BMS Student Conference 2021 - Sum of two squares

Branislav Šobot*

March 2021

Warning!

Dear reader, in this short talk I would like to explain why I like number theory. We will concentrate our attention on a theorem of Fermat whose various proofs fantastically illustrate diversity of mathematical methods that come into play when one deals with number theory. None of the result and arguments here will be deep, but (almost) every one of them has the goal of introducing some interesting method, notion or even entire subarea of number theory. If you have any questions or suggestions, don't hesitate to contact me. I hope you will enjoy this!

Contents

1 What is this talk about?

In his letter written in 1640 to Mersenne[1], Fermat[2] stated the following result.

Theorem 1.1 (Fermat's theorem on sum of two squares)**.** *Every prime number p of the form $4k+1$ can be expressed as sum of two squares, that is there are integers x and y with $p = x^2 + y^2$.*

Truth to be told, Albert Girard[3] was probably the first who conjectured this result, but here once again history gives advantage to a more famous mathematician. Anyhow, like many other of his "results", Fermat didn't really provide any proof of his claim. The first proof of this theorem

*banesobot@gmail.com, Humboldt University

[1]Marin Mersenne(1588–1648), a French mathematician

[2]Pierre de Fermat(1607–1665), a French lawyer and mathematician

[3]Albert Girard(1595–1632), a French mathematician

was provided by Euler[4] in 1749. In the following 300 years many new interesting proof were found and we will discuss some of them in the sections to come.

First, we will see Euler's original proof which uses famous method of infinite descent (probably the second most boring proof). After this, we will see two (combinatorial) proofs which are based on the so-called Pigeon-hole principle. Although these two are essentially the same, they can be viewed from different perspectives and open us different doors. In between them we will throw in Dedekind's[5] (algebraic) proof which exploit the machinery of Gaussian integers. Next comes a (geometric) proof via Minkowski's[6] theorem which is (in my modest opinion) probably the most beautiful one. It is followed by Lagrange's[7] (algebraic) proof (later simplified by Gauss[8]) which makes use of quadratic forms. While closing to the end, we have another two (combinatorial) proofs (via partitions by Christopher and "one sentence" by Zagier[9]) which use the same idea, but again viewed in different light. Finally, we have an exhaustive (analytic?) proof which uses formal series.

Before closing this section, let us mention several results and conjectures which are closely related to Fermat's theorem. First, we have a complete characterization of natural numbers which can be expressed as sum of two squares.

Theorem 1.2 (Sum of two squares theorem)**.** *Let n be a natural number with factorization to primes $n = 2^{\alpha}p_1^{\beta_1}...p_r^{\beta_r}q_1^{\gamma_1}...q_s^{\gamma_s}$, where p_i's and q_j's are primes of the form $4k+1$ and $4k+3$ respectively. Then n can be expressed as some of two squares iff all $\gamma_1, ..., \gamma_s$ are even.*

In the following section we will see a proof of this result using Fermat's theorem on some of two squares. Sum of two squares theorem has its two cousins which deal with sum of three squares (due to Legendre[10]) and sum of four squares (due to Lagrange).

Theorem 1.3 (Legendre's theorem on some of three squares)**.** *A natural number can be expressed as sum of three squares iff it is not of the form $4^a(8k+7)$ for some integers $a \geqslant 0$ and $k \geqslant 0$.*

Theorem 1.4 (Lagrange's theorem on some of four squares)**.** *Every natural number can be expressed as sum of four squares.*

When you think about it for a second, isn't it very paranormal that this story stops at four squares? This inspires us to make the following definition.

Definition 1.5. *We denote with $g(k)$ the smallest natural number n such that every natural number can be written as sum of n numbers which are all kth powers of some natural numbers.*

For example, we obviously have that $g(1) = 1$ while Lagrange's theorem (together with examination that 7 is not a sum of three squares) provides us $g(2) = 4$. Observe that it is far from obvious that $g(k)$ is finite in general. The problem of calculating $g(k)$ is known as Waring's[11] problem.

With a lot of afford, it can be proven that $g(3) = 9$, $g(4) = 19$,... In fact, a work of several people provides a complete description of all values of $g(k)$ which are all finite. It is actually known that $g(k) = 2^k + \lfloor \frac{3^k}{2^k} \rfloor - 2$ for all but finitely many $k \in \mathbb{N}$. The only potentially problematic $k \in \mathbb{N}$ are those satisfying a very mysterious relation

$$2^k \left\{ \frac{3^k}{2^k} \right\} + \left\lfloor \frac{3^k}{2^k} \right\rfloor > 2^k \tag{1}$$

and no number with this property is known! Therefore, providing a proof that no natural number satisfies (1) would put an end to the Waring's problem (but I am guessing this is not completely straightforward).

There is also a very important geometric interpretation of the Sum of two squares theorem. Namely, this theorem characterizes exactly does (closed) circles in $\mathbb{R}^2$ whose equation is of the form $x^2 + y^2 \leqslant n^2$ (for some $n \in \mathbb{N}$) and whose boundary contains at least one point with integer coordinates.

[4]Leonhard Euler(1707–1783), a Swiss mathematician, physicist, astronomer, geographer, logician, engineer and God knows what

[5]Richard Dedekind(1831–1916), a German mathematician

[6]Hermann Minkowski(1864–1909), a German mathematician

[7]Joseph-Louis Lagrange(1736–1813), an Italian-French mathematician and astronomer

[8]Carl Friedrich Gauss(1777-1855), a German mathematician

[9]Don Zagier(1951–), American-German mathematician

[10]Adrien Marie Legendre(1752–1833), a French mathematician

[11]Edward Waring(1736–1798), a British mathematician

Open Problem 1.6 (Gauss's circle problem)**.** *Given a real number $r \geqslant 0$, how many points with integer coordinates are there in the circle $x^2 + y^2 \leqslant r^2$?*

Although this problem has completely elementary and quite simple formulation, it is considered one of the hardest problems in number theory. It is not too hard to obtain some boundary of this number.

Exercise 1.7. *Prove that the number of points with integer coordinates in the circle $x^2 + y^2 \leqslant r^2$ equals to $r^2\pi + O(r)$.*

It is conjectured that the error is actually of order $O(r^{1/2+\varepsilon})$, but currently it is only known that this error has order $O(r^{0.629\ldots})$.

2 Preliminaries

In this short section we will prove several elementary facts which we will need in later. Recall that for any prime number p we know that $\mathbb{Z}/p\mathbb{Z}$ is a (finite) field.

Theorem 2.1. *If F is a finite field, then its multiplicative group is cyclic.*

Proof. Suppose on the contrary and let $a \in F$ be an element of maximal multiplicative order. Since a is not a generator of group $F^* = F\backslash\{0\}$ its order is equal to some $m < |F^*|$. We claim that for every $b \in F^*$ we have $b^m = 1$, so let n be order of b. Suppose on the contrary, that we can find some prime number q such that $n = q^\alpha k$ and $m = q^\beta l$, where $q \nmid k$, $q \nmid l$ and $\alpha > \beta$. In this case element a^{q^β} has order l and b^k has order q^α. Therefore, element $a^{q^\beta}b^k$ has order $\mathrm{lcm}(l, q^\alpha) = q^\alpha l > q^\beta l = m$. This is a contradiction with the choice of a, thus we must have $b^m = 1$. Now, every nonzero element of F is a solution of the equation $x^m = 1$. However, the polynomial $x^m - 1$ can have at most m zeros, so we obtain a contradiction. Thus there must be an element of order $|F^*|$. □

Definition 2.2. *Let p be a prime. An integer g we call a **primitive root** modulo p if its residue modulo p is a generator of the multiplicative group of field $\mathbb{Z}/p\mathbb{Z}$.*

In other words, primitive roots modulo p are exactly integers $g \in \mathbb{Z}$ such that all numbers $g, g^2, ..., g^{p-1}$ have distinct residues modulo p. The following simply corollary

Corollary 2.3. *If p is a prime number of the form $4k + 1$, then the congruence $x^2 \equiv -1 (\mathrm{mod}\ p)$ has a solution.*

Proof. Pick some primitive root g modulo p. By Fermat's little theorem, we have that $p|g^{p-1} - 1 = (g^{(p-1)/2} - 1)(g^{(p-1)/2} + 1)$ and since $p \nmid g^{(p-1)/2} - 1$ (because g is a primitive root modulo p), we conclude that $p|g^{(p-1)/2} + 1$ thus $x := g^{(p-1)/4}$ is the wanted solution. □

Since there is no some special name for numbers which are representable as sum of two squares, we will be imaginative here.

Definition 2.4. *Natural number $n \in \mathbb{N}$ we call a **BMS number** if it can be expressed as a sum of two squares, i.e. if there are two integers $x, y \in \mathbb{Z}$ with $n = x^2 + y^2$.*

Lemma 2.5. *If m and n are BMS numbers, then so is their product.*

Proof. This is a simple consequence of the identity $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$. □

As we promised in the introduction, let us now prove the Sum of two squares theorem with the help of Fermat's theorem on sum of two squares.

Exercise 2.6. *Prove that prime numbers of the form $4k + 3$ are not BMS numbers.*

Lemma 2.7. *If p is a prime of the form $4k + 3$ and $p|x^2 + y^2$, then $p|x$ and $p|y$.*

Proof. Suppose on the contrary and let g be a primitive root modulo p. Then we can find unique $i, j \in \{1, 2, ..., p - 1\}$ such that $x \equiv g^i (\mathrm{mod}\ p)$ and $y \equiv g^j (\mathrm{mod}\ p)$, so wlog $i \geqslant j$. Therefore, we have that $p|x^2 + y^2 = g^{2i} + g^{2j}$, hence $p|g^{2(i-j)} + 1$. On the other side, recall that in the proof of corollary 2.3 we had that $p|g^{(p-1)/2} + 1$, thus we obtain $g^{2(i-j)} \equiv g^{(p-1)/2} (\mathrm{mod}\ p)$. Finally, since order of g is $p - 1$, the last relation implies that $\frac{p-1}{2} \equiv 2(i - j) (\mathrm{mod}\ p - 1)$, which is impossible since $\frac{p-1}{2}$ is odd. Contradiction! □

Proof of the Sum of two squares theorem. On one side suppose that $\gamma_j = 2\delta_j$ for all $j = 1, 2, ..., s$. Observe that all numbers $2, p_1, ..., p_r, q_1^2, ..., q_s^2$ are BMS numbers (for p_i it follows from Fermat's theorem on sum of two squares and for others its obvious), so we can just use lemma 2.5 a bunch of times to obtain that n is a BMS number.

