Hardy-Ramanujan Journal 47 (2024), 44-64 submitted 18/12/2024, accepted 17/03/2025, revised 17/03/2025

Geometric approach to the Diophantine equation $x^2 + xy - y^2 = m$

Norbert Hungerbühler and Maciej Smela

Abstract. We investigate the Diophantine equation $x^2 + xy - y^2 = m$, for $m \in \mathbb{Z}$ given, from a geometric point of view. The hyperbola given by the equation carries a known group structure, which we interpret in four different ways, firstly with the familiar parallel line construction. It turns out that the group defined by this construction corresponds to the restriction of a group operation on $\mathbb{R}^2$, which is induced by the number field $\mathbb{Q}(\sqrt{5})$. In this way, the group operation can be described using lean formulae. We also find a parametrisation of the hyperbola that is compatible with the group operation. This result is analogous to the fact that the parametrisation of a cubic curve using the Weierstrass $\wp$-function is compatible with the group structure of the elliptic curve. A fourth interpretation of the group structure is based on a geometric observation about the orientated area of triangles with one vertex in the origin and two vertices on the hyperbola. Our parametrisation allows to define intervals whose images are regions F_m on the hyperbola such that any integer solution is uniquely given by $\pm\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ for $\begin{pmatrix} x \\ y \end{pmatrix} \in F_m$. We also expand the considerations for solvability in Cohn [Coh78] of binary quadratic forms obtained from quadratic number fields and give descriptions of the integer solutions to $x^2 + xy - y^2 = m$ using the ideals in the number field $\mathbb{Q}(\sqrt{5})$.

Keywords. diophantine equations, binary quadratic forms, number fields.

2010 Mathematics Subject Classification. 11D09, 11D85.

1. Introduction

We investigate the Diophantine equation

$$x^2 + xy - y^2 = m, \tag{1.1}$$

for $m \in \mathbb{Z}$ given. We define the sets $\mathbb{P}_S(m) := \{(x, y) \in S^2 : x^2 + xy - y^2 = m\}$ for $m \in \mathbb{R}$ and $S \subseteq \mathbb{R}$. In particular, $\mathbb{P}_\mathbb{R}(m), \mathbb{P}_\mathbb{Q}(m)$, and $\mathbb{P}_\mathbb{Z}(m)$ are the sets of real, rational, and integer solutions of (1.1).

For given $m \in \mathbb{R}, m \neq 0$, equation (1.1) represents a hyperbola in the real plane. In Section 2 we will describe a parametrisation of these curves which will be used later to analyse a group structure on the curve, similar to the case of an elliptic curve which is parametrised by the Weierstrass $\wp$-function.

Note that $x^2 + xy - y^2$ is a binary quadratic form. Such forms have been widely studied, for example in Buell [Bue89] and Cohn [Coh78]. Of particular interest are the integer solvability and solutions of such equations and especially primitive integer solutions, that is solutions $(x, y) \in \mathbb{Z}^2$ with $\gcd(x, y) = 1$. We will denote the set of the primitive integer solutions of (1.1) by $\mathbb{P}_\mathbb{Z}^{\mathrm{pr}}(m)$. In [OSIS24a] the sequence of integers m is given for which primitive integer solutions exist. Lang [Lan19] proved a conjecture in [OSIS24a, Conjecture] which we rephrase slightly here as follows.

Theorem 1.1. *[OSIS24a, Conjecture] Equation (1.1) has primitive integer solutions exactly for those integers m whose prime factorization has prime factors which are $\equiv 0, \pm 1$ mod 5 and at most one factor 5.*

For the case of general integer solutions the following is known.

Theorem 1.2. *[OEIS24b, "Formula"] Equation (1.1) has integer solutions exactly for those integers m in which primes $\equiv 2$ or 3 mod 5 occur with even exponents.*

We thank episciences.org for providing open access hosting of the electronic journal *Hardy-Ramanujan Journal*

In Section 3 we give alternative proofs for both theorems using the theory of number fields with tools from Pink [Pin24] and inspired by Cohn [Coh78]. Indeed, Cohn explains the solvability of binary quadratic forms

$$Q_D := \begin{cases} x^2 - Dy^2 & \text{if } D \not\equiv 1 \bmod 4, \\ x^2 + xy + \dfrac{1-D}{4}y^2 & \text{if } D \equiv 1 \bmod 4, \end{cases}$$

obtained from quadratic number field norms. In particular, Cohn proves the following.

Theorem 1.3. *[Coh78, Theorem 3.14] If* $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ *is factorial, then for primes* $p \nmid 2D$,

$$p = \left\{ \begin{array}{c} Q_D(x,y) \\ \text{or} \\ -Q_D(x,y) \end{array} \right\} \iff m^2 \equiv D \bmod p \text{ is solvable for } m \in \mathbb{Z}.$$

This gives the connection of the problem to number fields. From this Cohn obtains the special case of Theorem 1.1 for $m = p$ prime:

$$p = x^2 + xy - y^2 \iff p = 5 \text{ or } p \equiv \pm 1 \bmod 5$$

in [Coh78, Equation 3.18f]. Additionally, Cohn explains the connection between the solvability of $Q_D(x,y) = \pm p$ for p prime and the principal prime ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ [Coh78, Section 14]. We will carry out a similar but more general analysis in Section 3.A for the equation $x^2 + xy - y^2 = m$. In Corollary 3.5 we work out the ideal structure in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ in detail. In Theorem 3.13 we describe the integer solutions of (1.1) using ideals in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ utilizing some general results and approaches from [Pin24]. For this we use the concept of a *primitive ideal* as in [Coh78, Definition 14.11] to describe the sets of primitive solutions. Also from Theorem 3.13 we derive Theorem 3.14 which combines Theorem 1.1 and Theorem 1.2. We then apply Theorem 3.13 to give descriptions of the (primitive) integer solutions of (1.1). First, in Theorem 3.15 we give a characterisation of $\mathbb{P}_{\mathbb{Z}}(m)$ using what we call *norm-m-generators*. Second, in Theorem 3.16 we explain the solutions as "built up" from integer solutions to the equations $x^2 + xy - y^2 = p$ for the prime factors p of m.

The problem of describing the integer solutions can also be approached geometrically. This is done by Lemmermeyer for example in [Lem21] using an operation on the solution sets and Vieta jumping. In Section 4 we give a different geometric approach to the integer solutions using the parametrisation of the hyperbolas given by (1.1) from Section 2. With this strategy we will be able to localise integer solutions on "intervals" of $\mathbb{P}_{\mathbb{R}}(m)$, where *representative* integer solutions can be found in the sense that all other solutions can be obtained from them. This is done in the Propositions 4.2 and 4.3.

In Section 5 we define an operation on the sets $\mathbb{P}_{\mathbb{R}}(m)$ for fixed $m \in \mathbb{R}$ in several different ways starting from a geometric approach by Lemmermeyer ([Lem18], [Lem03], [Lem12]). Lemmermeyer's construction is as follows.

Definition 1.1. *[Lem03, Section 1.1] Let* $\mathcal{C}$ *be a non-degenerate conic over a field* F *and fix a rational point* N *on* $\mathcal{C}$. *The sum* $A \oplus_N B$ *of two rational points* A, B *on* $\mathcal{C}$ *is given as*

- *the "other" intersection with* $\mathcal{C}$ *of the line parallel to* AB *and through* N *if* $A \neq B$,
- *the "other" intersection with* $\mathcal{C}$ *of the line parallel to the tangent to* $\mathcal{C}$ *at* A *and through* N *if* $A = B$.

It is known that this defines a group structure as in [Lem03] and Shirali [Shi09]. A detail worth noting is the associativity which follows from Pascal's hexagon theorem. Such an operation has also been considered in [Bel21] as a group law for cryptographic applications. Additionally, the following is known.

Theorem 1.4. *[Shi09, p. 6 Conclusion] The group $(\mathcal{C}, \oplus_N, N)$ as in Definition 1.1 is*

- *isomorphic to the group $(\mathbb{R}/\mathbb{Z}, +)$ if $\mathcal{C}$ is a circle or an ellipse,*
- *isomorphic to the group $(\mathbb{R}, +)$ if $\mathcal{C}$ is a parabola,*
- *isomorphic to the group $(\mathbb{R}^\times, \cdot)$ if $\mathcal{C}$ is a hyperbola.*

In [Lem21], Lemmermeyer studies the integer points on some conics in connection with this operation. For instance, Lemmermeyer considers the Fibonacci Hyperbola $x^2 - xy - y^2 = 1$ and shows that if there are two known distinct integer points, then there are infinitely many integer points on it and they are given as $\oplus$ multiples of $(2, 1)$ or their negatives. We use a different approach in Section 4 that does not require knowledge of two solutions. We will also give various views on the group operation using the construction in Definition 1.1: An algebraic approach based on number fields, a different geometric construction using triangle areas, and a connection with the parametrisation in Section 2. We also obtain an explicit formula for the algebraic operation in Lemma 5.1. In Theorem 5.2 we show that these views are equivalent. Finally, in Theorem 5.2 and Corollary 5.5 we explain the abstract group structure proving Theorem 1.4 for the hyperbola $x^2 + xy - y^2 = m$.

2. Parametrisation of the curve $x^2 + xy - y^2 = m$

The curves in $\mathbb{R}^2$ which are described by the quadratic equation $x^2 + xy - y^2 = m$, for $0 \neq m \in \mathbb{R}$, are hyperbolas. We need the following functions to obtain a suitable parameterisation of these curves:

$$X_m(t) := \begin{cases} \sqrt{2m}\big(A\cosh(t) - B\sinh(t)\big)/5^{1/4} & \text{if } m > 0, \\ \sqrt{2|m|}\big(-B\cosh(t) - A\sinh(t)\big)/5^{1/4} & \text{if } m < 0, \end{cases}$$

$$Y_m(t) := \begin{cases} \sqrt{2m}\big(B\cosh(t) + A\sinh(t)\big)/5^{1/4} & \text{if } m > 0, \\ \sqrt{2|m|}\big(A\cosh(t) - B\sinh(t)\big)/5^{1/4} & \text{if } m < 0, \end{cases}$$

where $A = \sqrt{\frac{1}{2} + \frac{1}{\sqrt{5}}}$ and $B = \sqrt{\frac{1}{2} - \frac{1}{\sqrt{5}}}$. It is then elementary to check that

$$P_m : \mathbb{R} \to \mathbb{R}^2, \quad t \mapsto \begin{pmatrix} X_m(t) \\ Y_m(t) \end{pmatrix},$$

parametrises one, and $-P_m$ the other branch of the hyperbola given by (1.1), as illustrated in Figure 1. We will see later that this parametrisation is compatible with the group structure on the curves. We note that we have $X_{-|m|} = -Y_{|m|}$ and $Y_{-|m|} = X_{|m|}$ and so $P_{-|m|} = R_\pm P_{|m|}$, where $R_\pm$ is the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, that is $P_{-|m|}$ is $P_{|m|}$ rotated by $\pi/2$ counter-clockwise.

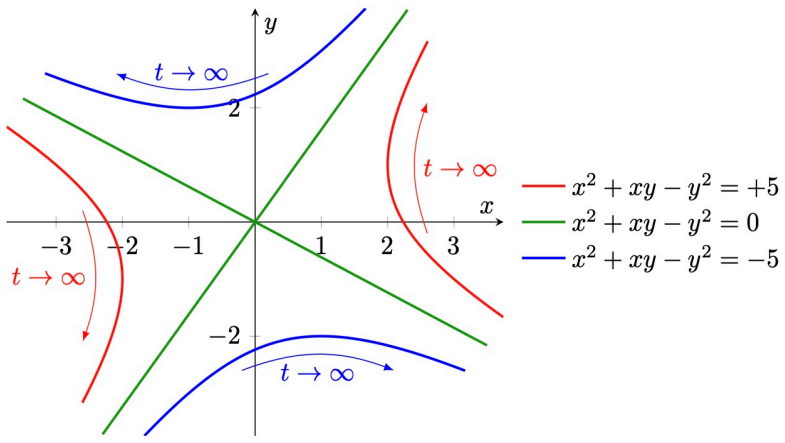

Figure 1: Plots of $x^2 + xy - y^2 = m$ for $m = 5, 0, -5$. The arrows indicate the direction in which the curves are travelled under the given parametrisation. The right branch or the upper branch of the hyperbola is parametrised by P_m, the other branches by $-P_m$.

