The Origin of the Beauregard–Suryanarayan Product on Pythagorean Triples

Shaul Zemel

October 17, 2018

Introduction

Pythagorean triples are one of the oldest and most studied objects in elementary mathematics. They appear as the basic examples in many mathematical questions, and trying to generalize them has led to the development of several fascinating fields in mathematics over the centuries—one such direction was the research revolving around, and stemming from, Fermat’s Last Theorem. Several papers containing also historical perspectives already appear in the literature, including some remarks of the rather recent reference [M]. Since the literature about this subject is vast, any attempt to treat a reasonable amount of references will do injustice with many unmentioned authors. We therefore consider here only those papers that are closely related to our point of view, leaving the more comprehensive lists of references for more historical surveys.

Normalizing a Pythagorean triple according to the largest number of the triple produces elements of the complex unit circle, thus giving one type of product on Pythagorean triples. This product is based on the imaginary quadratic field obtained by adjoining the complex number \( \sqrt{-1} \) to the rational field \( \mathbb{Q} \) (see, e.g., [E] and [T]). On the other hand, the reference [BS] defines another product, one that is inherently based on one of the smaller coordinates of the triple. Several results are proved about the structure of this product in that reference, as well as about the basic involution arising from interchanging the two coordinates. It is this product that lies in the heart of our presentation.

In this note we explain the geometric origin of the product defined in [BS], also giving more conceptual reasonings for the results of that reference. The idea is that apart from quadratic fields, there is another 2-dimensional extension \( E \) of the rationals that involves no nilpotent elements (i.e., a quadratic étale algebra over \( \mathbb{Q} \)). As quadratic fields appear in the theory of anisotropic rational binary quadratic forms, this algebra \( E \) is the corresponding counterpart for the isotropic quadratic form, also known as the hyperbolic plane. The resulting investigation of \( E \) yields naturally the product from [BS] on Pythagorean triples, and produces directly the structure theorems from that reference. Using the involution (which is a Cayley transform in this point of view) we obtain new insights into the
relation between right triangles that are almost isosceles and Pell’s equation
with discriminant 2, and also prove an analogue involving the discriminant 3.

This paper is divided into 5 sections. Section 1 presents the rational binary
quadratic forms, and shows how the algebra \( E \) arises in this context. Section 2
relates the Pythagorean triples to the algebra \( E \), while more explicit expressions
and the structure theorem are proved in Section 3. Section 4 introduces and
investigates the natural involution on Pythagorean triples. Finally, Section 5
explains how differences in Pythagorean triples (such as “almost fixed points”
of the involution) relate to quadratic fields, and proves some related theorems.

1 Quadratic Fields and Binary Quadratic Forms

We begin by presenting the setup in which we shall later view the group structure
on Pythagorean triples. Consider a non-degenerate quadratic space \( V \) of
dimension 2 over \( \mathbb{Q} \), and recall that the determinants of all the possible Gram
matrices for \( V \) differ from one another by invertible rational squares, i.e., by el-
ments of the group \( (\mathbb{Q}^\times)^2 \). Hence \( V \) determines a determinant in the quotient
\( \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 \), and since the dimension is 2 we define the
discriminant \( d \) of \( V \) to be minus that determinant.

We can take an orthogonal basis for \( V \), rendering it isomorphic to the space
\( \mathbb{Q}^2 \) with the quadratic form \( q(x, y) = ax^2 - ady^2 \) for some pre-image of \( d \) in \( \mathbb{Q}^\times \)
(which we also denote by \( \mathbb{Q}^\times \)). The orthogonal group \( O(V) \), the special orthogonal
group \( SO(V) \), and the kernel \( SO^1(V) \) of the spinor norm from \( SO(V) \) are all
unaffected by rescaling of \( V \) (and so is the discriminant in even dimensions), so
that we may consider just the quadratic form \( q(x, y) = x^2 - dy^2 \) for investigating
them.

Assume first that \( d \) is not a rational square, and let \( K \) be the (real or imag-
inary) quadratic field \( \mathbb{Q}(\sqrt{d}) \), whose unique non-trivial Galois automorphism
over \( \mathbb{Q} \) we denote by \( \sigma \). We can identify an element \((x, y)\) of \( \mathbb{Q}^2 \) with the el-
ement \( z = x + y\sqrt{d} \) of \( K \), and then \( q \) is just the norm map \( N_K \) from \( K \) to
\( \mathbb{Q} \). There is an operation of the group \( K^\times \) on the rational vector space \( K \) that
preserves the quadratic form (i.e., the norm), in which \( \xi \in K^\times \) multiplies \( z \) by \( \xi \)
but divides it by its Galois conjugate \( \xi^\sigma \). We therefore obtain a map from \( K^\times \) into
the orthogonal group \( O(V) = O(K) \). A classical result from the theory of
quadratic forms, which is easily verified directly, is the following.

Proposition 1.1. The image of \( K^\times \) in \( O(K) \) is precisely the special orthogonal
group \( SO(K) \), and the kernel of that map is \( \mathbb{Q}^\times \). The spinor norm of the image
of an element \( \xi \in K^\times \) inside \( SO(K) \) is the image of \( N_K^{\mathbb{Q}}(\xi) \) in \( \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 \).

Proposition 1.1 can be described as a short exact sequence
\[
1 \to \mathbb{Q}^\times \to K^\times \to SO(K) \to 1
\]
of Abelian groups, or equivalently by the statement that \( K^\times \) is the Gspin
group of the quadratic space \( K \) (hence of \( V \)), which in symbols is written as
$G\text{Spin}(V) = \mathbb{K}^\times$. The full group $O(V)$ is obtained by adding the action of $\sigma$, so the appropriate cover $G\text{pin}(V)$ of $O(V)$ is the semi-direct product in which the Galois group $\text{Gal}(\mathbb{K}/\mathbb{Q})$, of order 2, operates on $\mathbb{K}^\times$.

Combining the second assertion of Proposition 1.1 with the obvious fact that $N_\mathbb{Q}(r) = r^2$ for any $r \in \mathbb{Q}^\times$ produces the following classical result. Denote by $\mathbb{K}^1$ the subgroup of $\mathbb{K}^\times$ consisting of those elements $\xi$ with $N_\mathbb{K}(\xi) = 1$.

