Problem 1

(a)

Calculate $|20|_p, |-20/3|_p$, and $|e^p|_p$ for all primes p.

Note that if $(a,p)=1$ then $|a|_p = 1$

$$|20|_p = |2^2 \cdot 5|_p = |2|_p^2 \cdot |5|_p = \begin{cases} 1/4 & p=2, \\ 1 & p=3, \\ 1/5 & p=5, \\ 1 & p>5, \end{cases}$$

and

$$|-20/3|_p = |-1|_p \cdot |2|_p^2 \cdot |5|_p \cdot |3|_p^{-1} = |20/3|_p = \begin{cases} 1/4 & p=2, \\ 3 & p=3, \\ 1/5 & p=5, \\ 1 & p>5. \end{cases}$$

$|e^p|_p = 1$

Proof. Note that $e^p = \sum_{i=0}^{\infty} p^n/n!$. I will prove that the nth partial sum has p-adic norm 1. Since the partial sums converge to e^p this will imply that $|e^p|_p = 1$.

Here is the idea: I will rewrite $S_n = r/s$ where r and s are integers, then I will show that p does not divide r or s and thus $|S_n|_p = 1$. Notice that $p^n/n!$ upon canceling out p's will continue to have a power of p in the numerator and no factors of p in the denominator. Call the reduced form of $p^n/n!$, p^{k_n}/r_n. Then we have

$$\begin{aligned} S_m &= 1 + p + \frac{p^{k_2}}{r_2} + \cdots + \frac{p^{k_m}}{r_m}, \\ &= \frac{\sum_{i=0}^{m} \left[p^{k_i} \prod_{0=j\neq i}^{m} r_j \right]}{\prod_{i=0}^{m} r_i}. \end{aligned}$$

Each r_i is not divisible by p, thus the denominator is not. If you notice, every term in the summation of the numerator has a power of p (since $k_i \geq 1$ for $i > 1$) except for the first term which is a product of all the r_i. Therefore p does not divide the numerator. $\square$

(b)

Compute the first 4 digits in the base 3 expansion of $e^6 \in \mathbb{Q}_3$.

$$\begin{aligned} e^6 &= \sum_{i=0}^{\infty} \frac{6^i}{i!}, \\ &= 1 + 2\cdot 3 + 2\cdot 3^2 + 2^2 \cdot 3^2 + 2\cdot 3^3 + \frac{2^2}{5} \cdot 3^4 + \cdots . \end{aligned}$$

Since the factors of 3 in $n!$ do not grow as fast as the factors of 3 in 3^n there will not be another term with $3^3, 3^2$, or 3. So

$$\begin{aligned}
&= 1 + 2\cdot 3 + 2\cdot 3^2 + 2^2\cdot 3^2 + 2\cdot 3^3 + \frac{2^2}{5}\cdot 3^4 + \dots,\\
&= 1 + 2\cdot 3 + 6\cdot 3^2 + 2\cdot 3^3 + \dots,\\
&= 1 + 2\cdot 3 + 0\cdot 3^2 + (2+2)\cdot 3^3 + \dots,\\
&= 1 + 2\cdot 3 + 0\cdot 3^2 + 1\cdot 3^3 + \dots.
\end{aligned}$$

Thus the first four coefficients are 1, 2, 0, 1.

Problem 2

(a)

Let $f(x) = x^4 2x^3 + 5x^2 + 3x + 6$. Compute $f(1)$ and $f'(1)$ and explain why there is a root of f in $\mathbb{Q}_{17}$.

Proof. $f(1) = 17$ so $|f(1)|_{17} = 1/17$. $f'(1) = 23$ so $|f'(1)|_{17} = 1$ since $(23, 17) = 1$. Checking the hypothesis of Hensel's lemma with $n = 1$ we see they are satisfied:

$$|f(1)|_{17} = 1/17 \le (1/17)^1 \qquad \text{and} \qquad |f'(17)| = 1 > (1/17)^{1/2}.$$

Hensel's lemma ensures us a root of f in $\mathbb{Z}_{17} \subseteq \mathbb{Q}_{17}$. □

(b)

Let b be an integer. If $f(x) \in \mathbb{Z}[x]$ has p divide $f(b)$ but p does not divide $f'(b)$, explain why $f(x)$ has a root α in the p-adic integers $\mathbb{Z}_p$, such that $\alpha \equiv b \pmod{p}$.