The converse direction we will prove via induction on n. It is obvious that 1 and 2 are BMS numbers, so suppose that the claim is true for all numbers less than n. Now suppose that $n = x^2+y^2$ and if n doesn't have a prime factor of the form $4k+3$, then we are done. Otherwise, take its arbitrary prime factor $p = 4k + 3$ and use lemma 2.7 to conclude that $p|x$ and $p|y$. Therefore, we have that $p^2|n$ so $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$ implies that n/p^2 is a BMS number. Now we just apply induction hypothesis on n/p^2 and it is clear that this will imply the wanted conclusion for n. □

3 Proof via infinite descent

The principle of infinite descent is just another way of using the fact that the set of natural numbers is well-order. Therefore, this method is just one variation of simple induction.

Here we will present Euler's original proof of Fermat's theorem on sum of two squares. We will need three preperatory lemmas among which the third one is the main step in the proof.

Lemma 3.1. *If n is a BMS number and its prime divisor p is also a BMS number, then n/p is a BMS number.*

Proof. Let us write $n = a^2 + b^2$ and $p = c^2 + d^2$, and observe that we have

$$(cb - ad)(cb + ad) = c^2b^2 - a^2d^2 = c^2(a^2 + b^2) - a^2(c^2 + d^2) = c^2n - a^2p.$$

Since p is a prime and $p|n$, we must have $p|cb - ad$ or $p|cb + ad$. Wlog suppose that $p|cb - ad$ (the other case is very similar) and recall that from lemma 2.5 we have $np = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$. Therefore, it also must hold $p|ac + bd$ which finally gives us

$$\frac{n}{p} = \frac{a^2 + b^2}{c^2 + d^2} = \left(\frac{ac + bd}{p}\right)^2 + \left(\frac{ad - bc}{p}\right)^2$$

□

Lemma 3.2. *If n is a BMS number and its divisor $m|n$ isn't, then n/m has a (positive) divisor which is not a BMS number.*

Proof. Let us write $n = mp_1p_2...p_r$, where all p_i are prime numbers. We claim that one of the numbers p_1, p_2,...,p_r (which all are divisors of n/m) is not a BMS number. Suppose on the contrary and apply first lemma 3.1 on n and p_1 to obtain that n/p_1 is a BMS number. Then apply this same lemma on numbers n/p_1 and p_2 to obtain that $n/(p_1p_2)$ is a BMS number. Continuing in this fashion (at the end) we obtain that $n/(p_1p_2...p_r) = m$ is a BMS number, which is a contradiction. □

Lemma 3.3. *If m and n are coprime integers, then every divisor of $m^2 + n^2$ is a BMS number.*

Proof. If $m^2 + n^2$ is prime, then the claim is trivial, so suppose this is not the case. Suppose on the contrary and among all triples (m, n, a) for which we have

(i) m and n are coprime;

(ii) $a|m^2 + n^2$;

(iii) a is not a BMS number,

pick one with $x := m^2 + n^2$ minimal and among all such one with a minimal. Our goal is to find a "smaller" triple (m_1, n_1, a_1).

Observe that $a > 2$ and let us choose natural numbers $\alpha, \beta \in \mathbb{N}$ such that $|m - \alpha a|$ and $|n - \beta a|$ are minimal. Then numbers $b := m - \alpha a$ and $c := n - \beta a$ definitely satisfy $|b| \leqslant \frac{a}{2}$ and $|c| \leqslant \frac{a}{2}$. Easy calculation give us that

$$x = m^2 + n^2 = (b + \alpha a)^2 + (c + \beta a)^2 = b^2 + c^2 + a(2\alpha b + 2\beta c + \alpha^2 a + \beta^2 a) \tag{2}$$

so $a|x$ implies that $a|b^2+c^2$. Then we can write $b^2+c^2=ra$ (for some $r\in\mathbb{N}$) and let $d:=\gcd(b,c)$. Since $m=b+\alpha a$ and $n=c+\beta a$ are coprime, we conclude that $(a,d)=1$. Since we also have $d^2|b^2+c^2=ra$, we conclude that $d^2|r$. So, let us denote $b=dm_1$, $c=dn_1$ and $r=d^2s$ to obtain $m_1^2+n_1^2=as$. Since a is not a BMS number, we can apply lemma 3.2 on numbers $m_1^2+n_1^2$ and a to obtain some divisor a_1 of $s=(m_1^2+n_1^2)/a$ which is not a BMS number.

Finally, we claim that (m_1,n_1,a_1) is a smaller triple which satisfies (i)-(iii). By our definitions of those numbers, we definitely have properties (i)-(iii). On one hand we have that (2) implies $m_1^2+n_1^2\leqslant b^2+c^2\leqslant m^2+n^2$ and on the other side

$$a_1a\leqslant sa=m_1^2+n_1^2\leqslant b^2+c^2\leqslant\frac{a^2}{4}+\frac{a^2}{4}=\frac{a}{2}a,$$

thus $a_1\leqslant a/2<a$. □

The reason why thus method is called "infinite descent" is because more-or-less we constructed an infinite sequence of triples which is not possible in $\mathbb{N}^3$. Now the main theorem will be an easy corollary of our last result.

Proof of Fermat's theorem on sum of two squares. Take arbitrary prime number $p=4k+1$ and we need to prove that it is a BMS number. From Fermat's little theorem, we know that all numbers $1^{4k},2^{4k},...,(4k)^{4k}$ have residue 1 modulo p. Therefore, all differences $2^{4k}-1^{4k},...,(4k)^{4k}-(4k-1)^{4k}$ are divisible by p. Observe that every $i\in\{1,2,...,4k-1\}$ we have that

$$(i+1)^{4k}-i^k=((i+1)^{2k}+i^{2k})((i+1)^{2k}-i^{2k})$$

and that $p|[(i+1)^k]^2+[i^k]^2$ would with lemma 3.3 imply that p is a BMS number. Therefore, the only interesting case is when $p|(i+1)^{2k}-i^{2k}$ for all $i\in\{1,2,...,4k-1\}$. In other words, in this case all numbers $2^{2k},3^{2k},...,(4k)^{2k}$ must have residue 1 modulo p, which is a contradiction with existence of the primitive root modulo p. □

The principle of infinite descend is a very useful method when one wants to prove that a certain equation has no solutions. For example, one can easily solve the following special case of Fermat's equation (without citing Fermat's Last Theorem).

Exercise 3.4 (Fermat's equation for $n=4$)**.** *Prove that $x^4+y^4=z^4$ has no solutions in $\mathbb{N}$.*

4 Proof via Dirichlet principle

In this section, we will actually prove a stronger result which deals with the number of possible ways to express a number as a sum of two squares.

Definition 4.1. *For a natural number $n\in\mathbb{N}$, with $r_2(n)$ we will denote the number of distinct ways to express n as a sum of two squares, that is*

$$r_2(n):=|\{(a,b)\in\mathbb{Z}^2:a^2+b^2=n\}|.$$

Now we can reformulate Fermat's theorem on sum of two squares as follows: For every prime number $p=4k+1$ we have $r_2(p)>0$. Just to be sure that we are on the same page, let us look at the following example.

Example 4.2. *We have that $r_2(1)=4$, since $1=1^2+0^2=(-1)^2+0^2=0^2+1^2=0^2+(-1)^2$.*

Definition 4.3. *We say that expressing $n=x^2+y^2$ of number n as a sum of two squares is **primitive** if $(x,y)=1$. We will also denote*

$$Q(n):=|\{(x,y)\in\mathbb{Z}^2:n=x^2+y^2\ \textit{is primitive}\}|\ \textit{and}$$

$$P(n):=|\{(x,y)\in\mathbb{N}_0^2:n=x^2+y^2\ \textit{is primitive}\}|.$$

Directly from definitions we obtain that for $n > 1$ we have $4P(n) = Q(n)$ (observe that $n^2 = n^2 + 0^2$ is not a primitive expressing). Moreover, for every $n > 1$ we also have that

$$r_2(n) = \sum_{d^2|n} Q\left(\frac{n}{d^2}\right),$$

where the sum ranges over all $d \in \mathbb{N}$ with $d^2|n$. The previous formula follows directly from the following observation: For every $n > 1$ and every expressing $n = x^2 + y^2$ if we denote $d := (x, y)$ we obtain a primitive expressing $\frac{n}{d^2} = (\frac{x}{d})^2 + (\frac{y}{d})^2$.

Theorem 4.4. *For every $n > 1$ number $P(n)$ is exactly the number of solutions of the congruence $x^2 \equiv -1 (\mathrm{mod}\ n)$ (in group $\mathbb{Z}/n\mathbb{Z}$).*

Proof. The claim is easily checked for $n = 2, 3, 4$, so suppose that $n > 4$. Let us consider sets

$$A := \{(x, y) \in \mathbb{N}_0^2 : n = x^2 + y^2 \text{ primitive}\} \text{ and}$$

$$B := \{x \in \mathbb{Z}/n\mathbb{Z} : n|x^2 + 1\},$$

where our goal is to show that $|A| = |B|$. First, let us define a function $F : A \to B$, so take arbitrary $(x, y) \in A$. Since $\gcd(x, y) = 1$ and $n = x^2 + y^2$, we also have that $\gcd(n, y) = 1$. Therefore, the equation $sy = x$ in $\mathbb{Z}/n\mathbb{Z}$ has a unique solution and we define $F(x, y) := s$. To see that F is well-defined, just observe that we have

$$s^2y^2 \equiv x^2 \equiv -y^2 (\mathrm{mod}\ n)$$

and since $\gcd(y, n) = 1$ also $s^2 \equiv -1 (\mathrm{mod}\ n)$.

To see that F is injective, suppose that for $(x_1, y_1), (x_2, y_2) \in A$ we have $F(x_1, y_1) = F(x_2, y_2) = s$. Then congruences $sy_1 \equiv x_1 (\mathrm{mod}\ n)$ and $sy_2 \equiv x_2 (\mathrm{mod}\ n)$ imply that

$$x_1y_2 \equiv sy_1y_2 \equiv y_1x_2 (\mathrm{mod}\ n). \tag{3}$$

Since $n = x_1^2 + y_1^2 = x_2^2 + y_2^2$, we must have $0 \leqslant x_1, y_1, x_2, y_2 \leqslant \sqrt{n}$, thus (3) implies that $x_1y_2 = x_2y_1$. Since $\gcd(x_1, y_1) = \gcd(x_2, y_2) = 1$, we conclude that $x_1 = x_2$ and $y_1 = y_2$.