**Corollary 1.2.** The group $\mathbb{K}^1$ maps onto the spinor kernel $SO^1(\mathbb{K})$, with kernel $\{\pm 1\}$.

The short exact sequence associated with Corollary 1.2 is

$$1 \to \{\pm 1\} \to \mathbb{K}^1 \to SO^1(\mathbb{K}) \to 1,$$

so that $\mathbb{K}^1$ is the spin group of $V = \mathbb{K}$, i.e., $\text{Spin}(V) = \mathbb{K}^1$. With our normalization of $V = \mathbb{K}$ with $q = N_\mathbb{K}$, an element of order 2 and spinor norm 1 in $G\text{pin}(V)$ is the combination of $\sqrt{d} \in \mathbb{K}^\times$ with the action of $\rho$ (since $\sqrt{d} \sigma = -\sqrt{d}$, this action sends $z = x + y\sqrt{d}$ to $-z = -x + y\sqrt{d}$, indeed representing the reflection in the vector $1 \in \mathbb{K}$ with $q(1) = 1$). The pin group $pin(\mathbb{K})$ is therefore a semi-direct product similar to $G\text{pin}(\mathbb{K})$. However, as this group does vary with different rescalings of $V$, we shall not consider it further.

Note that the group $\mathbb{K}^1$ from Corollary 1.2 is not the group of units in the ring of integers of $\mathbb{K}$, but is much larger. Indeed, in case $\mathbb{K}$ has class number 1, every prime number $p$ that splits in $\mathbb{K}$ produces a generator $\pi$ for $\mathbb{K}^1$ for some generator $\pi$ of a prime ideal in $\mathbb{K}$ lying over $p$, and it is clear (by considering ideals) that all these generators are independent in the group $\mathbb{K}^1$ (also modulo units in the ring of integers). Replacing $\pi$ by another generator simply multiplies the generator by a unit, and taking the generator for the other ideal lying over $p$ replaces that generator by its inverse (again, perhaps up to units).

### 2 Pythagorean Triples

Let $(a, b, c)$ be a Pythagorean triple, i.e., a triplet of integers satisfying the Pythagorean equality $a^2 + b^2 = c^2$, and assume that $a \neq 0$. Then the rational numbers $\alpha = \frac{a}{b}$ and $\beta = \frac{b}{a}$ satisfy the equality $\alpha^2 - \beta^2 = 1$, which is the norm 1 condition associated with the case of the trivial discriminant $d = 1$.

While $\mathbb{Q}(\sqrt{d})$ is no longer a quadratic field, we recall that for a non-square $d$ the quadratic field $\mathbb{K}$ can be presented as the quotient $\mathbb{Q}[X]/(X^2 - d)$ of the polynomial ring $\mathbb{Q}[X]$. This construction produces, with $d = 1$, a ring called the split quadratic étale algebra $\mathbb{E} = \mathbb{Q}[\varepsilon]$ with $\varepsilon$ being a formal element satisfying $\varepsilon^2 = 1$. This algebra is not a field, but has two non-trivial ideals, generated by the complementary idempotents $\frac{1 + \varepsilon}{2}$ and $\frac{1 - \varepsilon}{2}$ respectively. The quotient ring associated with each such ideal is canonically isomorphic to $\mathbb{Q}$, so that as a ring we get $\mathbb{E} \cong \mathbb{Q} \times \mathbb{Q}$. It has a (Galois) automorphism $\iota$, extending $\sigma$ from the field case, taking $\varepsilon$ to $-\varepsilon$, hence inverting the two factors in the isomorph
Indeed, the product of a pair of elements \( \alpha \times \beta \) does appear there, with vanishing with the structure result for \( \{\pm \} \). The projective relation involves only positive scalars (hence the extra multiplier of \( \epsilon \)). Theorem 4 of [M], but with the difference that in that reference the \( \epsilon \) is associated only with those elements. The fact that we get \( \epsilon \) of the ring of integers in \( \{\pm \} \) are just distinct ideals in that “ring of integers” lying over it. The units in that “ring” are those units associated with any scalar multiple \( \langle ta, tb, tc \rangle \) for some \( t \in \mathbb{Q}^\times \), and it is associated only with those elements. The fact that we get \( \mathbb{Q}^\times=1 \) is the isomorph \( \mathbb{Q}^\times \) (resp. \( \mathbb{Q}^\times \)) by this element \( \langle r, \frac{1}{r} \rangle \) and dividing by its conjugate \( \langle \frac{1}{r}, r \rangle \) indeed multiplies our idempotent by the square \( r^2 \) (resp. \( \frac{1}{r^2} \)), an operation with trivial spinor norm in \( \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \).

Combining all these observations produces the following result.

**Proposition 2.1.** The set of Pythagorean triples \( (a, b, c) \) with \( a \neq 0 \) up to scalar multiplication carries a natural structure of a group that is isomorphic to \( \mathbb{Q}^\times \).

Indeed, the element of \( \mathbb{E}^1 \) associated with the Pythagorean triple \( (a, b, c) \) (that is integral or rational) is \( \alpha + \beta \epsilon \) with \( \alpha = \frac{c}{a} \) and \( \beta = \frac{b}{a} \). It is also the element associated with any scalar multiple \( \langle ta, tb, tc \rangle \) for some \( t \in \mathbb{Q}^\times \), and it is associated only with those elements. The fact that we get \( \mathbb{E}^1 \cong \mathbb{Q}^\times \) is in line with the structure result for \( \mathbb{K}^1 \) with non-square \( d \) above: Indeed, the equivalent of the ring of integers in \( \mathbb{E} \) is generated by any one of the idempotents \( \frac{1+i \epsilon}{2} \), it is isomorphic to \( \mathbb{Z} \times \mathbb{Z} \), and every prime ideal of \( \mathbb{Z} \) splits there (since there are two distinct ideals in that “ring of integers” lying over it). The units in that “ring of integers” are just \( \pm 1 \) and \( \pm \epsilon \) (even though \( d = 1 > 0 \)), producing only the \( \pm 1 \) factor in \( \mathbb{Q}^\times \) since the units \( \pm \epsilon \) have norm \( -1 \). Note that Proposition 2.1 is essentially Theorem 4 of [M], but with the difference that in that reference the projective relation involves only positive scalars (hence the extra multiplier of \( \{\pm 1 \} \) appearing in that reference), and the excluded Pythagorean triples with \( a = 0 \) do appear there, with vanishing \( \mathbb{Q} \)-image.

Two remarks are in order here. First, the group from Proposition 2.1 is the projective image (i.e., modulo global scalars) of the semi-group from [BS]. Indeed, the product of a pair of elements \( \alpha + \beta \epsilon \) and \( \gamma + \delta \epsilon \) of \( \mathbb{E}^1 \) (or just of \( \mathbb{E} \)) is \( \langle \alpha \gamma + \beta \delta + (\alpha \delta + \beta \gamma) \epsilon \rangle \), which is the extension of the multiplication rule of \( \alpha + \beta \sqrt{d} \) and \( \gamma + \delta \sqrt{d} \) from the field \( \mathbb{K} = \mathbb{Q}(\sqrt{d}) \) to the case \( d = 1 \). If the

\[ Q \times Q. \]
first element arises from the Pythagorean triple from above and the second one comes from another triple, say \((f, g, h)\), then the product of these triples from [BS] is \((af, bh+cg, bg+ch)\), which indeed corresponds to our product element in \(E^1\). Second, the underlying spinor kernel \(SO^1(E)\) from Corollary 1.2 is obtained by dividing by \(\pm 1\). But the group \(\mathbb{Q}^x\) from Proposition 2.1 admits a natural splitting as the product of \(\{\pm 1\}\) and the group \(\mathbb{Q}_{\geq}^x\) of positive rational numbers. Therefore the spin group in question is isomorphic to \(\mathbb{Q}_{\geq}^x\), and the corresponding subgroup of \(E^1\) is the one in which \(\alpha > 0\) (more on this later in this section).

