p-ADIC NUMBERS LECTURE NOTES

VINCENT TRAN

Abstract. I will give an introduction to the p-adic numbers, starting with their construction and structure and covering some aspects of p-adic analysis (i.e., padic functions of a p-adic variable). I will discuss some applications, such as the Skolem-Mahler-Lech theorem about linear recurrence relations.

Contents

1. Lecture 1

Let $N \geq 1$ be an integer (later N will be assumed prime).

Observation 1.1. Any $x \in \mathbb{Z}_{\geq 0}$ has a unique N-adic expansion, i.e. we can write

$$x = x_j N^j + \cdots + x_1 N + x_0 0$$

where each $x_i \in \{0, 1, \ldots, N-1\}$.

With $N = 10$, this is the usual decimal expansion.

Definition 1.2. An **N-adic integer** is a formal infinite sum $\sum_{i=0}^{\infty} x_i N^i$ with each $x_i \in \{0, \ldots, N-1\}$.

So each N-adic integer has a unique N-adic expansion.

Analogy: every element of $[0, 1]$ has a decimal expansion (including irrationals). The differences are that it goes in the opposite direction (bases are growing here) and are unique ($.\overline{9} = 1$ makes it non-unique in $[0, 1]$). Then $\mathbb{Z}_N$, by definition is the set of all sequences $x_0, x_1, \ldots \in \{0, 1, \ldots, N_1\}$.

Corollary 1.3. *The usual rules of addition and multiplication in $\mathbb{Z}$ (by carrying N-adic expansions) make sense for formal infinite N-adic expansions. In this way, $\mathbb{Z}_N$ acquires the structure of a commutative ring.*

This is nice in that in that the first k-terms are of the N-adic expansion only depends on the first k-terms. Equivalently, this is addition mod N^k. Similarly, we can define multiplication like that too. But, we also need to check that we have additive inverses too.

Example 1.4. $\ldots 9999 + \ldots 0001 = 0$. Hence $-1 = \ldots 9999$.

This is the general pattern for additive inverses in N-adics. I.e. $\ldots x_3x_2x_1x_0$ has additive inverse $\ldots (N-x_3-1)(N-x_2-1)(N-x_1-1)(N-x_0)$. This should remind you of the fact that $.\overline{9} = 1$ in $\mathbb{R}$.

Example 1.5. Let $N = 10$. Then $\ldots 3333 \times 3 = \ldots 9999 = -1$. So $\ldots 3333 = \frac{-1}{3}$.

Question 1.1. Which fractions can we not get?

Example 1.6. Here is an example of something you can't get: $\frac{1}{N}$. This is because Nx shifts the digits to the left and appending a zero on the rightmost digit, but we need a 1 on the rightmost for it to equal 1.

Proposition 1.7. *Any fraction $\frac{a}{b}$ such that b is coprime to N is represented by an N-adic integer. In fact, the N-adic expansion is eventually periodic. This is analogous to what happens in the real numbers.*

Example 1.8. $\frac{1}{1-N^k} = 1 + N^k + N^{2k} + \cdots$.

Hence we get an N-adic expansion for $a'/(1-N^k)$ for any a'. This lets us represent a/b if b is coprime to N. This uses the fact that if b is coprime to N, there is k such that $b|1-N^k$.

Remark 1.9. We will focus on the case where N is prime. This is because the N-adic integers are only an integral domain iff N is prime.

Example 1.10. $\mathbb{Z}_{10}$ isn't an integral domain. In fact, $\mathbb{Z}_{10} = \mathbb{Z}_5 \times \mathbb{Z}_2$.

Here's an idea: we have a good notion of convergence in $\mathbb{Z}_N$.

Definition 1.11. Say that a sequence $a_1, a_2, \ldots$ in $\mathbb{Z}_N$ converges to a_∞ if $\forall k$, the first k terms of the N-adic expansion of a_I stabilize (for $i >> 0$) of that of a_∞, which happens iff $a_i - a_\infty$ is divisible by N^k for $i >> 0$.

To construct the counter example to $\mathbb{Z}_{10}$'s integral domainness, we construct some sequences. Consider $5, 5^2, 5^4, \ldots$. This converges 10-adicly.

$$\begin{array}{r|r} 5^1 = 5 & 5^8 = 390625 \\ 5^2 = 25 & 5^{16} = 152587890625 \\ 5^4 = 625 & \end{array}$$

The last digits seem to converge, which is due to the sequence converging.

