

## Elliptic Curves. MT 2025. Sheet 2.

### Section A

1. Let  $K$  be a field with non-Archimedean valuation  $|\cdot|$ .
  - (a) For any  $x, y \in K$  show that, if  $|x| \neq |y|$  then  $|x \pm y| = \max(|x|, |y|)$ .
  - (b) If  $x_1, \dots, x_n \in K$  and if there exists  $\ell$  such that  $|x_\ell| > |x_i|$  for all  $i \neq \ell$ , then show that  $|x_1 + \dots + x_n| = |x_\ell|$ .
  - (c) Suppose that  $s_n \rightarrow s$  in  $K, |\cdot|$ . Show that  $|s_n| \rightarrow |s|$  in  $\mathbb{R}, |\cdot|_\infty$ . When  $s \neq 0$ , show that there exists  $N$  such that, for all  $n > N$ ,  $|s_n| = |s|$ .
2. (a) Find:  $|3/50|_5, |3/50|_3, |3/50|_7, d_5(2/3, 1/5), d_7(2/3, 1/5), d_{11}(2/3, 1/5)$ .  
  
(b) Describe  $|3/7|_p$  for all  $p$ . What is the product  $\prod |3/7|_i$ , taken over  $i = p$ , for all primes  $p$ , and  $i = \infty$ ? Given any  $x \in \mathbb{Q}$  ( $x \neq 0$ ), what is  $\prod |x|_i$ ?
3. Which of the following are convergent in  $\mathbb{Q}_5$ ?  
(a)  $1/5^n$ . (b)  $n$ . (c)  $n!$  (d)  $3 + 10^n$ . (e)  $\sum_0^\infty 10^n$ . (f)  $\sum_0^\infty 7^n$ .

### Section B

4. For each  $p, m, r$ , either find an  $x \in \mathbb{Z}$  such that  $|x^2 - r|_p \leq p^{-m}$  or show that no such  $x$  exists.  
(a)  $p = 5, r = -1, m = 4$ . (b)  $p = 3, r = 7/8, m = 7$ . (c)  $p = 5, r = 5/4, m = 4$ .
5. Find the 7-adic expansion of each of: 200 and  $3/14$ . Determine the member of  $\mathbb{Q}$  expressed by the 5-adic expansion  $2, \overline{34}$ .
6. For which primes  $p$  does there exist  $x \in \mathbb{Q}_p$  such that  $x^2 = -28$ ? Your answer should be given in terms of a congruence condition on  $p$ .
7. Show that  $(X^2 - 2)(X^2 - 17)(X^2 - 34)$  has a root in  $\mathbb{R}$  and in every  $\mathbb{Q}_p$ , but not in  $\mathbb{Q}$ .
8. Is 4 a cube in  $\mathbb{Q}_3$ ? Is 28 a cube in  $\mathbb{Q}_3$ ? Is 13 a cube in  $\mathbb{Q}_7$ ?
9. Let  $p \equiv 2 \pmod{3}$ . For any  $a \in \mathbb{Z}$  such that  $p \nmid a$ , show that there exists  $x \in \mathbb{Z}_p$  with  $x^3 = a$ .

Section C

10. For any odd prime  $p$  and any positive integer  $m$  not divisible by  $p$ , show that there is a primitive  $m$ th root of unity in  $\mathbb{Q}_p$  if and only if  $m|(p-1)$ .  
*(In fact, the roots of unity in  $\mathbb{Q}_p^\times$  are a cyclic subgroup of order  $(p-1)$ .)*
11. (a) Show that  $|n!|_p = p^{-M}$  where  $M = \sum_{i=1}^{\infty} \left[ \frac{n}{p^i} \right]$  (where  $[x]$  denotes the greatest integer  $\leq x$ ).
- (b) Let  $K$  be a field containing  $\mathbb{Q}_p$ , let  $|\cdot|$  be a non-Archimedean valuation on  $K$  which extends  $|\cdot|_p$ , and assume that  $K$  is complete with respect to this valuation. For any  $x \in K$ , show that  $\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$  converges if and only if  $|x| < p^{-\frac{1}{p-1}}$ .
- (c) For  $p \neq 2$ , show that  $\exp_p$  defines a continuous group isomorphism

$$\exp_p : \{x \in \mathbb{Q}_p : |x|_p < 1\} \rightarrow \{x \in \mathbb{Q}_p : |x-1|_p < 1\}$$

where the group law on the left hand side is addition, whilst on the right hand side it is multiplication.