Sums of Squares: Talk 10

Eric Ceglie

4.5.2023

This talk is based on the book "A Journey Through The Realm of Numbers" by Menny Aka et al.

1. The Challenge $\square + 5\square$

Definition. A prime $p \in \mathbb{N}$ is called *possible* if $p = 2$, $p = 5$, or $p \equiv 1, 3, 7, 9 \mod 20$. A natrual number $n \in \mathbb{N}$ is called *possible* if it is of the form

$$n = m^2 p_1 \cdots p_k$$

for some $m \in \mathbb{N}$ and $k \in \mathbb{N}_0$ possible primes $p_1, \ldots, p_k \in \mathbb{N}$. Furthermore, if n is non-zero and of the form

$$n = x^2 + 5y^2$$

for $x, y \in \mathbb{Z}$ it is called an *actual number* and if it is of the form

$$n = 2u^2 + 2uv + 3v^2$$

for $u, v \in \mathbb{Z}$ it is called a *flipped number.*

Remark. Remember that this definition was chosen in such a way that for every possible prime p the number -5 is a square in $\mathbb{F}_p$.

Definition. Let $P \subseteq \mathbb{N}$ be the set of all possible numbers, $A \subseteq \mathbb{N}$ the set of all actual numbers and $F \subseteq \mathbb{N}$ the set of all flipped numbers.

Lemma 1. (Exercise 8.47) We have $A \cup F \subseteq P$.

Lemma 2. (Exercise 8.50) We have

$$\begin{aligned} \forall a \in A: &\quad a \equiv 0, 1, 4, 5, 6 \mod 8 \\ \forall f \in F: &\quad f \equiv 0, 2, 3, 4, 7 \mod 8. \end{aligned}$$

Furthermore, we have

- $n \in A \iff 2n \in F \iff 4n \in A$.
- $n \in F \iff 2n \in A \iff 4n \in F$.
- $A \cap F = \emptyset$.

Note that **Lemma 1** and **2** were already proven in Talk 9 (or in previous exercise sheets).

Lemma 3. (Exercise 8.53) For every possible odd prime $p \in \mathbb{N}$ there exist $n \in \mathbb{N}_0$ and $a, b \in \mathbb{Z}$ such that $2^n p = a^2 + 5b^2$ holds.

Proof. Let $p > 2$ be a possible odd prime number. By definition, this means that there exists a $k \in \mathbb{Z}$ such that

$$k^2 \equiv -5 \mod p$$

holds. Let us now define

$$w := k + i\sqrt{5} \in R := \mathbb{Z}[\tfrac{1}{2}, i\sqrt{5}]$$

and observe that

$$p \mid k^2 + 5 = N(w) = \phi(w),$$

where ϕ is the function defined in **Exercise 8.52**. Now by the same exercise, the Ring (R, ϕ) is an Euclidean domain and thus we may apply our Swiss army knife to obtain a greatest common divisor of w and p represented by

$$q = aw + bp \in R$$

for $a, b \in R$. Now since

$$R = \{x + i\sqrt{5}y \mid a, b \in \mathbb{Z}[\tfrac{1}{2}]\}$$

holds, there exists a $n \in \mathbb{N}_0$ such that we have $2^n a, 2^n b \in \mathbb{Z}[i\sqrt{5}]$. Using this, we get

$$\tilde{q} := 2^n q \in \mathbb{Z}[i\sqrt{5}].$$

Furthermore, since $q \mid p$ holds in R, we get $\tilde{q} \mid 2^n p$ in $\mathbb{Z}[i\sqrt{5}]$ and thus $N(\tilde{q}) \mid 2^{2n} p^2$ in $\mathbb{Z}$. But from the definition of w, we have $p \nmid w$ and thus $p \nmid q$ (otherwise it would contradict $q \mid w$) both in R. But then $\frac{p}{q}$ is not a unit in R and since all units in R have norm equal to 1 this implies

$$1 < \phi\left(\frac{p}{q}\right) = \frac{p^2}{\phi(q)}$$

and thus $\phi(q) < p^2$. From this we get $p^2 \nmid N(\tilde{q})$ in $\mathbb{Z}$ because we have $N(\tilde{q}) = \phi(\tilde{q}) = \phi(q)$. Hence we arrive at

$$N(\tilde{q}) \mid 2^{2n} p. \tag{1}$$

Now observe that

$$\begin{aligned} N(\tilde{q}) &= N(2^n aw + 2^n bp) \equiv N(2^n aw) \\ &= N(2^n a) \underbrace{N(w)}_{\equiv 0 \mod p} \equiv 0 \mod p \end{aligned}$$

and thus $p \mid N(\tilde{q})$. Combining this with (1), there now exists a $m \in \mathbb{N}_0$ such that

$$N(\tilde{q}) = 2^m p$$

holds and since we have $\tilde{q} \in \mathbb{Z}[i\sqrt{5}]$, there exist integers $x, y \in \mathbb{Z}$ such that $\tilde{q} = x + i\sqrt{5}y$. Hence we may now conclude that

$$2^m p = N(\tilde{q}) = x^2 + 5y^2$$

holds which proves our claim. □

Theorem 8.54 (□ + 5□). Let $n \in \mathbb{N}$ be a possible number.

