \mathcal{C}(\mathbb{Q})[2]$.

Proof. Let us first prove that [2] is surjective. Given $(r,s) \in \mathcal{C}(\overline{\mathbb{Q}})$, we find that $2(x,y) = (r,s)$ implies $r = x^2 - 2$ and $s = xy$. Thus $x^2 = r + 2$, and either $y = 0$ (if $r = -2$) or $y = \frac{s}{x}$. In either case, $(x,y) \in \mathcal{C}(\overline{\mathbb{Q}})$ satisfies $2(x,y) = (r,s)$.

The same formulas show that $\ker[2] = \{(\pm 2, 0)\}$: in fact, if $(r,s) = (2,0)$, then $x^2 = r + 2 = 4$ implies $x = \pm 2$ and $y = 0$. □

Now let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote the absolute Galois group of $\mathbb{Q}$. Since $\mathcal{C}(\overline{\mathbb{Q}})[2]$ consists of rational points, we have $\mathcal{C}(\overline{\mathbb{Q}})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ as Galois modules, and the long exact cohomology sequence gives

$$\mathcal{C}(\mathbb{Q}) \xrightarrow{[2]} \mathcal{C}(\mathbb{Q}) \longrightarrow \mathrm{H}^1(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathrm{H}^1(\mathcal{C}) \xrightarrow{[2]} \mathrm{H}^1(\mathcal{C}), \tag{3}$$

where $\mathrm{H}^1(A) = \mathrm{H}^1(G, A)$ and $\mathcal{C} = \mathcal{C}(\overline{K})$.

Next we compute $\mathrm{H}^1(\mathbb{Z}/2\mathbb{Z})$; we start with the Kummer sequence

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \overline{\mathbb{Q}}^\times \xrightarrow{[2]} \overline{\mathbb{Q}}^\times \longrightarrow 1$$

Taking Galois cohomology and using Hilbert's Theorem 90 we find

$$\mathbb{Q}^\times \xrightarrow{[2]} \mathbb{Q}^\times \longrightarrow \mathrm{H}^1(G, \mathbb{Z}/2\mathbb{Z}) \longrightarrow 1.$$

Thus $\mathbb{Q}^\times/\mathbb{Q}^{\times\,2} \simeq \mathrm{H}^1(G, \mathbb{Z}/2\mathbb{Z})$, and (3) gives rise to an exact sequence

$$\mathcal{C}(\mathbb{Q}) \xrightarrow{[2]} \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}.$$

It remains to identify the last map.

To this end, recall the construction of H^1: given an exact sequence of G-modules

$$0 \longrightarrow A \longrightarrow B \xrightarrow{f} C \longrightarrow 0,$$

we get a homomorphism $C^G \longrightarrow \mathrm{H}^1(G,A)$ as follows: for $c \in C^G$, pick a $b \in B$ such that $f(b) = c$ and then define the cocycle x by $x(\sigma) = \sigma(b) - b$; the image of c is then the equivalence class of x.

This provides us with the isomorphism $\mathbb{Q}^\times/\mathbb{Q}^{\times\,2} \simeq \mathrm{H}^1(G,\mathbb{Z}/2\mathbb{Z})$: given a coset $a\mathbb{Q}^{\times\,2}$, pick a preimage $\sqrt{a} \in \overline{\mathbb{Q}}$, and then define the cocycle $x : G \longrightarrow \mathbb{Z}/2\mathbb{Z}$ by $x(\sigma) = \sigma(\sqrt{\alpha})/\sqrt{\alpha}$.

Next we study the connecting homomorphism $\delta : \mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}) \longrightarrow \mathrm{H}^1(\mathbb{Z}/2\mathbb{Z})$. Let $P = (r,s) \in \mathcal{C}(\mathbb{Q})$. The points $Q = (x,y) \in \mathcal{C}(\overline{\mathbb{Q}})$ such that $2Q = P$ are given by

$$Q = \begin{cases} (\sqrt{r+2}), s/\sqrt{r+2})\,) & \text{if } r \ne -2, \\ (0, 2/\sqrt{-\Delta}\,) & \text{if } r = -2. \end{cases}$$

Via the homomorphism $\mathrm{H}^1(\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$, the cocycle corresponding to Q is identified with the coset

$$\delta(P) = \begin{cases} (r+2)\mathbb{Q}^{\times\,2} & \text{if } r \ne -2, \\ -\Delta\mathbb{Q}^{\times\,2} & \text{if } r = -2. \end{cases}$$

Thus δ can be identified with the Weil map $\alpha : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$, and in particular α is a group homomorphism with kernel $2\mathcal{C}(\mathbb{Q})$.

4. Heights

For proving that $\mathcal{C}(\mathbb{Z})$ is finitely generated, we need more than just the fact that $\mathcal{C}(\mathbb{Z})/2\mathcal{C}(\mathbb{Z})$ is finite. This missing piece of information will be provided by the theory of heights.

4.1. **The Naive Height.** For rational numbers $x = \frac{r}{s}$ in lowest terms, we define

$$H(x) = \max\{|r|, |s|\};$$

note that $H(0) = 1$ and $H(x) \ge 1$ for all $x \in \mathbb{Q}$. The following lemma is easy to prove:

Lemma 4.1. *For $x, y \in \mathbb{Q}$ we have*

(1) $H(xy) \le H(x)H(y)$;
(2) $H(x^2) = H(x)^2$;
(3) $\frac{1}{2H(y)}Hx) \le H(x+y) \le 2H(x)H(y)$;
(4) *for any $c > 0$, the set of all $x \in \mathbb{Q}$ with height $H(x) < c$ is finite.*

The lower bound in (3) follows from the upper bound upon replacing x by $x+y$ and y by $-y$.