Proof. Since p divides $f(b)$, $\nu_p f(b) \ge 1$. Since p does not divide $f'(b)$, we have $\nu_p f'(b) = 0$. Therefore

$$|f(b)|_p \le \frac{1}{p} \qquad \text{and} \qquad |f'(b)|_p = 1 > \left(\frac{1}{p}\right)^{1/2}.$$

Hensel's lemma applies to give us a $\xi \in \mathbb{Z}_p$ such that $f(\xi) = 0$ and $d_p(\xi, b) < (1/p)^{1-0} = 1/p$. Since $d_p(\xi, b) = (1/p)^{\nu(\xi - b)}$, we have $\nu_p(\xi - b) > 1$. Therefore $p | \xi - b$ and hence $\xi \equiv b \pmod{p}$. □

Problem 3

Find $|\mathbb{Q}_p[\alpha] : \mathbb{Q}_p|$ for $p = 2, 3, 5, 7, 11$ and for $\alpha = \sqrt{2}, \sqrt[3]{5}$ and i where i is a root of $x^2 + 1$.

Here is a summary of the results

	2	3	5	7	11
$\sqrt{2}$	2	2	2	1	2
$\sqrt[3]{5}$	1	3	3	3	1
i	2	2	1	2	2

Case: $\alpha = \sqrt{2}$

Since $x^2 - 2$ is satisfied by α, if $\alpha \in \mathbb{Q}_p$ then $|\mathbb{Q}_p[\alpha] : \mathbb{Q}_p| = 1$ otherwise $|\mathbb{Q}_p[\alpha] : \mathbb{Q}_p| = 2$. Suppose $\alpha \in \mathbb{Q}_p$, then $\alpha = p^k u$ where $k \in \mathbb{Z}$ and u is a unit of $\mathbb{Z}_p$. We have that $\alpha^2 = 2$ so $p^{2k}u^2 = 2$.

When $p = 2$, $\nu_p p^{2k}u^2 = 2k = \nu_p 2 = 1$. There is no integer k that satisfies that equation. Therefore $\alpha \notin \mathbb{Q}_2$.

When $p \neq 2$, $\nu_p p^{2k}u^2 = 2k = \nu_p 2 = 0$. Therefore $k = 0$ and hence we may assume α is a unit in $\mathbb{Z}_p$. It's an easy check that $x^2 - 2$ has no root in $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$, or $\mathbb{Z}/11\mathbb{Z}$ – that contradicts $\alpha \in \mathbb{Z}_p$. So $\alpha \notin \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_{11}$.

Using Hensel's lemma with $x_0 = 4$ we can conclude that $x^2 - 2$ actually has a root in $\mathbb{Q}_7$: $x_0^2 - 2 = 14 \equiv 0 \pmod 7$ and $2x_0 = 8 \equiv 1 \pmod 7$ so there is a root and thus $\mathbb{Q}_7[\alpha] = \mathbb{Q}_7$.

Case: $\alpha = \sqrt[3]{5}$

Since $f(x) = x^3 - 5$ is satisfied by α, if $\alpha \in \mathbb{Q}_p$ then $|\mathbb{Q}_p[\alpha] : \mathbb{Q}_p| = 1$ otherwise it must be that $|\mathbb{Q}_p[\alpha] : \mathbb{Q}_p| = 3$. Suppose $\alpha \in \mathbb{Q}_p$, then $\alpha = p^k u$ where $k \in \mathbb{Z}$ and u is a unit of $\mathbb{Z}_p$. We have that $\alpha^3 = 5$ so $p^{3k}u^3 = 5$.

When $p = 5$, $3k = \nu_5 \alpha^3 = \nu_5 5 = 1$. Since there is no integer k that satisfies that equation we have a contradiction. Therefore $\alpha \notin \mathbb{Q}_5$.