Observing that the \(a\)-entries are simply multiplied in the product rule from [BS], the structure of the corresponding rational group is as follows.

**Corollary 2.2.** The set of all rational Pythagorean triples \((a, b, c)\) with \(a \neq 0\) forms, with the group law from [BS], a group that is isomorphic to \(\mathbb{Q}^x \times \mathbb{Q}^x\). The subset of classical, integral Pythagorean triples \((a, b, c)\) with \(a \neq 0\), is a sub-semi-group of this group.

Indeed, knowing \(a\) and the associated element \(\alpha + \beta \varepsilon \in E^1\) determines the (rational) Pythagorean triple \((a, b, c)\) uniquely, and every pair of such elements is possible. Therefore the map sending a rational Pythagorean triple \((a, b, c)\) to the pair \((a, \alpha + \beta \varepsilon)\) in \(\mathbb{Q}^x \times E^1\) is bijective, and since it is easily seen to be an isomorphism of groups, The first assertion in Corollary 2.2 is an immediate consequence of Proposition 2.1 and the \(a\)-entry of the formula for the product. The second assertion of Corollary 2.2 is also obvious from the product rule.

However, for our purposes it will be more convenient to consider only the projection onto \(E^1\), i.e., to put the group from Corollary 2.2 is the short exact sequence

\[
1 \to \{(a, 0, a)|a \in \mathbb{Q}^x\} \to \text{rational Pythagorean triples} \to E^1 \to 1.
\]

The kernel of the projection to \(a\) splits this short exact sequence using the subgroup \(\{1, \beta, a|\alpha + \beta \varepsilon \in E^1\}\). However, we shall use a different set-theoretic splitting when we investigate the sub-semi-group of integral Pythagorean triples in Section 3 below.

Note that the product rule from [BS] implies that a Pythagorean triple \((a, b, c)\) is related to the element \(c + b \varepsilon\) of \(E\). Indeed, this element has norm \(a^2\), and since we require that \(a \neq 0\), such elements are all invertible. They comprise the subgroup of \(E^x\) defined by the condition that the norm is a square in \(\mathbb{Q}\). A similar subgroup of \(\mathbb{K}^x\) can be considered also for non-square \(d\), and in the language of Proposition 1.1 Corollary 2.2 and the short exact sequences, this group is the inverse image of \(SO^1(V)\) inside \(GSpin(V)\). The difference, for \(d = 1\), between this group and the group from Corollary 2.2 is that while \(c + b \varepsilon\) determines \(a^2\) as its norm, the sign of \(a\) is an extra piece of information from a Pythagorean triple \((a, b, c)\). It therefore follows from Corollary 2.2 that this subgroup of \(E^x\) is isomorphic to \(\mathbb{Q}_{\geq}^x \times \mathbb{Q}^x\) (by canonically taking \(a\) to be the positive square root of the norm of the element \(c + b \varepsilon\)). We also note that \(|\alpha| > |\beta|\) for any element \(\alpha + \beta \varepsilon\) of \(E^1\) (and, in fact, for any element of \(E^x\) whose norm is positive), meaning that in the product of this element with another such
element $\gamma + \delta \varepsilon$, the sign of the first coefficient $\alpha \gamma + \beta \delta$ is the product of the signs of $\alpha$ and $\gamma$. Moreover, the inverse of $\alpha + \beta \varepsilon$ is the conjugate $\alpha - \beta \varepsilon$ divided by the norm, and the first coordinate has the same sign as $\alpha$ when the norm is positive (in particular for elements of $E^1$). Hence $E^1$ factors as $\{\pm 1\}$ times the subgroup $E^1_{K}$ of $E$ consisting of those elements $\alpha + \beta \varepsilon \in E^1$ in which $\alpha > 0$ (this is the spin group mentioned above). Such elements come from Pythagorean triples $(a, b, c)$ in which $a$ and $c$ have the same sign. We remark that such a splitting of $K$ is possible also for quadratic fields $K = Q(\sqrt{d})$ for non-trivial $d$ when $d$ is positive (i.e., when $K$ is a real quadratic field).

As mentioned in the Introduction, references like [E] and [T] put the $c$-coordinate of the Pythagorean triple $(a, b, c)$ in the denominator, thus obtaining the group $K^1$, for the Gaussian field $K = Q(\sqrt{-1})$, as a subgroup of the circle group $\{z \in C||z| = 1\}$. This group is isomorphic, canonically up to local inversions, to the subgroup of $Q^\times$ generated by the primes $p$ that are congruent to 1 modulo 4 times the torsion group of order 4 generated by $\sqrt{-1}$ (the reference [E] essentially divides by the latter torsion subgroup to get a free Abelian group). Some of the results of this section and the following ones have analogues in this point of view as well, but we shall concentrate on the group structure coming from $E$, which is much more canonical (the only choice involved here is the distinction between $\varepsilon$ and $-\varepsilon$; inversion of which means global multiplicative inversion of $r$, while for $K^1$ one must choose a generator for every prime in $1 + 4Z$ independently).

## 3 Explicit Expressions

Let us now write the explicit relation between $E^1$, classes of Pythagorean triples, and the group $Q^\times$. The element $\alpha + \beta \varepsilon$ of $E^1$ is related to $r \in Q^\times$ if it equals $r \frac{1}{\alpha} + \frac{1}{\beta} \cdot \frac{1}{\varepsilon}$ (since the map onto $Q^\times$ is multiplying by the first idempotent, and the coefficient of the second one is $\frac{1}{\beta}$ because of the norm 1 condition). It follows that $r = \alpha + \beta$ and $\frac{1}{\beta} = \alpha - \beta$, so that $\alpha = \frac{s}{n} + \frac{1}{\beta}$ and $\beta = \frac{t}{n} - \frac{1}{\beta}$. Moreover, we recall that when $(a, b, c)$ is a Pythagorean triple that is associated with $\alpha + \beta \varepsilon \in E^1$ then $\alpha = \frac{s}{n}$ and $\beta = \frac{t}{n}$. Therefore the Pythagorean triple in question is a multiple of $(1, \beta, \alpha)$, and more precisely it equals $(a, a\beta, a\alpha)$. These formulae combine to the following relation.