It is convenient to combine the parametrisation of both branches and consider the bijection

$$\mathcal{P}_m : \{\pm 1\} \times \mathbb{R} \to \mathbb{P}_{\mathbb{R}}(m), \quad (s,t) \mapsto sP_m(t).$$

Remark 2.1. (The case $m=0$). *We note that x^2+xy-y^2 has the factorization*

$$x^2+xy-y^2 = \big(x+\beta y\big)\big(x+(1-\beta)y\big).$$

Here, and in what follows, $\beta = (1+\sqrt{5})/2$ denotes the golden ratio. Hence, for $m=0$, the curve $x^2+xy-y^2=0$ corresponds to the two green lines in Figure 1 which are the asymptotes common to all hyperbolas in the family.

Next, we identify some special points on $\mathbb{P}_{\mathbb{R}}(m)$ and how this is expressed using the parametrisation above.

Proposition-Definition 2.1. (Special points on $\mathbb{P}_{\mathbb{R}}(m)$). *Fix $m \in \mathbb{R}_{>0}$. Then for $t \in \mathbb{R}$ we have*

- $X_m(t) = Y_m(t) \iff t = t^{(+)}_{X=Y} := \frac{3}{2}\ln(\beta) \approx 0.721818$ *and we have* $P_m(t^{(+)}_{X=Y}) = (\sqrt{m}, \sqrt{m})$.
- *If* $x_0 \geq 2\sqrt{m/5}$, *then* $X_m(t) = x_0 \iff t = \frac{1}{2}\ln(\beta) + \ln(\sqrt{5x_0^2} \pm \sqrt{5x_0^2-4m}) - \ln(2\sqrt{m})$.
- *For $y_0 \in \mathbb{R}$ it holds that* $Y_m(t) = y_0 \iff t = -\frac{1}{2}\ln(\beta) + \ln(\sqrt{5}y_0 + \sqrt{5y_0^2+4m}) - \ln(2\sqrt{m})$, *and in particular* $Y_m(t) = 0 \iff t = t^{(+)}_{Y=0} := -\frac{1}{2}\ln(\beta)$ *and we have* $P_m(t^{(+)}_{Y=0}) = (\sqrt{m}, 0)$.

For $m<0$ similar results can be formulated using the relations $X_{-|m|} = -Y_{|m|}$ and $Y_{-|m|} = X_{|m|}$.

Proof. We just prove the condition for $X_m(t) = Y_m(t)$. We rewrite this as

$$0 = X_m(t) - Y_m(t) = \sqrt{2m}\left((A-B)\cosh(t) - (A+B)\sinh(t)\right)/5^{1/4}.$$

The solutions t to this equation satisfy $t \in \{\ln(\pm\sqrt{-(A-B)^2+(A+B)^2}/(2B))\}$. Only the "+" solution is real and one can check that it simplifies to $t = \ln\left(\frac{\sqrt{2}}{2\cdot 5^{1/4}B}\right) = 3/2\ln(\beta)$. □

Next, we give some properties of the functions X_m, Y_m, P_m.

Lemma 2.2. *Let $\beta := \frac{1+\sqrt{5}}{2}$. Then for any $m \in \mathbb{R}_{>0}$ the function $Y_m : \mathbb{R} \to \mathbb{R}$ is strictly increasing and bijective. Moreover, the function X_m satisfies $X_m'' = X_m$ and has a global minimum at $t = t^{(m)}_{min} := \frac{1}{2}\ln(\beta)$ and we have $P_m(t^{(m)}_{min}) = \sqrt{\frac{m}{5}}\cdot(2,1)$. In particular, $X_m = X_m'' > 0$ and $P_m(t^{(m)}_{min})$ lies on the line $y = \frac{1}{2}x$. For $m \in \mathbb{R}_{<0}$ analogous results can be obtained using the relations $X_{-|m|} = -Y_{|m|}$ and $Y_{-|m|} = X_{|m|}$.*

Proof. Let $m > 0$. We just show that Y_m is strictly increasing. This holds as the derivative Y_m' is positive. Indeed, we have $Y_m'(t) = \frac{\sqrt{2m}}{2\cdot 5^{1/4}}\left((A+B)e^t + (A-B)e^{-t}\right)$, which is positive since $A+B>0$ and $A-B>0$. The other properties can also be easily shown when the functions are expressed using exponentials. □

We will frequently use the following matrices which map $\mathbb{P}_{\mathbb{R}}(m)$ to itself:

$$A_{(*)} := \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad K := \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \qquad A_1 := \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}.$$

Indeed, the matrices all have non-zero determinants and so define bijective maps. Moreover, if $(x_0,y_0) \in \mathbb{P}_{\mathbb{R}}(m)$ then also $X\binom{x_0}{y_0} \in \mathbb{P}_{\mathbb{R}}(m)$, for $X \in \{A_{(*)}, K, A_1\}$. For example, we have $A_{(*)}\binom{x_0}{y_0} = \binom{x_0}{x_0-y_0}$, and $x_0^2 + x_0(x_0-y_0) - (x_0-y_0)^2 = x_0^2 + x_0y_0 - y_0^2 = m$. For the other two matrices this can also be directly verified. Note that these matrices have the following properties.

- $A_{(*)}^2 = I_2 = K^2$ and so $A_{(*)}^{-1} = A_{(*)}$ and $K^{-1} = K$.
- A_1 is symmetric.
- $A_{(*)}$ and K are not symmetric but we have $A_{(*)}^T = K$.
- $A_1 = KA_{(*)}$.

3. Integer solutions of $x^2 + xy - y^2 = m$

For completeness we start with the case $m = 0$. It follows immediately from Remark 2.1 that the only rational point on the curve $x^2 + xy - y^2 = 0$ is the point $(0, 0)$. Thus, in the following we will mostly consider $m \neq 0$.

3.A. Connecting solutions to $x^2 + xy - y^2 = m$ and elements in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ of norm m

In this section we describe the integer solvability and integer solutions of $x^2 + xy - y^2 = m$ using number fields based on but adapted from [Coh78] and using results from [Pin24]. For this we consider the quadratic number field $K := \mathbb{Q}(\sqrt{5})$. It is real quadratic with the two real embeddings given by the mappings $\sqrt{5} \mapsto \pm\sqrt{5}$. Moreover, it is known that the ring of integers is

$$\mathcal{O}_K = \mathbb{Z}[\beta] = \{x + y\beta : x, y \in \mathbb{Z}\}, \text{ for the golden ratio } \beta := (1 + \sqrt{5})/2,$$

and the discriminant of K is equal to 5. Additionally, it is known that $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ has class number equal to 1 and is therefore a PID.

The main reason why we are interested in this number field is the following key observation from [Coh78]. The norm $\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}$ in the number field $\mathbb{Q}(\sqrt{5})$ is given by

$$\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(x + y\beta) = x^2 + xy - y^2, \tag{3.2}$$

for $x, y \in \mathbb{Z}$.

Consequence 3.1. *We obtain a bijection:*

$$\mathbb{P}_{\mathbb{Z}}(m) \to \{z \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})} : N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(z) = m\}, \quad (x, y) \mapsto x + y\beta. \tag{3.3}$$

Recall that the absolute norm of a principal ideal (a) is equal to the absolute value of the norm of the element a, that is $\mathrm{N}((a)) = |\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(a)|$. With this we have the following.

Lemma 3.1. *The following statements are equivalent.*

(a) There exists an integer solution to $x^2 + xy - y^2 = m$.

(b) There exists an element $x + y\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ of norm equal to m.

(c) There exists a principal ideal $(x + y\beta) \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ of absolute norm equal to $|m|$.

(d) There exists an ideal $I \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ of absolute norm equal to $|m|$.

Proof. "$(a) \Rightarrow (b)$": By equation (3.2) the element $x+y\beta$ has norm $x^2+xy-y^2 = m$. "$(b) \Rightarrow (c)$": The absolute norm of the principal ideal $(x + y\beta)$ is $|\mathrm{N}(x + y\beta)| = |m|$. "$(c) \Rightarrow (d)$": A principal ideal of absolute norm equal to $|m|$ is in particular an ideal. "$(d) \Rightarrow (a)$": Suppose I is an ideal of norm equal to $|m|$. Then as $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ is a principal ideal domain, we can write $I = (x + y\beta)$ for some $x + y\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. Moreover, $|\mathrm{N}(x + y\beta)| = \mathrm{N}((x + y\beta)) = \mathrm{N}(I) = |m|$. Thus, $x^2+xy-y^2 = \mathrm{N}(x+y\beta) \in \{\pm m\}$. If $x^2+xy-y^2 = m$ we are done. Otherwise, $x^2+xy-y^2 = -m$. But then, $(-y, x)$ satisfies $(-y)^2 + (-y)x - x^2 = m$. □

In particular, by Lemma 3.1 the equation $x^2 + xy - y^2 = m$ has integer solutions if and only if an ideal of norm equal to $|m|$ exists. Therefore we will describe the ideals in $\mathbb{Q}(\sqrt{5})$ in Section 3.E.

3.B. A ring structure on $\mathbb{R}^2$

Motivated by (3.3) we observe that since $\beta^2=\beta+1$ we have

$$(x+y\beta)(u+v\beta)=xu+(xv+yu)\beta+yv\beta^2=xu+yv+(xv+yu+yv)\beta,$$

for any $x,y,u,v\in\mathbb{R}$. This leads us to define the following.

Definition 3.2. *Let* $(x,y),(u,v)\in\mathbb{R}^2$. *Set*

$$\begin{aligned}(x,y)\boxplus(u,v)&:=(x+u,y+v)\in\mathbb{R}^2,\\(x,y)\boxdot(u,v)&:=(xu+yv,xv+yu+yv)\in\mathbb{R}^2.\end{aligned}$$

We also define

$$(x,y)^{\boxdot k}:=(x,y)\boxdot\ldots(k\ \textit{times})\ldots\boxdot(x,y)$$

for $k\in\mathbb{Z}_{>0}$ *and* $(x,y)^{\boxdot 0}:=(1,0)$. *For* $k\in\mathbb{Z}_{<0}$ *and if* $x^2+xy-y^2\neq 0$ *we set*

$$(x,y)^{\boxdot k}:=\left(\frac{x+y}{x^2+xy-y^2},\frac{-y}{x^2+xy-y^2}\right)^{\boxdot(-k)}.$$

In particular, by Lemma 3.3 below the element $(x,y)^{\boxdot(-1)}$ *is the inverse of* (x,y) *with respect to* $\boxdot$. *Additionally, if* $(u,v)\notin\mathbb{P}_{\mathbb{R}}(0)$ *we set*

$$(x,y)\boxdiv(u,v):=(x,y)\boxdot(u,v)^{\boxdot(-1)}.$$

In accordance with (3.2) we define the norm

$$N\left((x,y)\right):=x^2+xy-y^2,$$

for $(x,y)\in\mathbb{R}^2$, *writing sometimes just* $N(x,y)$, *and the conjugate* $\overline{(x,y)}:=(x+y,-y)$.

For $(x,y)\in\mathbb{Z}^2$ we have $N(x,y)=\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(x+y\beta)$ and $\overline{(x,y)}$ corresponds with (3.3) to $\sigma(x+y\beta)$ for $\sigma\in\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{5}),\mathbb{C})$ given by $\sqrt{5}\mapsto-\sqrt{5}$. This leads directly to the following result.

Proposition 3.3. *The tuple* $(\mathbb{R}^2,\boxplus,0_{\boxplus}=(0,0),\boxdot,1_{\boxdot}=(1,0))$ *is a commutative unitary ring with* $1_{\boxdot}\neq 0_{\boxplus}$. *It contains the commutative unitary subrings* $(\mathbb{Z}^2,\boxplus,0_{\boxplus},\boxdot,1_{\boxdot})$ *and* $(\mathbb{Q}^2,\boxplus,0_{\boxplus},\boxdot,1_{\boxdot})$.

A direct computation shows the following.

Lemma 3.2. *The norm on* $\mathbb{R}^2$ *as in Definition 3.2 is multiplicative, in the sense that*

$$N((x,y)\boxdot(u,v))=N(x,y)N(u,v),$$

for any $(x,y),(u,v)\in\mathbb{R}^2$.