We must also prove that F is surjective, so take arbitrary $0 \leqslant s \leqslant n - 1$ with $n|s^2 + 1$. Consider the set $\{(u, v) \in \mathbb{Z}^2 : 0 \leqslant u, v \leqslant \sqrt{n}\}$ which has $(\lfloor\sqrt{n}\rfloor + 1)^2 > n$ elements. By the Pigeon-hole principle, we can find two pairs (u_1, v_1) and (u_2, v_2) such that $u_1 - sv_1$ and $u_2 - sv_2$ have the same residue modulo n. Therefore, if we define $x := u_1 - u_2$ and $y := v_1 - v_2$, we will have that $n|x - sy$ and $0 \leqslant |x|, |y| \leqslant \sqrt{n}$. Also, observe that not both x and y are zero (since $(u_1, v_1) \neq (u_2, v_2)$), hence $x^2 + y^2 > 0$.

We claim that also not both x and y can be equal to $\sqrt{n}$, which is only not obvious if $n = t^2$ for some $t \in \mathbb{N}$. If this in fact is the case, then $x = y = t$ would imply that $n|x - sy = t - st$, thus $s \equiv 1 (\mathrm{mod}\ t)$. However, we already have that $s \equiv -1 (\mathrm{mod}\ n)$, thus also $s \equiv -1 (\mathrm{mod}\ t)$. Now we obtained that $-1 \equiv 1 (\mathrm{mod}\ t)$ which leaves $t \in \{1, 2\}$ and this is impossible since $n > 4$.

Therefore, at least one of x and y is strictly less than $\sqrt{n}$, so $x^2 + y^2 < 2n$. Also $n|x - sy$ implies that $x^2 \equiv s^2y^2 \equiv -y^2 (\mathrm{mod}\ n)$, i.e. $n|x^2 + y^2$. We proved that $n|x^2 + y^2$ and $0 < x^2 + y^2 < 2n$, thus it must hold $n = x^2 + y^2$. We also claim that $\gcd(x, y) = 1$ and to see this, denote $d := \gcd(x, y)$. Then $x^2 + y^2 = n$ implies $d^2|n$ and $sy \equiv x (\mathrm{mod}\ n)$ implies that $s\frac{y}{d} \equiv \frac{x}{d} (\mathrm{mod}\ \frac{n}{d})$, thus

$$\frac{n}{d^2} = \frac{x^2 + y^2}{d^2} \equiv \left(s\frac{y}{g}\right)^2 + \left(\frac{y}{d}\right)^2 \equiv -\left(\frac{y}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = 0 (\mathrm{mod}\ n/d),$$

thus $d = 1$. Finally, if x and y have the same sign, then we have $F(|x|, |y|) = s$ and if they have the opposite sign, then $F(|y|, |x|) = s$. In any case, we proved that F is surjective. □

I believe that the key part of the previous proof was the use of pigeon-hole principle. All other stuff is just playing with elementary number theory.

The previous theorem was the main step in the proof of the Fermat's theorem on some of two squares and now comes the easy part.

Proof of Fermat's theorem on sum of two squares. Let $p = 4k + 1$ be a prime and we need to prove that $r_2(p) \neq 0$. Since we have that

$$r_2(p) = \sum_{d^2|p} Q\left(\frac{p}{d^2}\right) = Q(p) = 4P(p),$$

it is enough to see why $P(p) \neq 0$. The previous theorem tells us that this is equivalent to proving that equation $x^2 \equiv -1 (\text{mod } p)$ has a non-trivial solution, and this is just a corollary 2.3. □

However, the story doesn't end here. We promised to "provide" some kind of a formula for $r_2(n)$, so this is our next goal. We need to introduce here several classical notions from number theory.

Definition 4.5. *Function $f : \mathbb{N} \to \mathbb{C}$ is **multiplicative** if for all coprime natural numbers m and n we have $f(mn) = f(m)f(n)$.*

Observe that every multiplicative function $\mathbb{N} \to \mathbb{C}$ is completely determined by its values in powers of primes (use this to solve exercise 4.9).

Definition 4.6. *For functions $f : \mathbb{N} \to \mathbb{C}$ and $g : \mathbb{N} \to \mathbb{C}$ we define their **Dirichlet**[12] **convolution** $f * g$ as a function $\mathbb{N} \to \mathbb{C}$ given with*

$$(f * g)(n) := \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

This operation is some kind of a discrete analogon of the classical analytical convolution which we define for two functions $\mathbb{R}^n \to \mathbb{R}$.

Exercise 4.7. *Prove that the set of all functions $\mathbb{N} \to \mathbb{C}$ with addition $+$ and Dirichlet convolution $*$ builds an integral domain. Which elements of this integral domain are invertible?*

Dirichlet convolution is an incredible useful tool when we assign to every function $\mathbb{N} \to \mathbb{C}$ a certain Dirichlet series (for example, Dirichlet series of function $n \mapsto 1$ will be the well-known Riemann's zeta function $\zeta(s)$). These Dirichlet series enable us to throw into play a strong machinery of complex analysis to try solving various number-theoretic problems. For example, if one decides on following this road, soon he will be able to understand proofs of (very deep) theorems like Dirichlet's theorem on prime numbers in arithmetic progressions[13] and the Prime number theorem[14]. I drifted away a little bit here, so let me get back to our story.

Lemma 4.8. *If functions $f : \mathbb{N} \to \mathbb{C}$ and $g : \mathbb{N} \to \mathbb{C}$ are multiplicative, then so is $f * g$.*

Proof. We just check that for arbitrary coprime m and n we have

$$\begin{aligned}(f * g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{d_1|m, d_2|n} f(d_1 d_2)g\left(\frac{m}{d_1}\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} f(d_1)g\left(\frac{m}{d_1}\right) \sum_{d_2|n} f(d_2)g\left(\frac{n}{d_2}\right) \\ &= (f * g)(m) \cdot (f * g)(n).\end{aligned}$$

□

Exercise 4.9. *If we denote with $\varphi(n)$ Euler function[15], prove that $\sum_{d|n} \varphi(d) = n$.*

[12] Peter Gustav Lejeune Dirichlet(1805–1859)

[13] If $\gcd(a, b) = 1$ then the sequence $a, a + b, a + 2b, ...$ has infinitely many primes!

[14] If we denote with $\pi(x)$ the number of primes less than x, then it holds $\lim_{x\to\infty}(\pi(x) \log x)/x = 1$

[15] We define $\varphi(n)$ to be the number of elements of $\{1, 2, ..., n\}$ which are coprime with n. One can easily prove via combinatorial argument or via Chinese Remainder theorem that φ is multiplicative

So, what does this have to do with sums of two squares? Recall that our notions lead us to the formula

$$r_2(n) = \sum_{d^2|n} Q\left(\frac{n}{d^2}\right)$$

and if denote with $N(n)$ the number of solutions of the congruence $x^2 \equiv -1 (\text{mod } n)$ (in group $\mathbb{Z}/n\mathbb{Z}$), then theorem 4.4 gives us

$$r_2(n) = 4 \sum_{d^2|n} N\left(\frac{n}{d^2}\right).$$

If we define a function $\rho : \mathbb{N} \to \mathbb{C}$ which is a detector of perfect squares

$$\rho(n) := \begin{cases} 1, & n \text{ is a perfect square} \\ 0, & \text{otherwise} \end{cases},$$

then we obtain a formula

$$r_2(n) = 4 \sum_{d^2|n} N\left(\frac{n}{d^2}\right) = 4 \sum_{d|n} N\left(\frac{n}{d}\right) \rho(d) = r(N * \rho)(n).$$

This is a classical cheap trick in analytic number theory to obtain some new information by introducing an appropriate helping function.

Theorem 4.10. *Function $r_2(n)/4$ is multiplicative.*

Proof. Since this function is given as a Dirichlet's convolution, by lemma 4.8 it is enough to prove that functions $N(n)$ and $\rho(n)$ are multiplicative. For function $\rho(n)$ this is straightforward, while for $N(n)$ one just have to check that the restriction of the isomorphism

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

that we have from the Chinese Remainder theorem will map bijectively solutions of the equation $x^2 \equiv -1 (\text{mod } mn)$ to pairs of solution of equations $x^2 \equiv -1 (\text{mod } m)$ and $x^2 \equiv -1 (\text{mod } n)$. □

Now we are ready to define our main player which will encode the necessary analytical information.

Definition 4.11. *Let G be a finite abelian group. Every homomorphism from G to the multiplicative group $\mathbb{C}^\times$ we call a* ***character*** *of group G.*

Wow, this is actually much more general definition then the thing that we need, but I couldn't resist not mentioning it. In representation theory one can prove that irreducible representations of a finite abelian group are all one dimensional, thus can be identified with their characters (this sentence is here to "explain" where does the motivation for something like this come from).

Since we are interested in a finite group in which every element has a finite order, every character is actually a homomorphism $G \to \mathbb{S}^1 \subseteq \mathbb{C}$ (to the unit circle). These characters naturally form a group (Pontryagin dual of G) which is naturally isomorphic to G. The most interesting cases are $G = \mathbb{Z}/n\mathbb{Z}$ and $G = (\mathbb{Z}/n\mathbb{Z})^\times$. In the first one we have a very explicit description of all characters and we can do a very nice discrete Fourier analysis without much troubles. On the other side, in the second cases we come to a very mysterious objects which we call **Dirichlet characters**. These can be naturally identified with n-periodic completely multiplicative[16] functions $\mathbb{N} \to \mathbb{C}$ which vanish for all $m \in \mathbb{N}$ not coprime with n. These functions encode incredibly many analytic information and play a central role in the theory of L-series. Ups, I did it again...

Here we will need only one simple example of a Dirichlet character $\chi_4 : \mathbb{N} \to \mathbb{C}$ which is given by

$$\chi_4(n) := \begin{cases} 1, & n \equiv 1 (\text{mod } 4) \\ -1, & n \equiv 3 (\text{mod } 4) \\ 0, & \text{otherwise} \end{cases}.$$

One can easily check that this defines a (completely) multiplicative function on $\mathbb{N}$.