Lemma 1.12. *$5^{2^n} - 5^{2^{n-1}}$ is divisible by 10^n. I.e. they have the same first n terms in the decimal expansion.*

Proof. It suffices to check that it is divisible by 2^n since there are so many powers of 5. We can do this by induction. Notice that we have this factorization: $(5^{2^{n-1}} - 5^{2^{n-2}})(5^{2^{n-1}} + 5^{2^{n-2}})$, and the first term is by induction divisible by 2^{n-1}, which in conjunction with the latter term's divisiblility by 2 finishes the lemma. □

Notice that with $x_5 = \lim_{k\to\infty} 5^{2^k}$, $x_5^2 = x_5$ because squaring it just shifts each term up one ($\lim_{k\to\infty} 5^{2^{k+1}} = x_5$). Hence $x_5(x_5 - 1) = 0$ but neither terms are 0 by checking the last digit. The square goes through the limit because squaring is continuous, allowing it to pass through the limit. We can use the concept of continuity because we have a metric.

1.1. **Topology.** More systematically, $\mathbb{Z}_N$ is a metric space because we have the following metric:

Definition 1.13. Given two $x, y \in \mathbb{Z}_N$, $d(x,y) \coloneqq p^{-n}$ where n is the largest N s.t. $N^n | x - y$.

Proposition 1.14. *The above function is a metric and $\mathbb{Z}_N$ is complete.*

Remark 1.15. The metric space $\mathbb{Z}_N$ is very unlike $[0,1]$ in that the latter is connected, and the former is totally disconnected and is in fact homeomorphic to the Cantor set. In particular, $\mathbb{Z}_N$ is uncountable.

From here on, $N = p$ is prime.

Exercise 1.1.1. $\mathbb{Z}_p$ is an integral domain.

Example 1.16. $i \in \mathbb{Z}_5$ (with $i = \sqrt{-1}$). Consider the sequence $2, 2^5, 2^{5^2}, 2^{5^3}$. This converges 5-adically because of the following lemma.

Lemma 1.17. *$\forall p > 2$, $\mathbb{Z}_p$ contains ζ_{p-1}, a primitive $p-1$-th root of unity.*

Lemma 1.18. *With $x, y \in \mathbb{Z}_p$ and $x \equiv y \pmod{p^k}$, then $x^p \equiv y^p \pmod{p^{k+1}}$.*

So $\cdot^p$ is like a contraction mapping.

Proof.

$$x^p - y^p = (x-y)(x^{p-1} + yx^{p-2} + \cdots + y^{p-2}).$$

The first term is divisible by p^k. The other term is a sum of p monomial terms because $x \equiv y \pmod{p}$, so they are all congruent mod p, implying that this term is divisible by p. □

Corollary 1.19. *If $x \in \mathbb{Z}_p$, then the sequence $x, x^p, x^{p^2}, \ldots$.*

Proof. First note that $x^p - p$ is divisible by p by Fermat's Little Theorem. By the lemma with $y = x^p$, $x^{p^k} - x^{p^{k-1}}$ is divisible by p^k. This is just giving us convergence in $\mathbb{Z}_p$. □

Observation 1.20. With the above converging to $\alpha(x)$, $\alpha(x) = \alpha(x')$ if $x \equiv x' \pmod{p}$ by the lemma.

In our example, we find that 2^{5^k} convergences in $\mathbb{Z}_5$. Now how do we show that this is the square root of -1. Let α be the limit. Then $\alpha^2 = \lim_{k\to\infty} 4^{5^k}$. By the corollary, this also convergences. As $4 \equiv -1 \pmod{)5}$ and $4^{5^k} \equiv -1 \pmod{5^{k+1}}$, $\lim_{k\to 4^{5^k}} = -1$.

Example 1.21. With $p \neq 2$, there are way more square roots.

$$\sqrt{1+p} = 1 + \frac{1}{2}p + \binom{1/2}{2}p^2 + \binom{1/2}{3}p^3 + \cdots.$$

The RHS converges because $\binom{\frac{1}{2}}{n} \in \mathbb{Z}_p$. In fact, we can get $\sqrt{1+py} \forall y \in \mathbb{Z}_p$.

Example 1.22. This is from Gouvea's text.

$$\log(1+x) = x - x^2/2 + x^3/3 \pm \cdots.$$

In the reals, the denominators help us. Here, they hurt our convergence. But in fact, if $n|x$, then the x^n/n will be absorbed and we can get convergence.

Example 1.23. With $p = 2, x = -2$,

$$0 = \log(-1) = -\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots + \frac{2^n}{n} + \cdots\right)$$

As a consequence, $0 = 2 + \frac{2^2}{2} + \cdots$.

