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 account of Elsholtz [6]. The essential ingredients 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.

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 1.3. *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 $\frac{1}{n}$.

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

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

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

$$ad - bc = 1 \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

By applying a suitable iterate of the parabolic transformation $z \mapsto z+1$, one can choose w such that $0 \leq \operatorname{Re} w < 1$. So if $n = c^2 + d^2$ then $\frac{ai+b}{ci+d}$ is on one of the lines of the family in the statement.

□

The principal congruence subgroup $\Gamma(p)$ is the subgroup of $(2, \mathbb{Z})$ 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)

[3] A. Baragar, *On the Unicity Conjecture for Markoff Numbers* Canadian Mathematical Bulletin , Volume 39 , Issue 1 , 01 March 1996 , pp. 3 - 9

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

[5] 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

[6] 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)

[7] Lester R Ford, *Automorphic Functions*

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

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

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

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

[12] Northshield, Sam. *A Short Proof of Fermat's Two-square Theorem.* The American Mathematical Monthly. 127. 638-638. (2020).
[13] J-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, Springer-Verlag New York 1973
[14] 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