When $p \neq 5$. We may assume α is an unit in $\mathbb{Z}_p$ because $k = 0$. One may check that there is no root of f modulo $3^2, 7$, or 11. Therefore $\alpha \notin \mathbb{Q}_3, \mathbb{Q}_7, \mathbb{Q}_{11}$.

Like before we use Hensel's lemma to conclude there is a root of f in $\mathbb{Q}_2$. Use $x_0 = 1$: $f(x_0) \equiv 0 \pmod 2$ and $f'(x_0) = 3 \equiv 1 \pmod 2$. Therefore there exists a root of f in $\mathbb{Q}_2$.

Case: $\alpha = i$

Let $f(x) = x^2 + 1$. Suppose $\alpha \in \mathbb{Q}_p$ and write $\alpha = p^k u$ as usual. Note $2k = \nu_p p^{2k}u^2 = \nu_p - 1 = 0$ so $k = 0$ and hence $\alpha \in \mathbb{Z}_p$ and a unit.

Some quick computation shows $x^2 + 1$ has no roots modulo $2^2, 3, 7$, or 11.

However $i \in \mathbb{Q}_5$. This is because $5 \equiv 1 \pmod 4$ (a sufficient condition as we showed in class).

Problem 4

Let i be a root of x^2+1. Find the base 13 expansions of i in $\mathbb{Q}_{13}$. up to the first 4 digits by using Newton's method.

We need to find a number x such that $d_{13}(x,i) < (1/13)^4$ to guarantee that x will have the same expansion in the first 4 digits.

Step 1

Let $x_0 = 5$. Note that x_0 satisfies the conditions of Hensel's lemma

$$|f(5)|_{13} = |26|_{13} = 1/13 \qquad \text{and} \qquad |f'(5)|_{13} = |10|_{13} = 1 > (1/13)^{1/2}$$

therefore $d_{13}(i, x_0) < (1/13)$.

Step 2

Let $x_1 = x_0 - f(x_0)/f'(x_0) = 12/5$. Note that x_1 satisfies the conditions of Hensel's lemma

$$|f(12/5)|_{13} = \left|\frac{13^2}{5^2}\right|_{13} = (1/13)^2 \qquad \text{and} \qquad |f'(12/5)|_{13} = \left|\frac{2^3 \cdot 3}{5}\right|_{13} = 1$$

therefore $d_{13}(i, x_1) < (1/13)^2$.

Step 3

Let $x_2 = x_1 - f(x_1)/f'(x_1) = 119/120$. Note that x_2 satisfies the conditions of Hensel's lemma

$$|f(x_2)|_{13} = \left|\frac{13^4}{2^6 \cdot 3^2 \cdot 5^2}\right|_{13} = (1/13)^4 \qquad \text{and} \qquad |f'(x_2)|_{13} = \left|\frac{7 \cdot 17}{2^2 \cdot 3 \cdot 5}\right|_{13} = 1$$

therefore $d_{13}(i, x_2) < (1/13)^4$.

Expansion

I will write down the expansion of 119/120. It should be easy to check that $119/120 \cdot 120 = 119 = 2 + 9 \cdot 13$.

$$119/120 = 5 + 5 \cdot 13 + 1 \cdot 13^2 + 0 \cdot 13^3 + 4 \cdot 13^4 + \cdots$$

So the first four digits are $(5, 5, 1, 0)$

Problem 5

(a)

Let $\mathbb{Q}_p \subseteq K$ be a finite unramified extension of degree n. Explain why every element in K can be written uniquely in the form for all i where $D = \{x \in K : x^{p^n} = x\}$.

Proof. Since K is an unramified extension we have $|K^\times| = \{|p|^m\}$. Furthermore since $n = ef$, the residue degree is n. Thus $|k : \mathbb{F}_p| = n$ where k is the residue field of K. A degree n extension of a finite field is simply the splitting field of the polynomial $x^{p^n} - x$, so $k = D$.