Our next goal is the definition of the 'naive height' $H(P)$ of rational points P on Pell conics. For rational points $P = (x,y) \in \mathcal{C}(\mathbb{Q})$ on a conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$ put $H(P) = H(x)$. We clearly have

Proposition 4.2. *Let $\mathcal{C} : X^2 - \Delta Y^2 = 4$ be a Pell conic. For a given constant $c > 0$, the set of all rational points $P \in \mathcal{C}(\mathbb{Q})$ with height $H(P) < c$ is finite.*

These rational points have a special form:

Lemma 4.3. *Let $(x,y) \in \mathcal{C}(\mathbb{Q})$ be a rational point on the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$. Then there exist integers r, s, n such that $x = \frac{r}{n}$, $y = \frac{s}{n}$ and* $\gcd(r,n) = \gcd(s,n) = 1$.

Proof. Write $x = \frac{r}{n}$, $y = \frac{s}{m}$ with $r, s \in \mathbb{Z}$, $m, n \in \mathbb{N}$ and $\gcd(r, n) = \gcd(s, m) = 1$. Then $r^2m^2 - \Delta s^2 n^2 = 4m^2n^2$ shows that $n^2 \mid r^2m^2$, and since $\gcd(r, n) = 1$, we find $n^2 \mid m^2$ and $n \mid m$.

Thus $m = kn$ for some integer k. This gives $r^2k^2 - \Delta s^2 = 4k^2n^2$, hence $k^2 \mid \Delta s^2$; since $k \mid m$ and $\gcd(s, m) = 1$ we conclude that $k^2 \mid \Delta$, which implies that $k = 1$ if $\Delta \equiv 1 \bmod 4$ and $k \mid 2$ if $\Delta \equiv 0 \bmod 4$. In the latter case, $4k^2 \mid \Delta$ implies $4k^2 \mid r^2k^2$, hence $2 \mid r$; but this implies $k^2 \mid d$ and thus $k = 1$ as claimed. □

We also need some information on the height of the Y-coordinates.

Lemma 4.4. *Let $(x, y) \in \mathcal{C}(\mathbb{Q})$ with $y = \frac{s}{n}$; then $|\Delta| s^2 \leq 4H(P)^2$.*

Proof. We have $|\Delta| s^2 \leq \max\{r^2, 4n^2\} \leq 4H(P)^2$. □

Now we claim

Proposition 4.5. *Let $Q \in \mathcal{C}(\mathbb{Q})$ be fixed. Then for all $P \in \mathcal{C}(\mathbb{Q})$ we have*

(1) $\frac{1}{4}H(P)^2 \leq H(2P) \leq 4H(P)^2$;

(2) $\frac{1}{c}H(P) \leq H(P + Q) \leq cH(P)$ *for* $c = 5H(Q)$.

Proof. For $P = (x, y)$ we have $2P = (x^2 - 2, xy)$, hence $H(2P) = H(x^2 - 2)$. Lemma 4.1.(3) applied with $y = 2$ now proves the first claim. For the proof of the second claim let $P = (x, y)$, $Q = (z, w)$ with $x = \frac{r}{m}$, $y = \frac{s}{m}$, $z = \frac{t}{n}$, $w = \frac{u}{n}$, and $\gcd(r, m) = \gcd(t, n) = 1$. Then $P + Q = (\frac{xz+yw\Delta}{2}, \frac{xw+yz}{2}) = (\frac{rt+su\Delta}{2mn}, \frac{ru+st}{2mn})$.

Clearly $2|mn| \leq 2H(P)H(Q)$; thus it is sufficient to bound the numerator. Here we find

$$\begin{aligned} H(P + Q) &\leq |r| \cdot |t| + |s|\sqrt{\Delta} \cdot |u|\sqrt{\Delta} \\ &\leq H(P)H(Q) + 4H(P)H(Q) = 5H(P)H(Q). \end{aligned}$$

Replacing Q by $-Q$ shows that $H(P - Q) \leq 5H(P)H(Q)$. Applying this result to $P + Q$ instead of P shows that $H(P) \leq 5H(P + Q)H(Q)$, and this finally shows that $H(P + Q) \geq \frac{1}{5}H(P)$. □

4.2. **The Canonical Height.** The (naive) logarithmic height of a rational point $P \in \mathcal{C}(\mathbb{Q})$ is defined by $h_0(P) = \log H(P)$. Recall that

- $|h_0(2P) - 2h_0(P)| < \log 4$ for all $P \in \mathcal{C}(\mathbb{Q})$;
- given $Q \in \mathcal{C}(\mathbb{Q})$, put $c = h_0(Q) + \log 5$; then $h_0(P + Q) \leq h_0(P) + c$ for every $P \in \mathcal{C}(\mathbb{Q})$.

Now let us define a function $h : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ by putting

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

In order to see that this definition makes sense we have to check that the sequence $\{2^{-n} h_0(2^n P)\}$ is Cauchy.

We know that $|h_0(2Q) - 2h_0(Q)| \le \log 4$; then $n > m \ge 0$ implies

$$\begin{aligned}|2^{-n}h_0(2^nP) - 2^{-m}h_0(2^mP)| &= \Big|\sum_{j=m}^{n-1}(2^{-j-1}h_0(2^{j+1}P) - 2^{-j}h_0(2^jP))\Big| \\ &\le \sum_{j=m}^{n-1} 2^{-j-1}|h_0(2^{j+1}P) - 2h_0(2^jP)| \\ &\le \sum_{j=m}^{n-1} 2^{-j-1}\log 4 < 2^{-m}\log 4.\end{aligned}$$

Since this expression can be made arbitrarily small by choosing m sufficiently large, the sequence is Cauchy, and $h(P)$ is defined. Taking $m = 0$ in the inequality above and letting $n \longrightarrow \infty$ proves

Proposition 4.6. *For all $P \in \mathcal{C}(\mathbb{Q})$, we have $|h(P) - h_0(P)| \le \log 4$.*