[16] Function $f : \mathbb{N} \to \mathbb{C}$ is completely multiplicative if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$

Theorem 4.12. *For all $n \in \mathbb{N}$ we have $r_2(n) = 4\sum_{d|n} \chi_4(d)$.*

Proof. According to theorem 4.10 and lemma 4.8 we have that functions $r_2(n)/4$ and $\sum_{d|n} \chi_4(d)$ are multiplicative, so it is enough to prove that equality holds for all powers of primes. Here details become a little bit (elementary but) messy, so I am gonna skip this part (please contact me if you would like to discuss this). □

The previous theorem gives us a very nice way to calculate $r_2(n)$ in concrete cases. It also provides us an important analytic approach if function $r_2(n)$ turns up in some other calculations. In particular, it reduces the Gauss circle problem to the problem of estimating the expression

$$\sum_{n \leqslant r} r_2(n) = \sum_{n \leqslant r} \sum_{d|n} \chi_4(d)$$

which gives us some starting point at this hard problem. I will close this section with another proof of the Sum of two squares theorem.

Proof of the Sum of two squares theorem. Let $n = 2^\alpha p_1^{\beta_1} ... p_r^{\beta_r} q_1^{\gamma_1} ... q_s^{\gamma_s}$ (where p_is and q_js are of the form $4k+1$ and $4k+3$ respectively) be any natural number and consider

$$r_2(n) = 4\sum_{d|n} \chi_4(d).$$

We have that n is a BMS number iff $r_2(n) \neq 0$, therefore iff $\sum_{d|n} \chi_4(d) \neq 0$. Since function $\sum_{d|n} \chi_4(d)$ is multiplicative, we have that

$$\sum_{d|n} \chi_4(d) = \sum_{d|2^\alpha} \chi_4(d) \cdot \prod_{i=1}^{r} \sum_{d|p_i^{\beta_i}} \chi_4(d) \cdot \prod_{j=1}^{s} \sum_{d|q_j^{\gamma_j}} \chi_4(d).$$

The first sum and all sums in the first product all have a positive value. Therefore, we have that n is a BMS number iff every sum in the second product has a positive value and this happens iff all γ_js are even. □

5 Proof via Gaussian integers

The proof which we will give in this section is due to Dedekind. The central object which we will study in this section will be the ring of Gaussian integers.

Definition 5.1. *The subring*

$$\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$$

of the field $\mathbb{C}$ of complex numbers we call the ***ring of Gaussian integers****.*

Equivalently, the ring of Gaussian integers is exactly the ring of imaginary quadratic field extension $\mathbb{Q}[i]$ of $\mathbb{Q}$ (but we will not need this).

This ring has some very nice properties. We define the norm $N : \mathbb{Z}[i] \to \mathbb{N}_0$ with $N(a+ib) := a^2 + b^2$ which is just the square of the module of a complex number. One can easily show that this is an euclidean norm on integral domain $\mathbb{Z}[i]$ which will give him a structure of euclidean ring. In particular, we have that $\mathbb{Z}[i]$ is a principal ideal ring, Dedekind domain and a unique factorization domain. We actually only need the fact that it is unique factorization domain, because we are interested in characterizing its prime elements.

Observe that every invertible element of $u \in \mathbb{Z}[i]$ must have norm 1 since $N(u)N(u^{-1}) = N(uu^{-1}) = N(1) = 1$, while $N(u)$ and $N(u^{-1})$ are non-negative integers. Now one can easily check that those are exactly 1, -1, i and $-i$. Since we are in a unique factorization domain, every element in $\mathbb{Z}[i]$ whose norm is a prime integer must be a prime element of $\mathbb{Z}[i]$.

Lemma 5.2. *Every prime integer $p \in \mathbb{Z}$ of the form $4k+3$ is also a prime Gaussian integer.*

Proof. Suppose that $p = (x + iy)(z + it)$ and we have to prove that one of $x + iy$ and $z + it$ is a unit. If we suppose on the contrary, then both of them must have norm larger than 1. Since $N(x + iy)N(z + it) = N(p) = p^2$, we have that $N(x + iy) = p$ so $p = x^2 + y^2$. However, a prime number of the form $4k + 3$ is not a BMS number, so we obtain a contradiction. □

Theorem 5.3. *Gaussian integer $x \in \mathbb{Z}[i]$ is prime iff it is associated to one of the following*

(a) $1 + i$ or $1 - i$;

(b) A prime integer of the form $4k + 3$;

(c) Element $y = a + ib \in \mathbb{Z}[i]$ such that $a^2 + b^2$ is a prime integer of the form $4k + 1$.

Proof. Two numbers in (a) have prime norm 2, so they are both prime. Lemma 5.2 tells us that all numbers in (b) are Gaussian primes. Finally, if $a^2 + b^2 = p$ is a prime number of the form $4k + 1$, then we have that $N(a + ib) = p$ is a prime, so $a + ib$ is a prime Gaussian integer.

Conversely, suppose that $x = a + ib$ is a Gaussian prime. Suppose first that $b \neq 0$ and $a \neq 0$. In this case $n := a^2 + b^2 = (a + ib)(a - ib)$ is a prime integer, because otherwise we could write him as a product of primes and obtain a contradiction with the fact that $\mathbb{Z}[i]$ is a unique factorization domain. Therefore, we have that n is a BMS prime number, so it must be 2 (in which case we get (a)) or of the form $4k + 1$ (in which case we get (c)).

Next, suppose that $b = 0$. Clearly, integer $p := x = a$ must also be a prime integer (besides being a prime Gaussian integer). Since $2 = (1 + i)(1 - i)$ is not a prime Gaussian integer, we have that $p \neq 2$. If p is of the form $4k+3$ then we obtain (b), so we must prove that p is not of the form $4k+1$. Suppose on the contrary, that $p = 4k + 1$ and find some $m \in \mathbb{Z}$ such that $p|m^2 + 1 = (m + i)(m - i)$ (using corollary 2.3). Since p is a prime, we must have that $p|m + i$ or $p|m - i$. However, in both cases we get an easy contradiction since p doesn't divide the imaginary parts of $m + i$ and $m - i$.

Finally, suppose that $b \neq 0$ and $a = 0$. In this case $x = ib$ is associated with $ix = -b$ which is just the case $b = 0$. This proves the theorem. □

Proof of Fermat's theorem on sum of two primes. Suppose $p = 4k+1$ is a prime. Then theorem 5.3 says that p is not a prime Gaussian integer, so we have that $p = (a+ib)(c+id)$ for some $a, b, c, d \in \mathbb{Z}$. Then also $N(a + ib)N(c + id) = N(p) = p^2$ and since $a + ib$ and $c + id$ are not invertible, we must have $N(a + ib) = N(c + id) = p$. However, this exactly means that $p = a^2 + b^2$. □

The ring $\mathbb{Z}[i]$ is just one example of a ring extension of $\mathbb{Z}$ with nice properties. In general, for any finite field extension K of $\mathbb{Q}$ we can consider all elements of K which are zeros of monic polynomials in $\mathbb{Z}[x]$. These elements form a subring of K which we denote with $\mathcal{O}_K$ and call the **ring of integers** of K. Although we are often without the luck with $\mathcal{O}_K$ not being a unique factorization domain (unlike $\mathbb{Z}[i]$), there are some other incredibly important properties which we always have. Namely, the ring $\mathcal{O}_K$ is always a Dedekind domain, which implies that every ideal of $\mathcal{O}_K$ has a unique factorization into (powers of) prime ideals. Therefore we get some kind of analogon of the Fundamental theorem of arithmetic.

Next, if we denote with $n := [K : \mathbb{Q}]$ the degree of the extension, then one can show that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. This enables us, among other things, to very nicely describe elements of rings of integers. For example, in the case of $\mathcal{O}_K = \mathbb{Z}[i]$ (when $K = \mathbb{Q}[i]$) we have that all elements are of the form $a + ib$ for $a, b \in \mathbb{Z}$, i.e. $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$. One can even associate to every Dedekind domain (hence to every ring of integers) a certain class group (which can be shown to be finite in the case of rings of integers) which codes some important algebraic information about that ring. For example, the class group is trivial iff the ring is a unique factorization domain (iff this ring is a principal ideal domain). This the beginning of the class field theory where also Galois theory plays a very important role.

6 Proof via Dirichlet approximation

In this section we will once again see how does Pigeon-hole principle come into play when it comes to the Fermat's theorem on sum of two squares.

Recall that every real number $\alpha \in \mathbb{R}$ and every $\varepsilon > 0$ we can find a rational number[17] $p/q \in \mathbb{Q}$ such that

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Well, this is just another way of saying that $\mathbb{Q}$ is dense in $\mathbb{R}$ (topologically and orderwise). The next interesting question would be, how complicated this fraction $\frac{p}{q}$ needs to be and can we control that somehow? Some partial answer to this question is provided by the following theorem of Dirichlet.

Theorem 6.1 (Dirichlet's approximation theorem)**.** *For arbitrary $\alpha \in \mathbb{R}$ and $n \in \mathbb{N}$ there is a rational number $\frac{p}{q} \in \mathbb{Q}$ such that $0 < q \leqslant n$ and*

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q(n+1)}.$$

Proof. Let us divide interval $[0,1]$ on $n+1$ (almost) equal parts

$$\left[0, \frac{1}{n+1}\right), \left[\frac{1}{n+1}, \frac{2}{n+1}\right), ..., \left[\frac{n}{n+1}, 1\right].$$

We can consider $n+2$ numbers $0, \alpha - \lfloor\alpha\rfloor, 2\alpha - \lfloor 2\alpha\rfloor, ..., n\alpha - \lfloor n\alpha\rfloor$ i 1 (some of them can be equal) and Pigeon-hole principle tells us that two of those fellas most drop into the same interval.

If one of them is zero, then for some $m \in \{1, 2, ..., n\}$ we have that $|m\alpha - \lfloor m\alpha\rfloor| < \frac{1}{n+1}$ so we can take $p := \lfloor m\alpha\rfloor$ and $q := m$. If one of them is 1, then we have that for some $m \in \{1, 2, ..., m\}$ it holds $|m\alpha - \lfloor m\alpha\rfloor - 1| \leqslant \frac{1}{n+1}$, so we can take $p := \lfloor m\alpha\rfloor - 1$ and $q := m$.

Finally, suppose that for some $1 \leqslant m_1 < m_2 \leqslant n$ we have

$$|\alpha m_2 - \lfloor \alpha m_2\rfloor - (\alpha m_1 - \lfloor \alpha m_1\rfloor)| < \frac{1}{n+1}.$$

Then we can take $p := \lfloor m_2\alpha\rfloor - \lfloor m_1\alpha\rfloor$ and $q := m_2 - m_1$, thus we are done. □

By the way, there are some pretty interesting results that deal with the sequence $\{\alpha\}, \{2\alpha\}, ...$ (here we denoted with $\{x\} := x - \lfloor x\rfloor$ fractional part of x) which we used in the proof of Dirichlet's approximation theorem. For example, the following theorem of Weyl is one of the starting points of ergodic theory.