**Proposition 3.1.** Let $r = \frac{m}{n}$ be a non-zero rational number, presented as a reduced quotient of integers. Then the unique primitive integral Pythagorean triple with positive $c$ that is associated with $r$ is $(2mn, m^2 - n^2, m^2 + n^2)$ in case $nm$ is even and $(mn, \frac{m^2-n^2}{2mn}, \frac{m^2+n^2}{2})$ if $mn$ is odd.

Indeed, the associated element of $E^1$ is $\frac{m^2+n^2+(m^2-n^2)r}{2mn}$, and when $m$ and $n$ are co-prime integers the greatest common divisor of $2mn$, $m^2-n^2$, and $m^2+n^2$ is 2 for odd $m$ and $n$ and 1 otherwise. In particular, the parity of $a$ in primitive form is the parity of $mn$. It is also evident that inverting $r$ (multiplicatively) is the same as inverting the sign of $b$ in the Pythagorean triples (indeed, both
correspond to replacing $\varepsilon$ by $-\varepsilon$, i.e., to the “Galois” automorphism $\iota$ of $\mathbb{E}$ over $\mathbb{Q}$). In addition, we deduce from these formulae that $r > 0$ if and only if $\alpha > 0$ (i.e., if and only if the associated element of $\mathbb{E}^1$ lies in $\mathbb{E}_1^+$), which happens if and only if $a$ and $c$ have the same sign.

Note that difference $c - b$ of the Pythagorean triple from Proposition 3.1, which is called the height in $[M]$ (and denoted by $h$), is $2n^2$ or $n^2$ respectively. Therefore quotient $\frac{a}{h}$ (with $a$ being $2mn$ or $mn$ respectively) is indeed our parameter $r$, yielding the relation between our Proposition 2.1 and Theorem 4 of that reference more explicitly. The excess $e = a + b - c$ from that reference amounts to $2n(m - n)$ or $n(m - n)$ (for $r > 1$, i.e., for positive $a$, $b$, and $c$), and as the maximal number $d$ whose square divides $2h$ is $2n$ or $n$ respectively, we find that the increment $k$ from that reference is just $m - n$.

Considering the usual generating set of $\mathbb{Q}^\times$, we immediately deduce the following result.

**Corollary 3.2.** The group from Proposition 2.1 is generated by the elements associated with the Pythagorean triples $(-1, 0, 1)$ (or equivalently $(1, 0, -1)$), $(4, 3, 5)$, and $(p, p^2 - 1, \frac{p^2 + 1}{2})$ for odd prime $p$. The positive subgroup $\mathbb{Q}_1^+$ is generated by the same set of Pythagorean triples, with the first one excluded.

Indeed, these are the triples that are associated with $-1$ and the usual primes in Proposition 3.1 (the prime 2 is separated from the odd primes because of the parity issue in that Proposition). Note that for elements with $\alpha = \frac{c}{a} < 0$ we can take either representatives with $a > 0$ (as Corollary 2.2 implicitly suggests) or those with $c > 0$ as in Proposition 3.1. This is the reason for the two different choices of the representative for the sign generator $-1$ in Corollary 3.2.

In addition, we can use the formulae from Proposition 3.1 for obtaining the semi-group structure of integral Pythagorean triples. For simplicity we shall restrict attention to elements of the subgroup $\mathbb{Q}^\times \times \mathbb{E}^1_1$ defined by both $a$ and $c$ being positive, and the full group is obtained as the direct product with the Klein 4-group consisting of the Pythagorean triples $(\pm 1, 0, \pm 1)$ with unrelated signs (the sign of $b$, or more generally of $\frac{n}{a}$, is determined by whether the parameter $r$ is larger or smaller than 1, as Proposition 3.1 and the paragraph preceding it show). For doing so we recall that the group from Proposition 3.2 is a quotient group of the one from Corollary 2.2, so that we shall have to say, for every element of the former group, which pre-image (or “lift”) of it we consider in the latter group. In the direct product from Corollary 2.2 we have taken the “lift” with $a = 1$, but when we are interested in integral triples this is not a very good choice. With the restriction $a > 0$ and $c > 0$, the only natural candidate for that “lift” is the primitive integral Pythagorean triple from Proposition 3.1. We therefore obtain a one-to-one correspondence between rational Pythagorean triple with positive $a$ and $c$ and elements of $\mathbb{Q}^\times_1 \times \mathbb{E}^1_1$, where the pair consisting of $t \in \mathbb{Q}^\times_1$ and the element of $\mathbb{E}^1_1$ that is associated with $r = \frac{b}{k} \in \mathbb{Q}^\times_1$ is $t$ times the integral Pythagorean triple from Proposition 3.1. We identify $\mathbb{E}^1_1$ with $\mathbb{Q}^\times_1$ as in Proposition 2.1, and in these coordinates the description of the group from Corollary 2.2 (with the positivity restriction) is as follows.
Theorem 3.3. Consider the rational Pythagorean triples associated with the pairs \((h, \frac{m}{n})\) and \((g, \frac{k}{l})\) in \(\mathbb{Q}^+ \times \mathbb{Q}^+\) (with the two fractions being reduced). Their product from Corollary 2.2 is the Pythagorean triple associated with the pair \((gh \gcd(km, ln)^2, km, ln)\), unless both \(mn\) and \(kl\) are even, where the product is associated with \((4gh \gcd(km, ln)^2, km, ln)\) or \(\mathbb{N} \times \mathbb{E}_1\) with the same product rule. For allowing the signs of \(a\) and \(c\) to be arbitrary one simply takes the direct product with the Klein 4-group from the previous paragraph.

The only thing that remains to verify is the formula for the product, where the part involving \(g\) and \(h\) is also obvious. For this note that the reduced form of the product \(km, ln\) is obtained by canceling \(\gcd(km, ln)\) (which equals the product of \(\gcd(k, n)\) and \(\gcd(m, l)\)), and the appearance of the parameters \(m\) and \(n\) in Proposition 3.1 is quadratic. By considering the various possibilities for the parity conditions in that proposition (observe that if \(mn\) and \(kl\) are odd then so is the reduced version of \(klmn\), and when one precisely one of \(mn\) and \(kl\) is even then so is the reduced version of \(klmn\), but when both \(mn\) and \(kl\) are even then the reduced version of \(klmn\) can be either odd or even) we find that the extra power of 2 in the first coordinate is indeed as stated. The symbol \(\mathbb{N}\) in Theorem 3.3 stands, of course, for the natural numbers starting from 1 (with 0 excluded).

The product rule from Theorem 3.3 is illustrated by the formula from [BS] in which the product of the primitive integral Pythagorean triples associated with the multiplicative inverses \(\frac{m}{n} > 0\) and \(\frac{n}{m}\) is not the Pythagorean triple \((1, 0, 1)\) representing the identity element, but rather its multiple by \(m^2n^2\) for odd \(mn\) and \(4m^2n^2\) for even \(mn\).