As a consequence of Lemma 3.2 we see that $(\mathbb{R}^2,\boxplus,\boxdot)$ is not a field as no element of $\mathbb{P}_{\mathbb{R}}(0)$ can have an $\boxdot$-inverse since $\mathrm{N}((1,0))=1$. However, using Proposition 3.3 and Lemma 3.2 the next lemma is easily verified.

Lemma 3.3. *The tuples* $(\mathbb{R}^2\setminus\mathbb{P}_{\mathbb{R}}(0),\boxdot,1_{\boxdot}=(1,0))$ *and* $(\mathbb{Q}^2\setminus\mathbb{P}_{\mathbb{Q}}(0),\boxdot,1_{\boxdot}=(1,0))$ *are abelian groups. Moreover, for* $(x,y)\in\mathbb{R}^2\setminus\mathbb{P}_{\mathbb{R}}(0)$ *the inverse element with respect to* $\boxdot$ *is given by*

$$(x,y)^{\boxdot(-1)}=\left(\frac{x+y}{x^2+xy-y^2},\frac{-y}{x^2+xy-y^2}\right).$$

3.C. Connection to the matrices A_1 and K

In this section we briefly explain how the matrices A_1 and K from Section 2 are connected to the product $\boxdot$ and to the number field $\mathbb{Q}(\sqrt{5})$. Indeed, let $\binom{x}{y} \in \mathbb{R}^2$. Then $A_1\binom{x}{y} = \binom{2x-y}{-x+y}$. On the other hand, we have $(x,y)\boxdot(2,-1) = (2x-y,-x+y)$. In this sense, multiplying with the matrix A_1 corresponds to multiplying with $(2,-1)$ with respect to $\boxdot$, which in turn corresponds to multiplying $x+y\beta$ with $2-\beta=\beta^{-2}$ in $\mathbb{Q}(\sqrt{5})$. For the matrix K we have $K\binom{x}{y} = \binom{x+y}{-y}$. This corresponds to conjugation in $\mathbb{Q}(\sqrt{5})$ as the conjugate of $x+y\beta$ is $\sigma(x+y\beta) = x+y-y\beta$ for $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{5}),\mathbb{C})$ given by $\sqrt{5}\mapsto -\sqrt{5}$.

3.D. Integer solutions to $x^2+xy-y^2=\pm 1$ and units in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$

In this section, we give a description of the solutions to the equations $x^2+xy-y^2=\pm 1$ connected to the set $\mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{5})}$ of units in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ of the number field $\mathbb{Q}(\sqrt{5})$.

Theorem 3.4. (Integer solution sets for $m\in\{\pm 1\}$). *We have*

$$\mathbb{P}_{\mathbb{Z}}(+1) = \{\xi(0,1)^{\boxdot k} : \xi\in\{\pm1\}, k\in\mathbb{Z} \text{ even}\}, \qquad \mathbb{P}_{\mathbb{Z}}(-1) = \{\xi(0,1)^{\boxdot k} : \xi\in\{\pm1\}, k\in\mathbb{Z} \text{ odd}\}.$$

Proof. By equation (3.3) the integer solutions to $x^2+xy-y^2=1$ correspond bijectively to the elements of $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ of norm 1. In the same way, solutions to $x^2+xy-y^2=-1$ correspond to the elements of norm -1. Now, the units in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ are exactly the elements with norm in $\mathbb{Z}^{\times}=\{\pm1\}$. Moreover, it is known that β is a fundamental unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, that is any element of norm ±1 is uniquely of the form $\pm\beta^k$. Next, $\mathrm{N}(\pm\beta)=-1$ and so by multiplicativity of the norm we have $\mathrm{N}(\pm\beta^k)=(-1)^k$. Thus, $\mathbb{P}_{\mathbb{Z}}(+1)$, $\mathbb{P}_{\mathbb{Z}}(-1)$ correspond to the even respectively odd powers of β which correspond with equation (3.3) and the definition of $\boxdot$ to the elements $\pm(0,1)^{\boxdot k}$. □

3.E. Ideals

In this section we work out the ideals in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. We usually write principal ideals using the notation $xR=\{xr : r\in R\}$ for x an element and R a ring. Sometimes we use the notation (x) and then we always refer to the ideal $x\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. For the readers convenience we start by citing some well-known number theory results. Firstly, as $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ is a Dedekind ring, each ideal $\mathfrak{a}\neq(1)$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ can be uniquely written as a product of non-zero prime ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. Thus, we determine the prime ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ and for this we use the following.

Lemma 3.5. *[Neu99, 44] Let K be a number field. Then every prime ideal $\mathfrak{p}\neq 0$ of $\mathcal{O}_K$ contains a rational prime number p and is therefore a divisor of the ideal $p\mathcal{O}_K$.*

Now we describe the prime ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. This has been studied generally for quadratic number fields for instance in [Pin24, Example 6.2.6] and [Con24]. In the special case of $\mathbb{Q}(\sqrt{5})$ we have the following.

Proposition-Definition 3.4. *The non-zero prime ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ are exactly*

a unique prime ideal $\mathfrak{q}_5$ of norm 5,
two distinct prime ideals $\mathfrak{q}_p$ and $\bar{\mathfrak{q}}_p$ of norm p, for p prime such that $p\equiv\pm1$ mod 5,
the unique prime ideal (p) of norm p^2, for p prime such that $p\equiv 2,3$ mod 5.

Moreover, we have $\mathfrak{q}_5^2=(5)$ and $\mathfrak{q}_p\bar{\mathfrak{q}}_p=(p)$ for p prime such that $p\equiv\pm1$ mod 5.

Proof. From Lemma 3.5 we see that all prime ideals occur in the prime factorizations of the ideals $p\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ for all $p \in \mathbb{Z}$ prime. Now, for $p \neq 2$ it is known (see for example [Pin24, Example 6.2.6]) that the prime factorization of the ideal $p\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ is given by the Legendre symbol. We have

$$p\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \begin{cases} \mathfrak{q}_p^2 \text{ is totally ramified} & \text{if } \left(\frac{5}{p}\right) = 0, \\ \mathfrak{q}_p\bar{\mathfrak{q}}_p \text{ is totally split} & \text{if } \left(\frac{5}{p}\right) = +1, \\ p\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \text{ is inert} & \text{if } \left(\frac{5}{p}\right) = -1. \end{cases}$$

In particular, $\left(\frac{5}{p}\right) = 0$ if and only if $p = 5$ and this is the first claimed case so assume for the rest $p \neq 5$. Now, as $p \neq 2, 5$ by Gauss's quadratic reciprocity law we have $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Now, $\left(\frac{p}{5}\right) = \pm 1$ depending on whether p is a quadratic residue modulo 5. Indeed, p is a quadratic residue modulo 5 if $p \equiv \pm 1 \bmod 5$ and it is not in the remaining cases $p \equiv 2, 3 \bmod 5$. For the case $p = 2 (\equiv 2 \bmod 5)$ one can deduce from the Dedekind-Kummer-theorem that $2\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ indeed remains prime as the minimal polynomial of β, which is $X^2 - X - 1$, is irreducible modulo 2. □

Remark 3.6. *The conjugation* $\bar{\mathfrak{q}}$ *for the prime ideals in Proposition-Definition 3.4 is taken from Conrad [Con24, Definition 4.20]. Indeed, for* p *prime,* $p \equiv \pm 1$ *mod* 5 *we have* $\sigma(\mathfrak{q}_p) = \bar{\mathfrak{q}}_p$*, where* $\sigma \in Hom_{\mathbb{Q}}(\mathbb{Q}(\sqrt{5}), \mathbb{C})$ *is the conjugation map given by* $\sqrt{5} \mapsto -\sqrt{5}$*. This can be shown abstractly as in [Pin24, Theorem 6.3.2] noting that* $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ *is galois.*

Corollary 3.5. *The non-zero ideals in* $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ *of a given norm* $m \in \mathbb{Z}_{>0}$ *with prime factorization* $m = 5^{\lambda_5} p_1^{\lambda_{p_1}} \cdots p_t^{\lambda_{p_t}} q_1^{\lambda_{q_1}} \cdots q_s^{\lambda_{q_s}}$*, for* $\lambda_* \in \mathbb{Z}_{\geq 0}$ *and with distinct primes* $p_i \equiv \pm 1$ *mod* 5*, and* $q_i \equiv 2, 3$ *mod* 5*, are precisely the ideals of the form*

$$I_{\underline{\mu}}^{(m)} := \mathfrak{q}_5^{\lambda_5} \mathfrak{q}_{p_1}^{\mu_{p_1}} \bar{\mathfrak{q}}_{p_1}^{\bar{\mu}_{p_1}} \cdots \mathfrak{q}_{p_t}^{\mu_{p_t}} \bar{\mathfrak{q}}_{p_t}^{\bar{\mu}_{p_t}} (q_1)^{\lambda_{q_1}/2} \cdots (q_s)^{\lambda_{q_s}/2}, \text{ with } I_{\underline{\mu}}^{(1)} := (1), \text{ and}$$

for $\mu_*, \bar{\mu}_* \in \mathbb{Z}_{\geq 0}$ *such that* $\mu_{p_j} + \bar{\mu}_{p_j} = \lambda_{p_j}$ *and when* λ_{q_j} *are even and none otherwise. Moreover, if the* λ_{q_j} *are even, then the ideals* $I_{\underline{\mu}}^{(m)}, I_{\underline{\mu}'}^{(m)}$ *are distinct for* $\underline{\mu} \neq \underline{\mu}'$ *and there are* $(\lambda_{p_1}+1)\cdots(\lambda_{p_t}+1)$ *distinct ideals of norm* m*.*

Proof. This follows from unique factorization of ideals [Neu99, (3.3) Theorem], the description of prime ideals in Proposition-Definition 3.4 and the multiplicativity of the absolute norm. □

Next, we introduce the notion of a primitive ideal. These ideals turn out to be connected to the primitive integer solutions of $x^2 + xy - y^2 = m$.

Definition 3.6. *(Rephrased from and equivalent to [Coh78, Definition 14.11].) We call an ideal* $I \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ *a* primitive ideal *if for all prime numbers* p *we have* $p\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \nmid I$*, i.e.* $I \nsubseteq p\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$*.*

The next lemma gives an equivalent description of a primitive ideal which will be used in the proof of Lemma 3.8.

Lemma 3.7. *An ideal* $I \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ *is a primitive ideal if and only if*

- $\mathfrak{q}_5^2 \nmid I$*,*
- $\forall q$ *prime such that* $q \equiv 2, 3$ *mod* 5 *we have* $(q) \nmid I$*, and*
- $\forall p$ *prime such that* $p \equiv \pm 1$ *mod* 5 *we have* $\mathfrak{q}_p \nmid I$ *or* $\bar{\mathfrak{q}}_p \nmid I$*.*

Proof. For an ideal I we have $(p) \mid I$ if and only if (p) appears in the unique factorization of I. Thus, the result follows from unique factorization of ideals [Neu99, (3.3) Theorem] and the description of prime ideals in Proposition-Definition 3.4. □

Next we describe all primitive ideals of a fixed norm.

Lemma 3.8. (Primitive ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$). *Let $m \in \mathbb{Z}_{>0}$ with prime factorization*

$$m = 5^{\lambda_5} p_1^{\lambda_{p_1}} \cdots p_t^{\lambda_{p_t}} q_1^{\lambda_{q_1}} \cdots q_s^{\lambda_{q_s}},$$

for some $\lambda_* \in \mathbb{Z}_{\geq 0}$ and with distinct primes $p_i \equiv \pm 1 \bmod 5$, and $q_i \equiv 2,3 \bmod 5$. If $s > 0$ or $\lambda_5 \geq 2$, then there are no primitive ideals of absolute norm equal to m. Otherwise, $s = 0$ and $\lambda_5 \leq 1$ and the primitive ideals of absolute norm equal to m are the ideals of the form

$$\mathfrak{q}_5^{\lambda_5} \mathfrak{q}_{p_1}^{\mu_{p_1}} \bar{\mathfrak{q}}_{p_1}^{\bar{\mu}_{p_1}} \cdots \mathfrak{q}_{p_t}^{\mu_{p_t}} \bar{\mathfrak{q}}_{p_t}^{\bar{\mu}_{p_t}},$$

for $\mu_{p_i}, \bar{\mu}_{p_i} \in \{0, \lambda_{p_i}\}$ and $\mu_{p_i} + \bar{\mu}_{p_i} = \lambda_{p_i}$. Moreover, in that case there are 2^t distinct primitive ideals.