By the representation theorem, every element in K can be written uniquely as $\sum_{i \geq m}^{\infty} a_i p^i$ where $a_i \in D$. □

(b)

Let $\mathbb{Q}_p \subseteq K$ be an extension of degree n with ramification index e and residue degree f. Write $|K^\times| = \{|\pi|^m : m \in \mathbb{Z}\}$ with $0 < |\pi| < 1$. Show every element in K can be written uniquely in the form $\sum_{i \geq m}^{\infty} \sum_{j=0}^{e-1} a_{ij} p^i \pi^j$ where $a_{ij} \in D$ for all i, j.

Proof. Let $R = B_{\leq}^{K}$. We can write any element in K as $\sum_{i \geq m} b_i p^i$ where b_i come from the set of representatives of the cosets R/pR. We have that $pR = \pi^e R$ (by definition) so $R/pR = R/\pi^e R$. By the canonical representation of elements in K, each $b_i = \sum_{j \geq m} a_{ij} \pi^j$ where a_{ij} are taken as representatives from the residue field k. However each b_i is only unique modulo $\pi^e R$ so we may write $b_i = \sum_{j=0}^{e-1} a_{ij} \pi^j$. As in (a) we can say $a_{ij} \in D$ (which is now a degree f extension). Substituting into the original representation we get that every element in K can be written as $\sum_{i \geq m}^{\infty} (\sum_{j=0}^{e-1} a_{ij} p^i) \pi^j$ □

Problem 6

(a)

Show that any element $\alpha \in \overline{\mathbb{Q}}_p$ is a root of a polynomial in $\mathbb{Z}_p[x]$ such that at least one of the coefficients is a unit of $\mathbb{Z}_p$.

Proof. α is algebraic over $\mathbb{Q}_p$ so there exists $f \in \mathbb{Q}_p[x]$ with $f(\alpha) = 0$. Suppose $f(x) = a_n x^n + \cdots + a_0$. Let a_i be the element of the set $\{a_0, \ldots, a_n\}$ of maximal p-adic norm. Then let

$$g(x) = \frac{f(x)}{a_i} = \frac{a_n}{a_i} x^n + \cdots \frac{a_i}{a_i} x^i + \cdots + \frac{a_0}{a_i}$$

Clearly the ith coefficient is a unit, namely 1. Every other coefficient has $|a_j / a_i| \leq 1$ since $|a_j| \leq |a_i|$. So all the coefficients are in $\mathbb{Z}_p$. □

(b)

$1/p$ is not integral over $\mathbb{Z}_p$.

Proof. Suppose for contradiction that $1/p$ was integral over $\mathbb{Z}_p$. Let $f(x) \in \mathbb{Z}_p[x]$ be the monic polynomial that $1/p$ satisfies. We could factor $f(x) = (x-1/p)g(x)$ where $g(x) \in \mathbb{Q}_p[x]$. Clearly g must be monic. Also we may assume that $g(0) \neq 0$ for it were we could just factor out x^j and the remaining polynomial would work instead. So we can assume the constant term of g is nonzero. Let $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then

$$(x-1/p)g(x) = x^{n+1} + (c_{n-1} - 1/p)x^n + \cdots + (c_0 - c_1/p)x + (-c_0/p) \in \mathbb{Z}_p[x]$$

Therefore $-c_0/p \in \mathbb{Z}_p$ so $p|c_0$ which implies $c_0 \in \mathbb{Z}_p$. Since $c_0 \in \mathbb{Z}_p$, $c_0 - c_1/p \in \mathbb{Z}_p$ implies that $c_1 \in \mathbb{Z}_p$. Continuing this way we can conclude that every coefficient is in $\mathbb{Z}_p$. □

(c)

Let X be the integral closure of $\mathbb{Z}_p$ in $\overline{\mathbb{Q}}_p$. Show that X is contained in the closed unit ball of $\overline{\mathbb{Q}}_p$, B.