This immediately implies

Proposition 4.7. *Let $\mathcal{C} : X^2 - \Delta Y^2 = 4$ be a Pell conic. For a given constant $c > 0$, the set of all rational points $P \in \mathcal{C}(\mathbb{Q})$ with canonical height $h(P) < c$ is finite.*

Now we can easily derive the basic properties of the canonical height:

Theorem 4.8. *The canonical height $h : \mathcal{C}(\mathbb{Q}) \longrightarrow \mathbb{R}_{\ge 0}$ on the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$ has the following properties:*

1. *$h(T) = 0$ if and only if $T \in \mathcal{C}(\mathbb{Q})_{\rm tors}$;*
2. *$h(2P) = 2h(P)$;*
3. *$h(P + Q) \le h(P) + h(Q)$;*
4. *$h(P) + h(Q) \le h(P - Q) + h(P + Q) \le 2h(P) + 2h(Q)$;*
5. *the square of the canonical height satisfies the parallelogram equality*

$$h(P - Q)^2 + h(P + Q)^2 = 2h(P)^2 + 2h(Q)^2$$

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

Proof. (1) If T is a torsion point, then $h_0(T^k)$ attains only finitely many values, hence is bounded; this implies that $h(T) = 0$.

Now assume that $h(T) = 0$. Then $h(kT) = k \cdot h(T)$ for all $k \ge 1$. Since $|h(P) - h_0(P)|$ is bounded, the naive heights of the points kT are bounded. But there are only finitely many points with bounded height, hence $\{kT : k \in \mathbb{N}\}$ is finite, and this implies that T is a torsion point.

(2) Directly from the definition we get

$$h(2P) = \lim_{n\to\infty} \frac{h_0(2^{n+1}P)}{2^n} = 2\lim_{n\to\infty} \frac{h_0(2^{n+1}P)}{2^{n+1}} = 2h(P).$$

(3) Now recall that $h_0(P + Q) \le h_0(P) + h_0(Q) + \log 2$; this implies

$$\begin{aligned}h(P + Q) &= \lim_{n\to\infty} \frac{h_0(2^n(P + Q))}{2^n} \\ &\le \lim_{n\to\infty} \Big(\frac{h_0(2^nP)}{2^n} + \frac{h_0(2^nQ)}{2^n} + \frac{\log 2}{2^n}\Big) \\ &= h(P) + h(Q).\end{aligned}$$

(4) Replacing Q by $-Q$ shows that $h(P-Q) \leq h(P)+h(Q)$, and adding these inequalities yields
$$h(P+Q)+h(P-Q) \leq 2h(P)+2h(Q).$$
Applying this inequality to $P-Q$ and $P+Q$ instead of P and Q yields
$$h(P)+h(Q) \leq h(P+Q)+h(P-Q),$$
where we have used $h(2P)=2h(P)$ and $h(2Q)=2h(Q)$.

(5) Let us return to $h(P+Q) \leq h(P)+h(Q)$; replacing P by $P-Q$ yields $h(P-Q) \geq h(P)-h(Q)$. Similarly, $h(P+Q) \geq h(P)-h(Q)$. Squaring and adding yields $h(P+Q)^2+h(P-Q)^2 \geq 2h(P)^2+2h(Q)^2$.

Replacing P and Q by $P+Q$ and $P-Q$ shows $4h(P)^2+4h(Q)^2 = h(2P)^2+h(2Q)^2 \geq 2h(P+Q)^2+2h(P-Q)^2$, that is, $h(P+Q)^2+h(P-Q)^2 \leq 2h(P)^2+2h(Q)^2$.

These two inequalities imply the desired equality.

This concludes the proof. □

As a corollary we note:

Corollary 4.9. *We have $h(mP)=mh(P)$ for all $m \geq 1$.*

Proof. Put $P=mQ$ in the parallelogram equality. □

It is not hard to give explicit formulas for the canonical height of rational points on Pell conics:

Proposition 4.10. *The canonical height of $P=(x,y) \in \mathcal{C}(\mathbb{Q})$, where $\mathcal{C}$ is the Pell conic given by $X^2-\Delta Y^2=4$ with $\Delta>0$, is $h(P)=\log \frac{|r|+|s|\sqrt{\Delta}}{2}$, where $x=\frac{r}{n}$, $y=\frac{s}{n}$ with $(r,n)=(s,n)=1$.*

Proof. Observe that $2P=(\frac{r^2-2n^2}{n^2}, \frac{rs}{n})$ with $(r^2-2n^2, n^2)=1$, hence $H(2P)=r^2-2n^2$. Also note that $r^2-2n^2=n^2[(\frac{r+s\sqrt{\Delta}}{2n})^2+(\frac{r-s\sqrt{\Delta}}{2n})^2]$. By induction, we conclude that for $k=2^m$ and $r,s>0$ we have
$$\begin{aligned} h(P) &= \lim_{k\to\infty} \frac{h_0(kP)}{k} = \lim_{k\to\infty} \frac{1}{k} \log n^k \Big[\Big(\frac{r+s\sqrt{\Delta}}{2n} \Big)^k + \Big(\frac{r-s\sqrt{\Delta}}{2n} \Big)^k \Big] \\ &= \log n + \lim_{k\to\infty} \frac{1}{k} \log \Big(\frac{r+s\sqrt{\Delta}}{2n} \Big)^k = \frac{r+s\sqrt{\Delta}}{2}, \end{aligned}$$
where we have used that $-1 < \frac{r-s\sqrt{\Delta}}{n} < 1$. The other cases (e.g. $r>0$, $s<0$) are handled similarly. □

There is an even simpler formula if $\Delta<0$:

Proposition 4.11. *The canonical height of $P=(x,y) \in \mathcal{C}(\mathbb{Q})$, where $\mathcal{C}$ is the Pell conic given by $X^2-\Delta Y^2=4$ with $\Delta<0$, is $h(P)=\log n$, where $x=\frac{r}{n}$, $y=\frac{s}{n}$ with $n>0$ and $(r,n)=(s,n)=1$.*

Proof. We have $2^j P=(x_j,y_j)$, where (x_k) is the sequence defined recursively by $x_1=x$ and $x_{j+1}=x_j^2-2$. Clearly we have $|x_j|<2$ for all $j \geq 1$, so the sequence is bounded.