Proof. By Corollary 3.5 the ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ are of the form $I_{\underline{\mu}}^{(m)}$ with $\mu_*, \bar{\mu}_* \in \mathbb{Z}$ such that $\mu_{p_j} + \bar{\mu}_{p_j} = \lambda_{p_j}$ and when λ_{q_j} are even. By Lemma 3.7 such an ideal is a primitive ideal if and only if

- $\mathfrak{q}_5^2 \nmid I$, so we need $\lambda_5 \leq 1$,
- $\forall q$ prime such that $q \equiv 2,3 \bmod 5$ have $(q) \nmid I$, so we need that the corresponding λ_* are 0, and
- $\forall p$ prime such that $p \equiv \pm 1 \bmod 5$ have $\mathfrak{q}_p \nmid I$ or $\bar{\mathfrak{q}}_p \nmid I$. For this we need $\mu_{p_i}, \bar{\mu}_{p_i} \in \{0, \lambda_{p_i}\}$.

Moreover, in that case there are 2^t such ideals as there are 2^t choices for $\mu_{p_j}, \bar{\mu}_{p_j} \in \{0, \lambda_{p_j}\}$ to satisfy $\mu_{p_j} + \bar{\mu}_{p_j} = \lambda_{p_j}$. □

3.F. Solvability and solutions

In this section we describe the connection between the (primitive) integer solutions to $x^2+xy-y^2 = m$ and the (primitive) ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. We start by observing that if (x, y) is an integer solution to $x^2+xy-y^2 = m$, then also $(u, v) := (x+y, x+2y)$ is one. Indeed, these two solutions are related. Observe that we have $(u, v)^T = A_1^{-1}(x, y)^T$ and $(x, y)^T = A_1(u, v)^T = (2u - v, -u + v)$. Also note that $(x+y, x+2y) = (x, y) \boxdot (1, 1)$ where $(1, 1)$ corresponds with (3.3) to $1 + \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. In this sense the solutions (x, y) and (u, v) are connected. This motivates an equivalence relation on the solution set $\mathbb{P}_{\mathbb{Z}}(m)$ which will be used to derive Theorem 3.13. We show more ways to understand this in Section 4.

Definition 3.7. *For any fixed $m \in \mathbb{R}$ we define an equivalence relation $\sim$ on the solutions set $\mathbb{P}_{\mathbb{Z}}(m)$ by*

$$(x, y) \sim (u, v) :\Leftrightarrow \exists \xi \in \{\pm 1\}, k \in \mathbb{Z} : u + v\beta = \xi(x + y\beta)\beta^{2k}. \tag{3.4}$$

In the same way we define an equivalence relation on the primitive integer solution set $\mathbb{P}_{\mathbb{Z}}^{pr}(m)$, and also denote it by $\sim$. Equivalence classes are indicated with square brackets as usual.

Remark 3.9. *We can equivalently write the condition in equation (3.4) in two other ways as*

$$(x, y) \sim (u, v) \iff \exists \xi \in \{\pm 1\}, k \in \mathbb{Z} : (u, v) = \xi(x, y) \boxdot (1, 1)^{\boxdot k},$$

and

$$(x, y) \sim (u, v) \iff \exists \xi \in \{\pm 1\}, k \in \mathbb{Z} : \begin{pmatrix} u \\ v \end{pmatrix} = \xi A_1^k \begin{pmatrix} x \\ y \end{pmatrix}.$$

Remark 3.10. *It is easy to verify that if $(x, y), (u, v) \in \mathbb{P}_{\mathbb{Z}}(m)$ are such that $(x, y) \sim (u, v)$, then $(x, y) \in \mathbb{P}_{\mathbb{Z}}^{pr}(m)$ if and only if $(u, v) \in \mathbb{P}_{\mathbb{Z}}^{pr}(m)$. Hence, the relation $\sim$ on $\mathbb{P}_{\mathbb{Z}}^{pr}(m)$ is just the restriction of $\sim$ on $\mathbb{P}_{\mathbb{Z}}(m)$ to $\mathbb{P}_{\mathbb{Z}}^{pr}(m)$.*

Next, we define the *norm-m-generator* of an ideal, which we need in the proof of Theorem 3.13 below.

Definition 3.8. *If* $m \in \mathbb{Z}$ *and* $I \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ *is an ideal of absolute norm* $|m|$*, then we call an element* $x+y\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ *such that* $I=(x+y\beta)$ *and* $N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(x+y\beta)=m$*, a* norm-$m$-generator of I.

Norm-m-generators exist but to show this we need the following basic result from algebra.

Lemma 3.11. *Let* R *be an integral domain. Then* $(a)=(b)$ *if and only if* $b=ua$ *for some* $u \in R^\times$.

Lemma 3.12. *If* $m \in \mathbb{Z}$ *and* $I \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ *is an ideal of absolute norm* $|m|$*, then there exists a norm-*m*-generator of* I.

Proof. As $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ is a PID, we can write $I=(z)$ for some $z=a+b\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, i.e. $a,b \in \mathbb{Z}$. Additionally, we have $|\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(a+b\beta)| = \mathrm{N}(I) = |m|$, so $\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(a+b\beta) = \pm m$. Moreover, the element βz also generates the ideal I by Lemma 3.11 as $\beta \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{5})}$ and it has norm $\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(\beta)\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(z) = (-1)\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(z) = \mp m$. So either z or βz is a norm-m-generator of I. □

Now we can state the key theorem of this section.

Theorem 3.13. (Equivalence classes of solutions and ideals). *Let* $m \in \mathbb{Z}\setminus\{0\}$*. Then we have bijections*

$$\begin{aligned} \mathbb{P}_{\mathbb{Z}}(m)/_{\sim} &\longrightarrow \{\textit{Ideals in } \mathcal{O}_{\mathbb{Q}(\sqrt{5})} \textit{ of absolute norm equal to } |m|\} \\ [(x,y)] &\longmapsto (x+y\beta) = (x+y\beta)\mathcal{O}_{\mathbb{Q}(\sqrt{5})}, \end{aligned} \tag{a}$$

and

$$\begin{aligned} \mathbb{P}^{pr}_{\mathbb{Z}}(m)/_{\sim} &\longrightarrow \{\textit{Primitive ideals in } \mathcal{O}_{\mathbb{Q}(\sqrt{5})} \textit{ of absolute norm equal to } |m|\} \\ [(x,y)] &\longmapsto (x+y\beta) = (x+y\beta)\mathcal{O}_{\mathbb{Q}(\sqrt{5})}. \end{aligned} \tag{b}$$

Proof. Denote the respective maps by ψ and ψ^{pr}.

- The maps ψ and ψ^{pr} are well defined: Let $(x,y),(u,v) \in \mathbb{P}_{\mathbb{Z}}(m)$ such that $(x,y)\sim(u,v)$. So $u+v\beta = (x+y\beta)(\pm\beta^{2k})$. Now, $\pm\beta^{2k} \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{5})}$, and by Lemma 3.11 we get that

$$\psi([(x,y)]) = (x+y\beta) = (u+v\beta) = \psi([(u,v)]).$$

  Moreover, we have $\mathrm{N}((x+y\beta)) = |\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(x+y\beta)| = |m|$, for $(x,y) \in \mathbb{P}_{\mathbb{Z}}(m)$. Finally, it remains to show that if $(x,y) \in \mathbb{P}^{\mathrm{pr}}_{\mathbb{Z}}(m)$, then $I=\psi^{\mathrm{pr}}((x+y\beta))$ is a primitive ideal. Indeed, suppose for some p prime we have $(p) \mid I$. Now, this is equivalent to $p \mid x+y\beta$ which in turn is only possible if $p \mid x,y$. This contradicts $\gcd(x,y)=1$ as (x,y) is a primitive solution.

- We define maps ρ and ρ^{pr} in the other direction: Let $I \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ be an ideal of absolute norm equal to $|m|$. Then by Lemma 3.12 there exists a norm-m-generator $x+y\beta$ of I. We map I to $[(x,y)]$. This is well defined. Firstly, we have $(x,y) \in \mathbb{P}_{\mathbb{Z}}(m)$ as $x^2+xy-y^2 = \mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(x+y\beta) = m$. Next, if $u+v\beta$ is another norm-m-generator of I, then by Lemma 3.11 we get that $u+v\beta = (x+y\beta)w$ for $w \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{5})}$. Now, as β is a fundamental unit, we can write $w=\xi\beta^k$ for some $\xi \in \{\pm 1\}$ and $k \in \mathbb{Z}$. Thus, $u+v\beta = \xi(x+y\beta)\beta^k$. As $\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(\beta) = -1$ and $\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(x+y\beta) = m = \mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(u+v\beta)$ by the multiplicativity of the norm we must have $k=2k'$ is even. Thus, $(x,y)\sim(u,v)$ and so $[(x,y)]=[(u,v)]$. Next, if I is a primitive ideal, then we claim that for any norm-m-generator $x+y\beta$ of I the solution (x,y) is primitive. Indeed, suppose this is not the case. Then there exists a prime p such that $p \mid x,y$. But then $p \mid x+y\beta$ so $(p) \mid I$ a contradiction to I being a primitive ideal.

- The maps are mutual inverses: Let $[(x, y)] \in \mathbb{P}_{\mathbb{Z}}(m)/\!\sim$ and $I \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ be an ideal of absolute norm $|m|$. We have
$$\rho(\psi([(x, y)])) = \rho(I = (x + y\beta)) = [(x, y)],$$
and if $x + y\beta$ is a norm-m-generator of I then
$$\psi(\rho(I)) = \psi([(x, y)]) = (x + y\beta) = I. \qquad \square$$

Using Theorem 3.13 we can determine (primitive) integer solvability of $x^2 + xy - y^2 = m$. Thus, we can now state and prove both Theorem 1.1 and Theorem 1.2 in the introduction.

Theorem 3.14. (Solvability). *[OSIS24a, Conjecture] and [OEIS24b, "Formula"]. Let $m \in \mathbb{Z}\backslash\{0\}$ with prime factorization $m = 5^{\lambda_5} p_1^{\lambda_{p_1}} \cdots p_t^{\lambda_{p_t}} q_1^{\lambda_{q_1}} \cdots q_s^{\lambda_{q_s}}$, with distinct primes $p_i \equiv \pm 1 \bmod 5$, $q_i \equiv 2, 3 \bmod 5$. Then*

(a) there exists an integer solution to $x^2 + xy - y^2 = m$ if and only if all the λ_{q_i} are even.

(b) there exists a primitive integer solution to $x^2 + xy - y^2 = m$ if and only if $\lambda_5 \leq 1$ and $s = 0$.

Proof. We note that $\mathbb{P}_{\mathbb{Z}}(m) \neq \emptyset$ if and only if $\mathbb{P}_{\mathbb{Z}}(m)/\!\sim \neq \emptyset$ and analogously $\mathbb{P}^{\text{pr}}_{\mathbb{Z}}(m) \neq \emptyset$ if and only if $\mathbb{P}^{\text{pr}}_{\mathbb{Z}}(m)/\!\sim \neq \emptyset$. Thus, the result follows using Theorem 3.13, Corollary 3.5 and Lemma 3.8. $\square$

Theorem 3.13 also allows us to describe the solutions as follows. Every ideal I of absolute norm $|m|$ corresponds to the equivalence class of integer solutions to $x^2 + xy - y^2 = m$ given by any norm-m-generator $x + y\beta$ of I. Using this we get the following.