Theorem 6.2 (Weyl's theorem)**.** *If $\alpha \in \mathbb{R}$ is irrational number, then the sequence $\{\alpha\}, \{2\alpha\}, \{3\alpha\}, ...$ is equidistributed in the interval $[0,1]$, i.e. for every measurable set $B \subseteq [0,1]$ we have that*[18]

$$\lim_{n\to\infty} \frac{|\{m \leqslant n : \{m\alpha\} \in B\}|}{n} = m(B).$$

We can actually immediately proceed to the proof of our main theorem (of this talk). Let us just note that nothing prevents us of taking a rational number α in Dirichlet's theorem.

Proof of the Fermat's theorem on sum of two squares. Let $p = 4k+1$ be a prime and using corollary 2.3 pick some $m \in \mathbb{N}$ with $p|m^2+1$. Let us take $\alpha := -\frac{m}{p}$ and $n := \lfloor\sqrt{p}\rfloor$ in Dirichlet's approximation theorem to obtain a rational number $\frac{a}{b} \in \mathbb{Q}$ such that $0 < b \leqslant \lfloor\sqrt{p}\rfloor \leqslant \sqrt{p}$ and

$$\left|-\frac{m}{p} - \frac{a}{b}\right| < \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}.$$

If we denote $c := mb + pa$, we obtain that $|c| < \frac{pb}{b\sqrt{p}} = \sqrt{p}$. Therefore, we have that $0 < b^2 + c^2 < 2\sqrt{p}^2 = 2p$ and

$$b^2 + c^2 = b^2 + (mb + pa)^2 \equiv b^2 + m^2b^2 \equiv b^2 - b^2 = 0 (\text{mod } p),$$

thus $p = b^2 + c^2$. □

[17] Here and later, we suppose that p and q are coprime integers in situations like this

[18] Where we denote with m the Lebesgue measure on $[0,1]$

How crazy is this?!? We approximated a rational number by a "less complicated" rational number and obtained some very non-trivial information from that. Strange are the ways of number theory...

Until the end of this section, I would like to shortly discuss two more things that are closely related to the Dirichlet's approximation theorem. On one side, we have the following direct corollary.

Corollary 6.3. *For every $\alpha \in \mathbb{R}$ there is a rational number $\frac{p}{q} \in \mathbb{Q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.*

Now we can ask a question whether or not we can strengthen up this somehow and this opens the door for entirely new subarea of number theory called Theory of Diophantine Approximations. For example, it is not too hard to prove Hurwitz's theorem which replaces $\frac{1}{q^2}$ with $\frac{1}{\sqrt{5}q^2}$ for irrational numbers α. There is also the following nice theorem of Liouville which he used to construct the very first explicit example of a transcendental number.

Theorem 6.4 (Liouville's theorem)**.** *If $\alpha \in \mathbb{R}$ is an algebraic number whose minimal polynomial has degree d, then there is a constant $C > 0$ such that for every rational number $\frac{p}{q} \in \mathbb{Q}$ we have*

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{C}{q^d}.$$

Exercise 6.5. *Using Liouville's theorem, prove that the Liouville's number*

$$L := \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$$

is transcendental.

Finally, the following deep theorem of Roth partially answers the starting question and for this theorem he won a Field's medal.

Theorem 6.6 (Roth's theorem)**.** *For every algebraic irrational number α and every $\varepsilon > 0$ there are only finitely many rational numbers $\frac{p}{q} \in \mathbb{Q}$ with $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$.*

On the other side, we can start complaining of non-counstructiveness[19] of the Dirichlet's approximation theorem. Here, continued fraction can come very handy. Namely, every real number $\alpha \in \mathbb{R}$ can be uniquely written in the form

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}},$$

where $a_0, a_1, a_2, \ldots$ are integers. Therefore, to every natural number we can assign a sequence $[a_0, a_1, \ldots]$ which we call a **continued fraction**. Here, we can see with out naked eye how does our approximation looks like. More precisely, we can look at the finite sequence of integers $[a_0, a_1, \ldots, a_n]$ which induces a rational number

$$\frac{p_n(\alpha)}{q_n(\alpha)} := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_n}}}.$$

Then one can show (these are just some exhausting inductions) that for every $m \in \mathbb{N}$ we have

$$\left|\alpha - \frac{p_n(\alpha)}{q_n(\alpha)}\right| < \frac{1}{q_n(\alpha) q_{n+1}(\alpha)}$$

which almost immediately implies the Dirichlet's approximation theorem and gives us more explicit construction of the approximation.

By the way, these continued fractions are very mysterious and somewhat random objects. For example, one can use ergodic theory to prove the following (I will be gentle here) what-in-the-name-of-fuck result.

[19] It is in some way constructive, but computationally deadly I would say

Theorem 6.7. *For almost every real number*[20] $x = [0, a_1, a_2, ...] \in (0, 1)$ *the digit* j *appears in the continued fraction with density*

$$\frac{2\log(1+j) - \log j - \log(2+j)}{\log 2}$$

and

$$\lim_{n\to\infty} \frac{1}{n} \log \left| x - \frac{p_n(\alpha)}{q_n(\alpha)} \right| = -\frac{\pi^2}{6\log 2}.$$

I would like to finish this section with a very unexpected connection of continued fractions with algebraic number theory.

While examining real quadratic field K of $\mathbb{Q}$, one can prove that the group of invertible elements in the ring of integers $\mathcal{O}_K$ is always a cyclic group (via Dirichlet's theorem on the group of units of $\mathcal{O}_K$). Therefore, it is generated by one single element which we can pick to be larger than 1 and we call him the **fundamental unit** of extension K.

Theorem 6.8. *Let* $\mathcal{O} = \mathbb{Z}[\delta]$ *where* δ *is a real quadratic integer which is the bigger of two solutions of the minimal equation for* δ*. Then the continued fraction of* δ *has some minimal period* l *and* $\varepsilon := p_{l-1}(\delta) - \delta q_{l-1}(\delta)$ *is the fundamental unit of* $\mathcal{O}$*.*

7 Proof via Minkowski theorem

In this section we will see a very intuitive (but incredibly powerful) theorem of Minkowski. For this, we will need a few basic notations.

Definition 7.1. *For an additive subgroup* $H \leqslant \mathbb{R}^n$ *we say that it is* ***discrete*** *iff* $B \cap H$ *is a finite set for every bounded subset* $B \subseteq \mathbb{R}^n$*.*

Equivalently, a subgroup $H \leqslant \mathbb{R}^n$ is discrete iff it is a discrete topological subgroup of $\mathbb{R}^n$ (with inherited topology).

It is not too hard to prove that every discrete subgroup of $\mathbb{R}^n$ must be finitely generated and since it is abelian, from the Fundamental theorem for finitely generated abelian groups we obtain that it must be isomorphic to $\mathbb{Z}^k$ for some $k \in \mathbb{N}$. Moreover, its $\mathbb{Z}$-basis will be consisted of $\mathbb{R}$-linearly independent vectors, so we will have $k \leqslant n$. We will not actually use any of these results (so they are more like a teaser), thus I omitted these proofs.

Definition 7.2. *Let* $\mathcal{B} = \{v_1, ..., v_n\}$ *be some basis of* $\mathbb{R}^n$*. A* ***lattice*** *generated by* $\mathcal{B}$ *we define with*

$$\Lambda_{\mathcal{B}} := \{c_1 v_1 + ... + c_n v_n : c_1, ..., c_n \in \mathbb{Z}\}.$$

Also, we define the ***fundamental parallelogram*** *of lattice* $\Lambda_{\mathcal{B}}$ *with*

$$\mathcal{P}_{\mathcal{B}} := \{\alpha_1 v_1 + ... + \alpha_n v_n : \alpha_1, ..., \alpha_n \in [0, 1)\}.$$

Therefore, a lattice in $\mathbb{R}^n$ is exactly some fully-dimensional discrete subgroup of $\mathbb{R}^n$. The canonical example of a lattice would be $\mathbb{Z}^n$, which we actually call the **integer lattice**.

Lemma 7.3. *If* $\mathcal{B} = \{v_1, ..., v_n\}$ *is a basis of* $\mathbb{R}^n$ *and* $v_i = (a_{i1}, ..., a_{in})$ *for all* $i \in \{1, 2, ..., n\}$*, then* $\mathrm{Vol}(\mathcal{P}_{\mathcal{B}}) = |\det([a_{ij}])| \neq 0$.

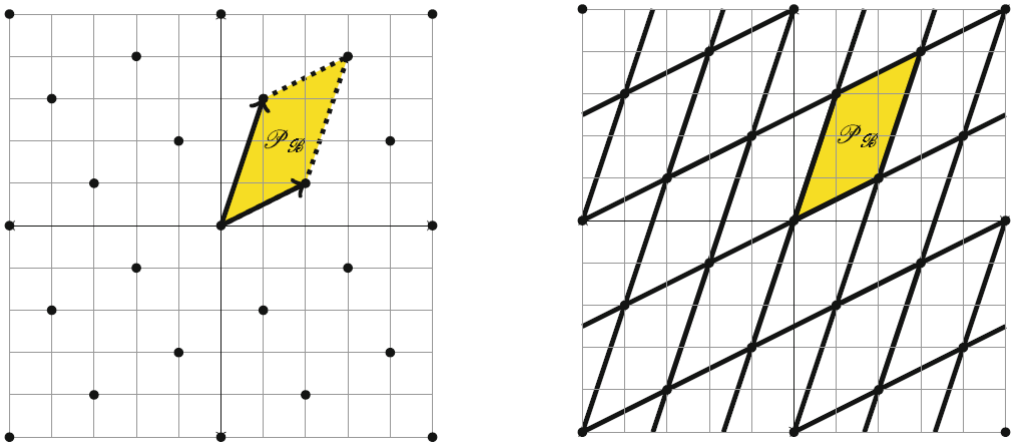
Proof. We just apply the simple change of coordinates $v_i \mapsto e_i$ to obtain

$$\mathrm{Vol}(\mathcal{P}_{\mathcal{B}}) = \int_{\mathcal{P}_{\mathcal{B}}} 1 dm = \int_{[0,1]^n} |\det(a_{ij})| dm = |\det(a_{ij})|.$$

□

Since among us there are some people who like examples, let me give you one. Consider vectors $v_1 = (2, 1)$ and $v_2 = (1, 3)$ which form a basis $\mathcal{B} = \{v_1, v_2\}$ of $\mathbb{R}^2$. Then we will obtain a lattice on the left picture whose fundamental parallelogram is coloured in yellow and elements of the lattice are bolded. As the picture on the right suggests, it should be the case that the space $\mathbb{R}^n$ is tilled with translated copies of the fundamental parallelogram and this indeed is the case.

