Reference Formulae

Focus : $(ae, 0)$
Directrix : $x = \frac{a}{e}$

Parabola $(e = 1)$

Equation :

$$y^2 = 4ax$$

Parametric form : $(at^2, 2at)$

Ellipse $(0 < e < 1)$

Equation :

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

Parametric form : $(a\cos t, b\sin t)$

Hyperbola $(e > 1)$

Equation :

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

Parametric form : $(a\sec t, b\tan t)$

Group law on Parabola

Given any parabola, there exists an affine transformation that takes it to the curve $y = x^2$.

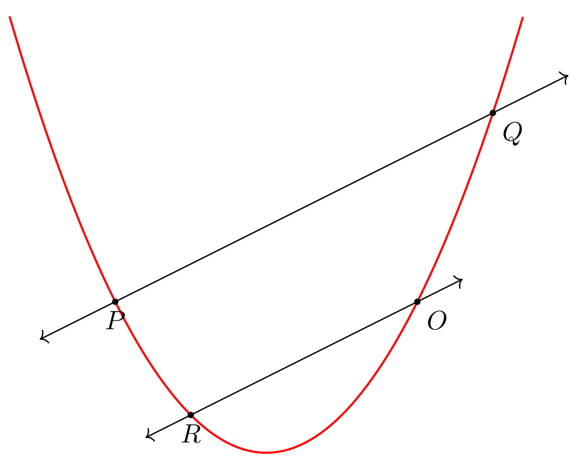

Figure 1: $R = P \oplus Q$

We define the parametric coordinates of the point R as (r, r^2). We compare the slopes of the two lines PQ and OR to obtain the co-ordinates of R.

$$\frac{r^2 - o^2}{r - o} = \frac{p^2 - q^2}{p - q}$$
$$r = p + q - o$$

We define a homomorphism from the points on the parabola to R as $\phi((x, x^2)) = x - o$. The map that is defined is a bijection hence it is an isomorphism. The curve shown in the figure is $\mathbb{R}^2$ however the algebra performed remains the same if the field is changed to $\mathbb{C}^2$.

Solving for curves in finite fields

We first investigate the solution set of a curve when working with finite field $\mathbb{Z}_p$.

$$\mathcal{C} = \{(x_1, x_2, \cdots, x_n) \in \mathbb{Z}_p^n \mid \textit{condition}\} \subseteq \mathbb{Z}_p^n$$

We notice that $\mathbb{Z}_p^n$ contains a finite number of points (p^n) and so will V. So it is a valid approach to just verify which points out of these will satisfy the condition.

We now see the solution for one such problem

$$V = \{(x, y, z) \in \mathbb{Z}_p^3 \,|x^2 + y^2 = z^2\}$$

We take a different approach to the problem. We set z as a parameter and plot the various curves for different values of z. Now the problem is simplified to two variables for each value of z. We see that we can embed $\mathbb{Z}_p^2$ in $\mathbb{R}^2$ such that $\mathbb{Z}_p^2 \subset \mathbb{R}^2$.

For every $z \in \mathbb{Z}_p$, Define $\mathcal{V}_z = \{(x, y) \,|x^2 + y^2 = z^2\}$

Notice that:

$$V = \bigcup_{z \in \mathbb{Z}_p} \mathcal{V}_z \cap \mathbb{Z}_p^2$$

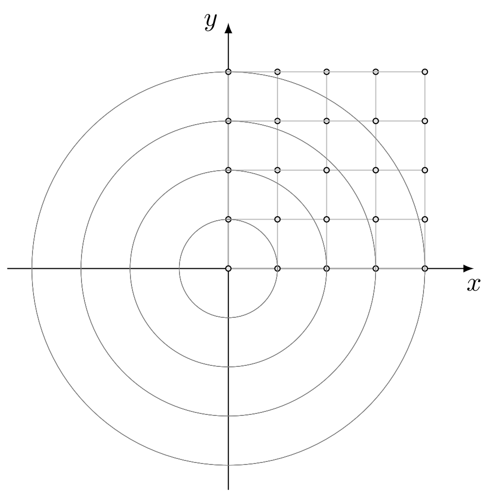

Figure 2: The figure represents the *mod* 5 solutions