Theorem 3.15. (Solution 1). *Fix $m \in \mathbb{Z}\backslash\{0\}$ and let $x_1 + y_1\beta, \ldots, x_\ell + y_\ell\beta$ be norm-m-generators of each of the ℓ ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ of absolute norm $|m|$. Then $\mathbb{P}_{\mathbb{Z}}(m)$ is the disjoint union of the sets*
$$\{\xi(x_i, y_i) \boxdot (1, 1)^{\boxdot j} : j \in \mathbb{Z}, \xi \in \{\pm 1\}\}, \text{ for } i = 1, \ldots, \ell.$$
Moreover, if without loss of generality $x_1 + y_1\beta, \ldots, x_k + y_k\beta$ are the norm-m-generators of the absolute norm $|m|$ primitive ideals, then $\mathbb{P}^{pr}_{\mathbb{Z}}(m)$ is the disjoint union of the sets
$$\{\xi(x_i, y_i) \boxdot (1, 1)^{\boxdot j} : j \in \mathbb{Z}, \xi \in \{\pm 1\}\}, \text{ for } i = 1, \ldots, k.$$

Proof. As $\sim$ is an equivalence relation, the set $\mathbb{P}_{\mathbb{Z}}(m)$ is the disjoint union of the $\sim$ equivalence classes. Now, by Theorem 3.13 each equivalence class is represented by any norm-m-generator $x+y\beta$ of the corresponding (primitive) ideal. Finally, for any other element (u, v) of the equivalence class we have by definition
$$u + v\beta = \xi(x + y\beta)\beta^{2j},$$
for some $\xi \in \{\pm 1\}$ and $j \in \mathbb{Z}$. Now, $\beta^2 = \beta + 1$ so we can write $u + v\beta = \xi(x + y\beta)(1 + 1\beta)^j$. Using the bijection (3.3) this corresponds to $(u, v) = \xi(x, y) \boxdot (1, 1)^{\boxdot j}$, and so the equivalence class of (x, y) is
$$\{\xi(x, y) \boxdot (1, 1)^{\boxdot j} : j \in \mathbb{Z}, \xi \in \{\pm 1\}\}$$
which is of the desired form and the result follows. $\square$

We can also see the solutions as "built up" based on the prime factorization of m as follows.

Theorem 3.16. (Solution 2). *Let $m \in \mathbb{Z}\backslash\{0\}$ with prime factorization $m = 5^{\lambda_5} p_1^{\lambda_{p_1}} \cdots p_t^{\lambda_{p_t}} q_1^{\lambda_{q_1}} \cdots q_s^{\lambda_{q_s}}$, with primes $p_i \equiv \pm 1 \bmod 5$, $q_i \equiv 2, 3 \bmod 5$.*

(a) If for some i the exponent λ_{q_i} is odd, then there are no integer solutions to $x^2 + xy - y^2 = m$.

(b) *Otherwise, all prime factors* q_i *have even exponents. In this case the integer solutions to* $x^2+xy-y^2=m$ *are* $(x,y)\in\mathbb{Z}^2$ *of the form*

$$z^{(m)}_{\underline{\mu},k} := (x_5,y_5)^{\boxdot\lambda_5}\boxdot(x_{p_1},y_{p_1})^{\boxdot\mu_{p_1}}\boxdot\overline{(x_{p_1},y_{p_1})}^{\boxdot\overline{\mu}_{p_1}}\boxdot\ldots\boxdot(x_{p_t},y_{p_t})^{\boxdot\mu_{p_t}}\boxdot\overline{(x_{p_t},y_{p_t})}^{\boxdot\overline{\mu}_{p_t}}\boxdot(q_1,0)^{\boxdot\lambda_{q_1}/2}\boxdot\ldots\boxdot(q_s,0)^{\boxdot\lambda_{q_s}/2}\boxdot(0,1)^{\boxdot\gamma}\boxdot(1,1)^{\boxdot k},$$

where $\mu_{p_i},\overline{\mu}_{p_i}\in\mathbb{Z}\cap[0,\lambda_{p_i}]$ *are such that* $\mu_{p_i}+\overline{\mu}_{p_i}=\lambda_{p_i}$, $k\in\mathbb{Z}$ *and* $\gamma=0$ *for* $m>0$ *and* $\gamma=1$ *for* $m<0$, *and the* x_p,y_p *for* $p\in\{5,p_1,\ldots,p_t\}$ *are such that* $x_p+y_p\beta$ *are norm-*p*-generators of* $\mathfrak{q}_p$. *Moreover,* $z^{(m)}_{\underline{\mu},k}\neq z^{(m)}_{\underline{\mu}',k'}$, *for* $(\underline{\mu},k)\neq(\underline{\mu}',k')$.

(c) *There exist primitive integer solutions if and only if* $s=0$ *and* $\lambda_5\leq 1$, *and in this case they are those* $z^{(m)}_{\underline{\mu},k}$ *that in addition to the requirements in* (b) *satisfy* $\mu_{p_i},\overline{\mu}_{p_i}\in\{0,\lambda_{p_i}\}$, *that is either* $\mu_{p_i}=0$ *or* $\overline{\mu}_{p_i}=0$.

Proof. (a) Was already shown in Theorem 3.14. (b) Writing $z^{(m)}_{\underline{\mu},k}=(x^{(m)}_{\underline{\mu},k},y^{(m)}_{\underline{\mu},k})$ we show that the element $x^{(m)}_{\underline{\mu},0}+y^{(m)}_{\underline{\mu},0}\beta$ is a norm-m-generator of the ideal $I^{(m)}_{\underline{\mu}}$. By Corollary 3.5, the ideals of absolute norm $|m|$ are exactly the $I^{(m)}_{\underline{\mu}}$ with the same conditions for μ_* as in (b) for the $z^{(m)}_{\underline{\mu},k}$. Thus, since $z^{(m)}_{\underline{\mu},k}=z^{(m)}_{\underline{\mu},0}\boxdot(1,1)^k$, the result then follows from Theorem 3.15. Firstly, by multiplicativity of the norm $\mathrm{N}:=\mathrm{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}$ and with σ as in Remark 3.6 we have

$$\begin{aligned}\mathrm{N}(z^{(m)}_{\underline{\mu},0}) &= \mathrm{N}(x^{(m)}_{\underline{\mu},0}+y^{(m)}_{\underline{\mu},0}\beta)\\ &= \mathrm{N}(x_5+y_5\beta)^{\lambda_5}\prod_{i=1}^{t}\mathrm{N}(x_{p_i}+y_{p_i}\beta)^{\mu_{p_i}}\mathrm{N}(\sigma(x_{p_i}+y_{p_i}\beta))^{\bar{\mu}_{p_i}}\prod_{j=1}^{s}\mathrm{N}(q_j)^{\lambda_{q_j}/2}\mathrm{N}(\beta^\gamma)\\ &= 5^{\lambda_5}\prod_{i=1}^{t}p_i^{\mu_{p_i}}p_i^{\overline{\mu}_{p_i}}\prod_{j=1}^{s}(q_j^2)^{\lambda_{q_j}/2}(-1)^\gamma = m,\end{aligned}$$

where in the second line we used that $\sigma(x_{p_i}+y_{p_i}\beta)$ corresponds to $\overline{(x_{p_i},y_{p_i})}$ and the connection of $\boxdot$ with multiplication in $\mathbb{Q}(\sqrt{5})$ and in the third line we used that $\mathrm{N}(x_{p_*}+y_{p_*}\beta)=p_*$. Next, by Remark 3.6 we have $\bar{\mathfrak{q}}_{p_i}=\sigma(\mathfrak{q}_{p_i})=\sigma((x_{p_i}+y_{p_i}\beta))=(\sigma(x_{p_i}+y_{p_i}\beta))$, and using this, the correspondence $\sigma(x_{p_i}+y_{p_i}\beta)\equiv\overline{(x_{p_i},y_{p_i})}$, and the definition of $\boxdot$ we get

$$\begin{aligned}I^{(m)}_{\underline{\mu}} &= \mathfrak{q}_5^{\lambda_5}\mathfrak{q}_{p_1}^{\mu_{p_1}}\bar{\mathfrak{q}}_{p_1}^{\bar{\mu}_{p_1}}\cdots\mathfrak{q}_{p_t}^{\mu_{p_t}}\bar{\mathfrak{q}}_{p_t}^{\bar{\mu}_{p_t}}(q_1)^{\lambda_{q_1}/2}\cdots(q_s)^{\lambda_{q_s}/2}\\ &= (x_5+y_5\beta)^{\lambda_5}\prod_{i=1}^{t}(x_{p_i}+y_{p_i}\beta)^{\mu_{p_i}}\,(\sigma(x_{p_i}+y_{p_i}\beta))^{\bar{\mu}_{p_i}}\prod_{j=1}^{s}(q_j)^{\lambda_{q_j}/2}(\beta^\gamma)\\ &= \Big((x_5+y_5\beta)^{\lambda_5}\prod_{i=1}^{t}(x_{p_i}+y_{p_i}\beta)^{\mu_{p_i}}\sigma(x_{p_i}+y_{p_i}\beta)^{\bar{\mu}_{p_i}}\prod_{j=1}^{s}(q_j)^{\lambda_{q_j}/2}(\beta^\gamma)\Big) = \big(x^{(m)}_{\underline{\mu},0}+y^{(m)}_{\underline{\mu},0}\beta\big).\end{aligned}$$

Altogether, $x^{(m)}_{\underline{\mu},0}+y^{(m)}_{\underline{\mu},0}\beta$ is a generator of $I^{(m)}_{\underline{\mu}}$ and by the first computation above it has norm m. For (b) it remains to show that $z^{(m)}_{\underline{\mu},k}\neq z^{(m)}_{\underline{\mu}',k'}$ for $(\underline{\mu},k)\neq(\underline{\mu}',k')$. Indeed, suppose $z^{(m)}_{\underline{\mu},k}=z^{(m)}_{\underline{\mu}',k'}$. Then

$$I^{(m)}_{\underline{\mu}}=(z^{(m)}_{\underline{\mu},k})=(z^{(m)}_{\underline{\mu}',k'})=I^{(m)}_{\underline{\mu}'},$$

which by unique factorization of ideals ([Neu99, (3.3) Theorem]) is only possible for $\mu=\mu'$. Next, we also need $k=k'$ as

$$\big|z^{(m)}_{\underline{\mu},k}\big|=\big|z^{(m)}_{\underline{\mu},0}\big|\,|\beta|^{2k+\gamma}\quad\text{and}\quad|\beta|>1,$$

so all the absolute values are distinct for k distinct.

(c) If $s=0$ and $\lambda_5\leq 1$, then the primitive ideals are the $I^{(m)}_{\underline{\mu}}$ with $\mu_{p_i}+\overline{\mu}_{p_i}\in\{0,\lambda_{p_i}\}$. Their generators correspond to the $z^{(m)}_{\underline{\mu},k}$ with $\mu_{p_i}+\overline{\mu}_{p_i}\in\{0,\lambda_{p_i}\}$ by the above computation. □

4. Generating integer solutions

In Section 3 we have seen that if (x, y) is an integer solution to $x^2 + xy - y^2 = m$, then other solutions can be obtained by

$$(x', y') = \xi(x, y) \boxdot (1, 1)^{\boxdot k}$$

for $\xi \in \{\pm 1\}$ and $k \in \mathbb{Z}$. For $\xi = 1$ and $k = -1$ this is

$$(x', y') = (x, y) \boxdot (1, 1)^{\boxdot(-1)} = (2x - y, -x + y),$$

which corresponds to multiplying (x, y) by the matrix A_1. The parametrisation from Section 2 has the following property.

Proposition 4.1. *Let $\beta = (1 + \sqrt{5})/2$. Then*

$$A_1\mathcal{P}_m(s,t) = \mathcal{P}_m(s, t - 2\ln\beta) \text{ if } m > 0, \qquad A_1\mathcal{P}_m(s,t) = \mathcal{P}_m(s, t + 2\ln\beta) \text{ if } m < 0,$$
$$A_1^{-1}\mathcal{P}_m(s,t) = \mathcal{P}_m(s, t + 2\ln\beta) \text{ if } m > 0, \qquad A_1^{-1}\mathcal{P}_m(s,t) = \mathcal{P}_m(s, t - 2\ln\beta) \text{ if } m < 0.$$

Proof. It is straightforward to verify the relations when the hyperbolic functions are expressed by the exponential function. □

Thus, if there exists an integer solution to $x^2 + xy - y^2 = m$, then there must be an integer solution in any set

$$J_m(a) := P_m\left([a, a + 2\ln(\beta)) \right) = \{P_m(t) : a \le t < a + 2\ln(\beta)\}$$

for $a \in \mathbb{R}$. Indeed, let more generally $(x, y) \in \mathbb{P}_{\mathbb{R}}(m)$. Then using the parametrisation from Section 2 we can write $(x, y) = \mathcal{P}_m(s, t)$ for unique $s \in \{\pm 1\}$ and $t \in \mathbb{R}$. Then by Proposition 4.1 we have

$$sA_1^{\xi k}\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in J_m(a) \text{ for } k = \left\lfloor \frac{t - a}{2\ln(\beta)} \right\rfloor, \text{ and } \xi = \begin{cases} +1 & \text{if } m > 0, \\ -1 & \text{if } m < 0. \end{cases}$$

In particular, if $(x, y) \in \mathbb{P}_{\mathbb{Z}}(m)$, then also $A_1^{\xi k}\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in \mathbb{P}_{\mathbb{Z}}(m)$ because A_1 and all its integer powers have integer coefficients (observe that $\det(A_1) = 1$ so A_1^{-1} also has integer coefficients). Using this "interval" observation we obtain the following.