4 The Involution

It is clear that once \((a, b, c)\) is a Pythagorean triple, so is \((b, a, c)\), and that the operation taking the former to the latter is an involution. On the other hand, our choice of map to \(E^1\), hence to \(\mathbb{Q}^\times\), distinguishes a triple from its image under the involution. Moreover, we shall have to restrict attention to triples in which \(b \neq 0\) as well, in order for the \(a\)-coordinate of the image under the involution not to vanish. Hence in the relevant element \(\alpha + \beta \varepsilon\) of \(E^1\) associated with \((a, b, c)\), the parameter \(\beta = \frac{b}{a}\) does not vanish, and applying the involution will replace \(\beta\) by \(\frac{1}{\beta}\). Moreover, instead of \(\alpha = \frac{r}{\beta}\) we now have \(\frac{r}{\beta} = \frac{r}{\beta}\). Going over to the coordinate \(r = \alpha + \beta \in \mathbb{Q}^\times\), we observe that the new number is \(\frac{r}{r - 1}\). Substituting the values \(\alpha = \frac{r}{r + 1}\) and \(\beta = \frac{r}{r - 1}\), the latter quotient becomes \(\frac{r - 2 + 1}{r - 1}\), and after multiplying the numerator and denominator by \(r\) and canceling the factor \(r - 1\) (which is possible since the case \(r = 1\) corresponds to the excluded case with \(\beta = 0\) hence \(b = 0\)) we establish the following result.

Proposition 4.1. The involutions on the non-trivial elements of \(E^1\) and \(\mathbb{Q}^\times\)
that correspond to inverting the first two entries of Pythagorean triples take the respective elements \( \alpha + \beta \varepsilon \) and \( r \) to \( \frac{\alpha + \beta \varepsilon}{r^2 - 1} \) and to the Cayley transform \( \frac{r + 1}{r - 1} \).

The elements that are considered trivial in Proposition 4.1 are, of course, those corresponding to triples with \( b = 0 \), i.e., with \( \beta = 0 \). They are just the elements \( \pm 1 \) of both \( \mathbb{E}^1 \) and \( \mathbb{Q}^\times \). Indeed, on \( \mathbb{E}^1 \) the involution requires division by \( \beta \), while the numbers \( r = \pm 1 \) are sent by the Cayley transform to 0 and \( \infty \), both of which are not in \( \mathbb{Q}^\times \).

As for the action of the involution on the larger group \( \mathbb{Q}^\times \times \mathbb{Q}^\times \) (minus the appropriate trivial elements), it depends on the splitting which we choose to use. With the group-theoretic splitting, in which \( \mathbb{Q}^\times \cong \mathbb{E}^1 \) is lifted as the subgroup of rational Pythagorean triples of the form \( (1, \beta, \alpha) \), the other \( \mathbb{Q}^\times \)-coordinate changes from \( a \) to \( b \), or equivalently is multiplied by \( \beta = \frac{b}{a} = \frac{r}{1} \) (with \( \beta \neq 0, b \neq 0, \) and \( r \notin \{\pm 1\} \)). On the other hand, we had the set-theoretic splitting from Theorem 3.3 which is based on primitive integrality. With these coordinates the second entry from \( \mathbb{Q}^\times \) remains invariant under the involution (since \( (a, b, c) \) is integral and primitive if and only if \( (b, a, c) \) is), perhaps up to a sign. More precisely, we presented one lift in which \( a \) is assumed to be positive (like in Corollary 2.2), and another one in which \( c \) is taken to be positive (see Proposition 3.1). With the latter convention the involution always leaves the second \( \mathbb{Q}^\times \) coordinate invariant, but with the former one it will change sign in case \( \beta < 0 \) (i.e., \( 0 < r < 1 \) or \( r < -1 \)).

On the other hand, the following result of [BS] is a consequence of Proposition 4.1.

**Corollary 4.2.** All the Pythagorean triples are generated, up to global scalars, by the triples \((4, 3, 5)\) and \((-1, 0, 1)\) (or \((1, 0, -1)\)) using the multiplication and the involution.

Indeed, we may investigate the question in the coordinate \( r \). It suffices to generate the rational primes the triple \((4, 3, 5)\), since then the multiplication allows us to generate all the other elements (and the sign is covered by the other triple appearing in Corollary 4.2). Now, the triple \((4, 3, 5)\) is the one associated with the prime 2, and we work by induction on the primes (ordered by magnitude, of course). Assuming that we have generated all the primes that are smaller than the odd prime \( p > 2 \), we can construct the numerator and the denominator of its Cayley transform image \( \frac{r + 1}{r - 1} \) (since they are products of smaller primes), thus producing \( p \) itself by the formula for the involution from Proposition 4.1. Hence the latter proposition and Corollary 3.2 imply Corollary 4.2.

Once we have an involution, it is interesting to consider points that are fixed by it, or almost fixed by it. A triple that is fixed by the involution would have to be with \( a = b \), so that \( \beta = 1 \), and \( r \) is a solution to any of the two equations \( \frac{r}{2} - \frac{1}{b^2} = 1 \) or \( r = \frac{b + 1}{b - 1} \), both of which are equivalent to the quadratic equation \( r^2 - 2r - 1 = 0 \). The real solutions of that equation are \( r = 1 \pm \sqrt{2} \), which are no longer rational, but by extending scalars in \( \mathbb{E} \) this parameter indeed corresponds to the norm 1 element \( \pm \sqrt{2} + \varepsilon \) as well as to the “real Pythagorean
triple” \((1, 1, \pm \sqrt{2})\). While these numbers are not allowed in the rational world, we would like to see how can we approximate them using rational numbers, and what Pythagorean triples arise in the process (these should be with \(a\) and \(b\) entries that are very close to one another).

For this we observe that the number \(1 + \sqrt{2}\) is the fundamental unit of the ring of integers in the field \(\mathbb{K} = \mathbb{Q}(\sqrt{2})\) (the other solution for \(r\) is minus its inverse), so that it generates (with \(-1\)) the group of units of that ring of integers, and note that \(N_{\mathbb{K}}(1 + \sqrt{2}) = -1\) (this will be important for some signs later). Regardless of fixed points, this number also generates pairs of rational numbers that are related via the involution, when one works inside that ring.

