Elliptic curves: homework 12
Mastermath / DIAMANT, Spring 2019
Martin Bright and Marco Streng

1. (Cassels §17, exercise 1) For a prime p and a non-zero rational number a, let $|a|_p$ denote the *p-adic absolute value* of a, defined as

$$|a|_p = p^{-r}$$

where r is the (positive or negative) power of p occurring in the factorisation of a into primes. Let $|a|_\infty$ denote the usual absolute value of a, and let

$$\Omega = \{p \in \mathbb{N} \mid p \text{ prime}\} \cup \{\infty\}$$

be the set of all these absolute valuations.

(a) Prove the product formula:

$$\text{for all } a \in \mathbb{Q}^\times, \quad \prod_{v \in \Omega} |a|_v = 1.$$

(b) Let $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n(\mathbb{Q})$ be a point of projective space. Show that the quantity

$$\prod_{v \in \Omega} \max_i |a_i|_v$$

is equal to the height $H(P)$ as defined in the lecture.

2. For a positive real number B, let $N(B)$ denote the number of points of $\mathbb{P}^1(\mathbb{Q})$ having height at most B. Show that

$$N(B) \sim \frac{2}{\zeta(2)} B^2 \qquad \text{as } B \to \infty,$$

where ζ is the Riemann zeta function.

3. (a) Show that, if A is a finite Abelian group, then the groups $A[2]$ and $A/2A$ have the same order.

(b) Deduce a formula allowing you to compute the rank of an elliptic curve E over $\mathbb{Q}$, given the order of $E(\mathbb{Q})/2E(\mathbb{Q})$ and the order of $E[2](\mathbb{Q})$.

4. For each of the following elliptic curves E over $\mathbb{Q}$, find the group structure of $E(\mathbb{Q})$. Give explicit generators for the torsion part; for the free part, give points that generate it up to finite index. *(Without doing more work on height bounds, we do not know how to tell the difference between a set of generators for the free part, and a set of generators for a subgroup of finite index.)*

(a) $y^2 = x(x^2 + 3x + 5)$;

(b) $y^2 = x(x^2 - 2x + 9)$.