Proposition-Definition 4.2. *Fix $m \in \mathbb{R} \setminus \{0\}$.*

- *If $m > 0$ and $\mathbb{P}_{\mathbb{Z}}(m) \neq \emptyset$, then*

$$F_m := \mathbb{P}_{\mathbb{Z}}(m) \cap \left([2\sqrt{\frac{m}{5}}, \sqrt{m}] \times [0, \sqrt{m}) \right) \neq \emptyset.$$

- *If $m < 0$ and $\mathbb{P}_{\mathbb{Z}}(m) \neq \emptyset$, then*

$$F_m := \mathbb{P}_{\mathbb{Z}}(m) \cap \left((-\sqrt{m}, 0] \times [2\sqrt{\frac{m}{5}}, \sqrt{m}] \right) \neq \emptyset.$$

Moreover, for any $m \in \mathbb{R} \setminus \{0\}$, we have

$$\mathbb{P}_{\mathbb{Z}}(m) = \bigsqcup_{(x,y) \in F_m} \{\pm A_1^k(x, y)^T : k \in \mathbb{Z}\},$$

with a disjoint union as indicated by $\sqcup$. That is, any integer solution to $x^2 + xy - y^2 = m$ is of the form $(u, v)^T = \pm A_1^k(x, y)^T$, for a unique $(x, y) \in F_m$. In other words, the set F_m contains exactly one representative for each equivalence class of solutions with respect to the relation $\sim$ as in Definition 3.7.

Proof. As usual we start with the case $m>0$. We first claim that

$$F_m = \mathbb{P}_{\mathbb{Z}}(m) \cap \{P_m(t) : t^{(+)}_{Y=0} \le t < t^{(+)}_{X=Y}\}, \tag{4.5}$$

where $t^{(+)}_{Y=0} = -\ln(\beta)/2$, $t^{(+)}_{X=Y} = 3/2\ln(\beta)$ are as in Proposition-Definition 2.1 that is we have $P_m(t^{(+)}_{Y=0}) = (\sqrt{m},0)$ and $P_m(t^{(+)}_{X=Y}) = (\sqrt{m},\sqrt{m})$. This follows from Proposition-Definition 2.1 and Lemma 2.2. Now, using (4.5) and the interval observation above we get that if $(x,y)\in\mathbb{P}_{\mathbb{Z}}(m)$ there exist unique $s\in\{\pm1\}$ and $k\in\mathbb{Z}$ such that

$$sA_1^k\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) \in F_m, \tag{4.6}$$

where we use that $t^{(+)}_{X=Y} - t^{(+)}_{Y=0} = 2\ln(\beta)$ so the "interval" $[t^{(+)}_{Y=0}, t^{(+)}_{X=Y})$ is wide enough for this to work. In particular, this shows that $\mathbb{P}_{\mathbb{Z}}(m)\neq\emptyset$ implies $F_m\neq\emptyset$. On the other hand, we can rewrite equation (4.6) by multiplying on both sides with A_1^{-k} to get $\mathbb{P}_{\mathbb{Z}}(m)\ni\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) = sA_1^{-k}\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$, for an also unique $(u,v)\in F_m$ proving the last part of the proposition. For the case $m<0$ we have $\mathbb{P}_{\mathbb{Z}}(m) = R_{\pm}\mathbb{P}_{\mathbb{Z}}(-m)$ for the matrix $R_{\pm}$ as in Section 2 and one can check that $F_m = R_{\pm}F_{-m}$ so the results follow from the $m>0$ case. □

Next, we observe that if $(x,y)\in\mathbb{Z}^2$ is a solution, then also $A_{(*)}\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)$ is an integer solution. Moreover, for $m\in\mathbb{R}_{>0}$ and any $t\in\mathbb{R}$ and $s\in\{\pm1\}$ we have

$$A_{(*)}\mathcal{P}_m(s,t) = \mathcal{P}_m(s,-t+\ln(\beta)). \tag{4.7}$$

Proof. This can be verified similarly to Proposition 4.1 by expressing the hyperbolic functions by the exponential function. □

Keeping $m>0$ we can rewrite equation (4.7) in the form

$$A_{(*)}P_m(t) = P_m(\ln(\beta)/2 - (t-\ln(\beta)/2)).$$

So we see that $A_{(*)}$ maps the interval $(-\ln(\beta)/2, 3/2\ln(\beta))$ of $\mathbb{P}_{\mathbb{R}}(m)$ to itself. In particular, $P_m(t^{(m)}_{\min} = \ln(\beta)/2) = (2\sqrt{\frac{m}{5}}, \sqrt{\frac{m}{5}})$ is the midpoint of this interval so it is a fixed point of $A_{(*)}$. With this we obtain the following.

Proposition 4.3. *Fix $m\in\mathbb{R}_{>0}$. If $\mathbb{P}_{\mathbb{Z}}(m)\neq\emptyset$, then*

$$\tilde{F}^{\downarrow}_m := \mathbb{P}_{\mathbb{Z}}(m)\cap\left([2\sqrt{\frac{m}{5}},\sqrt{m}]\times[0,\sqrt{\frac{m}{5}}]\right)\neq\emptyset,$$

and

$$\tilde{F}^{\uparrow}_m := \mathbb{P}_{\mathbb{Z}}(m)\cap\left([2\sqrt{\frac{m}{5}},\sqrt{m}]\times[\sqrt{\frac{m}{5}},\sqrt{m}]\right)\neq\emptyset.$$

For $m<0$ similar results can be formulated using the relations $X_{-|m|} = -Y_{|m|}$ and $Y_{-|m|} = X_{|m|}$.

Proof. We start with the case of $m>0$. First note that

$$\tilde{F}^{\downarrow}_m \cup \tilde{F}^{\uparrow}_m = F_m \cup \{P_m(t^{(+)}_{X=Y}) = (\sqrt{m},\sqrt{m})\}. \tag{4.8}$$

Thus, if $\mathbb{P}_{\mathbb{Z}}(m)\neq\emptyset$, then by Proposition 4.2 we have $F_m\neq\emptyset$ and hence by equation (4.8) we have $\tilde{F}^{\downarrow}_m\neq\emptyset$ or $\tilde{F}^{\uparrow}_m\neq\emptyset$. To finish the proof we note that $A_{(*)}$ maps $\tilde{F}^{\downarrow}_m$ bijectively to $\tilde{F}^{\uparrow}_m$. To see this, we claim that

$$\tilde{F}^{\downarrow}_m = P_m([t^{(+)}_{Y=0}, t^{(m)}_{\min}]), \text{ and } \tilde{F}^{\uparrow}_m = P_m([t^{(m)}_{\min}, t^{(+)}_{X=Y}]),$$

which can be shown similarly to the description of F_m using P_m in the proof of Proposition-Definition 4.2. Then using the observation that $A_{(*)}$ bijectively maps $P_m(t)$ to $P_m(\ln(\beta)/2-(t-\ln(\beta)/2))$ we are done. □

5. Geometry of the group operation on the curve $x^2+xy-y^2=m$

In this section we investigate the geometry of the group operation on the curve $x^2+xy-y^2=m$ for fixed $m \in \mathbb{R}\setminus\{0\}$ using an approach from [Lem03]. As a preparation, we start with the algebraic description.

5.A. Algebraic definition

In this section we use the ring structure on $\mathbb{R}^2$ from Section 3.B in order to obtain a group operation on the curves $x^2+xy-y^2=m$. Recall that the ring structure was based on the algebraic properties of the number field $\mathbb{Q}(\sqrt{5})$ as explained in Section 3.A. Fix $m \in \mathbb{R}\setminus\{0\}$. For $A, B, N \in \mathbb{P}_{\mathbb{R}}(m)$ we define

$$A \oplus_N^{\mathrm{Alg}} B := A \boxdot B \boxdot N. \tag{5.9}$$

Proposition 5.1. *The operation (5.9) is well defined and $A\oplus_N^{Alg}B \in \mathbb{P}_{\mathbb{R}}(m)$. For fixed $N \in \mathbb{P}_{\mathbb{R}}(m)$ the tuple $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{Alg}, N)$ is an abelian group with neutral element N.*

Proof. First, as $m \neq 0$ there exists an inverse for N with respect to $\boxdot$ so "$\boxdot N$" is well defined. Next, by multiplicativity of the norm (Lemma 3.2) we have

$$\mathrm{N}(A \boxdot B \boxdot N) = \mathrm{N}(A)\mathrm{N}(B)/\mathrm{N}(N) = m \cdot m/m = m,$$

and hence $A \oplus_N^{\mathrm{Alg}} B \in \mathbb{P}_{\mathbb{R}}(m)$.

By the results from Section 3.B, we know that $(\mathbb{R}^2\setminus\mathbb{P}_{\mathbb{R}}(0), \boxdot)$ defines an abelian group. Thus, the second part of the proposition follows from the first part and the general group theoretic fact that if $(G,*)$ is an abelian group and $n \in G$, then $(G, \tilde{*})$, where $a\tilde{*}b := a*b*n^{(*)-1}$, is an abelian group with neutral element n. □

We can also derive an explicit formula for $A \oplus_N^{\mathrm{Alg}} B$ in terms of the coordinates of A, B, N:

Lemma 5.1. (Explicit formula for $\oplus_N^{\mathrm{Alg}}$). *Fix $m \in \mathbb{R}\setminus\{0\}$ and let $A=(x_A,y_A), B=(x_B,y_B)$, $N=(x_N,y_N) \in \mathbb{P}_{\mathbb{R}}(m)$. Then*

$$A \oplus_N^{\mathrm{Alg}} B = \\ = \frac{1}{m}\big(x_N(x_Ax_B+y_Ay_B)+y_N(x_Ax_B-x_By_A-x_Ay_B), x_N(x_By_A+x_Ay_B+y_Ay_B)-y_N(x_Ax_B+y_Ay_B)\big).$$

Proof. We have

$$\begin{aligned} A \oplus_N^{\mathrm{Alg}} B &= A \boxdot B \boxdot N = \\ &= (x_Ax_B + y_Ay_B, x_By_A + x_Ay_B + y_Ay_B) \boxdot N \\ &= (x_Ax_B + y_Ay_B, x_By_A + x_Ay_B + y_Ay_B) \boxdot \frac{1}{m}(x_N + y_N, -y_N) \\ &= \frac{1}{m}\big(x_N(x_Ax_B+y_Ay_B)+y_N(x_Ax_B-x_By_A-x_Ay_B), x_N(x_By_A+x_Ay_B+y_Ay_B)-y_N(x_Ax_B+y_Ay_B)\big), \end{aligned}$$

as claimed. □

5.B. Geometric definition

In this section we introduce the geometrically defined operation on $\mathbb{P}_{\mathbb{R}}(m)$ using the construction found in [Lem03]. Since the curves are hyperbolas, it follows from elementary geometry that a line in $\mathbb{R}^2$ intersects $\mathbb{P}_{\mathbb{R}}(m)$ in either zero, one or two points, and at any point P of $\mathbb{P}_{\mathbb{R}}(m)$ there is a uniquely defined tangent. Using this we can geometrically define an operation $\oplus_N^{\text{Geo}}$ on $\mathbb{P}_{\mathbb{R}}(m)$ as given by [Lem03, Section 1.1]. We fix a point $N \in \mathbb{P}_{\mathbb{R}}(m)$ which will turn out to be the neutral element. Now, to add two points $A, B \in \mathbb{P}_{\mathbb{R}}(m)$ we proceed as follows: If $A \neq B$, then we take the line $\ell = AB$ connecting A and B. Then $A \oplus_N^{\text{Geo}} B$ is the other intersection with $\mathbb{P}_{\mathbb{R}}(m)$ of the line ℓ_N which is parallel to ℓ and going through N. This case is illustrated in Figure 2 on the left. If $A = B$, then we take the tangent t to $\mathbb{P}_{\mathbb{R}}(m)$ at A as the line ℓ. Then $A \oplus_N^{\text{Geo}} A$ is the