[20] with respect to the Lebesgue measure



Lemma 7.4. *For any basis $\mathcal{B}$ of $\mathbb{R}^n$ we have that*

$$\mathbb{R}^n = \bigsqcup_{\lambda \in \Lambda_{\mathcal{B}}} (\lambda + \mathcal{P}_{\mathcal{B}}),$$

where $\bigsqcup$ denotes the disjoint union.

Proof. This is a straightforward check without interesting details. □

Now we come to the central theorem of this section whose statement is (I would say) pretty intuitive.

Theorem 7.5 (Minkowski's theorem Vol. 1)**.** *Let $\mathcal{B}$ be a basis of $\mathbb{R}^n$ and let $U \subseteq \mathbb{R}^n$ be a Lebesgue-measurable subset such that*[21] *$m(U) > \mathrm{Vol}(\mathcal{P}_{\mathcal{B}})$. Then there are distinct vectors $u_1, u_2 \in U$ such that $u_1 - u_2 \in \Lambda_{\mathcal{B}}$.*

Proof. From lemma 7.4 we obtain that

$$U = \bigsqcup_{\lambda \in \Lambda_{\mathcal{B}}} [U \cap (\lambda + \mathcal{P}_{\mathcal{B}})].$$

Now by the well-known property of Lebesgue measure, we have that

$$m(U) = m\left(\bigsqcup_{\lambda \in \Lambda_{\mathcal{B}}} [U \cap (\lambda + \mathcal{P}_{\mathcal{B}})]\right) = \sum_{\lambda \in \Lambda_{\mathcal{B}}} m(U \cap (\lambda + \mathcal{P}_{\mathcal{B}})).$$

Since m is a translation-invariant measure (the Haar measure on the locally compact topological group $\mathbb{R}^n$), we have that for all $\lambda \in \Lambda_{\mathcal{B}}$ holds $m(U \cap (\lambda + \mathcal{P}_{\mathcal{B}})) = m((U - \lambda) \cap \mathcal{P}_{\mathcal{B}})$. Therefore, we obtain that

$$m(U) = \sum_{\lambda \in \Lambda_{\mathcal{B}}} m((U - \lambda) \cap \mathcal{P}_{\mathcal{B}})$$

and since $m(U) > \mathrm{Vol}(\mathcal{P}_{\mathcal{B}}) = m(\mathcal{P}_{\mathcal{B}})$ and since every set $(U - \lambda) \cap \mathcal{P}_{\mathcal{B}}$ of the last sum is contained in $\mathcal{P}_{\mathcal{B}}$, we can find two $(U - \lambda) \cap \mathcal{P}_{\mathcal{B}}$ and $(U - \lambda') \cap \mathcal{P}_{\mathcal{B}}$ which overlap. Therefore, there is some $x \in \mathcal{P}_{\mathcal{B}}$ such that $u_1 := x + \lambda, u_2 := x + \lambda' \in U$ and now just observe that $u_1 - u_2 = \lambda - \lambda' \in \Lambda_{\mathcal{B}}$. □

We will need actually a different (weaker) version of Minkowski's theorem here, so let us quickly prove it.

Corollary 7.6 (Minkowski's theorem Vol. 2)**.** *Let $\mathcal{B}$ be a basis of $\mathbb{R}^n$ and let $S \subseteq \mathbb{R}^n$ be a Lebesgue-measurable convex symmetric subset which satisfies $m(S) > 2^n \mathrm{Vol}(\mathcal{P}_{\mathcal{B}})$. Then the intersection $\Lambda_{\mathcal{B}} \cap S$ contains a nonzero element.*

[21] Here, we again denote with m Lebesgue measure on $\mathbb{R}^n$

Proof. Let us consider the set $S_1 := S/2 = \{x/2 : x \in S\}$ which is obviously convex symmetric, Lebesgue-measurable and satisfies $m(S_1) > \mathrm{Vol}(\mathcal{P}_\mathcal{B})$. From Minkowski's theorem Vol. 1 we obtain two points $u_1, u_2 \in S_1$ such that $u_1 - u_2 \in \Lambda_\mathcal{B}$. First symmetry of S_1 gives us that $-u_2 \in S_1$ and then convexity of S_1 gives us that $\frac{1}{2}u_1 + \frac{1}{2}(-u_2) \in S_1$. This means that $u_1 - u_2 \in S$, so we found an element $u_1 - u_2 \in \Lambda_\mathcal{B} \cap S$ which is not zero. □

What the hell does this game with lattices has to do with sum of two square? Well, we just look at the circle!

Proof of Fermat's theorem on sum of two squares. Let $p = 4k + 1$ be prime and pick $m \in \mathbb{N}$ with $p|m^2 + 1$ using corollary 2.3. On one side, consider the open ball

$$S := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 2p\}$$

which is open (hence Lebesgue-measurable), convex, symmetric and has volume $m(S) = \sqrt{2p}^2\pi = 2p\pi$. On the other side, consider the lattice Λ generated by vectors $u := (p, 0)$ and $v = (m, 1)$. The volume of the fundamental parallelogram equals

$$\mathrm{Vol}(\mathcal{P}_\Lambda) = \begin{vmatrix} p & 0 \\ m & 1 \end{vmatrix} = p < \frac{2p\pi}{2^2},$$

so we can apply Minkowski's theorem Vol. 2! Therefore, we obtain some nonzero point $(a, b) \in S \cap \Lambda$ and let us write $(a, b) = cu + dv$ for some $c, d \in \mathbb{Z}$. Then we have that $a = cp + dm$ and $b = d$, thus

$$a^2 + b^2 = (cp + dm)^2 + d^2 \equiv d^2m^2 + d^2 \equiv -d^2 + d^2 = 0 (\mathrm{mod}\ p).$$

Since also $0 < a^2 + b^2 < 2p$ (because (a, b) is a nonzero point in S), we conclude that $p = a^2 + b^2$. Voilá! □

Actually, Minkowski's theorem is so strong that we can prove Legendre's theorem on sum of three squares and Lagrange's theorem on sum of four squares. To avoid some technical details, we will only prove Lagrange's theorem which itself requires some small amount of additional work. The following two preparational lemmas will be analogons of lemma 2.5 and corollary 2.3.

Lemma 7.7. *If m and n can be written as sums of four squares, then mn can also be written as sum of four squares.*

Proof. This follows from the following "beautiful" identity

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) = (ae - bf - cg - dh)^2 + (af + be + ch - dg)^2 \\ + (ag - bh + ce + df)^2 + (ah + bg - cf + de)^2.\end{aligned}$$

□

Lemma 7.8. *If p is a prime odd number, then there are integers r and s such that $p|r^2 + s^2 + 1$.*

Proof. Let g be a primitive root modulo p. First, observe that the congruence $x^2 \equiv m (\mathrm{mod}\ p)$ has a solution for all $m \in \{0, g^2, g^4, ..., g^{p-1}\}$, therefore for at least $(p + 1)/2$ values of m. On the other side, by the same argument the congruence $x^2 \equiv -m - 1 (\mathrm{mod}\ p)$ has a solution for at least $(p+1)/2$ values of m. Since $\frac{p+1}{2} + \frac{p+1}{2} > p$, we can find some $m \in \mathbb{N}$ such that congruences $x^2 \equiv m (\mathrm{mod}\ p)$ and $x^2 \equiv -m - 1 (\mathrm{mod}\ p)$ simultaneously have some solutions r and s respectively. This means that $p|r^2 - m$ and $p|s^2 + m + 1$, thus $p|r^2 + s^2 + 1$. □

Proof of Lagrange's theorem on some of four squares. The claim is obvious for $n = 1$ and $n = 2$, and according to lemma 7.7, it is enough to prove that every prime number can be written as a sum of four squares. Fix some prime number $p > 2$ and find $r, s \in \mathbb{N}$ such that $p|r^2 + s^2 + 1$ using lemma 7.8. On one side, consider the open ball

$$S := \{(x, y, z, t) \in \mathbb{R}^4 : x^2 + y^2 + z^2 + t^2 < 2p\}$$

which is open (hence Lebesgue-measurable), convex, symmetric and has volume[22]

$$m(S) = \frac{\pi^{4/2}}{\Gamma(\frac{4}{2}+1)}\sqrt{2p}^4 = 2\pi^2 p^2.$$

On the other side, consider the four vectors $u_1 = (p,0,0,0)$, $u_2 = (0,p,0,0)$, $u_3 = (r,s,1,0)$ i $u_4 = (s,-r,0,1)$ which generate a lattice Λ whose fundamental parallelogram has volume

$$\begin{vmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ r & s & 1 & 0 \\ s & -r & 0 & 1 \end{vmatrix} = p^2 < \frac{2\pi^2 p^2}{2^4} = \frac{1}{2^4} m(S).$$

Now Minkowski's theorem Vol. 2 gives us some nonzero point $(a,b,c,d) \in S \cap \Lambda$ and let us write $(a,b,c,d) = c_1u_1 + c_2u_2 + c_3u_3 + c_4u_4$ for some $c_1, c_2, c_3, c_4 \in \mathbb{Z}$. This gives us equalities

$$a = c_1p + c_3r + c_4s,\ b = c_2p + c_3s - c_4r,\ c = c_3,\ d = c_4$$

which we use to see that

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &= (c_1p + c_3r + c_4s)^2 + (c_2p + c_3s - c_4r)^2 + c_3^2 + c_4^2 \\ &\equiv (c_3r + c_4s)^2 + (c_3s - c_4r)^2 + c_3^2 + c_4^2 \\ &= c_3^2(r^2+s^2+1) + c_4^2(r^2+s^2+1) \equiv 0 (\text{mod } p). \end{aligned}$$

Since also $0 < a^2 + b^2 + c^2 + d^2 < 2p$ (because (a,b,c,d) is a nonzero element of S) we conclude that $p = a^2 + b^2 + c^2 + d^2$. □

Before ending this section, let us make some addition comments. Minkowski's theorem has its very important application in algebraic number theory. Namely, for any finite extension K of $\mathbb{Q}$, we have the ring of integers $\mathcal{O}_K$ is a lattice in $\mathbb{R}^n$ (where n is the degree of extension $K/\mathbb{Q}$). Moreover, one can prove that every ideal of $\mathfrak{a} \subseteq \mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-submodule of $\mathcal{O}_K$ (recall that $\mathcal{O}_K$ is noetherian) of rank n and to conclude that $\mathfrak{a}$ is also a lattice in $\mathbb{R}^n$. Then Minkowski's theorem can be used to bound the norm of ideal $\mathfrak{a}$, and after that it is not two hard to conclude that the class group of extension $K/\mathbb{Q}$ is finite. Sorry, I am drifting away again here. In any case, this theorem plays a very important rule in algebraic number theory.