(a) n is either a flipped number or an actual number. Furthermore, we have $P = A \sqcup F$.

(b) If n is not divisible by 4, then we have

$$\begin{aligned} n \text{ is an actual} &\iff n \equiv 1, 5, 6 \mod 8 \\ n \text{ is flipped} &\iff n \equiv 2, 3, 7 \mod 8. \end{aligned}$$

(c) Products of two actual numbers are actual numbers, products of two flipped numbers are actual number, and a product of one actual number and one flipped number is a flipped number. In a more concise notation, this says that

$$\begin{aligned} \forall a_1, a_2 \in A: &\quad a_1 a_2 \in A \\ \forall f_1, f_2 \in F: &\quad f_1 f_2 \in A \\ \forall a \in A\, \forall f \in F: &\quad af \in F \end{aligned}$$

holds.

Proof. Let $n \in \mathbb{N}$ be a possible number, hence it is by definition of the form

$$n = m^2 p_1 \cdots p_k$$

for some $m \in \mathbb{N}$ and $k \in \mathbb{N}_0$ possible primes $p_1, \ldots, p_k \in \mathbb{N}$.

- First assume that all p_i are odd. Let $i \in \{1, \ldots, k\}$ be arbitrary. Then by **Lemma 3** there exists a $\mu_i \in \mathbb{N}_0$ and $a_i, b_i \in \mathbb{Z}$ such that

  $$2^{\mu_i} p_i = a_i^2 + 5b_i^2$$

  holds and thus we have $2^{\mu_i} p_i = N(z_i)$ for $z_i := a_i + i\sqrt{5}b_i \in \mathbb{Z}[i\sqrt{5}]$. Now since $\mathbb{Z}[i\sqrt{5}]$ is a ring, there exist integers $a, b \in \mathbb{Z}$ such that

  $$a + i\sqrt{5}b = m z_1 \cdots z_k$$

holds. Using the multiplicity of the norm N we obtain

$$\begin{aligned} a^2 + 5b^2 &= N(mz_1 \cdots z_k) = N(m)N(z_1) \cdots N(z_k) \\ &= m^2 2^{\mu_1} p_1 \cdots 2^{\mu_k} p_k = 2^{\mu} n \end{aligned}$$

for $\mu := \mu_1 + \ldots + \mu_k \in \mathbb{N}_0$ and thus we have $2^{\mu} n \in A$. By repeatedly dividing out 2 and using **Lemma 2** we can conclude that $n \in A \cup F$ holds.

- Now assume that w.l.o.g. p_1 is even. In this case, define $n' := m^2 p_2 \cdots p_k$ and apply the same strategy as in the case above to obtain $n' \in A \cup F$. Then by multiplying n' by 2 and using **Lemma 2**, we can conclude that $n \in A \cup F$ holds.

Thus we have now shown that $P \subseteq A \cup F$ holds. But from **Lemma 1** we also know that $A \cup F \subseteq P$ holds and we obtain equality. Since in **Lemma 2** it was shown that a natural number cannot be both actual and flipped, we may now conclude that $P = A \sqcup B$ holds as claimed in (a).

Now for part (b) assume that n is not divisible by 4, so

$$n \not\equiv 0, 4 \mod 8 \tag{1}$$

holds. Since in (a) we have shown that $n \in A \sqcup F$ holds, the claim in (b) follows immediately by applying **Lemma 2** and using (1).

To prove part (c), we start by computing the following tables using SageMath.

·	0	1	4	5	6
0	0	0	0	0	0
1	0	1	4	5	6
4	0	4	0	4	0
5	0	5	4	1	6
6	0	6	0	6	4

Table 1: Actual times actual modulo 8.

·	0	1	4	5	6
0	0	0	0	0	0
2	0	2	0	2	4
3	0	3	4	7	2
4	0	4	0	4	0
7	0	7	4	3	2

Table 2: Actual times flipped modulo 8.

·	0	2	3	4	7
0	0	0	0	0	0
2	0	4	6	0	6
3	0	6	1	4	5
4	0	0	4	0	4
7	0	6	5	4	1

Table 3: Flipped times flipped modulo 8.

Also note that products of possible numbers are again prossible numbers, which follows from the definition. Let $a, b \in A$ and $f, g \in F$ be arbitrary. We start by assuming that a, b, f, g are all not divisible by 4, so

$$\begin{aligned} a, b &\equiv 1, 5, 6 \mod 8 \\ f, g &\equiv 2, 4, 7 \mod 8 \end{aligned}$$

holds. Observe that if a, b, f, g are all odd then just by looking at Tables 1-3 and applying part (b) we already get

$$ab \in A, \quad af \in F, \quad fg \in A. \tag{2}$$

Now we have to deal with the all the even cases.