Assume that $|x_k|>1$ for some k; we claim that there is a $j>0$ such that $|x_{k+j}|<1$. If not, we may assume that $x_k>1$ (the case $x_k<-1$ is treated in an analogous way); then $|x_{k+1}|>1$ implies $x_{k+1}>1$. On the other hand, it is

easily seen that in this case $x_{k+1} < x_k$. Thus $1 < x_{k+j} > 1$ for all $j \ge 0$, hence the sequence converges, and we have $1 \le \lim x_j \le x_k < 2$; but the only possible limits are the roots of the equation $0 = x^2 - x - 2 = (x+1)(x-2)$, that is, $x = -1$ or $x = 2$: contradiction.

Thus there are infinitely many x_k with $|x_k| < 1$; if we write $x = \frac{r}{n}$ with $n > 0$, then $x_k = r'/n^k$, hence $H(2^k P) = H(x_k) = n^{2^k}$. We know that $\log 2^{-j} H(2^j P)$ converges to $h(P)$, hence so does the subsequence $2^{-k} \log H(x_k) = \log n$. □

Finally, let us look at the heights of points on descendants. If $P = (r,s)$ is a rational point on the descendant $\mathcal{T}_a : ar^2 - bs^2 = 4$ with $ab = \Delta > 0$ and $a > 0$, then $Q = (ar^2 - 2, rs) \in \mathcal{C}(\mathbb{Q})$, and now Lemma 4.1 implies

$$\frac{1}{4a} H(r)^2 \le \frac{1}{4} H(ar^2) \le H(Q) \le 4H(ar)^2 \le 4aH(r^2).$$

We have proved

Proposition 4.12. *If If $P = (r,s)$ is a rational point on the descendant $\mathcal{T}_a : ar^2 - bs^2 = 4$ with $ab = \Delta > 0$ and $a > 0$, then $Q = (ar^2 - 2, rs) \in \mathcal{C}(\mathbb{Q})$ satisfies*

$$\frac{1}{4a} H(P)^2 \le H(Q) \le 4aH(P)^2.$$

5. The Theorem of Mordell-Weil

The Theorem of Mordell-Weil states that the group of rational points on an elliptic curve defined over $\mathbb{Q}$ is finitely generated. Its analog for conics says that the group of integral points on a Pell conic is finitely generated (more generally it can be shown that the group of S-integral points on a Pell conic is finitely generated if S is finite).

5.1. **Mordell-Weil.** We now show that $\mathcal{C}(\mathbb{Z})$ is finitely generated. The following result is the abstract kernel of the proof:

Theorem 5.1. *Let G be an abelian group such that $G/2G$ is finite. Assume that there exists a function $h : G \longrightarrow \mathbb{R}_{\ge 0}$ with the following properties:*

1. *For every $c > 0$, the set $\{g \in G : h(g) < c\}$ is finite;*
2. *We have $h(2g) = 2h(g)$ for all $g \in G$;*
3. *$h(g - g')^2 + h(g + g')^2 = h(g)^2 + h(g')^2$ for all $g, g' \in G$.*

Then G is finitely generated.

Proof. Let Γ be a set of representatives of the finitely many cosets of $G/2G$. Then each $g \in G$ can be written as $g - \gamma = 2g'$ for some $\gamma \in \Gamma$ and a $g' \in G$. Put $c = \max\{h(\gamma) : \gamma \in \Gamma\}$.

Now let Ω denote the subgroup of G generqated by all the elements of Γ and the (finitely many) elements $g \in G$ with $h(g) \le c$. We claim that $G = \Omega$.

If not, then let g be an element in G with minimal height such that $g \notin \Omega$; observe that $h(g) > c$. We can write $g - \gamma = 2g'$ for some $\gamma \in \Gamma$ and $g' \in G$, and find

$$4h(g')^2 = h(g - \gamma)^2 = 2h(g)^2 + 2h(\gamma)^2 - h(g + \gamma)^2 \le 2h(g)^2 + 2c^2 < 4h(g)^2.$$

Thus $h(g') < h(g)$, hence $g' \in \Omega$. But then so is $g = 2g' + \gamma$: contradiction. □

Applying this to our situation we find

Corollary 5.2. *Let $\mathcal{C} : X^2 - \Delta Y^2 = 4$ be a Pell conic. Then the group $\mathcal{C}(\mathbb{Z})$ is finitely generated, that is, $\mathcal{C}(\mathbb{Z}) \simeq \mathcal{C}(\mathbb{Z})_{\mathrm{tors}} \oplus \mathbb{Z}^r$ for some finite group $\mathcal{C}(\mathbb{Z})_{\mathrm{tors}}$ and some integer $r \geq 0$ called the rank of $\mathcal{C}$. Moreover, $\operatorname{im}\alpha = 2^{r+1}$.*

The torsion group of $\mathcal{C}(\mathbb{Q})$ is easy to determine: torsion points (x, y) have integral coordinates, and we have $y = 0$ or $y = \pm 1$. In fact, if $k \geq 2$ is an integer and $P \neq N = (2, 0)$ a rational point on $\mathcal{C}$ with $kP = N$, then $\mathbb{Q}(\zeta_k) \subseteq \mathbb{Q}(\sqrt{\Delta}\,)$. Thus

$$\mathcal{C}(\mathbb{Q})_{\mathrm{tors}} = \begin{cases} \{(\pm 2, 0), (\pm 1, \pm 1)\} & \text{if } \Delta = -3, \\ \{(\pm 2, 0), (0, \pm 2)\} & \text{if } \Delta = -4, \\ \{(\pm 2, 0)\} & \text{otherwise} \end{cases}$$

