

Elliptic Curves MT25: Solutions to Sheet 2

(1) (a). Let $x, y \in K$ be such that $|x| \neq |y|$, without loss of generality, say that $|x| < |y|$. Since K is non-Archimedean, we know that $|x \pm y| \leq \max(|x|, |y|) = |y|$, and so it is sufficient to show that $|x \pm y| \not< |y|$. Imagine $|x \pm y| < |y|$; then $|y| = |(x \pm y) - x| \leq \max(|x \pm y|, |x|) < |y|$, a contradiction, as required. [Note that an immediate consequence is the implication: $|u \pm v| < |u| \Rightarrow |u| = |v|$].

(b). Let $x_1, \dots, x_n \in K$ be such that $|x_\ell| > |x_i|$ for all $i \neq \ell$. Let $x = x_1 + \dots + x_{\ell-1} + x_{\ell+1} + \dots + x_n$ and let $y = x_\ell$. Then $|x| \leq \max(|x_i| : 1 \leq i \leq n, i \neq \ell) < |y|$ and so: $|x_1 + \dots + x_n| = |x + y| = |y| = |x_\ell|$, by part (a).

(c). Since $K, |\cdot|$ satisfies the triangle inequality $|x + y| \leq |x| + |y|$, we can apply the standard trick from first year Analysis: $|x| \leq |(x - y) + y| \leq |x - y| + |y|$ to give: $|x| - |y| \leq |x - y|$; similarly $|y| - |x| \leq |x - y|$, and so: $||x| - |y|| \leq |x - y|$. If $s_n \rightarrow s$ in $K, |\cdot|$ then $|s_n - s| \rightarrow 0$ in $\mathbb{R}$, and so $||s_n| - |s|| \leq |s_n - s| \rightarrow 0$, giving $|s_n| \rightarrow |s|$ in $\mathbb{R}, |\cdot|_\infty$, as required.

Suppose $s \neq 0$; then $|s| > 0$ and taking $\epsilon = |s|$, there exists N such that $|s_n - s| < |s|$ for all $n > N$, so that $|s_n| = |s|$ for all $n > N$ (since if $|s_n| \neq |s|$ then (a) would give $|s_n - s| = \max(|s_n|, |s|) \geq |s|$, a contradiction).

(2) (a). $3/50 = 5^{-2} \cdot 3/2$ (where 5 has no common factor with either the numerator and denominator of $3/2$) and so $|3/50|_5 = 5^2$. Similarly, $3/50 = 3^1 \cdot 1/50$ and so $|3/50|_3 = 3^{-1}$. Similarly, $3/50 = 7^0 \cdot 3/50$, and so $|3/50|_7 = 7^0 = 1$.

$$d_5(2/3, 1/5) = |2/3 - 1/5|_5 = |7/15|_5 = 5, \quad d_7(2/3, 1/5) = |7/15|_7 = 7^{-1}, \\ d_{11}(2/3, 1/5) = |7/15|_{11} = 1.$$

(b). $|3/7|_3 = 3^{-1}$, $|3/7|_7 = 7$. For all other primes p , $\gcd(p, 3) = \gcd(p, 7) = 1$ and so $|3/7|_p = 1$. Note also that $|3/7|_\infty = 3/7$. The given product $\prod |3/7|_i$ has all factors equal to 1 apart from the factors: $|3/7|_3 = 3^{-1}$, $|3/7|_7 = 7$ and $|3/7|_\infty = 3/7$, whose product is 1. Hence the given product $\prod |3/7|_i$ is 1. For any $x \in \mathbb{Q}$, write $x = \pm n/d$, where n and d are integers with $\gcd(n, d) = 1$, and write n, d in terms of their primes factorisations: $n = p_1^{s_1} \dots p_k^{s_k}$ and $d = q_1^{t_1} \dots q_\ell^{t_\ell}$, where $p_1, \dots, p_k, q_1, \dots, q_\ell$ are distinct primes. For any prime p , if $p = p_i$ for some i , then $|x|_p = p_i^{-s_i}$. If $p = q_j$ for some j , then $|x|_p = q_j^{t_j}$. If $p = \infty$, then $|x|_p = n/d = (p_1^{s_1} \dots p_k^{s_k}) / (q_1^{t_1} \dots q_\ell^{t_\ell})$. For all other primes p , we have $|x|_p = 1$. It follows that the product $\prod |x|_i$ is equal to $(p_1^{-s_1} \dots p_k^{-s_k}) \cdot q_1^{t_1} \dots q_\ell^{t_\ell} \cdot (p_1^{s_1} \dots p_k^{s_k}) / (q_1^{t_1} \dots q_\ell^{t_\ell})$, which is again equal to 1.