To see this, consider a reduced fraction \(\frac{m}{n}\) with \(mn\) odd and \(m > n > 0\), so that \(m = n + 2l\) for some integer \(l > 0\) that is co-prime to \(n\), and set \(k = n + l\). Then it is easy to verify that \(k\) and \(l\) are co-prime, \(kl\) is even, and the quotient \(\frac{k}{l}\) is the image of \(\frac{m}{n}\) under the involution. The relations between \(n\), \(m\), \(k\), and \(l\) are equivalent to the equality \(m + k\sqrt{2} = (1 + \sqrt{2})(n + l\sqrt{2})\). From the odd part of Proposition 3.1 with \(m = n + 2l\) we extract the primitive Pythagorean triple \((n^2 + 2ln, 2l^2 + 2ln, n^2 + 2l^2 + 2ln)\), and one can also verify that from \(n + l\) with even \(l\) we indeed get the same Pythagorean triple with the first two coordinates inverted. Observe that the difference between the first two entries here is the norm \(n^2 - 2l^2\) of \(n + l\sqrt{2}\), and as \(N_{\mathbb{K}}(m + k\sqrt{2})\) is the additive inverse of the latter norm (by the value of \(N_{\mathbb{K}}(1 + \sqrt{2})\)), we have established the following result.

**Lemma 4.3.** Let \(n\) and \(l\) be co-prime positive integers with \(n\) odd, and define \(m\) and \(k\) via the equality \(m + k\sqrt{2} = (1 + \sqrt{2})(n + l\sqrt{2})\). Then the two quotients \(\frac{m}{n}\) and \(\frac{k}{l}\) are related by our involution. Moreover, if \((a, b, c)\) and \((b, a, c)\) are the associated primitive integral Pythagorean triples then \(|a - b|\) coincides with \(|N_{\mathbb{K}}(n + l\sqrt{2})|\), or equivalently with \(|N_{\mathbb{K}}(m + k\sqrt{2})|\).

In fact, Lemma 4.3 holds also for non-positive \(n\) and \(l\), when the signs are normalized correctly, and when one avoids the cases where \(l = -n = \pm 1\) in order for \(k = l + n\) not to vanish. Note that the assumption that \(n\) is odd can always be obtained by dividing by the right power of \(\sqrt{2}\), without affecting the relations in Lemma 4.3 (or at most interchanging the roles of \(n\) and \(l\) as well as those of \(m\) and \(k\)). The choice of \(mn\) being odd is arbitrary—alternatively, every fraction \(\frac{k}{l}\) with even \(kl\) is of the form \(\frac{m}{n}\) with odd \(n\), and we let the involution work in the other direction. Lemma 4.3 also provides a different point of view on Corollary 1 of [M].

We also remark that with the multiplication law of \([E]\) and \([T]\), which is based on \(\mathbb{K} = \mathbb{Q}(\sqrt{-1})\), our involution corresponds to complex conjugation times a power of \(\sqrt{-1}\). Dividing by scalars, as well as by the torsion part (as \([E]\) does), this involution reduces to the inversion on the free quotient group of \(\mathbb{K}^1\).
5 Differences and Quadratic Units

Many possible ways for ordering the set of integral Pythagorean triples are based on the appropriate differences. The most classical one, appearing in [M] and many references therein, uses the height \( h = c - b \) of the Pythagorean triple \((a, b, c)\) already mentioned above. For the primitive integral Pythagorean triple from Proposition 3.1 this parameter is \( n^2 \) if \( m \) and \( n \) are odd and \( 2n^2 \) otherwise (compare with Proposition 1 of [M], and note that in our Proposition 3.1 we assume that \( c > 3 \)).

For the difference \( c - a \) all that we have to do is interchange \( a \) and \( b \), i.e., apply our involution. The image of \( r = \frac{m}{n} \) is, in reduced terms, \( \frac{m+n}{m-n} \) when \( m \) and \( n \) are both odd (and then this fraction involves an even number) and just \( \frac{m+n}{m-n} \) (with odd numerator and denominator) otherwise. Indeed, the difference \( \frac{m^2+n^2}{m-n} \) is twice the square of the denominator \( \frac{m-n}{2} \) in the odd \( mn \) case, and \( (m^2+n^2) - 2mn \) is the exact square of the denominator \( m-n \) when \( mn \) is even. The integral Pythagorean triples for which \( c - a = 1 \) are thus those of the form \( (\frac{m^2-1}{2}, m, \frac{m^2+1}{2}) \) for odd \( m \), associated with the number \( r = \frac{(m+1)^2}{(m-1)^2} \), while those for which \( c - a = 2 \) are those taking the form \( (m^2-1, 2m, m^2+1) \) with even \( m \), for which \( r = \frac{m+1}{m-1} \). The first few examples are \( (\pm 1, 0, 1), (\pm 3, 4, 5), (\pm 5, 12, 13), (\pm 7, 24, 25), \) and \( (\pm 9, 40, 41) \) with odd \( m \), \( (0, -1, 1), (\pm 4, 3, 5), (\pm 8, 15, 17), (\pm 12, 35, 37), \) and \( (\pm 16, 63, 65) \) with even \( m \), and their images under the involution.

The next value of that difference is \( h = 9 \), with \( n = 3 \) and odd \( m \) not divisible by 3. The first few values of \( r \) are \( \frac{1}{3}, \frac{2}{3}, \frac{5}{7}, \) and \( \frac{4}{7} \), with the Pythagorean triples \( (3, -4, 5), (15, 8, 17), (21, 20, 29), \) and \( (33, 56, 65) \). When the difference \( c - a \) is 9 we obtain the involution images \( -2, 4, \frac{5}{2}, \) and \( \frac{7}{2} \), with the respective Pythagorean triples.

However, in relation with our involution and its approximate fixed points, we are interested in those integral Pythagorean triples for which \( |a - b| \) is small. By Lemma 4.3 such Pythagorean triples arise from quotients of the form \( \frac{m}{n} \) (or \( \frac{1}{n} \) after the involution), where \( m + k \sqrt{2} = (1 + \sqrt{2})(n + l \sqrt{2}) \) and the norm of \( n + l \sqrt{2} \) (or equivalently of \( m + k \sqrt{2} \)) is small in absolute value. Now, this norm is \( \pm 1 \) precisely for the units of the ring of integers in the field \( \mathbb{K} = \mathbb{Q} (\sqrt{2}) \), which are (up to sign) just the (positive or negative) powers of the fundamental unit \( 1 + \sqrt{2} \). We shall thus write, for every natural \( j \), the number \( (1 + \sqrt{2})^j \) as \( s_j + t_j \sqrt{2} \), so that \( s_1 = t_1 = 1 \) and we have the recursive rule \( s_{j+1} = s_j + 2t_j \) and \( t_{j+1} = s_j + t_j \) (one may apply these formulae for \( j = 0 \) as well, with \( s_0 = 1 \) and \( t_0 = 0 \), and the same recursive rule relates them to \( s_1 \) and \( t_1 \)). Note that this recursive rule implies that \( s_j \) is odd for every \( j \) (since so is \( s_1 \), or equivalently \( s_0 \)), and hence \( t_j \) has the same parity as \( j \).
If \( j \) is large then so are \( s_j \) and \( t_j \), but on the other hand we have the equality
\[
s_j^2 - 2t_j^2 = N_K^s(1 + \sqrt{2})^j = (-1)^j \text{ implying that } s_j \text{ and } t_j\sqrt{2} \text{ are very close. In particular, it follows that the quotients } \frac{s_{j+1}}{s_j} \text{ and } \frac{t_{j+1}}{t_j} \text{ are very close to one another, and they are also close to the ratio } \frac{s_{j+1} + t_{j+1}\sqrt{2}}{s_j + t_j\sqrt{2}} = 1 + \sqrt{2}. \text{ They should therefore be almost fixed by our involution. Indeed, using Lemma 4.3 one immediately deduces the following result.}

**Theorem 5.1.** The quotients \( \frac{s_{j+1}}{s_j} \) and \( \frac{t_{j+1}}{t_j} \) correspond to primitive integral Pythagorean triples \((a, b, c)\) in which \( a \) and \( b \) differ by 1, and for each \( j \) they are related to one another via the involution.