6. Selmer and Tate-Shafarevich Groups

The subset of curves $\mathcal{T}(a) : ar^2 - bs^2 = 4$ with a rational point corresponds to a subgroup $\mathrm{Sel}_2(\mathcal{C})$ of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ called the 2-Selmer group of $\mathcal{C}$; we have already shown that if $\mathcal{T}_a$ and $\mathcal{T}_{a'}$ have a rational point, then so does $\mathcal{T}a''$, where $aa' = a''k^2$ for some positive and squarefree integer $a'' \mid \Delta$. The same argument shows that the curves $\mathcal{T}_a$ with an integral point form a group $W_2(\mathcal{C})$, which is clearly a subgroup of $\mathrm{Sel}_2(\mathcal{C})$ isomorphic to $\operatorname{im}\alpha$. The 2-part of the Tate-Shafarevich group $\mathbf{Ш}_2(\mathcal{C})$ is then defined by the exact sequence

$$1 \longrightarrow W_2(\mathcal{C}) \longrightarrow \mathrm{Sel}_2(\mathcal{C}) \longrightarrow \mathbf{Ш}_2(\mathcal{C}) \longrightarrow 1. \tag{4}$$

In this section, we shall study these groups.

6.1. The 2-Selmer Group.

Proposition 6.1. *The first descendant $\mathcal{T}(a) : ax^2 - by^2 = 4$, where $ab = \Delta$ and $a > 0$, has a rational point if and only if $(a/q) = (-b/p) = +1$ for all odd primes $p \mid a$ and $q \mid b$.*

Proof. Legendre's theorem states that the ternary quadratic form $ax^2 + by^2 + cz^2$, where $a, b, c \in \mathbb{Z}$ are coprime and squarefree, represents 0 over the integers if and only if it represents 0 over the reals and over the fields $\mathbb{Z}/p\mathbb{Z}$, where p runs through the odd primes dividing abc. □

Note that $ax^2 - by^2 = 4$ has rational solutions if and only if $X^2 = aY^2 + \Delta Z^2$ has integral solutions, hence the criteria in Proposition 6.1 are equivalent to $(\frac{a,\Delta}{p}) = +1$ for all odd primes $p \mid \Delta$; since $\Delta > 0$, the Hilbert symbol at ∞ is trivial; finally, $(\frac{a,\Delta}{p}) = +1$ for all odd primes $p \nmid \Delta$, and now the product formula implies that we have $(\frac{a,\Delta}{2}) = +1$ as well. This shows

Corollary 6.2. *The first descendant $\mathcal{T}(a) : ax^2 - by^2 = 4$, where $ab = \Delta$ and $a > 0$, has a rational point if and only if $(\frac{a,\Delta}{p}) = +1$ for all primes p.*

Example. Consider $\mathcal{C}(\mathbb{Z})$ for $\mathcal{C}: x^2-1045y^2=4$. The associated descendants with an integral point (r,s) and the corresponding point (x,y) on $\mathcal{C}$ are given below:

a	$\mathcal{T}_a(\mathcal{C})$	(r,s)	(x,y)
1	$r^2-1045s^2=4$	$(2,0)$	$(2,0)$
5	$5r^2-209s^2=4$	$(\frac{7}{3},\frac{1}{3})$	
11	$11r^2-95s^2=4$	$(3,1)$	$(97,3)$
19	$19r^2-55s^2=4$	$--$	
55	$55r^2-19s^2=4$	$(\frac{4}{7},\frac{6}{7})$	
95	$95r^2-11s^2=4$	$--$	
209	$209r^2-5s^2=4$	$--$	
1045	$1045r^2-s^2=4$	$--$	

Thus $\mathrm{Sel}_2(\mathcal{C})$, viewed as a subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, is isomorphic to $\langle 5,11\rangle$; moreover $W_2(\mathcal{C})=\langle 11\rangle$, and the nontrivial element of $\mathbf{Ш}(\mathcal{C})[2]\simeq\mathbb{Z}/2\mathbb{Z}$ is generated by $\mathcal{T}_5$.

6.2. **Rédei.** Recall from [Lem2003b] that a factorization of the discriminant $\Delta=\mathrm{disc}k$ into discriminants $\Delta=\Delta_1\Delta_2$ is called a splitting of the second kind if $(\Delta_1/p_2)=(\Delta_1/p_2)=+1$ for all primes $p_i\mid\Delta_i$.

Proposition 6.3. *Assume that Δ is a product of positive prime discriminants. Then the factorization $\Delta=\Delta_1\Delta_2$ is a splitting of the second kind if and only if the descendant $\Delta_1X^2-\Delta_2Y^2=4$ is everywhere locally solvable.*

Thus Rédei's group structure on splittings of the second kind induces a group structure on $\mathrm{Sel}_2(\mathcal{C})$ that coincides with ours. Since there are exactly e_4+1 independent splittings of the second kind (including the trivial factorization $\Delta=1\cdot\Delta$), this shows that Rédei's results imply that $\#\mathrm{Sel}_2(\mathcal{C})=2\#\mathrm{Cl}^+(k)^2/\mathrm{Cl}^+(k)^4$.

