COUNTING POINTS ON ELLIPTIC CURVES

OLE ANDRE BIRKEDAL

Abstract. hei hei

Contents

1. P-adic numbers

There are several definitions of p-adic integers, we will start with the easiest. Later we will see an algebraic contructions.

Definition 1. *A p-adic integer is a formal power series with coefficients $a_i \in \mathbb{Z}/p\mathbb{Z}$*

$$\sum_{i=0}^{\infty} a_i p^i$$

With this in mind you can identify a p-adic integer with a sequence of coefficients $(a_i)_{i>0}$. This is in fact a Cauchy sequence with the p-adic metric in $\mathbb{Q}$ given as follows: let x be a rational number then we can write $x = p^n \frac{a}{b}$ where p does not divide a or b. If they do not contain p as a factor we set $n = 0$. We then let the p-adic metric be given as $|x|_p = p^{-n}$. This is similar to how the real numbers are constructed using equivalence classes of Cauchy sequences from analysis.

Already we can see that the ring of p-adic integers is not countable. We do this by taking a countable sequence of p-adic integers

$$a = \sum a_i p^i \quad b = \sum b_i p^i \quad c = \sum c_i p^i \quad \dots$$

then we construct a new p-adic integer

$$x = \sum x_i p^i$$

where we choose $x_0 \neq a_0$, $x_1 \neq b_1$, $x_2 \neq c_2$, ... This new p-adic integer is different from those already in the set, thus they do not exhaust the whole set of p-adic integers. This shows that a mapping from $\mathbb{N}$ into the p-adic integers is never a surjection.