GEODESICS AND VALUES OF QUADRATIC FORMS

GREG MCSHANE

1. Introduction

Theorem 1.1. *Let p be a prime then the equation*

$$x^2 = -1$$

admits a solution in $\mathbb{F}_p$ iff $p = 2$ or $p - 1$ is a multiple of 4.

Theorem 1.2 (Fermat)**.** *Let p be a prime then the equation*

$$x^2 + y^2 = p$$

has a solution in integers iff $p = 2$ or $p - 1$ is a multiple of 4.

There are many proofs of these theorems but the approach initiated by Heath-Brown in [8] has inspired many admirers if not imitators see for example the very nice account of Elsholtz [5]. In some senses this manuscript is a companion to Elsholtz's where instead of looking at the number theory as combinatorics we work in an explicitly geometric context. As such we refer the reader to Elsholtz for historical perspective and the like.

The essential ingredients in the Heath-Brown paper are : a finite set X equipped with a pair of involutions

- any fixed point of the one of the involutions, should it exist, is a solution of the equation.
- the other involution has a unique fixed point which is easy to compute.

The existence of the unique fixed point of the second involution allows one to conclude that the X has an odd number of elements and so that any involution has a fixed point.

2.

3. Klein four group and the Burnside Lemma

We give a proof of Theorem 1.1 using the Burnside Lemma. Recall that if G is a group acting on a finite set X then the Burnside Lemma says

$$|G||X/G| = \sum_g |X^g| \tag{1}$$

where, as usual, X^g denotes the set of fixed points of the element g and X/G the orbit space.

Let $p \neq 2$, $X = \mathbb{F}_p^*$ and G be the group generated by the two involutions

$$\begin{aligned} x &\mapsto -x \\ x &\mapsto 1/x. \end{aligned}$$

The group G has exactly four elements namely:

- the trivial element which has $p-1$ fixed points
- $x \mapsto -x$ which has no fixed points
- $x \mapsto 1/x$ has exactly two fixed points namely 1 and -1.
- $g : x \mapsto -1/x$ is the remaining element and the theorem is equivalent to the existence of a fixed point for it.

Note that since $\mathbb{F}_p$ is a field $|X^g| = \sharp\{x^2 = -1,\, x \in \mathbb{F}_p^*\}$ is either 0 or 2. Now for our choice of X and G equation (1) yields

$$4|X/G| = (p-1) + 2 + |X^g|. \tag{2}$$

The LHS is always divisible by 4 so the RHS is too and it follows from this that

$$|X^g|. = \begin{cases} 0 & (p-1) = 2 \mod 4 \\ 2 & (p-1) = 0 \mod 4 \end{cases}$$

This proves Theorem 1.1.

4. Counting sums of squares

The transformation $z \mapsto z+1$ generates an infinite cyclic group acting on $\mathbb{H}$. The standard fundamental domain for this group is an infinite strip, which we will refer to as the *fundamental strip*, consisting of all the $z \in \mathbb{C}$ such that the real part is between 0 and 1.

Lemma 4.1. *Let $n \geq 2$ be an integer. The number of ways of writing n as a sum of squares*

$$n = c^2 + d^2$$

with c, d coprime integers is equal to the number of points of $\Gamma.\{i\}$, the $\mathrm{SL}(2,\mathbb{Z})$ orbit of i, in the fundamental strip at height $\frac{1}{n}$.

Note that we are counting $c^2 + d^2$ and $d^2 + c^2$ as *different* representations of n.

Proof. Suppose there is such a point which we denote w verifying the hypotheses in particular

$$w = \frac{ai+b}{ci+d}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

then

$$\operatorname{Im} w = \operatorname{Im} \frac{ai+b}{ci+d} = \frac{\operatorname{Im} i}{c^2+d^2}.$$

So $n = c^2 + d^2$.

Conversely if c, d are coprime integers then there exists a, b such that

$$ad - bc = 1 \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

By applying a suitable iterate of the parabolic transformation $z \mapsto z+1$, one can choose w such that $0 \leq \operatorname{Re} w < 1$.

□

Suppose that n is can be written as a sum of squares $c^2 + d^2$ and w is the corresponding point in the fundamental stripthen we can associate a Poincaré geodesic to w in a natural way, we simply take the vertical line that passes through w. This geodesic joins two points in the ideal boundary of $\mathbb{H}$ namely ∞ and $\frac{ac+bd}{n} \in \mathbb{R}$. Although not strictly necessary we choose to associate a geometric quantity to this geodesic - Penner's λ-length.