2. Lecture 2

Definition 2.1. An **absolute value** on F is a function

$$|\cdot| : F \to \mathbb{R}_{\geq 0}$$

such that

(1) $|x| = 0 \iff x = 0$
(2) $|xy| = |x||y|$
(3) $|x + y| \leq |x| + |y|$

Remark 2.2. The function $|\cdot|$ on F turns F into a metric space via $d(x, y) = |x-y|$.

Example 2.3. Let $F = \mathbb{Q}$ have the usual archimidean absolute value denoted by $|\cdot|_\infty$.

Example 2.4. Let p be a prime. Define the p-adic absolute value $|\cdot|_P$ on $\mathbb{Q}$ to be $|\frac{a}{b}|_p = p^{\mathrm{ord}_p(b)-\mathrm{ord}_p(a)}$ where $\mathrm{ord}_p(a)$ is the largest power of p that divides a.

For example, $|p|_p = \frac{1}{p}, |\frac{1}{p}|_p = p$. It isn't too hard to show that this is an absolute value, 2 comes from unique prime factorization, 3 comes from the p-adic absolute value satisfying the non-archimedean property, i.e. $|x + y|_p \leq \max(|x|_p, |y|_p)$ (because $p^m|x, p^n|y \implies p^{\min(m,n)}|(x + y)$). This is stronger than the usual triangle inequality.

Definition 2.5. Given $(F, |\cdot|)$, say that F is nonarchimedean if it satisfies $|x+y| \leq \max(|x|, |y|) \forall x, y \in F$.

Geometrically, this means that a disk of some radius doesn't determine a unique center and can be centered at any point in the disk. Also, if $|x| \neq |y|$, then $|x+y| = \max(|x|, |y|)$.

Remark 2.6. Any archimedean (not non-archimedean) field $(F, |\cdot|)$ is always a subfield of $\mathbb{C}$ with the usual absolute value up to scaling. As a consequence, we can't extend the usual absolute value on $\mathbb{C}$ to $\mathbb{C}(z)$. However, there are arbitrarily large nonarchimedean field.

Exercise 2.0.1. It is enough to show that $|2| > 1$ to show that a field is archimedean.

Something special about the nonarchimedean-ness of the absolute value is that points being a fixed distance away forms an equivalence relation (noticably transitivity).

Example 2.7. Let $F = K(t)$. Define an absolute value on K and we want to define $|\frac{f(t)}{g(t)}|$. We do so by letting it equal $2^{\mathrm{ord}_t(g)-\mathrm{ord}_t(f)}$. For example, $|t| = \frac{1}{2}, |t^{-1}| = 2, |t - 1| = 1$. Similarly to the case of $\mathbb{Z}$, we can define this p-adic valuation. In general, we can do this for any UFD, and (my personal addition) I think all valuation rings.

Theorem 2.8 (Ostrowski)**.** *Every absolute value on $\mathbb{Q}$ is one of:*

(1) trivial ($|0| = 0, |x| = 1$ otherwise)
(2) $|\cdot|_p^\alpha, \alpha > 0$
(3) $|\cdot|_\infty^\alpha$ *with* $0 < \alpha \leq 1$

Definition 2.9. Given $(F, |\cdot|)$, call it **complete** if F is complete as a metric space, i.e. every cauchy sequence converges.

Observation 2.10. Every pair $(F, |\cdot|)$ has a completion $(\hat{F}, |\cdot|)$ by letting $\hat{F}$ be the completion of F as a metric space, which is still a field because the field operations carry through limits as F is a topological field.

Definition 2.11. We can define $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value.

Definition 2.12. Given a non-archimedean field $(F, |\cdot|)$, define the **valuation ring** $\mathcal{O} = \{x \in F || x| \leq 1\}$.

Definition 2.13. Define $\mathbb{Z}_{\boldsymbol{p}}$ as the valuation ring of $\mathbb{Q}_p$.

Now we want to unify the two definitions.

Proposition 2.14. *Any $x \in \mathbb{Z}_p$ can be uniquely expressed as $\sum_{n=0}^{\infty} a_n p^n$ with each $a_n \in \{0, \ldots, p-1\}$.*

Observation 2.15.
(1) In any complete NA field, $\sum_{n=0}^{\infty} a_n$ converges iff $a_i \to 0$. This is due to the non-archimedean property.
(2) $|a_i p^i| \leq p^{-i}$ so that $a_i p^i \to 0$ in $\mathbb{Q}_p$.

Proof. For any $x \in \mathbb{Z}_p$, there is a unique $a_0 \in \{0, 1, \ldots, p-1\}$ such that $|x - a_0|_i \leq \frac{1}{p}$. WLOG, $x \in \mathbb{Q} \cap \mathbb{Z}_p = \{\frac{a}{b}\}$. Take $x = \frac{m}{n}, (n, p) = 1$. Then we can find a_0 s.t. $x - a_0 = \frac{m - na_0}{n}$ has p-adic absolute value $\leq \frac{1}{p}$. Simply pick a_0 s.t. $m - na_0$ is divisible by p. Then repeat this process. □

Observation 2.16. Given $x = \sum_{n=0}^{\infty} a_i p^i$, what is $|x|$? $|x| = p^i$ with i the minimal such $a_n \neq 0$.