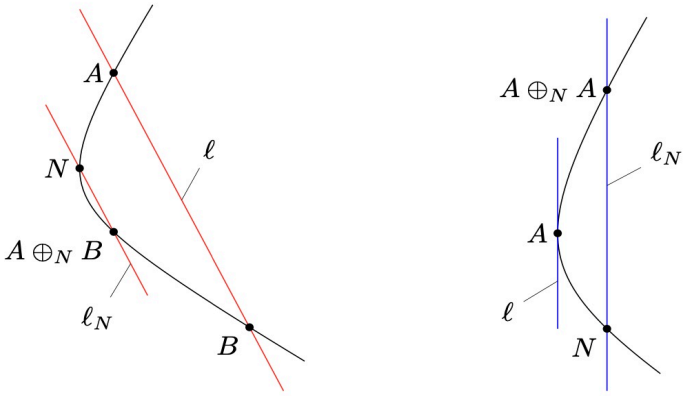

Figure 2: On the left: Geometric construction of $A \oplus_N^{\text{Geo}} B$ for $B \neq A$. The red lines are the line $\ell = AB$ and the parallel line ℓ_N through N. On the right: Geometric construction of $A \oplus_N^{\text{Geo}} A$. The blue lines are the tangent ℓ at A and its parallel through N.

other intersection with $\mathbb{P}_{\mathbb{R}}(m)$ of the parallel line ℓ_N to $\ell = t$ going through the point N. This case is depicted in Figure 2 on the right. It turns out that $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{\text{Geo}}, N)$ is an abelian group (see [Shi09] or [Lem03]). The key observation is the following.

Proposition 5.2. *The geometric operation* $\oplus_N^{Geo}$ *agrees with the algebraic operation* $\oplus_N^{Alg}$. *In particular, the groups* $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{Geo}, N)$ *and* $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{Alg}, N)$ *are isomorphic.*

Proof. Let $A = (x_A, y_A), B = (x_B, y_B), N = (x_N, y_N)$ be points on $\mathbb{P}_{\mathbb{R}}(m)$. Then the coordinates, say (x_C, y_C), of $C := A \oplus_N^{\text{Alg}} B$ are given by Proposition 5.1. The point C is a point on $\mathbb{P}_{\mathbb{R}}(m)$. So, for $A \neq B$, we only have to show that the lines AB and NC are parallel. Indeed, using the formula from Proposition 5.1 and that $x_P^2 + x_P y_P - y_P^2 = m$ for $P \in \{A, B\}$ as $A, B \in \mathbb{P}_{\mathbb{R}}(m)$, a short calculation shows that

$$\begin{cases} (y_A - y_B)(x_N - x_C) = (x_A - x_B)(y_N - y_C) & \text{if } C \neq N, \\ \nabla f(x_N, y_N)(x_A - x_B, y_A - y_B)^T = 0 & \text{if } C = N, \end{cases}$$

where $\nabla f(x, y) = (2x + y, x - 2y)$ is the gradient of $f(x, y) = x^2 + xy - y^2$ at the point (x, y). For the case $A = B \neq N$ we have to show that the scalar product of the vectors $\nabla f(x_A, y_A) = (2x_A + y_A, x_A - 2y_A)$ and $(x_N - x_{AB}, y_N - y_{AB})$ vanishes. A short calculation using that $x_A^2 + x_A y_A - y_A^2 = m$ confirms this. In the remaining case $A = B = N$ we have for both operations $N \oplus_N^{\text{Alg}} N = N \oplus_N^{\text{Geo}} N = N$. □

5.C. Parametric definition

In this section we explain another definition of an operation on the set $\mathbb{P}_{\mathbb{R}}(m)$ that turns out to be equivalent to the algebraic and the geometric definitions in the two previous sections. Recall that the group operation on an elliptic curve is compatible with its parametrisation by the Weierstrass

$\wp$-function. We only have to slightly modify the parametrisation of $\mathbb{P}_{\mathbb{R}}(m)$ which we introduced in Section 2 to obtain a similar result for the group operation on the hyperbolas. Recall that the function $\mathcal{P}_m : \{\pm 1\} \times \mathbb{R} \to \mathbb{P}_{\mathbb{R}}(m), (s,t) \mapsto sP_m(t)$ is a bijection. Choose σ and τ such that $\mathcal{P}_m(\sigma, \tau) = N$ and consider the reparametrisation $\mathfrak{p}_m = \mathfrak{p}_m^{(N)}$ given by $\mathfrak{p}_m(s,t) := \mathcal{P}_m(s\sigma, t+\tau)$. Then the operation $\oplus_N^{\mathrm{Par}}$ is given by

$$\mathfrak{p}_m(s_A, t_A) \oplus_N^{\mathrm{Par}} \mathfrak{p}_m(s_B, t_B) := \mathfrak{p}_m(s_A s_B, t_A + t_B).$$

Proposition 5.3. *The tuple $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{Par}, N)$ is an abelian group with neutral element $N = \mathfrak{p}_m(1,0)$. The inverse of $\mathfrak{p}_m(s_A, t_A)$ is given by $\mathfrak{p}_m(s_A, -t_A)$. Moreover, the parametric operation $\oplus_N^{Par}$ agrees with the geometric operation $\oplus_N^{Geo}$. In particular, the group $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{Par}, N)$ is isomorphic to the groups $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{Geo}, N)$ and $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{Alg}, N)$.*

Proof. The fact that $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{\mathrm{Par}}, N)$ is an abelian group with indicated neutral and inverse element is obvious. It remains to prove that the operations $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{\mathrm{Par}}, N)$ and $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{\mathrm{Geo}}, N)$ are the same. We proceed as in the proof of Proposition 5.2: Let $A = \mathfrak{p}(s_A, t_A) =: (x_A, y_A), B = \mathfrak{p}(s_B, t_B) =: (x_B, y_B), N = \mathfrak{p}(s_N, t_N) =: (x_N, y_N)$ be the points on $\mathbb{P}_{\mathbb{R}}(m)$. Then the coordinates of $C := A \oplus_N^{\mathrm{Par}} B$ are given by $C = \mathfrak{p}(s_A s_B, t_A + t_B) =: (x_C, y_C)$. For $A \neq B$, we have to show that the lines AB and NC are parallel. Indeed, using the definitions from Section 2 and writing $\mathfrak{p}$ using exponential functions, one can show that

$$\begin{cases} (y_A - y_B)(x_N - x_C) = (x_A - x_B)(y_N - y_C) & \text{if } C \neq N, \\ \nabla f(x_N, y_N)(x_A - x_B, y_A - y_B)^T = 0 & \text{if } C = N. \end{cases}$$

For the case $A = B \neq N$, we again have to check that the scalar product of the vectors $(2x_A + y_A, x_A - 2y_A)$ and $(x_N - x_{AB}, y_N - y_{AB})$ vanishes. A short calculation confirms this. The case $A = B = N$ is again trivial. □

5.D. Definition using areas

In this section we give another geometrically defined operation on $\mathbb{P}_{\mathbb{R}}(m)$ which also turns out to be equivalent to the previous definitions. For this we consider triangle areas in the plane $\mathbb{R}^2$ with corners $(0,0)$ and two other points P, Q on $\mathbb{P}_{\mathbb{R}}(m)$. Recall that the oriented area of a triangle with corners $O = (0,0)$, $P = (x_P, y_P)$ and $Q = (x_Q, x_Q) \in \mathbb{R}^2$ is given by

$$\mathcal{A}_O(P,Q) := \frac{1}{2} \det \begin{pmatrix} x_P & x_Q \\ y_P & y_Q \end{pmatrix} = \frac{1}{2}(x_P y_Q - x_Q y_P).$$

For given m we consider points $P, Q \in \mathbb{P}_{\mathbb{R}}(m)$. If we fix P then the value of the oriented area of the triangle $\triangle OPQ$ increases monotonically from $-\infty$ to $+\infty$ when Q moves along a branch of the hyperbola. This follows from elementary geometry when we consider the fixed line OP as base of the triangle. In particular, for any given value a we find a unique point Q_1 on one branch, and a unique point Q_2 on the other branch such that the oriented area of $\triangle OPQ_i$ equals a. More precisely, we have the following.

Proposition 5.4. *Let $A, B, N \in \mathbb{P}_{\mathbb{R}}(m)$. Then there is a unique point C such that*

$$\mathcal{A}_O(N, A) = \mathcal{A}_O(B, C) \text{ and } \mathcal{A}_O(C, A) = \mathcal{A}_O(B, N), \text{ and} \tag{5.10}$$

additionally C lies on the same branch as N if $A = B$. Moreover, the lines AB and NC are parallel.

Proof. First of all, we show that the point $D := (x_D, y_D) := A \oplus_N^{\text{Geo}} B$ defined by the help of the parallel lines $AB \parallel ND$ has the property (5.10) of the point C (see Figure 3). That is we show that

$$\frac{1}{2}(x_N y_A - x_A y_N) = \frac{1}{2}(x_B y_D - x_D y_B) \text{ and } \frac{1}{2}(x_D y_A - x_A y_D) = \frac{1}{2}(x_B y_N - x_N y_B), \tag{5.11}$$

and that D lies on the same branch as N if $A = B$. Now, by Proposition 5.2 we have $D = A \oplus_N^{\text{Alg}} B$ so in particular, we can use the formula from Proposition 5.1 to compute the coordinates of $D = (x_D, y_D)$ in terms of the coordinates of the points $A = (x_A, y_A), B = (x_B, y_B)$ and $N = (x_N, y_N)$. Using the formula from Proposition 5.1 a short calculation confirms both equalities in (5.11). Actually, the second equality easily follows geometrically from the first one, since the triangles $\triangle NDA$ and $\triangle NDB$ have the same oriented area. If $A = B$, then $D = A \oplus_N^{\text{Alg}} A = A \boxdot A \boxplus N$ so D lies on the same branch as A since the branch of A (which is given by its sign when written in the form $\pm P_m(t_A)$) "cancels" and the branch of N "remains".

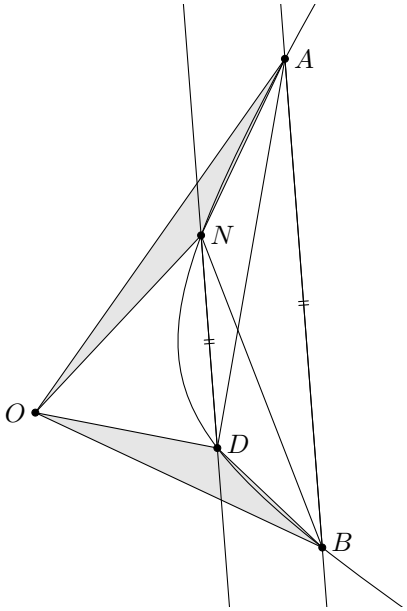

Figure 3: The triangles $\triangle ONA$ and $\triangle OBD$ have the same oriented area. Also the triangles $\triangle ODA$ and $\triangle OBN$ have the same oriented area.

To finish the proof we have to show for the case $A \neq B$ that on the other branch than the one on which we found D there is no point which satisfies the same equalities. To see this, we argue as follows. There is a unique point D' on the same branch as D such that

$$\mathcal{A}_O(N, A) = -\mathcal{A}_O(B, D') = \mathcal{A}_O(B, -D'),$$

where $-D'$ is on the other branch. Similarly, there is a unique point D'' on the same branch as D such that

$$\mathcal{A}_O(B, N) = -\mathcal{A}_O(D'', A) = \mathcal{A}_O(-D'', A),$$

where $-D''$ is on the other branch. However, since D' and D'' are clearly different points, the equalities $\mathcal{A}_O(N, A) = \mathcal{A}_O(B, -D')$ and $\mathcal{A}_O(B, N) = \mathcal{A}_O(-D', A)$ cannot hold simultaneously. □

By Proposition 5.4 we can now define

$$C := A \oplus_N^{\text{Area}} B,$$

where C is the unique point characterized by (5.10). In particular, it follows directly from Proposition 5.4 that the operation $\oplus_N^{\text{Area}}$ agrees with the operation $\oplus_N^{\text{Geo}}$ and we have the following.

