GEODESICS AND VALUES OF QUADRATIC FORMS

GREG MCSHANE AND VLAD SERGESCIU

Theorem 0.1. *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 0.2 (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.

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

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