5. Inversions

We denote by $\mathbb{H}$ the Poincaré upper half plane and $\partial\mathbb{H}$ its ideal boundary ie $\mathbb{R} \cup \{\infty\}$. Recall that an *inversion* is an orientation reversing isometry of $\mathbb{H} \cup \partial\mathbb{H}$. A Poincaré geodesic is either a vertical line or a semicircle orthogonal to $\mathbb{R}$. In both cases it is uniquely determined by its endpoints in the ideal boundary. To each Poincaré geodesic is associated a unique inversion which fixes it pointwise. The inversion $\phi_h : z \mapsto -\bar{z}$ fixes 0 and ∞ and so the arc joining them. The group of isometries acts transitively on pairs of distinct points $a, b \in \partial\mathbb{H}$ and so there is an inversion that fixes the geodesic joining them. The inversion fixing $1, -1$ is easily seen to be $\phi_v : z \mapsto \frac{1}{\bar{z}}$.

Note that if a, b are coprime integers then:

- The image of $\frac{a}{b}$ under ϕ_h is $-\frac{a}{b}$ and the λ-length of the geodesic joining them is $2ab$.
- The image of $\frac{a}{b}$ under ϕ_v is $\frac{b}{a}$ and the λ-length of the geodesic joining them is $|a^2 - b^2|$.

Lemma 5.1. *Let $p > 2$ be a prime then:*

- *There are exactly two arcs of λ-length p invariant under ϕ_v;*
- *There is no arc of λ-length p invariant under ϕ_h.*

6. Congruence subgroups

The principal congruence subgroup $\Gamma(p)$ is the subgroup of $\Gamma = \mathrm{SL}(2, \mathbb{Z})$ is a normal. It is a subgroup of $\Gamma_0(p)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod p.$$

For $p = 2$ this is generated by just two elements namely:

$$P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } Q = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

The product $P^{-1}Q$ is an element of order 2:

$$P^{-1}Q = \begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}.$$

So the quotient $\mathbb{H}/\Gamma_0(2)$ is a non-compact orbifold with two cusps and a single cone point.

References

[1] M. Aigner *Markov's Theorem and 100 Years of the Uniqueness Conjecture*, Springer(2013)

[2] Aigner M., Ziegler G.M. *Representing numbers as sums of two squares.* In: Proofs from THE BOOK. Springer, Berlin, Heidelberg. (2010)
barag A. Baragar, *On the Unicity Conjecture for Markoff Numbers* Canadian Mathematical Bulletin , Volume 39 , Issue 1 , 01 March 1996 , pp. 3 - 9

[3] J. O. Button, *The uniqueness of the prime Markoff numbers*, J. London Math. Soc. (2) 58 (1998), 9–17.

[4] Dolan, S. (2021). 105.38 A very simple proof of the two-squares theorem. The Mathematical Gazette, 105(564), 511-511. doi:10.1017/mag.2021.120

[5] Elsholtz C.A *Combinatorial Approach to Sums of Two Squares and Related Problems.* In: Chudnovsky D., Chudnovsky G. (eds) Additive Number Theory. Springer, New York, NY. (2010)

[6] Lester R Ford, *Automorphic Functions*

[7] Generalov, A.I. A combinatorial proof of Euler-Fermat's theorem on the representation of the primes p=8k+3 by the quadratic form $x^2 + 2y^2$. J Math Sci 140, 690–691 (2007). https://doi.org/10.1007/s10958-007-0008-6

[8] Heath-Brown, Roger. *Fermat's two squares theorem.* Invariant (1984)

[9] Neil Herriot, Communication with Jim Propp `https://faculty.uml.edu/jpropp/reach/Herriot/ptolemywriteup.html`

[10] Jackson, Terence H.. "A Short Proof That Every Prime $p = 3(\mod 8)$ Is of the Form $x^2 + 2y^2$." The American Mathematical Monthly 107 (2000): 447 - 447.

[11] M.L. Lang, S.P Tan, *A simple proof of the Markoff conjecture for prime powers* Geometriae Dedicata volume 129, pages15–22 (2007)

[12] G. McShane, *Simple geodesics and a series constant over Teichmuller space* Invent. Math. (1998)

[13] Northshield, Sam. *A Short Proof of Fermat's Two-square Theorem.* The American Mathematical Monthly. 127. 638-638. (2020).

[14] R. C. Penner, *The decorated Teichmueller space of punctured surfaces*, Communications in Mathematical Physics 113 (1987), 299–339.

[15] James Propp, The combinatorics of frieze patterns and Markoff numbers, in Integers, Volume 20 (2020) `http://math.colgate.edu/~integers/u12/u12.pdf`

[16] J-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, Springer-Verlag New York 1973

[17] D. Zagier, *A one-sentence proof that every prime p = 1 (mod 4) is a sum of two squares*, American Mathematical Monthly, 97 (2): 144

Institut Fourier 100 rue des maths, BP 74, 38402 St Martin d'Hères cedex, France
Email address: `mcshane at univ-grenoble-alpes.fr`