On the other side, lattice can be defined in a much more general environment. Namely, let G be any locally compact topological group, which then must have (left) Haar measure. A discrete subgroup $H \leqslant G$ we call a **lattice** if the fundamental domain of the quotient space G/H has finite measure. Two very important example we obtain when we take $G_1 = \mathrm{SL}_2(\mathbb{R})$ and $G_2 = \mathrm{PSL}_2(\mathbb{R})$ which have lattices $H_1 = \mathrm{SL}_2(\mathbb{Z})$ and $H_2 = \mathrm{PSL}_2(\mathbb{Z})$. In the case of $\mathrm{SL}_2(\mathbb{Z})$ we can geometrically see Fundamental domain as a consequence of an action of this group on the upper hyperbolic plane $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ via Möbious transformations. Some ergodic theory can be applied here to analyse geodesic flows on $\mathbb{H}$ and here we really find a mixture of several areas of mathematics.

8 Proof via quadratic forms

In this section we will concentrate our attention on Lagrange's proof of our main theorem which will use (binary) quadratic forms.

Definition 8.1. *Let* $A = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$ *be a symmetric matrix with integer entries. To this matrix we associate a formal expression* $f(x,y) = ax^2 + 2bxy + cy^2$ *which we call a* ***integer quadratic form.***

Another way of seeing a quadratic form associated with matrix A is simply

$$f(x,y) := \begin{bmatrix} x & y \end{bmatrix} A \begin{bmatrix} x \\ y \end{bmatrix}.$$

When we look at the formulation of our problem, this definition can't come as a surprise since we are exactly interested in the quadratic form $x^2 + y^2$. More concretely, we are interested in which integers can be represented by this quadratic form.

[22] Where $\Gamma(x)$ is the Gamma function

Definition 8.2. *We say that an integer $n \in \mathbb{N}$ is* ***representable*** *by an integer quadratic form $ax^2 + 2bxy + cy^2$ if there are integers $x_0, y_0 \in \mathbb{Z}$ such that $n = ax_0^2 + 2bx_0y_0 + cy_0^2$.*

We will need several more standard notations some of them being familiar from linear algebra course.

Definition 8.3. *We say that quadratic forms $ax^2+2bxy+cy^2$ and $a'x^2+2b'xy+c'y^2$ are* ***equivalent*** *if there is a matrix $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ with integer entries and determinant 1 (hence in $\mathrm{SL}_2(\mathbb{Z})$) such that*

$$ax^2 + bxy + cy^2 = a'(\alpha x + \beta y)^2 + b'(\alpha x + \beta y)(\gamma x + \delta y) + c'(\gamma x + \delta y)^2.$$

In other words, quadratic forms associated with matrices A and B are equivalent iff there is matrix $P \in \mathrm{SL}_2(\mathbb{Z})$ such that $A = P^TBP$. In this case we also say that matrices A and B are $\mathbb{Z}$-congruent and matrix P we call a **transition matrix**.

Of course, this defines an equivalence relation (because we are using only invertible matrices) and it is easy to see that equivalent forms represent same integers. Now we define an important invariant of quadratic form.

Definition 8.4. *The* ***discriminant*** *of a quadratic form associated with matrix A is defined to be $\det(A)$.*

We say that a quadratic form $ax^2 + 2bxy + by^2$ is ***positive definite*** *if for every $(x_0, y_0) \in \mathbb{Z}^2\backslash\{(0, 0)\}$ we have $ax_0^2 + 2bx_0y_0 + cy_0^2 > 0$.*

Since equivalent forms represent same numbers, we have that every form equivalent to a positive form must also be positive.

Lemma 8.5. *Equivalent forms have the same discriminant.*

Proof. Suppose that forms associated with matrices A and B are equivalent. This means that we can find a matrix $P \in \mathrm{SL}_2(\mathbb{Z})$ such that $A = P^TBP$, thus Cauchy-Binet formula gives us $\det(A) = \det(P^TBP) = \det(P^T)\det(B)\det(P) = \det(A)$ (since $\det(P) = 1$). □

The following theorem represents the main step in our proof of the Fermat's theorem on sum of two squares. It gives us some kind of canonical form of positive definite quadratic forms. Observe that we can't just use well-known canonical forms from linear algebra because there transition matrices can have real/complex entries.

Theorem 8.6. *Every positive definite quadratic form is equivalent to a (positive definite) form with matrix $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ such that $2|b| \leqslant a \leqslant c$. This canonical form of positive definite form we call* ***reduced****.*

Proof. Consider the positive definite quadratic form $g(x, y) = \alpha x^2 + 2\beta xy + \gamma y^2$ and let a be the smallest natural number representable by g. Then we can find some $r, t \in \mathbb{Z}$ such that $g(r, t) = a$. We claim that $\gcd(r, t) = 1$, so suppose on the contrary that $p|r$ and $p|t$ (for some prime p). Then equality $a = g(r, t) = \alpha r^2 + 2\beta rt + \gamma t^2$ implies that $p^2|a$. But now we have that $g\left(\frac{r}{p}, \frac{t}{p}\right) = \frac{a}{p^2}$ which is a contradiction with minimality of a.

Now, since $\gcd(r, t) = 1$ (by Bézout's theorem) the equation $ru - st = 1$ with variables $u, s \in \mathbb{Z}$ has a solution. Moreover, if we fix a solution $(u_0, s_0) \in \mathbb{Z}^2$, then all other solutions are of the form $(s(h), u(h))$ where $s(h) = s_0 + rh$ and $u(h) = u_0 + ht$ (while $h \in \mathbb{Z}$ sprints). Observe quickly that not both $s(h)$ and $u(h)$ can be zero. The idea is to take the matrix

$$P := \begin{bmatrix} r & s(h) \\ t & u(h) \end{bmatrix}$$

to be the transition matrix, where we are going to choose a suitable $h \in \mathbb{Z}$. Since $\det(P) = ru(h) - ts(h) = 1$ always holds we don't need to worry about P living in $\mathrm{SL}_2(\mathbb{Z})$. After the transformation by matrix P we will obtain

$$\begin{bmatrix} a(h) & b(h) \\ b(h) & c(h) \end{bmatrix} = \begin{bmatrix} r & s(h) \\ t & u(h) \end{bmatrix}^T \begin{bmatrix} \alpha & \beta \\ \beta & \gamma \end{bmatrix} \begin{bmatrix} r & s(h) \\ t & u(h) \end{bmatrix}$$

so after some ultra-interesting calculations we get

$$a(h) = a,\ b(h) = s_0(\alpha r + \beta t) + u_0(\beta r + \gamma t) + ah,\ c(h) = g(s(h_0), u(h_0)).$$

On one side, since g is positive definite and since a is the smallest number representable by g, we obtain that $c(h) = g(s(h_0), u(h_0)) \geqslant a = a(h)$ for any choice of $h \in \mathbb{Z}$. Finally, expression $b(h)$ has a fixed value modulo a, so by choosing an appropriate $h \in \mathbb{Z}$ we may obtain $|b(h_0)| \leqslant a/2$. This completes our construction of the desired matrix. □

Corollary 8.7. *Every positive-definite quadratic form of discriminant* 1 *is equivalent to* $x^2 + y^2$.

Proof. By theorem 8.6 any positive definite quadratic form with discriminant 1 is equivalent to a quadratic form f with matrix $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ such that $2|b| \leqslant a \leqslant c$. Moreover, by lemma 8.5 this f must also have discriminant 1, so we have that $ac - b^2 = 1$ (hence $a \neq 0$). How we have that

$$a^2 \leqslant ac = b^2 + 1 \leqslant \frac{a^4}{4} + 1,$$

which is only possible for $a = 1$ (because $a \neq 0$). Now $2|b| \leqslant a = 1$ implies $b = 0$ and $ac = 1$ implies $c = 1$. Therefore, we proved that $f(x, y) = x^2 + y^2$. □

Proof of Fermat's theorem on sum of two squares. Let $p = 4k + 1$ be a prime and pick some $m \in \mathbb{N}$ such that $p|m^2 + 1$. Then we can find some $k \in \mathbb{N}$ such that $m^2 + 1 = pk$ and consider the quadratic form

$$f(x, y) = px^2 + 2mxy + ky^2.$$

This quadratic represents p since $f(1, 0) = p$, has discriminant $pk - m^2 = 1$ and is positive-definite because we have

$$f(x, y) = p\left(x + \frac{my}{p}\right)^2 + ky^2 - \frac{m^2y^2}{p} = p\left(x + \frac{my}{p}\right)^2 + \frac{y^2}{p}.$$

By corollary 8.7 we know that f is equivalent to $x^2 + y^2$, so the form $x^2 + y^2$ also represents p. □

It is far from truth that interaction of quadratic forms with number theory stop here. In completely analogous way one can introduce ternary quadratic forms which are associated to 3×3 symmetric integer matrices and the corresponding notions of equivalence, discriminant and positive definiteness. Then one can prove that every positive definite ternary quadratic form with discriminant 1 is equivalent to $x^2 + y^2 + z^2$, and from this deduce Legendre's sum of three squares theorem. Details are little messier than in the 2×2 case, so we will skip them.

On the other side, the work of Lagrange and Gauss discovered some very unexpected connection of quadratic forms with algebraic number theory. Namely, there is a bijective correspondence between the class group of quadratic field extension $K/\mathbb{Q}$ with discriminant D and classes of equivalence of positive definite binary quadratic forms with discriminant D. Unfortunately, there is no natural operation which would make this collection of forms a group and thus make this correspondence an isomorphism. However, from this we (almost) immediately deduce the following very nice characterization.

Theorem 8.8. *Let* $K = \mathbb{Q}[\sqrt{D}]$ *be an imaginary quadratic field extension of* $\mathbb{Q}$ *(*$D < 0$ *square-free). Then the following statements are equivalent*

(a) Ring of integers $\mathcal{O}_K$ *is a unique factorization domain;*

(b) Ring of integers $\mathcal{O}_K$ *is a principal ideal domain;*

(c) The class group of $\mathcal{O}_K$ *is trivial;*

(d) There is a unique reduced positive definite (binary) quadratic form of discriminant D.