Proof. Let $\alpha \in X$. Suppose α satisfies $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}_p[x]$. For a contradiction suppose that $|\alpha| > 1$. Then we have

$$\begin{aligned} |\alpha^n| = |\alpha|^n &= |-1| \cdot |a_{n-1}\alpha^{n-1} + \cdots + a_0|, \\ &\leq \max\{|a_{n-1}| \cdot |\alpha|^{n-1}, \ldots, |a_0|\}, \\ &\leq \max\{|\alpha|^{n-1}, \ldots, 1\} \qquad \text{(since } |a_i| \leq 1\text{)}, \\ &= |\alpha|^{n-1} \end{aligned}$$

So $|\alpha|^n \leq |\alpha|^{n-1}$, a contradiction. □

(d)

Show that $X = B$

Proof. Let $\alpha_1 \in B$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_0 \in \mathbb{Q}_p[x]$ be its minimal polynomial. Let $\alpha_1, \cdots, \alpha_n \in \mathbb{Q}_p$ be all the roots of f.

Since Galois automorphisms are isotropies (with respect to the p-adic norm) and they act transitively on the roots of f , we have $|\alpha_1| = \cdots = |\alpha_n| \leq 1$.

Every coefficient is a sum and product of a number of roots. Hence

$$|c_i| = \left| \sum_{i\in I} \prod_{j \in J_i} \alpha_j \right| \leq \max_{i \in I} \left\{ \left| \prod_{j\in J_i} \alpha_j \right| \right\} = \max_{i\in I} \left\{ \prod_{j \in J_i} |\alpha_j| \right\} = 1$$

For some index sets I and J_i. Therefore α_1 is integral over $\mathbb{Z}_p$ and thus is inside of X. □

Problem 7

(a)

Show that $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ *is an irreducible polynomial over* $\mathbb{Q}_5$.

Proof. Suppose $z \in \mathbb{Q}_5$ is a root of Φ_5. Then $z = 5^k u$ for $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Note that $z^5 = 1$, so $5^{5k}u^5 = 1$ which taking the valuation of both sides implies $5k = 0$. Therefore $z \in \mathbb{Z}_p^\times$. Now simply check that Φ_5 has no roots modulo 5^2. □

Find a p *such that* Φ_5 *factors completely into linear factors over* $\mathbb{Q}_p$. $p = 11$.

Proof. Note $\Phi_5(3) \equiv 0 \pmod{11}$ and $\Phi_5'(3) = 142 \equiv 10 \pmod{11}$. By Hensel's lemma there is a root of $\Phi_5 \in \mathbb{Q}_{11}$. Since the roots of Φ_5 are the primitive roots of unity, the fact that $\mathbb{Q}_{11}$ contains one means it must contain them all (since they all generate the group of roots of unity). □

(b)

Find the minimum distance between distinct roots of Φ_5 *in* $\overline{\mathbb{Q}}_5$. The minimal distance is 1.

Proof. Let ξ_5 be a primitive 5th root of unity. The roots of Φ_5 are $\xi_5, \xi_5^2, \xi_5^3, \xi_5^4$. As we mentioned above $|\xi_5^i| = |\xi_5| = 1$. Note for $i < j$, $|\xi_5^i - \xi_5^j| = |\xi_5|^i \cdot |1 - \xi_5^{j-i}| = |1 - \xi_5^{j-i}|$. Hence

$$r(\xi_5) = \min_{1 \le i \le 3} |1 - \xi_5^i|.$$

Since $d(\xi_5^i, 0) = 1$ and $d(1, 0) = 1$ the ultra-metric property gives us that $d(\xi_5^i, 1) = 1$. Thus $r(\xi_5) = 1$. □

(c)

Find an $\epsilon > 0$ *such that if* f *is a monic quartic in* $\mathbb{Z}_5[x]$ *with* $d(f, \Phi_5) < \epsilon$ *then at least one root* α *of* f *has* $\mathbb{Q}_5[\alpha] = \mathbb{Q}_5[\xi_5]$.