For the first few examples of Theorem 5.1 we evaluate the next few powers of \( 1 + \sqrt{2} \) as \( 3 + 2\sqrt{2}, 7 + 5\sqrt{2}, 17 + 12\sqrt{2}, 41 + 29\sqrt{2}, \) and \( 99 + 70\sqrt{2}. \) The respective quotients \( \frac{t_{j+1}}{t_j} \) are \( 2, \frac{5}{3}, \frac{12}{7}, \frac{29}{17}, \) and \( \frac{70}{41}, \) producing the Pythagorean triples \((4, 3, 5), (20, 21, 29), (120, 119, 169), (696, 697, 985), \) and \((4060, 4059, 5741)\) (since \( t_jt_{j+1} \) is always even). The quotients \( \frac{s_{j+1}}{s_j} \) are \( 3, \frac{7}{3}, \frac{17}{9}, \frac{41}{21}, \) and \( \frac{99}{41}, \) always with odd numbers, and one can verify that they are the respective images of the previous numbers under the involution and that they produce the same Pythagorean triples with \( a \) and \( b \) inverted. As the inverse of \( 1 + \sqrt{2} \) is \( -1 + \sqrt{2}, \) with negative \( j \) we get \( t_j = (-1)^j t_{-j} \) and \( s_j = (-1)^j s_{-j}. \) The resulting quotients are thus obtained by replacing the previous values of \( r \) by \( -\frac{1}{r}. \) As replacing \( \frac{a}{b} \) by \( -\frac{b}{a} \) simply inverts the sign of both \( a \) and \( b \) in Proposition 3.1, this part gives essentially no new triples. Another possible operation is to invert the sign of \( c, \) and note that replacing \( r \) by \( \frac{1}{r} \) or \( -r \) here will give Pythagorean triples in which \( a \) and \( b \) have opposite signs and they satisfy \(|a + b| = 1. \)

Recall that the distance between \( a \) and \( b \) in a primitive Pythagorean triple has to be odd, and by Lemma 4.3 it also has to be a norm of an integral element from \( \mathbb{K}. \) Since numbers that are congruent to 3 or 5 modulo 8 cannot be such norms (this is seen either by investigating the behavior of rational primes in that field or simply by considering the expression \( n^2 - 2t^2 \) for the norm modulo 8), the smallest possible distance after 1 is 7. Indeed, the elements \( 3 - \sqrt{2} \) and \( -1 + 2\sqrt{2} \) have norms \( \pm 7, \) and we can multiplying them by powers of \( 1 + \sqrt{2} \) and take the quotients like in Lemma 4.3 and Theorem 5.1. This produces the quotients \(-2, \frac{1}{2}, \frac{3}{2}, 4, \) and \( \frac{5}{3}, \) with the Pythagorean triples \((-4, 3, 5), (4, -3, 5), (12, 5, 13), (8, 15, 17), \) and \((48, 55, 73), \) as well as their respective involution images \( \frac{1}{2}, -3, -5, \) and \( \frac{3}{5}, \) with their corresponding Pythagorean triples.

In fact, when investigating more general differences, units in other number fields arise, though the Pythagorean triples in question will no longer be nearly fixed by the involution. As another example we consider the difference \( c - 2a. \) Here we seek expressions for which \( a \) is close to 2, and the elements in \( \mathbb{E}^1 \) with extended scalars is \( 2 \pm \sqrt{3}, \) with the respective extended value of \( r \) being \( 2 \pm \sqrt{3}. \) Hence for investigating \( c - 2a \) on Pythagorean triples we shall need the field \( \mathbb{K} = \mathbb{Q}(\sqrt{3}). \) Indeed, the latter numbers are the fundamental unit in the ring of integers of that field and its inverse, but now the norm of that unit is \( N_{\mathbb{Q}}(2 + \sqrt{3}) = +1. \) Applying the involution, the resulting value of the extended
For obtaining an analogue of Lemma 4.3 we shall take a fraction $\frac{m}{n}$ with $m > 2n > 0$, and assume that 3 divides $m - 2n$ (so that it does not divide $n$). Hence we have $m = 2n + 3l$ for some $l > 0$, and by setting $k = n + 2l$ the relation is expressed as $m_k = k\sqrt{3} = (2 + \sqrt{3})(n + l\sqrt{3})$. The parity of $mn$ is that of $nl$, which also coincides with that of $kl$ and of $km$. Assuming first that all these numbers are even, Proposition 5.1 produces the primitive integral Pythagorean triple $(4n^2 + 6ln, 3n^2 + 12ln + 9l^2; 5n^2 + 12ln + 9l^2)$ for $\frac{m}{n}$, as well as $(4l^2 + 2ln, n^2 + 4ln + 3l^2, n^2 + 4ln + 5l^2)$ for $\frac{n}{l}$. The value of $c - 2a$ in the latter Pythagorean triple is the norm $n^2 - 3l^2$ of our number $n + l\sqrt{3}$ (here it coincides with that of $m + k\sqrt{3}$ by the value of $N_{Q_3}^N(2 + \sqrt{3})$), and in the former Pythagorean triple we get $9l^2 - 3n^2$ via this operation, which is $-3$ times that norm. If $nl$ is odd (and so are the other three products) then our norm is even, and all the numbers in the Pythagorean triples must be halved. The analogue of Lemma 4.3 that we have proved is thus as follows.

**Lemma 5.2.** Assume that $n$ and $l$ are co-prime positive integers with $n$ not divisible by 3, and let $m$ and $k$ be defined by $m_k = k\sqrt{3} = (2 + \sqrt{3})(n + l\sqrt{3})$. Denote by $(a, b, c)$ and $(f, g, h)$ the primitive integral Pythagorean triples that are associated with $\frac{m}{n}$ and $\frac{n}{l}$ respectively via Proposition 5.1. If $nl$ is even then the value of $c - 2a$ is $N_{Q_3}^N(n + l\sqrt{3})$ (which is the same as $N_{Q_3}^N(m + k\sqrt{3})$), and $h - 2f$ is the same value but multiplied by $-3$. On the other hand, when $nl$ is odd then the latter norm is even, $c - 2a$ equals half that norm, and $f - 2d$ is that norm times $-\frac{1}{2}$.