In general, however, the C_4-decompositions and the first descendants in the Selmer group are not related. Consider e.g. the example $d=12369=3\cdot7\cdot19\cdot31$; here the elements in the Selmer group and the corresponding rational points are given by

$$\begin{aligned}
r^2-12369s^2&=4 && (r,s)=(2,0)\\
7r^2-1767s^2&=4 && (r,s)=(\tfrac{32}{5},\tfrac{2}{5})\\
589r^2-21s^2&=4 && (r,s)=(\tfrac{1}{4},\tfrac{5}{4})\\
4123r^2-3s^2&=4 && (r,s)=(\tfrac{1}{32},\tfrac{3}{32})
\end{aligned}$$

The C_4-decompositions, on the other hand, are $\Delta=1\cdot12369$ and $\Delta=93\cdot133$, and the equation $93x^2+133y^2=z^2$ has the solution $(x,y,z)=(6,1,59)$.

6.3. **The 2-Part of the Tate-Shafarevich Group.** Consider the descendant $\mathcal{T}(a): ar^2-bs^2=4$; we know that $\mathcal{T}(a)\in\mathrm{Sel}_2(\mathcal{C})$ if and only if $(\frac{a,d}{p})=+1$ for all places p (observe that $(\frac{a,d}{p})=+1$ for all primes $p\nmid d$).

Consider the map $\mathrm{cl}:\mathrm{Sel}_2(\mathcal{C})\longrightarrow\mathrm{Cl}^+(k)[2]$ sending $\mathcal{T}(a)$ to the ideal class generated by the ambiguous ideal $\mathfrak{a}$ with norm a; clearly $\ker\mathrm{cl}=W(\mathcal{C})$. By Hilbert's genus theory (see [Lem2000]), we know that ideal classes coming from the Selmer group are squares, so the map above is actually a homomorphism $\mathrm{Sel}_2(\mathcal{C})\longrightarrow\mathrm{Cl}^+(k)^2\cap\mathrm{Cl}^+(k)[2]=\mathrm{Cl}^+(k)^2[2]$. Conversely, an ideal class in $\mathrm{Cl}^+(k)^2[2]$ is generated by an ambiguous ideal $\mathfrak{a}$ with norm $a\mid\Delta$, and since its class is a square, its character system is trivial, so the descendant $\mathcal{T}(a)$ is in the Selmer group.

Theorem 6.4. *We have an exact sequence*

$$0 \longrightarrow W(\mathcal{C}) \longrightarrow \mathrm{Sel}_2(\mathcal{C}) \longrightarrow \mathrm{Cl}^+(k)^2[2] \longrightarrow 0.$$

In particular, $\mathbf{Ш}_2(\mathcal{C}) \simeq \mathrm{Cl}^+(k)^2[2]$.

Observe that, for finite abelian groups G, we have the exact sequence

$$1 \longrightarrow G^2 \cap G[2] \longrightarrow G^2 \xrightarrow{[2]} G^4 \longrightarrow 1$$

showing that $G^2 \cap G[2] \simeq G^2/G^4$ (non-canonically via duality), hence $\mathrm{Cl}^+(k)^2[2] \simeq \mathrm{Cl}^+(k)^2/\mathrm{Cl}^+(k)^4$. Since this group can be made arbitrarily large, we find

Corollary 6.5. *For Pell conics* $\mathcal{C} : X^2 - \Delta Y^2 = 4$*, the Tate-Shafarevich group* $\mathbf{Ш}_2(\mathbb{C})$ *can have arbitrarily large* 2*-rank as* Δ *varies.*

6.4. **For Whom the Pell Tolls.** Let us now derive some results about Pell equations that follow from studying the 2-Selmer group.

Selmer Groups. The following result connects the structure of the Selmer group to various invariants studied in [Lem2003b]:

Proposition 6.6. *Let* Δ *be a discriminant not divisble by any prime* $\equiv 3 \bmod 4$*, let* $\mathcal{C} : X^2 - \Delta Y^2 = 4$ *be the corresponding Pell conic, and let* $\gamma(\Delta)$ *be the associated nondirected graph (see* [Lem2003b]*). Then the following claims are equivalent:*

1. $\gamma(\Delta)$ *is odd;*
2. $\mathrm{Sel}_2(\mathcal{C}) \simeq \mathbb{Z}/2\mathbb{Z}$*;*
3. $\mathbf{Ш}(\mathcal{C})[2] = 0$*;*
4. 4*-rank* $\mathrm{Cl}_2^+(k) = 0$.

Proof. The equivalence of the statements (2)-(4) follow from the exact sequence (4) and Theorem 6.4.

The fact that $\gamma(\Delta)$ is odd if and only if none of the equations $ar^2 - bs^2 = 4$ has $\mathbb{F}_p$-rational points for all primes p was proved in [Lem2003b]. □

Nontrivial Tate-Shafarevich Groups. If a is a quadratic residue modulo a prime p, then we write $(\frac{a}{p})_4 = +1$ or -1 according as a is a fourth power modulo p or not. If $p \equiv 1 \bmod 8$, then we define $(\frac{p}{2})_4 = (-1)^{(p-1)/8}$. We extend these residue symbols multiplicatively to composite denominators.

Theorem 6.7. *Let* $\Delta = p_1 \cdots p_n$ *be a product of primes* $p_i \equiv 1 \bmod 4$*. If* $ab = \Delta$ *and* $ar^2 - bs^2 = 4$ *has an integral solution, then the following conditions are satisfied:*

1. $(a/q) = 1$ *for all primes* $q \mid b$*;*
2. $(b/p) = 1$ *for all primes* $p \mid a$*;*
3. $(b/a)_4 = +1$.

Proof. The first two assertions are clear and follow from the existence of a rational point.