This is a very important characterization, since one of the major (Gauss's) problems was to determine when rings of integers $\mathcal{O}_K$ are unique factorization domains. One can prove that this happens for square-free $D < 0$ iff[23]

$$D \in \{-1, -2, -3, -7, -11, -19, -43, -67, 163\}.$$

Only Gauss himself knows why these numbers are so special.

Open Problem 8.9. *Find all square free $D > 0$ such that $\mathbb{Q}[\sqrt{D}]$ is UFD.*

It is not even know if there are infinitely many number fields whose rings of integers are UFD!

9 The one-line proof and a proof via partitions

In this section we will present two proofs which use essentially same ideas, but are interesting on their own. The first one is probably the most boring proof of our main theorem. The reason I don't really like it is because it doesn't give much insight about the problem and what is actually hiding behind the curtain. Sometimes I find it better to work harder to obtain some surrounding results in order to better understand the problem.

Anyways, it is definitely interesting to see that our problem has a very short solution which is due to Zagier. Recall that a function $f : A \to A$ we call **involution** if $f^2 = \mathrm{id}_A$. Observe a very simple fact that if A is a finite set, then the number of fixed points of f must be the same parity as $|A|$.

Proof of Fermat's theorem on sum of two squares. Let $p = 4k + 1$ be a prime and let us consider the finite set

$$S := \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\},$$

which is nonempty since $(1, p, 1) \in S$. One can easily check that the function

$$f(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z \\ (2y - x, y, x - y + z), & y - z < x < 2y \\ (x - 2y, x - y + z, y), & x > 2y \end{cases}$$

is one involution of set S whose only fixed point is $(1, 1, k)$. Therefore, set S must have an odd number of elements, so every other involution must have at least one fixed point. In particular, involution $(x, y, z) \mapsto (x, z, y)$ has at least one fixed point of the form (x, y, y) meaning that $x^2 + (2y)^2 = p$. □

The second proof uses partitions which are interesting objects themselves. From the number-theoretic point of view, partitions are pretty hard to work with as we will see soon.

Definition 9.1. *A **partition** of a natural number $n \in \mathbb{N}$ is any non-increasing sequence $(a_1, ..., a_m)$ of non-negative integers satisfying $a_1 + ... + a_m = n$. The total number of partitions of number $n \in \mathbb{N}$ we denote with $p(n)$.*

If one tries to analyse the function $p(n)$, he will soon realise he is in trouble. There are some nice ways to understand this function and the most popular one is via formal series. More precisely, the usual starting point of these investigations is the famous identity

$$\sum_{n=0}^{\infty} p(n)t^n = \prod_{j=1}^{\infty}(1 - t^j)^{-1}$$

where we put $p(0) := 0$. The real order of function $p(n)$ is known, but this result is very non-trivial to obtain.

Theorem 9.2 (Hardy-Ramanujan)**.** $p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{2n/3}}$.

[23]Observe that for $D = -1$ we get the ring of Gaussian integers which correspond to our quadratic form $x^2 + y^2$, i.e. the norm in $\mathbb{Z}[i]$

In his (unfortunately very short) career, Ramanujan also discovered what are now called Rogers-Ramanujan's identities. This are some identities involving formal series which have some very nice combinatorial interpretations.

The algebraic importance of the function $p(n)$ is actually quite big, since one can prove via the Fundamental theorem for finite abelian groups the following formula.

Exercise 9.3. *Prove that the number of finite abelian groups of order $n = p_1^{k_1}p_2^{k_2}...p_r^{k_r}$ is exactly $p(k_1)p(k_2)...p(k_r)$.*

Anyway, let us get back to our story. When we have a partition

$$(\underbrace{a_1, ..., a_1}_{f_1}, ..., \underbrace{a_m, ..., a_m}_{f_m}),$$

where $a_1 \geqslant a_2 \geqslant ... \geqslant a_m$, we will denote it with $(a_1^{f_1}...a_m^{f_m})$.

Why are we doing this and what does this have to do with our initial problem? Well, just observe that a natural number is a BMS number iff it has a partition of the form $(a^a b^b)$. Therefore, let us denote with $\mathcal{P}_2^n$ the set of all partitions of n of the form $(a_1^{f_1}a_2^{f_2})$.

Lemma 9.4. *If p is a prime odd number, then $|\mathcal{P}_2^p|$ is odd.*

Proof. Let us define a map $C : \mathcal{P}_2^p \to \mathcal{P}_2^p$ with

$$C(a_1^{f_1}a_2^{f_2}) = ((f_1 + f_2)^{a_2} f_1^{a_1 - a_2})$$

which is well-defined since $a_2(f_1+f_2)+(a_1-a_2)f_1 = a_1f_1+a_2f_2 = p$. Moreover, for any $(a_1^{f_1}a_2^{f_2}) \in C$ we have that

$$C(C(a_1^{f_1}a_2^{f_2})) = C((f_1 + f_2)^{a_2} f_1^{a_1-a_2}) = (a_2 + a_1 - a_2)^{f_1} a_2^{f_1+f_2-f_1} = (a_1^{f_1}a_2^{f_2}),$$

so C is an involution. Now to prove that $|\mathcal{P}_2^p|$ is odd, it is enough to see why C has an odd number of fixed points. So, if $(a_1^{f_1}a_2^{f_2})$ is a fixed point, then we have that

$$(a_1^{f_1}a_2^{f_2}) = C(a_1^{f_1}a_2^{f_2}) = ((f_1 + f_2)^{a_2} a_1^{a_1-a_2})$$

thus $f_1 = a_2$ and $a_1 = f_1 + f_2$. Since we also have $p = a_1f_1 + a_2f_2 = f_1(a_1 + f_2)$ which is prime, it must hold $f_1 = 1$ (since $a_1 + f_2 > 1$). Finally, this implies that $p = a_1 + f_2 = 2f_2 + 1$ so there is exactly one fixed point. □

Proof of Fermat's theorem on sum of two squares. Let $p = 4k + 1$ be a prime and the idea is to calculate the parity of $|\mathcal{P}_2^p|$ in a different way. Let us cook up the following set

$$\mathcal{A} := \{(a_1^{f_1}a_2^{f_2}) \in \mathcal{P}_2^n : f_1 \neq f_2 \text{ and } (a_1 \neq f_1 \text{ or } a_2 \neq f_2)\} \subseteq \mathcal{P}_2^p$$

and consider the function $T : \mathcal{A} \to \mathcal{A}$ given with

$$T(a_1^{f_1}a_2^{f_2}) := \begin{cases} (f_1^{a_1} f_2^{a_2}), & f_1 > f_2 \\ (f_2^{a_2} f_1^{a_1}), & f_1 < f_2. \end{cases}$$

This is clearly well-defined and one can easily check that this defines an involution. Moreover, this involution has no fixed points since a (potential) fixed point $(a_1^{f_1}a_2^{f_2}) \in \mathcal{A}$ would have to satisfy $a_1 = f_1$ (impossible because how we defined $\mathcal{A}$) or ($a_2 = f_1$ and $a_1 = f_2$) (impossible since $p = a_1f_1 + a_2f_2 > 2$ is a prime). Therefore, we have that $|\mathcal{A}|$ is even, so lemma 9.4 gives us that $|\mathcal{P}_2^p \backslash \mathcal{A}|$ is odd.

Now, let us consider an arbitrary element $(a_1^{f_1}a_2^{f_2}) \in \mathcal{P}_2^p \backslash \mathcal{A}$. We have two distinct possibilities (distinct because p is prime), so suppose first that $f_1 = f_2$. In this case we have that $p = f_1(a_1 + a_2)$ so $f_1 = 1$ (because p is prime). Therefore, we obtain a partition $p = a_1 + a_2$ and there are obviously exactly $\frac{p-1}{2}$ these partitions (so an even number).

On the other side, suppose that $a_1 = f_1$ and $a_2 = f_2$. In this case we get that $p = a_1^2 + a_2^2$, so the number of these partitions is the same as the number of ways to present p as a sum of two squares. Since $|\mathcal{P}_2^p \backslash \mathcal{A}|$ is odd and since partitions of the first kind we have even, we conclude that have odd number of partitions $p = a_1^2 + a_2^2$, hence we are done. □

10 Proof via formal series - only idea

It is not a great mystery that the theory of formal series is very useful in combinatorics, especially when dealing with reccurence formulas. In the previous section we have seen a certain identity which unravels some interesting properties of the partitions function and we will see a relatively similar idea here. More precisely, if we denote with $r_2(n)$ the number of ways to present n as sum of two squares, then we have the following identity

$$\sum_{n=1}^{\infty} r_2(n)t^n = \left(\sum_{k=-\infty}^{\infty} t^{k^2}\right)^2.$$

After much exiting calculations (which I was too lazy to go through) one can obtain the following equality

$$\left(\sum_{k=-\infty}^{\infty} t^{m^2}\right)^2 = 1 + 4\sum_{n=0}^{\infty}\left(\frac{t^{4n+1}}{1-t^{4n+1}} - \frac{t^{4n+3}}{1-t^{4n+3}}\right).$$

I turns out that the last two series have a very nice number-theoretic interpretation which gives us the following (surprisingly strong) theorem.

Theorem 10.1 (Jacobi's[24] theorem)**.** *If n is a natural number and we denote with $d_1(n)$ and $d_3(n)$ numbers of its divisors of n which are congruent 1 and 3 modulo 4, then we have that $r_2(n) = 4(d_1(n) - d_3(n)$.*

Now one can very easily deduce from this even the Sum of two squares theorem which we will leave to the reader.

References

[1] Tom Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, 2000.

[2] David Dummit, Richard Foote, *Abstract Algebra*, John Wiley & Sons, Inc, 2004.

[3] Manfred Einsiedler, Thomas Ward, *Ergodic Theory*. Springer Monograph in Mathematics, 2010.

[4] Pierre Samuel, *The Pythagorean Introduction to Number Theory*. Springer Undergraduate Texts in Mathematics, 2018.

[5] Ramin Takloo-Bighash, *Algebraic Theory of Numbers*. Hermann Publishers in Arts and Science, Paris, 1972.

[6] Mak Trifković, *Algebraic Theory of Quadratic Numbers*. Springer Unversitext, 2013.

[24] Carl Gustav Jacob Jacobi(1804-1851), a German mathematician