Proof. Choose $\epsilon = 1$. Let $g \in \mathbb{Z}_5[x]$ a monic degree 4 polynomial with $d(f, \Phi_5) < \epsilon$. Write $g(x) \prod(x - b_i)$ where $b_i \in \overline{\mathbb{Q}}_p$. Then we have

$$g(\xi_5) = \prod_{i=1}^{4} (\xi_5 - b_i) = g(\xi_5) - \Phi(\xi_5).$$

Let $M = \max_i |\xi_5|^i$. From part (b) we saw that $|\xi_5|^i = 1$ so $M = 1$. Then we have

$$\prod_{i=1}^{4} |\xi_5 - b_i| = |g(\xi_5) - \Phi_5(\xi_5)| \le M \cdot ||g - \Phi_5|| = ||g - \Phi_5||.$$

Let $|\xi_5 - b_j|$ be the smallest of all the $|\xi_5 - b_i|$. Then

$$|\xi_5 - b_j|^4 \leq \prod_i |\xi_5 - b_i| \leq ||g - \Phi_5|| < 1.$$

By Krasner's lemma $\mathbb{Q}_p(b_j) \supseteq \mathbb{Q}_p(\xi_5)$. But since $|\mathbb{Q}_p(b_j) : \mathbb{Q}_p| = 4 = |\mathbb{Q}_p(\xi_5) : \mathbb{Q}_p|$ we have $\mathbb{Q}_p(b_j) = \mathbb{Q}_p(\xi_5)$. $\square$

Problem 8

Let $f_i \in \mathbb{Z}_p[x, y]$ for $i = 1, 2$ and $f(x, y) = (f_1(x, y), f_2(x, y))$. Note f will give us a function $f : \mathbb{Q}_p^2 \to \mathbb{Q}_p^2$.

(a)

Show that we can write

$$f(x + h_1, y + h_2) = f(x, y) + Df(x, y) \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} + \begin{pmatrix} h_1^2 E + h_2^2 F + h_1 h_2 G \\ h_1^2 H + h_2^2 I + h_1 h_2 J \end{pmatrix}$$

where

$$Df(x, y) = \begin{pmatrix} \frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y} \\ \frac{\partial f_2}{\partial x} & \frac{\partial f_2}{\partial y} \end{pmatrix}$$

and $E, F, G, H, I, J \in \mathbb{Z}_p[x, y, h_1, h_2]$.

Proof. I will show equality in the first component, the equality in the other component will be a symmetric argument. Let

$$f_1(x, y) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j \qquad \text{and} \qquad f_2(x, y) = \sum_{i=0}^{n} \sum_{j=0}^{m} b_{ij} x^i y^j.$$

Then we have $f_1(x + h_1, y + h_2)$ equal to

$$\begin{aligned}
&= \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j, \\
&= \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} [x^i + i h_1 x^{i-1} + h_1^2(\cdots)][y^j + j h_2 y^{j-1} + h_2^2(\cdots)], \\
&= \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} [x^i y^j + j h_2 x^i y^{j-1} + i h_1 x^{i-1} y^j + h_1 h_2(\cdots) + h_1^2(\cdots) + h_2^2(\cdots)], \\
&= f_1(x, y) + h_1 \sum_{i \neq 0, j} i a_{ij} x^{i-1} y^j + h_2 \sum_{i, j \neq 0} j a_{ij} x^i y^{j-1} + h_1^2 E + h_2^2 F + h_1 h_2 G, \\
&= f_1(x, y) + h_1 \frac{\partial f_1}{\partial x}(x, y) + h_2 \frac{\partial f_1}{\partial y}(x, y) + h_1^2 E + h_2^2 F + h_1 h_2 G.
\end{aligned}$$

Which if you check is the first component of left side of the equation we're trying to prove. (whew - that was a lot of typing.) $\square$

(b)

If we use the L^infty-norm on $\mathbb{Q}_p^2$ show that for any 2×2 matrix A and vector x we have $||Ax|| \leq ||A|| \cdot ||x||$ where $||A|| = \max_{i,j} |a_{ij}|_p$.