For any prime $p \mid a$, we have $(-b/p)_4 = (2s/p)$; since $(-1/p)_4 = (2/p)$, this implies $(b/p)_4 = (s/p)$, hence $(b/a)_4 = (s/a)$. Now write $s = 2^j s'$ with s' odd; then $(b/a)_4 = (s/a) = (2/a)^j$. If $j = 0$ or $j = 2$, we are done. The case $j = 1$ is impossible: putting $r = 2r'$ we find $ar'^2 - bs'^2 = 1$, which leads to a contradiction modulo 4 since $bs'^2 \equiv 1 \bmod 4$. Finally, if $j \geq 3$, then dividing $ar^2 - bs^2 = 4$ through by 4 and reducing modulo 8 shows that $(2/a) = +1$. □

There are similar results for even Δ not divisible by primes $\equiv 3 \bmod 4$.

Let us now apply this result to the Pell equation $X^2 - pqY^2 = 1$, where $p \equiv q \equiv 1 \bmod 4$. The first descendants $pr^2 - qs^2 = \pm 1$ are not solvable in integers if $(p/q) = -1$, so in this case we conclude that $X^2 - pqY^2 = -1$ is solvable. Assume that $(p/q) = +1$. Then Theorem 6.7 provides us with necessary conditions for the descendant $\mathcal{T}_a$ to be solvable: Thus if $(p/q)_4 = (q/p)_4 = -1$, the negative Pell

a	equation	condition
1	$X^2 - pqY^2 = 1$	none
p	$pX^2 - qY^2 = 1$	$(q/p)_4 = 1$
q	$qX^2 - pY^2 = 1$	$(p/q)_4 = 1$
pq	$pqX^2 - Y^2 = 1$	?

TABLE 1. Solvability Criteria for $\mathcal{T}$

equation $X^2 - pqY^2 = -1$ must be solvable. If, say, $(p/q)_4 = -(q/p)_4$, however, we do not get a precise result because Theorem 6.7 does not give us any condition for the solvability of $\mathcal{T}_{pq}$. For this, we have to dig deeper:

Proposition 6.8. *If $\mathcal{T}_{pq} : pxr^2 - s^2 = 1$ has an integral solution, where $p \equiv q \equiv 1 \bmod 4$ are primes with $(p/q) = 1$, then $(p/q)_4 = (q/p)_4$.*

This implies the following result, parts of which were first proved by Scholz [Sch1934] using class field theory:

Proposition 6.9. *Let $p \equiv q \equiv 1 \bmod 4$ be primes. If the conditions $(*)$ are verified, the descendant $\mathcal{T}_a$ of the Pell conic $X^2 - pqY^2 = 1$ is solvable:*

$(*)$	a
$(p/q) = -1$	pq
$(p/q) = +1, (p/q)_4 = -1, (q/p)_4 = +1$	p
$(p/q) = +1, (p/q)_4 = +1, (q/p)_4 = -1$	q
$(p/q) = +1, (p/q)_4 = -1, (q/p)_4 = -1$	pq

Note that this implies e.g. that if $(p/q) = +1$, $(p/q)_4 = +1$ and $(q/p)_4 = -1$, then $\mathcal{T}_q$ is an element of the Selmer group without an integral point, hence represents an element of order 2 in $\mathbf{Ш}(\mathcal{C})$.

The proof of Proposition 6.9 presents no problems; thus it remains to prove Proposition 6.8. This is done as follows: factor the right hand side of $pqs^2 = r^2 + 1$ over the Gaussian integers $\mathbb{Z}[i]$. Since $\gcd(r+i, r-i)$ divides $2i$, and since r is even, the factors $r + i$ and $r - i$ are coprime. Now observe that $p = \pi\overline{\pi}$ and $q = \rho\overline{\rho}$ for $\pi, \rho \in \mathbb{Z}[i]$, where the bars denote the conjugates. Assume that π and ρ are primary, i.e., that $\pi \equiv \rho \equiv 1 \bmod 2 + 2i$. Then Unique Factorization in $\mathbb{Z}[i]$ implies that $r + i = \varepsilon\pi\rho\alpha^2$ for some $\alpha \in \mathbb{Z}[i]$ and some unit $\varepsilon \in \{\pm i, \pm 1\}$. Since $r + i \equiv i \bmod 2$, and since $\alpha^2 \equiv 1 \bmod 2$, we have $\varepsilon = \pm i$, and by subsuming the square $-1 = i^2$ into α if necessary we arrive at $r + i = i\pi\rho\alpha^2$.

If, from this equation, we subtract its conjugate and then divide by i, we arrive at

$$2 = \pi\rho\alpha^2 - \overline{\pi\rho}\overline{\alpha}^2.$$

Reducing modulo $\overline{\rho}$ we find $[2/\overline{\rho}] = [\pi/\overline{\rho}][\rho/\overline{\rho}]$, where $[\,\cdot\,/\,\cdot\,]$ is the quadratic residue symbol in $\mathbb{Z}[i]$ (see [Lem2000] for the necessary background). Then it is known that $[2/\overline{\rho}] = (2/q)$ and $[\rho/\overline{\rho}] = (2/q)$, as well as $[\pi/\overline{\rho}] = [\pi/\rho] = (p/q)_4(q/p)_4$. This concludes the proof of Proposition 6.8.

This allows us to complete Table 6.4:

a	equation	condition
1	$X^2 - pqY^2 = 1$	none
p	$pX^2 - qY^2 = 1$	$(q/p)_4 = 1$
q	$qX^2 - pY^2 = 1$	$(p/q)_4 = 1$
pq	$pqX^2 - Y^2 = 1$	$(p/q)_4(q/p)_4 = 1$

TABLE 2. Solvability Criteria for $\mathcal{T}$

In some sense, the solvability condition for the product $\mathcal{T}_{pq}$ of $\mathcal{T}_p$ and $\mathcal{T}_q$ is the 'product' of the conditions for $\mathcal{T}_p$ and $\mathcal{T}_q$; although we cannot make this more precise at the moment, this observation often helps to guess the right criteria.