For the difference $c - 2b$ we shall, of course, take the images of these numbers and triples under the involution. Our numbers $\frac{m}{n} = \frac{2n + 3l}{n}$ and $\frac{n}{l} = \frac{n + 2l}{l}$ are sent via this involution to $\frac{2n + 3l}{n + 3l}$ and $\frac{n + 2l}{l + 3n}$ respectively for even $nl$ and to $\frac{(n + 3l)/2}{(n + l)/2}$ and $\frac{(n + 3l)/2}{(n + l)/2}$ respectively when $nl$ is odd. This is also visible in the decomposition of the $b$-entry in the Pythagorean triples we used for proving Lemma 5.2.

As above, write the power $(2 + \sqrt{3})^j$ as $\xi_j + \eta_j\sqrt{3}$, so that $\xi_{j+1} = 2\xi_j + 3\eta_j$ and $\eta_{j+1} = \xi_j + 2\eta_j$, with $\xi_0 = 2$ and $\eta_0 = 1$ (and also $\xi_0 = 1$ and $\eta_0 = 0$). Note that the parity of $\eta_j$ is like that of $j$ while that of $\xi_j$ is the opposite one, implying that $\xi_j\eta_j$ is always even. In addition, the element $\sqrt{3} - 1$ of $K$ has norm $-2$, and we write $\lambda_j + \mu_j\sqrt{3}$ for $(\sqrt{3} - 1)(2 + \sqrt{3})^j$. Therefore $\lambda_j$ and $\mu_j$ satisfy the same recursive relation as above, but with the initial conditions $\lambda_0 = 1$ (and also $\lambda_0 = -1$ and $\mu_0 = 1$), and $\lambda_j$ and $\mu_j$ are odd for every $j$. The Pythagorean triples with small value of $|c - 2a|$ are now described, via Lemma 5.2, as follows.

**Theorem 5.3.** The positive integral Pythagorean triples $(a, b, c)$ for which the equality $c - 2a = 1$ holds are those associated with the quotients $\frac{\eta_j}{\xi_j}$, while those in which this expression is $-3$ come from the rational numbers $\frac{\eta_j}{\lambda_j}$. For obtaining such triples with $c - 2a = -1$ one takes the quotients $\frac{\eta_{j+1}}{\mu_j}$, and the numbers $\frac{\eta_j}{\lambda_j}$ produce the triples in which that difference equals 3.
The next first powers of \(2+\sqrt{3}\) are \(7+4\sqrt{3}\), \(26+15\sqrt{3}\), and \(97+56\sqrt{3}\). Hence the first few examples of the first assertion in Theorem 5.3 are the Pythagorean triples \((8, 15, 17)\), \((120, 209, 241)\), and \((1680, 2911, 3361)\) associated with the rational numbers \(4, \frac{15}{4}\), and \(\frac{56}{15}\). The second assertion there is illustrated by the quotients \(2, \frac{7}{2}, \frac{26}{7}\), and \(\frac{97}{26}\), with the Pythagorean triples \((4, 3, 5)\), \((28, 45, 53)\), \((364, 627, 725)\), and \((5044, 8733, 10085)\). Multiplying these four powers by our norm \(-2\) element \(\sqrt{3}-1\) gives \(1+\sqrt{3}\), \(5+3\sqrt{3}\), \(19+11\sqrt{3}\), and \(71+41\sqrt{3}\), so that for the third assertion of Theorem 5.3 we take the Pythagorean triples \((1, 0, 1)\), \((3, 4, 5)\), \((33, 56, 65)\), and \((451, 780, 901)\) associated with the numbers \(1, 3, \frac{11}{3}\), and \(\frac{41}{11}\). To demonstrate the fourth one we can use the numbers \(-1, 5, \frac{10}{5}\), and \(\frac{71}{19}\), associated with the Pythagorean triples \((-1, 0, 1)\), \((5, 12, 13)\), \((85, 168, 193)\), and \((1349, 2340, 2701)\). The decomposition of the \(b\)-entries as the products \((n+l)(n+3l)\), \(3(n+l)(n+3l)\), \((n+l)(n+3l)\), and \(3(n+l)(n+3l)\) respectively can also be easily verified in these examples.

For negative \(j\) we note that \(\frac{1}{2+\sqrt{3}} = 2-\sqrt{3}\), so that \(\xi_j = \xi_{-j}\) and \(\eta_j = -\eta_{-j}\). Similarly, for the other numbers we get \(\lambda_j = -\lambda_{1-j}\) and \(\mu_j = \mu_{1-j}\). The quotients for negative \(j\) are the multiplicative inverses of those with positive \(j\), yielding the same Pythagorean triples but with the sign of \(b\) inverted (not affecting \(c-2a\)). For obtaining the Pythagorean triples with \(c-2b \in \{\pm 1, \pm 3\}\) we take the involution images of those from Theorem 5.3 and we can express them by the appropriate combinations of the \(\xi_j\)s and the \(\eta_j\)s or of the \(\lambda_j\)s and the \(\mu_j\)s.

Other kinds of differences will put units in other real quadratic fields into the analysis. However, the existence of units of the form \(a+b\sqrt{d}\) with half-integral \(a\) and \(b\) (like the golden ratio \(1+\sqrt{5}/2\), which is an integral unit in \(K = \mathbb{Q}(\sqrt{5})\)) can lead to complications in general. This may also be the case when the quadratic field \(K\) in question has class number that is larger than 1. We leave these questions for later research.

References

[BS] Beauregard, R. A., Suryanarayan, E. R., PYTHAGOREAN TRIPLES: THE HYPERBOLIC VIEW, College Math. J., vol. 27 no. 3, 170–181 (1996).

[E] Eckert, E. J., THE GROUP OF PRIMITIVE PYTHAGOREAN TRIANGLES, Math. Magazine, vol. 57 no. 1, 22–27 (1984).

[M] McCullough, D., HEIGHT AND EXCESS OF PYTHAGOREAN TRIANGLES, Math. Magazine, vol. 78 no. 1, 26–44 (2005).

[T] Taussky, O., SUMS OF SQUARES, Am. Math. Monthly, vol. 77, 805–830 (1970).

EINSTEIN INSTITUTE OF MATHEMATICS, THE HEBREW UNIVERSITY OF JERUSALEM, EDMUND SAFRA campus, JERUSALEM 91904, ISRAEL
E-mail address: zemels@math.huji.ac.il