Proof. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \qquad x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

then

$$\begin{aligned}
||A|| \cdot ||x|| &= \max\{|a|, |b|, |c|, |d|\} \cdot \max\{|x_1|, |x_2|\}, \\
&= \max\{|ax_1|, |ax_2|, |bx_1|, |bx_2|, |cx_1|, |cx_2|, |dx_1|, |dx_2|\}, \\
&\geq \max\{|ax_1|, |bx_2|, |cx_1|, |dx_2|\}, \\
&= \max\{\max\{|ax_1|, |bx_2|\}, \max\{|cx_1|, |dx_2|\}\}, \\
&\geq \max\{|ax_1 + bx_2|, |cx_1 + dx_2|\}, \\
&= ||Ax||
\end{aligned}$$

where $|\cdot|$ is the p-adic norm. □

(c)

For a matrix $A \in GL_2(\mathbb{Q}_p)$ what is the relationship between $||A||$ and $||A^{-1}||$?
$||A|| = |\det A| \cdot ||A^{-1}||$.

Proof. Let A be as in part (b). Then

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Therefore

$$\begin{aligned}
||A^{-1}|| &= \max\left\{\left|\frac{a}{\det A}\right|, \left|\frac{-b}{\det A}\right|, \left|\frac{-c}{\det A}\right|, \left|\frac{d}{\det A}\right|\right\}, \\
&= \frac{1}{|\det A|} \cdot \max\{|a|, |b|, |c|, |d|\}, \\
&= \frac{||A||}{|\det A|}.
\end{aligned}$$

So $||A|| = |\det A| \cdot ||A^{-1}||$. □

(d)

Let $N(v) = v - (Df(v))^{-1} f(v)$ be the Newton map. What conditions do you need to ensure that $N(v)$ is a well-defined in $\mathbb{Q}_p^2$?

We need $\det Df(v) \neq 0$ so that $(Df(v))^{-1}$ exists. Otherwise it's easy to see that the vector you get out of $N(v)$ is actually in $\mathbb{Q}_p^2$.

What conditions do you need to ensure that $N(v)$ is well-defined in $\mathbb{Z}_p^2$?

We require that $||Df(v)|| \leq |\det Df(v)|$ (and of course that $\det Df(v) \neq 0$). If this is the case then

$$\begin{aligned}
1 &\geq \frac{||Df(v)||}{|\det Df(v)|} \\
&\geq \frac{||Df(v)||}{|\det Df(v)|} \cdot ||f(v)|| \qquad \text{(since } ||f(v)|| \leq 1\text{)} \\
&= ||(Df(v))^{-1}|| \cdot ||f(v)|| \qquad \text{(using part c)} \\
&\geq ||(Df(v))^{-1} f(v)|| \qquad \text{(using part b).}
\end{aligned}$$

Therefore $(Df(v))^{-1}f(v) \in \mathbb{Z}_p$, and hence $N(v) \in \mathbb{Z}_p$.

What conditions do you need to ensure that $||f(N(v))|| < ||f(v)||$?

We require that $||Df(v)|| < |\det Df(v)|$. Let $h = N(v) - v$. Denote the first and second components of h as h_1 and h_2, respectively. Note that

$$\begin{aligned}
|h_1| &= \left| \frac{d}{\det Df(v)} f_1(v) - \frac{b}{\det Df(v)} f_2(v) \right| \\
&\leq \max\left\{ \left| \frac{d}{\det Df(v)} f_1(v) \right|, \left| \frac{b}{\det Df(v)} f_2(v) \right| \right\} \\
&\leq \frac{||Df(v)||}{|\det Df(v)|} \max\{|f_1(v)|, |f_2(v)|\} \\
&< \max\{|f_1(v)|, |f_2(v)|\} \\
&= ||f(v)||
\end{aligned}$$