- If a is even and b is odd, then we get $ab \in A$ from Table 1.
- If a and b are both even, then by **Lemma 2** the numbers $\frac{a}{2}$ and $\frac{b}{2}$ are flipped. But they are also both odd because a, b were not divisible by 4. Hence by (2) we get $\frac{a}{2}\frac{b}{2} \in A$ and again using **Lemma 2** while multiplying by 4 this implies $ab \in A$.
- If a is even and f is odd, then we get $af \in F$ from Table 2.
- If a and f are both even, then $\frac{a}{2} \in F$ and $\frac{f}{2} \in A$ are odd and thus by (2) we have $\frac{a}{2}\frac{f}{2} \in F$. Hence we get $af \in F$ by multiplying by 4.
- If a is odd and f is even, then we get $af \in F$ From Table 2.
- If f is even and g is odd, then we get $fg \in A$ from Table 3.
- If f and g are both even, then $\frac{f}{2} \in A$ and $\frac{g}{2} \in A$ are odd and thus by (2) we have $\frac{f}{2}\frac{g}{2} \in A$. Hence we get $fg \in A$ by multiplying by 4.

Hence we have proven (c) in the case that none of a, b, f, g are divisible by 4. Now if some of them are divisible by 4, we can divide out all powers of 4, then apply what we have shown and again multiply by 4 while using **Lemma 2** to arrive back at the numbers we started at. This works since the sets A and F are closed under multiplication and division by 4. □

Remark. An interesting observation is that part (c) of the theorem hints to a hidden group structure resembling $\mathbb{Z}/2\mathbb{Z}$.

2. Binary Quadratic Forms

Definition. A *(binary) quadratic form* is an Element of the form

$$f(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$$

and f is called *primitive* if $\gcd(a,b,c) = 1$ holds. For a more concise notation, we may identify a quadratic form with its coefficients and write $f = [a,b,c]$.

Definition. For a quadratic form $f = [a,b,c]$ we define the *discriminant* by

$$\Delta_f := b^2 - 4ac.$$

Definition. Two quadratic forms f and g are called *equivalent* if there exists a $U \in \mathrm{SL}_2(\mathbb{Z})$ with

$$f(x,y) = g((x,y)U)$$

and we denote it by $f \sim g$.

Remark. Note that $\sim$ actually defines an equivalence relation.

Remark. Lagrange used a different notion of equivalence, in which he allowed $U \in \mathrm{GL}_2(\mathbb{Z})$. Since Gauss it has been recognized that this definition is inferior to that given above. If there is a need to distinguish, sometimes forms are called *properly equivalent* using the definition above and *improperly equivalent* if they are equivalent in Lagrange's sense.
[Wikipedia, https://en.wikipedia.org/wiki/Binary_quadratic_form, 1.5.2023]

Definition. For every $D < 0$, we call the number of equivalence classes under $\sim$ of quadratic forms with discriminant equal to D the *class number* $h(D)$.

From now on, we will only consider primitive quadratic forms with negative discriminant.

Theorem 1. Every quadratic form is equivalent to a form $[a,b,c]$ with

$$|b| \leq a \leq c.$$

Proof. See exercise sheet 10, task 3.

Corollary. For every $D < 0$ the class number $h(D)$ is finite.

Proof. See exercise sheet 10, task 4.

Definition. A quadratic form $[a,b,c]$ is said to be *reduced* if it fulfills

$$\begin{gathered} |b| \leq a \leq c \\ a = |b| \text{ or } a = c \implies b \geq 0. \end{gathered}$$

Theorem 2. Every quadratic form is equivalent to a unique reduced form.

Proof Idea. In a first step, we use **theorem 1** to show that every quadratic form is equivalent to a reduced form. For this, we assume that $[a, b, c]$ already fulfills $|b| \leq a \leq c$ and distinguish two cases.

- If $a = c$ and $b < 0$ holds, we use

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$$

  to show $[a, b, c] \sim [c, -b, a]$.

- If $a = |b|$ and $b < 0$ holds, we use

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$$

  to obtain

$$[a, b, c] \sim [a, 2a + b, a + b + c] = [a, -b, c].$$

In a second step, one shows that two different reduced forms never lie in the same equivalence class, which will prove the uniqueness. Note that this is a more technical step and uses the following lemma.

Lemma 4. Suppose that the quadratic form $f = [a, b, c]$ satisfies $|b| \leq a \leq c$. Then a is the minimum of f, that is

$$\forall (x, y) \in \mathbb{Z}^2 \setminus \{0\} : f(x, y) \geq a.$$

Furthermore, if (x, y) and (u, v) do not lie on the same line through the origin, then

$$f(x, y) f(u, v) \geq ac$$

holds.

With this lemma in mind and a good amount of optimism, the proof of **theorem 2** might pass the *"tie you to a tree test"*. A full proof as well as other interesting material can be found in Meier, Robert, and Paul Seidel. "Binary Quadratic Forms and the Class Number Formula." (2019).