- (3) (a). $|1/5^n|_5 = 5^n \rightarrow \infty$; this means that $|1/5^n|_5$ does not converge, and so $1/5^n$ does not converge in $\mathbb{Q}_5$ (since, if $a_n \rightarrow \ell$ then $|a_n|_p \rightarrow |\ell|_p$).
- (b). *Method 1.* $|n|_5 \leq 5^{-1}$ for $n = 5, 10, 15, \dots$ and $|n|_5 = 1$ otherwise; this means that $|n|_5$ does not converge (since there is a subsequence $|n|_5$ for $5 \nmid n$ converging to 1 and a subsequence $|n|_5$ for $5|n$ and $5^2 \nmid n$ converging to $1/5$), and so n does not converge in $\mathbb{Q}_5$ (since, if $a_n \rightarrow \ell$ then $|a_n|_p \rightarrow |\ell|_p$).
- (b). *Method 2.* $n = \sum 1$, which does not converge, since $|1|_5 = 1$ which does not converge to 0 (using the result from lectures which says that $\sum c_i$ converges iff $|c_i|_p \rightarrow 0$).
- (c). $n! = 5^r \cdot k$, where $r > n/5 - 1$, since every fifth factor of $1 \cdot 2 \cdot \dots \cdot n$ (i.e. the factors $5, 10, 15, \dots$) contributes at least one new factor of 5. Hence $|n! - 0|_5 = |n!|_5 < 5^{-(n/5-1)} \rightarrow 0$, and so $n!$ converges to 0 in $\mathbb{Q}_5$.
- (d). $|(3 + 10^n) - 3|_5 = |10^n|_5 = |5^n \cdot 2^n|_5 = 5^{-n} \rightarrow 0$, and so $3 + 10^n$ converges to 3 in $\mathbb{Q}_5$.
- (e). $|10^n|_5 = |5^n \cdot 2^n|_5 = 5^{-n} \rightarrow 0$ in $\mathbb{Q}_5$ and so $\sum 10^n$ converges in $\mathbb{Q}_5$ (using the result from lectures which says that $\sum c_i$ converges iff $|c_i|_p \rightarrow 0$).
- (f). $|7^n|_5 = 1$ which does not converge to 0, and so $\sum 7^n$ does not converge in $\mathbb{Q}_5$ (using the same result from lectures as used in part (e)).

- (10) We use Hensel's lemma again. First note that any root of unity lies in $\mathbb{Z}_p^\times$, since $|x^m|_p = 1$ implies $|x|_p = 1$. Suppose α is a primitive m th root of unity. Then the reduction $\bar{\alpha}$ is a m th root of unity in the residue field $\mathbb{F}_p$. Let m' be the order of $\bar{\alpha}$ in $\mathbb{F}_p^\times$. Since $\mathbb{F}_p^\times$ is cyclic of order $p-1$, m' divides $p-1$. We also have $m'|m$, since $\bar{\alpha}^m = 1$.

Consider the polynomials $f_n(x) = x^n - 1$ for $n \geq 1$. It follows from Hensel's lemma that $x^m - 1$ has a unique root which is $= \bar{\alpha} \bmod p$. This root must be α . But we can also apply Hensel's lemma to the polynomial $x^{m'} - 1$. This also has a unique root α' which is $= \bar{\alpha} \bmod p$. Since $\alpha'^{m'} = 1$, we also have $\alpha'^m = 1$. We deduce from uniqueness that $\alpha' = \alpha$, so α is an m' th root of unity. This means that $m' = m$ (since α was a *primitive* m th root). We deduce that m must divide $p-1$.

Conversely, if m divides $p-1$ then we have a primitive m th root of unity $\bar{\alpha} \in \mathbb{F}_p$. Applying Hensel's lemma as above, we find a root of $x^m - 1$ in $\mathbb{Q}_p$ which gives the desired primitive m th root of unity.

<https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf>

Theorem 3.1 proves the precise description of roots of unity in $\mathbb{Q}_p$.

- (11) (a). The number of positive multiples of an integer $k > 0$ which are $\leq n$ is clearly $\lfloor \frac{n}{k} \rfloor$. To count the power of p dividing $n!$, since p is prime, it is enough to count the powers of p dividing $1, 2, 3, \dots, n$ and add these powers up. Now, the number of multiples of p among $1, 2, 3, \dots, n$ is $\lfloor \frac{n}{p} \rfloor$. Each multiple of p^2 among $1, 2, 3, \dots, n$ gives an additional power of p dividing into $n!$, giving $\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor$ so far. Continuing in this way we get that the total power of p is as in the given formula.
- (b). We have shown that $|n!|_p = p^{-M}$, where $M = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \dots \leq \frac{n}{p} + \frac{n}{p^2} + \dots = \frac{n}{p-1}$. Hence $|n!| \geq p^{-\frac{n}{p-1}}$, and so $|1/n!| \leq p^{\frac{n}{p-1}}$. Suppose

that $|x| < p^{-\frac{1}{p-1}}$ and let $\tau = |x|/p^{-\frac{1}{p-1}} < 1$. Then $|\frac{x^n}{n!}| = \tau^n p^{-\frac{n}{p-1}} |\frac{1}{n!}| \leq \tau^n p^{-\frac{n}{p-1}} p^{\frac{n}{p-1}} = \tau^n \rightarrow 0$. Hence, $\exp_p(x)$ converges (using the result from lectures which says that $\sum c_i$ converges iff $|c_i|_p \rightarrow 0$).

On the other hand, if $|x| \geq p^{-\frac{1}{p-1}}$, note that, for any $n = p^\ell$, the above $\frac{n}{p}, \frac{n}{p^2}, \dots, \frac{n}{p^\ell} = p^{\ell-1}, p^{\ell-2}, \dots, 1 \in \mathbb{Z}$ and so $M = p^{\ell-1} + p^{\ell-2} + \dots + 1 = \frac{p^\ell - 1}{p - 1}$; this means that the subsequence $|\frac{x^{p^\ell}}{(p^\ell)!}| \geq (p^{-\frac{1}{p-1}})^{p^\ell} p^{\frac{p^\ell - 1}{p-1}} = p^{-\frac{1}{p-1}}$, and so $|\frac{x^n}{n!}| \not\rightarrow 0$. Hence $\exp_p(x)$ does not converge when $|x| \geq p^{-\frac{1}{p-1}}$.

(c). The idea is to define the p -adic logarithm map using the Taylor series $\log_p(1+x) = x - x^2/2 + \dots$ and show that this gives an inverse to $\exp_p$. It also needs to be verified that $\exp_p$ is a group homomorphism. See Theorem 8.13 in <https://kconrad.math.uconn.edu/blurbs/gradnumthy/infseriespadic.pdf> for details, as well as the cautionary Example 8.14 which shows that care is needed when computing the composition of two functions defined by power series.