

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 $5 \mid n$ 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)).

- (4) (a). We are looking for x such that $|x^2 + 1|_5 \leq 5^{-4}$. Take $x_0 = a_0 = 2$ as the initial approximation for which $|a_0^2 + 1|_5 = |5|_5 = 5^{-1}$. Take $x_1 = a_0 + 5a_1 = 2 + 5a_1$. Then we want $(2 + 5a_1)^2 \equiv -1 \pmod{5^2}$, and so $20a_1 \equiv -5 \pmod{5^2}$, which is the same as $4a_1 \equiv -1 \pmod{5}$, and so $a_1 = 1$. This gives a better approximation: $x_1 = 2 + 1 \cdot 5 = 7$, which satisfies $|x_1^2 + 1|_5 = 5^{-2}$. Similarly, we then find $a_2 = 2$ and so $x_2 = 7 + 2 \cdot 5^2 = 57$. Then, finally, we similarly find $a_3 = 1$ and so $x_3 = 57 + 1 \cdot 5^3 = 182$, satisfying $|x^2 + 1|_5 = 5^{-4}$, as required.

(b). If there were an integer x such that $|x^2 - 7/8|_3 \leq 3^{-7}$, then we would have $x^2 \equiv 7/8 \pmod{3^7}$ and so $x^2 \equiv 7/8 \pmod{3}$. But $7/8 \equiv 2 \pmod{3}$, which is not a quadratic residue (since $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 1 \pmod{3}$); this means that no such x can exist.

(c). If there were an integer x such that $|x^2 - 5/4|_5 \leq 5^{-4}$ then consider the possibilities for $|x^2|_5$. If $|x^2|_5 > |5/4|_5$ then (using the result that $|a + b|_p = \max(|a|_p, |b|_p)$ when $|a|_p \neq |b|_p$) we have $|x^2 - 5/4|_5 = \max(|x^2|_5, |5/4|_5) = |x^2|_5 > |5/4|_5 = 5^{-1} > 5^{-4}$, contradicting $|x^2 - 5/4|_5 \leq 5^{-4}$. If $|x^2|_5 < |5/4|_5$ then (using the same result) we have $|x^2 - 5/4|_5 = \max(|x^2|_5, |5/4|_5) = |5/4|_5 = 5^{-1} > 5^{-4}$, again contradicting $|x^2 - 5/4|_5 \leq 5^{-4}$. It must then be that $|x^2|_5 = |5/4|_5 = 5^{-1}$, but this is again impossible since $|x^2|_5 = 5^r$ where r is an even integer. Hence no such x exists.

- (5) $200 \pmod{7}$ is 4, so write: $200 = 4 + 7 \cdot 28 =$ (similarly) $4 + 7 \cdot (0 + 7 \cdot 4) = 4 + 0 \cdot 7^1 + 4 \cdot 7^2 = 4, 04$.

For $3/14$, it is easier first to write: $3/14 = 7^{-1} \cdot 3/2$. First find the 7-adic expansion of $3/2$, with the idea that the 7-adic expansion of $3/14$ will then just be the 7-adic expansion of $3/2$ shifted one place to the left). Now, $|3/2|_7 = 1$ and so $3/2 = a_0 + a_1 7 + a_2 7^2 + \dots$. Using $2(a_0 + 7a_1 + 7^2 a_2 + \dots) = 3$, we

first find $2a_0 \equiv 3 \pmod{7}$ and so $a_0 = 5$. Continuing as usual, we find that $a_1 = 3, a_2 = 3, a_3 = 3 \dots$. At this point, we suspect that $3/2 = 5, \bar{3}$. We can prove this rigorously as follows. Let $\alpha = 5, \bar{3}$. Then $\alpha - 5 = 0, \bar{3}$, and so $7^{-1}(\alpha - 5) - 3 = 3, \bar{3} - 3 = 0, \bar{3} = \alpha - 5$. Hence, $\alpha - 5 - 21 = 7\alpha - 35$ and so $\alpha = 3/2$, proving that $3/2 = 5, \bar{3}$ in $\mathbb{Q}_7$. Finally, $3/14 = 7^{-1} \cdot 3/2 = 53, \bar{3}$.

Let $\beta = 2, \bar{34} \in \mathbb{Q}_5$. Then $\beta - 2 = 0, \bar{34}$ and so $5^{-2}(\beta - 2) = 34, \bar{34}$, giving: $5^{-2}(\beta - 2) - 3 \cdot 5^{-1} - 4 \cdot 5^0 = 0, \bar{34} = \beta - 2$, and so: $\beta = -67/24$.

- (6) First we can simplify the question by dividing out the square factor 4 from -28 . So it suffices to determine the primes p such that -7 has a square root in $\mathbb{Q}_p$. Write $f(x) = x^2 + 7$. If $p \neq 2, 7$ it follows from Hensel's lemma that $f(x)$ has a root in $\mathbb{Q}_p$ if and only if it has a root in $\mathbb{F}_p$. This holds if and only if the Legendre symbol $\left(\frac{-7}{p}\right) = +1$. We apply quadratic reciprocity and Euler's formula $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ to tell us that $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$. This is equal to $+1$ when $p = 1, 2$ or $4 \pmod{7}$.

It remains to deal with $p = 2, 7$. For $p = 2$, we can again apply Hensel's lemma with $x_0 = 1$. Since $|f(x_0)|_2 = 2^{-3}$ and $|f'(x_0)|_2 = 2^{-1}$, the conditions for Hensel's lemma are satisfied and there is a square root of -7 in $\mathbb{Q}_2$.