And similarly $|h_2| < ||f(v)||$. Now we have

$$\begin{aligned}
||f(N(v))|| &= ||f(v+h)||, \\
&= \left|\left| f(v) - Df(v)(Df(v))^{-1}f(v) + \begin{pmatrix} h_1^2E + h_2^2F + h_1h_2G \\ h_1^2H + h_2^2I + h_1h_2J \end{pmatrix} \right|\right| \\
&= \left|\left| \begin{pmatrix} h_1^2E + h_2^2F + h_1h_2G \\ h_1^2H + h_2^2I + h_1h_2J \end{pmatrix} \right|\right| \\
&= ||h_1^2E + h_2^2F + h_1h_2G|| \qquad \text{(WLOG)} \\
&\leq \max\{|h_1|^2|E|, |h_2|^2|F|, |h_1||h_2||G|\} \\
&\leq \max\{|h_1|^2, |h_2|^2, |h_1||h_2|\} \qquad \text{(since } E, F, G \text{ have norm} \leq 1\text{)} \\
&\leq ||f(v)||^2 \\
&< ||f(v)|| \qquad \text{(since } ||f(v)|| \leq 1\text{)}
\end{aligned}$$

(e)

Prove a versions of Hensel's lemma for polynomial functions $f : \mathbb{Q}_p^2 \to \mathbb{Q}_p^2$

Lemma 1. *Let $v \in \mathbb{Z}_p^2$ be such that $||f(v)|| \equiv 0 \pmod{p^n}$. If $||Df(v)|| < |\det Df(v)| \neq 0$ then $w = N(v)$ has the following properties: $w \in \mathbb{Z}_p^2$, $||f(w)|| \equiv 0 \pmod{p^{n+1}}$, $w \equiv v \pmod{p^{n+1}}$, and $||Df(v)|| = ||Df(w)||$.*

Proof. We showed above that $w \in \mathbb{Z}_p^2$. Note that $w - v = -(Df(v))^{-1}f(v)$, so

$$\begin{aligned} ||w - v|| &= ||-(Df(v))^{-1}f(v)||, \\ &\leq \frac{||Df(v)||}{|\det Df(v)|}||f(v)||, \\ &\leq (1/p)\cdot(1/p)^n. \end{aligned}$$

So we see that $w \equiv v \pmod{p^{n+1}}$. Because $||f(w)|| < ||f(v)|| \leq (1/p)^n$ we have that $||f(w)|| \leq (1/p)^{n+1}$.

(unsure of how to prove $||Df(v)|| = ||Df(w)||$) □

Theorem. *With the conditions of the lemma, there exists a root of f in $\mathbb{Z}_p^2$.*

Proof. Same as proof of Hensel's lemma: Keep iterating the above lemma to get a sequence of points $v_1, v_2, \ldots$. From the conditions we see that the sequence is Cauchy and hence has a p-adic limit which must satisfy the polynomial. □

(f)

Find a prove a Hensel's lemma for a function $f \in \mathbb{Z}_p[x,y]$ where $f : \mathbb{Q}_p^2 \to \mathbb{Q}_p$.

Theorem. *If there exists $v \in \mathbb{Z}_p^2$ with $f(v) \equiv 0 \pmod{p^n}$ and*

$$\left|\frac{\partial f}{\partial x}(v) - \frac{\partial f}{\partial y}(v)\right| > 1$$

and $v_1 + v_2 \equiv 0 \pmod{p^n}$ then there exists a root in $\mathbb{Z}_p^2$ of f.

Proof. Define a function $g : \mathbb{Q}_p^2 \to \mathbb{Q}_p^2$ by

$$g\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} f(x,y) \\ x + y \end{pmatrix}.$$

We want to apply the Hensel's lemma from part (e) to this function so we must check the conditions:

$$Dg(v) = \begin{pmatrix} \frac{\partial f}{\partial x}(v) & \frac{\partial f}{\partial y}(v) \\ 1 & 1 \end{pmatrix}$$

So

$$|\det Dg(v)| = \left|\frac{\partial f}{\partial x}(v) - \frac{\partial f}{\partial y}(v)\right| > \max\{1, |\partial f/\partial x(v)|, |\partial f/\partial y(v)|\} = ||Dg(v)||.$$

Finally $||g(v)|| = \max\{|f(v)|, |v_1 + v_2|\} \leq (1/p)^n$. Apply the Hensel's lemma from (e) to get a root of g, which will be a root of f! □