Observe that the proof of Proposition 6.9 is fully analogous to the calculations done in [Lem2003a] for computing Tate-Shafarevich groups of elliptic curves connected to the congruent number problem.

REFERENCES

[Bal1999] N. Baldisserri, *The group of primitive quasi-Pythagorean triples* (Italian), Rend. Circ. Mat. Palermo (2) **48** (1999), 299–308; cf. p. 5

[BS1996] R.A. Beauregard, E.R. Suryanarayan, *Pythagorean triples: the hyperbolic view*, College Math. J. 1996; cf. p. 5

[BS1997] R.A. Beauregard, E.R. Suryanarayan, *Arithmetic Triangles*, Math. Mag. **70** (1997), 105–115; cf. p. 5

[BS1999] R.A. Beauregard, E.R. Suryanarayan, *Integral Triangles*, Math. Mag. **72** (1999), 287–294; cf. p. 5

[Daw1994] B. Dawson, *The ring of Pythagorean triples*, Missouri J. Math. Sci. **6** (1994), 72–77; cf. p. 5

[Dic1920] L.E. Dickson, *History of the Theory of Numbers*, vol I (1920); vol II (1920); vol III (1923); Chelsea reprint 1952; cf. p. 5

[Dic1930] L.E. Dickson, *Studies in the Theory of numbers*, Chicago 1930; cf. p. 7

[Eck1984] E. Eckert, *The group of primitive Pythagorean triangles*, Math. Mag. **54** (1984), 22–27; cf. p. 5

[Gry1997] A. Grytczuk, *Note on a Pythagorean ring*, Missouri J. Math. Sci. **9** (1997), 83–89; cf. p. 5

[Hla2000] E. Hlawka, *Pythagorean triples*, Number theory, Birkhäuser, Basel (2000), 141–155; cf. p. 5

[Jue1896] C. Juel, *Ueber die Parameterbestimmung von Punkten auf Curven zweiter und dritter Ordnung. Eine geometrische Einleitung in die Theorie der logarithmischen und elliptischen Funktionen*, Math. Ann. **47** (1896), 72–104; cf. p. 4

[Lem2000] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer Verlag 2000; cf. p. 16, 19

[Lem2003a] F. Lemmermeyer, *Some families of non-congruent numbers*, Acta Arith. **110** (2003), 15–36 19

[Lem2003b] F. Lemmermeyer, *Higher Descent on Pell Conics. I. From Legendre to Selmer*, preprint 2003; cf. p. 1, 6, 7, 9, 16, 17

[Lem2003c] F. Lemmermeyer, *Higher Descent on Pell Conics. II. Two Centuries of Missed Opportunities*, preprint 2003; cf. p. 1

[Mar1962] J. Mariani, *The group of the pythagorean numbers*, Amer. Math. Mon. **69** (1962), 125–128; cf. p. 5

[Mor1986] J. Morita, *A transformation group of the Pythagorean numbers*, Tsukuba J. Math. **10** (1986), no. 1, 151–153; cf. p. 5

[Nie1908] B. Niewenglowski, *Note sur les equations* $x^2 - ay^2 = 1$ *et* $x^2 - ay^2 = -1$, Bull. Soc. Math. France **35** (1907), 126–131; cf. also Wiadomi Mat. Warsaw **12** (1908), 1–26 (Polish); cf. p. 5

[PS1997] V. Prasolov, Y. Solovyev, *Elliptic Functions and Elliptic Integrals*, Transl. Math. Monographs **170**, AMS 1997; cf. p. 5

[Sch1990] N. Schappacher, *Développement de la loi de groupe sur une cubique*, Séminaire Théor. Nombres, Paris 1988–1989, 159–184; Progr. Math. **91** (1990); cf. p. 5

[Sch1839] Th. Schönemann, *Ueber die Congruenz* $x^2 + y^2 \equiv 1 \pmod p$, J. Reine Angew. Math. **19** (1839), 93–112; cf. p. 4

[Sch1934] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. **39** (1934), 95–111; cf. p. 18

[Sha2001] P. Shastri, *Integral points on the unit circle*, J. Number Theory **91** (2001), 67–70; cf. p. 5

[Sta1896] P. Stäckel, *Review JFM 27.0337.02*, Jahrbuch Fortschritte der Mathematik **27** (1896), p. 337; cf. p. 4

[Tan1996] L. Tan, *The group of rational points on the unit circle*, Math. Mag. **69** (1996), 163–171; cf. p. 5

[Tau1970] O. Taussky, *Sums of squares*, Amer. Math. Monthly **77** (1970), 805–830; cf. p. 5

[Tur1915] E. Turrière, *Le problème de Jean de Palerme et de Léonard de Pise*, Ens. Math. **17** (1915), 315–324; cf. p. 5

[Tur1916] E. Turrière, *Notions d'arithmogéométrie*, Ens. math. **18** (1916), 81–110, 397–428; cf. p. 5

[Tur1917] E. Turrière, *Notions d'arithmogéométrie*, Ens. math. **19** (1917), 159–191, 233–272; cf. p. 5

[Tur1918] E. Turrière, *Notions d'arithmogéométrie*, Ens. math. **20** (1918), 161–174; cf. p. 5

[VY1910] O. Veblen, J.W. Young, *Projective Geometry I*, Ginn & Co. 1910; cf. p. 5

[Woi2001] M. Wojtowicz, *Algebraic structures on some sets of Pythagorean triples. II*, Missouri J. Math. Sci. **13** (2001), 17–23; cf. p. 5

[ZZ1991] P. Zanardo, U. Zannier, *The group of Pythagorean triples in number fields*, Ann. Mat. Pura Appl. (4) **159** (1991), 81–88; cf. p. 5

Department of Mathematics, Bilkent University, 06800 Bilkent, Ankara, Turkey
E-mail address: franz@fen.bilkent.edu.tr