For $p = 7$, there are no solutions to $x^2 = -7$, since the 7-adic valuation of the right hand side is 7^{-1} , but the valuation of the left hand side lies in $7^{2\mathbb{Z}}$.

To conclude, -28 has a square root in $\mathbb{Q}_p$ if and only if $p = 1, 2$ or $4 \pmod{7}$.

- (7) In $\mathbb{R}$, we have for example the root $\sqrt{2}$. In $\mathbb{Q}_2$, note that $17 \equiv 1 \pmod{8}$, and so 17 is a square in $\mathbb{Q}_2$. In $\mathbb{Q}_{17}$, note that $|2|_{17} = 1$ and 2 is a quadratic residue mod 17, so that 2 is a square in $\mathbb{Q}_{17}$.

Finally, let $p \neq 2, 17$. Then each of $\left(\frac{2}{p}\right), \left(\frac{17}{p}\right), \left(\frac{34}{p}\right)$ is 1 or -1 . They cannot all be -1 since $\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right)$ [and $-1 \neq (-1)(-1)$], so at least one of them must be 1. Wlog, say that $\left(\frac{2}{p}\right) = 1$. Then $|2|_p = 1$ and 2 is a quadratic residue mod p , so that 2 must be a square in $\mathbb{Q}_p$.

- (8) Suppose there were an $x \in \mathbb{Q}_3$ such that $x^3 = 4$ in $\mathbb{Q}_3$. Then $|x|_3^3 = |4|_3 = 1$ and so $|x|_3 = 1$, which means that x can be written $x = a_0 + a_1a_2 \dots$. Reducing x modulo 9 would then give the integer $a_0 + 3a_1$ whose cube is 4 modulo 9. But $0, \dots, 8$ square to give: $0, 1, 8, 0, 1, 8, 0, 1, 8$, respectively, so that $x^3 = 4$ is an impossible congruence mod 9. Hence 4 is not a cube in $\mathbb{Q}_3$.

Let $f(x) = x^3 - 28$ and let $x_0 = 1$. Then $|f(x_0)|_3 = |-27|_3 = 3^{-3}$, whereas $|f'(x_0)|_3 = |3|_3 = 3^{-1}$. Hence $|f(x_0)|_3 < |f'(x_0)|_3^2$, and so by Hensel's Lemma there must be a root of $f(x)$ in $\mathbb{Q}_3$; that is 28 must be a cube in $\mathbb{Q}_3$.

Let $f(x) = x^3 - 13$ and let $x_0 = -1$. Then $|f(x_0)|_7 = |-14|_7 = 7^{-1}$, whereas $|f'(x_0)|_7 = |3|_7 = 1$. Hence $|f(x_0)|_7 < |f'(x_0)|_7^2$, and so by Hensel's Lemma again there must be a root of $f(x)$ in $\mathbb{Q}_7$; that is 13 must be a cube in $\mathbb{Q}_7$.

- (9) Since $p \equiv 2 \pmod{3}$, we have $\gcd(3, p-1) = 1$, and so there exist $\lambda, \mu \in \mathbb{Z}$ such that $3\lambda + (p-1)\mu = 1$. For any $x, y \in \mathbb{F}_p^*$, we have $x^{p-1} = y^{p-1} = 1$ [by Fermat's Little Theorem], and so:

$$\begin{aligned} x^3 = y^3 &\Rightarrow (x^3)^\lambda \cdot 1^\mu = (y^3)^\lambda \cdot 1^\mu \Rightarrow (x^3)^\lambda \cdot (x^{p-1})^\mu = (y^3)^\lambda \cdot (y^{p-1})^\mu \\ &\Rightarrow x^{3\lambda+(p-1)\mu} = y^{3\lambda+(p-1)\mu} \Rightarrow x = y. \end{aligned}$$

Thus the map $x \mapsto x^3$ is injective on $\mathbb{F}_p^*$ and so is a bijection.

Now, let $a \in \mathbb{Z}$ be such that $p \nmid a$. From above, there must exist $x_0 \in \mathbb{Z}$ such that $x_0^3 \equiv a \pmod{p}$; clearly $p \nmid x_0$. Let $f(x) = x^3 - a$. Then $|f(x_0)|_p = |x_0^3 - a|_p < 1$, since $x_0^3 - a \equiv 0 \pmod{p}$. Also, $|f'(x_0)|_p = |3x_0^2|_p = 1$, since $3 \nmid p$ and $p \nmid x_0$. Hence $|f(x_0)|_p < |f'(x_0)|_p^2$, and so by Hensel's Lemma, there exists $x \in \mathbb{Z}_p$ with $f(x) = 0$, that is, $x^3 = a$, as required.

- (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 $m' \mid m$, 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 $= \bar{\alpha} \pmod{p}$. 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 $= \bar{\alpha} \pmod{p}$. 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 $\left| \frac{x^{p^\ell}}{(p^\ell)!} \right| \geq (p^{-\frac{1}{p-1}})^{p^\ell} p^{\frac{p^\ell-1}{p-1}} = p^{\frac{-1}{p-1}}$, and so $\left| \frac{x^n}{n!} \right| \not\rightarrow 0$. 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 $\log_p(1+x) = x - x^2/2 + \cdots$ 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.