Theorem 5.2. *Let $m \in \mathbb{R} \setminus \{0\}$. Then for any $P, Q, N \in \mathbb{P}_{\mathbb{R}}(m)$ we have*

$$P \oplus_N^{Geo} Q = P \oplus_N^{Alg} Q = P \oplus_N^{Par} Q = P \oplus_N^{Area} Q,$$

that is the operations $\oplus_N^{Geo}$, $\oplus_N^{Alg}$, $\oplus_N^{Area}$, and $\oplus_N^{Par}$ coincide on $\mathbb{P}_{\mathbb{R}}(m)$. Moreover, for all four operations $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N^{\diamond}, N)$ is an abelian group isomorphic to $(\{\pm 1\}, \cdot) \times (\mathbb{R}, +)$.

Using this we can prove the special case of Theorem 1.4 for the hyperbola $x^2 + xy - y^2 = m$.

Corollary 5.5. *Special case of [Shi09, p. 6 Conclusion]. $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N, N)$ is an abelian group isomorphic to $(\mathbb{R}^\times, \cdot)$.*

Proof. By Theorem 5.2 we have $(\mathbb{P}_{\mathbb{R}}(m), \oplus_N, N) \cong (\{\pm 1\}, \cdot) \times (\mathbb{R}, +)$ as groups. The result follows by combining isomorphisms as we also have $(\{\pm 1\}, \cdot) \times (\mathbb{R}, +) \cong (\mathbb{R}^\times, \cdot)$ via the isomorphism

$$\rho : (\{\pm 1\}, \cdot) \times (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot), (\sigma, \tau) \mapsto \sigma e^\tau. \qquad \square$$

5.E. Parametrising rational solutions

We note that we can restrict the operation $\oplus$ to the set $\mathbb{P}_{\mathbb{Q}}(m)$ of rational solutions to $x^2 + xy - y^2 = m$. Indeed, this follows from the explicit formula for $\oplus_N^{\text{Alg}}$ (Proposition 5.1) as they only add subtract, multiply or divide the coefficients and so the result is rational if the coefficients are rational.

Using a standard technique we can parametrise the rational solution set $\mathbb{P}_{\mathbb{Q}}(m)$. Indeed, if $P = (x_P, y_P) \in \mathbb{P}_{\mathbb{Q}}(m)$ then we can consider lines $\ell : y = y_P + t(x - x_P)$ passing through P with rational slope t. Introducing this in the equation $x^2 + xy - y^2 = m$ and using the fact that x_P is a solution, the quadratic equation reduces to a linear one and we find for the second intersection of ℓ with the hyperbola

$$(x, y) = \left(\frac{(t^2+1)x_P + (1-2t)y_P}{t^2 - t - 1}, \frac{(t^2+2t)x_P - (t^2+1)y_P}{t^2 - t - 1} \right), \tag{5.12}$$

for $a \in \mathbb{Q}$. Similarly, for the line $\ell : x = x_P$, we get the point

$$(x, y) = (x_P, x_P - y_P). \tag{5.13}$$

Vice versa, it is clear that every line through (x_P, y_P) and a rational point (x, y) on the hyperbola $x^2 + xy - y^2 = m$ has either rational slope t or $x = x_P$. Hence, we have the following.

Proposition 5.6. *If (x_P, y_P) is a rational point on the hyperbola $x^2 + xy - y^2 = m$, then every rational point (x, y) on the hyperbola is given by (5.12) for rational t or by (5.13).*

5.F. Restricting to integer solutions

In this section we discuss what happens when adding integer solutions with the operation $\oplus$. In general it is not the case that if $P, Q, N \in \mathbb{P}_{\mathbb{Z}}(m)$, then $P \oplus_N Q \in \mathbb{P}_{\mathbb{Z}}(m)$. For instance, consider $m = 11$ and the points $P = (5, 7), Q = (4, -1), N = (3, 1) \in \mathbb{P}_{\mathbb{Z}}(11)$, then for example using the formula in Lemma 5.1 we have $P \oplus_N Q = \left(\frac{36}{11}, \frac{35}{11}\right) \notin \mathbb{P}_{\mathbb{Z}}(m)$. We can better understand this using Proposition 4.1 and Proposition 4.2. Indeed, by Proposition 4.1 and using the parametric definition of $\oplus$ for $t_i \in \mathbb{R}$, $k_i \in \mathbb{Z}$ we have

$$\begin{aligned} A_1^{k_1} P_m(t_1) \oplus_{A_1^{k_N} P_m(t_N)} A_1^{k_2} P_m(t_2) &= P_m(t_1 - k_1\delta_m) \oplus_{P_m(t_N - k_N\delta_m)} P_m(t_2 - k_2\delta_m) \\ &= P_m\left(t_1 + t_2 - t_N - (k_1 + k_2 - k_N)\delta_m\right), \end{aligned}$$

where $\delta_m = 2\xi_m \ln(\beta)$ for ξ_m as in Proposition 4.1. Next, by Proposition 4.2 any integer solution is uniquely of the form $\pm A_1^k \binom{u}{v}$ for $(u, v) \in F_m$. Using the parametrisation from Section 2

we can write $F_m = \{P_m(T_1), \dots, P_m(T_\ell)\}$, for $\ell = |F_m|$ and T_i distinct. Hence, the point $R = A_1^{k_1} P_m(t_1) \oplus_{A_1^{k_N} P_m(t_N)} A_1^{k_2} P_m(t_2)$, is an integer solution if and only if $t_1+t_2-t_N \equiv T_j \mod |\delta_m|$ for some j as then R is obtained from $P_m(T_j)$ using the matrix A_1. In particular, this is the case if $t_1 = t_2 = t_N = T_j$ for some j, that is if the points P, Q, N lie in one equivalence class of solutions for the relation $\sim$ as in Definition 3.7. In other words, we have the following.

Proposition 5.7. *Let* $P, Q \in \mathbb{P}_{\mathbb{Z}}(m)$. *If* $P \sim Q$, *then* $P \oplus Q \in \mathbb{P}_{\mathbb{Z}}(m)$ *and* $P \oplus Q \sim P, Q$, *where* $\sim$ *is as in Definition 3.7.*

5.G. Geometric view on the group action of $\mathbb{P}_{\mathbb{Z}}(1)$ on the set $\mathbb{P}_{\mathbb{Z}}(m)$

By Theorem 3.4 or by geometric considerations using the operation $\oplus^{\text{Geo}}$ we see that $G := (\mathbb{P}_{\mathbb{Z}}(1), \boxdot)$ is an abelian group isomorphic to the group $(\{\pm 1\}, \cdot) \times (\mathbb{Z}, +)$. This group G acts on the set $\mathbb{P}_{\mathbb{Z}}(m)$ as follows,

$$\triangleright : \mathbb{P}_{\mathbb{Z}}(1) \times \mathbb{P}_{\mathbb{Z}}(m) \to \mathbb{P}_{\mathbb{Z}}(m), (U, X) \mapsto U \triangleright X := U \boxdot X,$$

where $\boxdot$ is defined as in Section 3.B and one can directly verify that this defines a group action. Indeed, we can view this geometrically as follows. Let $X \in \mathbb{P}_{\mathbb{Z}}(m)$, $U \in \mathbb{P}_{\mathbb{Z}}(1)$ and set $N = (\sqrt{m}, 0)$. Then, $X \boxdot U = N \boxdot U \boxdot X \boxdot N = (\sqrt{m}U) \oplus_N^{\text{Alg}} X = (\sqrt{m}U) \oplus_N^{\text{Geo}} X$, by the definition of $\boxdot$ and using Theorem 5.2. That is, we obtain $U \triangleright X$ by scaling U with the factor $\sqrt{m}$ to obtain the point $\sqrt{m}U$ and then adding this point to X using the geometric construction $\oplus_N^{\text{Geo}}$. This is depicted in Figure 4. Finally, note that the orbits of the group action $\triangleright$ are precisely the equivalence classes of the relation $\sim$ as in Section 3 and so this construction gives us a geometric view on the results in that section.

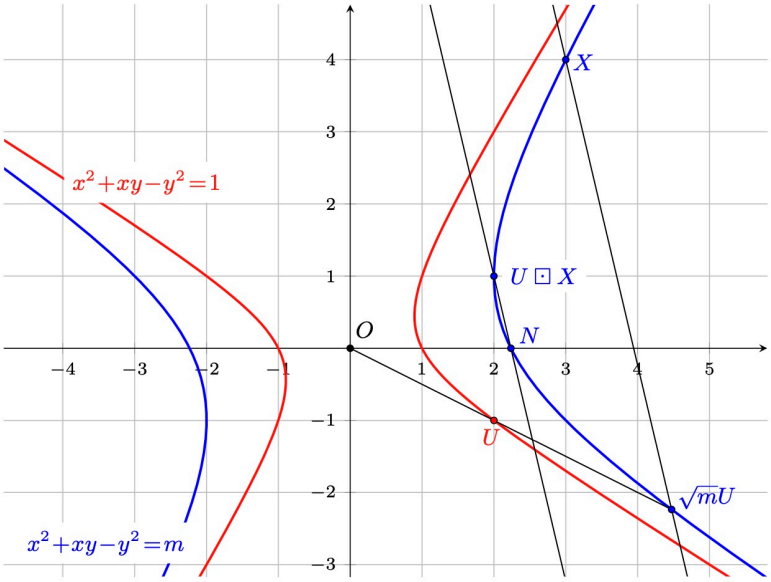

Figure 4: Geometric construction of $U \triangleright X$ for $m = 5$.

References

[Bel21] Emanuele Bellini et al, "Group law on affine conics and applications to cryptography", *Applied Mathematics and Computation* **409** (2021), p. 125537.

[Bue89] Duncan A. Buell, *Binary Quadratic Forms*, Springer New York, NY, 1989.

[Coh78] Harvey Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Universitext. Springer New York, NY, 1978.

[Con24] Keith Conrad, *Factoring in quadratic fields*, [Online; accessed 26-July-2024]. https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf.

[Lem03] Franz Lemmermeyer, *Conics – a Poor Man's Elliptic Curves*, 2003. arXiv: math/0311306.

[Lem12] Franz Lemmermeyer, *Pell Conics – An Alternative Approach to Elementary Number Theory*, 2012.

[Lem21] Franz Lemmermeyer, *Quadratic Number Fields. Springer Cham*, 2021.

[Lem18] Franz Lemmermeyer, *Vom Newton-Verfahren zu Gruppengesetzen auf Kegelschnitten*, 2018.

[Neu99] Jürgen Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften. Springer Berlin, Heidelberg, 1999.

[OSIS24a] OEIS Foundation Inc, *The On-Line Encyclopedia of Integer Sequences*, [Published electronically at http://oeis.org. Accessed 20-February-2024]. 2024. https://oeis.org/A089270.

[OEIS24b] OEIS Foundation Inc, *The On-Line Encyclopedia of Integer Sequences*, [Published electronically at http://oeis.org. Accessed 23-July-2024]. 2024. https://oeis.org/A031363.

[Pin24] Richard Pink, *Number Theory I und II Summary*, 2024.

[Shi09] Shailesh Shirali, "Groups associated with conics", *The Mathematical Gazette* **93** (Mar. 2009), pp. 27–41.

[Lan19] Wolfdieter Lang, *Fibonacci sequences with relative prime initial conditions, and the binary quadratic form [1, 1, -1]*, 2019. https://oeis.org/A089270/a089270.pdf.

Norbert Hungerbühler
Department of Mathematics
ETH Zürich, 8092 Zürich
Switzerland
e-mail: norbert.hungerbuehler@math.ethz.ch

Maciej Smela
Department of Mathematics
ETH Zürich, 8092 Zürich
Switzerland
e-mail: maciej.smela@gmail.com