Observation 2.17. Given $x \in \mathbb{Q}_p$, $\exists N$ such that $p^N x \in \mathbb{Z}_p$. Hence $x = \sum_{-N}^{\infty} a_i p^i$.

Exercise 2.0.2. Take $(K(t), |\cdot|_t)$ with the absolute value from before has completion $(K((t)), |\cdot|_p)$ where $K((t)) = \sum_{n=-N}^{\infty} a_i t^i, a_i \in K$, i.e. the Laurant series. The valuation ring here is $K[[t]]$.

The difference between this and the p-adics is that we don't have to carry. A similarity between the p-adics and reals is that $\mathbb{Q}_p$ is also locally compact. Further, $\mathbb{Z}_p$ is compact. It suffices to show that every sequence of $\mathbb{Q}_p$ has a convergent subsequence by finding a subsequence s.t. the first term converges (exists because $\mathbb{Z}/p\mathbb{Z}$ is finite) and then use Cantor's diagonal argument to prove sequential compactness is equivalent to local.

Remark 2.18. If $(F, |\cdot|)$ is a non-archimedean field, then the valuation ring $\mathcal{O} \subseteq F$ is a local ring, i.e. it has one maximal ideal, namely $\{x \in F : |x| < 1\}$. This is because $\mathcal{O} \setminus \Updownarrow = \{x \in F : |x| = 1\} = \mathcal{O}^\times$ is invertible, as the inverse will also have absolute value 1.

Example 2.19. The unique maximal ideal of $\mathbb{Z}_p$ is (p). In fact, all ideals are generated by powers of p.

2.1. **Hensel's Lemma.** This is a basic tool for solving equations in the p-adics.

Theorem 2.20. *Let F be a complete NA field, $\mathcal{O} \subseteq F$ its valuation ring. Next let $f(x) \in \mathcal{O}[x]$ be a polynomial and let $\alpha_0 \in \mathcal{O}$ such that $|f(\alpha_0)| < 1$ and $|f'(\alpha_0)| = 1$. This condition is saying that $\overline{\alpha_0}$ in the residue field is a simple root (multiplicity one) of f. Then there exists a unique element $\alpha \in \mathcal{O}$ such that*

(1) $|\alpha - \alpha_0| < 1$
(2) $f(\alpha) = 0$.

This will reprove everything about roots of a polynomial from the first lecture.

Proof. Construct the root α via Newton's method. Explicitly, define a sequence inductively

$$\alpha_{i+1} \coloneqq \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}.$$

Claim 2.1. *The α_i converge (rapidly) to a root α of $f(x)$.*

Proof.

Lemma 2.21. *If $g(x) \in \mathcal{O}[x]$ and $t, h \in \mathcal{O}$, then*

$$|g(t+h) - g(t) - hg'(t)| \leq |h|^2.$$

Proof. We use the Taylor expansion for $g(t+h)$ (turns out to be finite). Namely, we get $\sum_{n=2}^{\infty} \frac{g^{(i)}(t)h^i}{i!}$ Then by the NA property, we get the linear terms there and quadratic terms, and the quadratic terms dominate. □

To resume the proof of the claim, we let $\eta = |f(\alpha_0)| < 1$. Our inductive claim is that for each i, $|f'(\alpha_i)| = 1$, $|f(\alpha_i)| \leq \eta^{2^i}$, and $|\alpha_{i+1} - \alpha_i| \leq \epsilon^{2^i}$.

Notice that parts one and two imply three because $f'(\alpha_i) = 1$, so $\alpha_{i+1} - \alpha_i = -\frac{f(\alpha_i)}{f'(\alpha_i)}$, which has absolute value $|f(\alpha_i)|$. Now assume that one and two are true up to i. Then the lemma applied to the lemma with $t = \alpha_i, h = -\frac{f(\alpha_i)}{f'(\alpha_i)}$ gives us that $|f(\alpha_{i+1})| \leq |h|^2 \leq (\eta^{2^i})^2 = \eta^{2^{i+1}}$. So we have 2.

Finally, for property 1, $|\alpha_{i+1} - \alpha_i| < 1$, so $|f'(\alpha_{i+1}) - f'(a_i)| < 1 \implies |f'(\alpha_{i+1})| = 1$. This completes the induction (property 3 was needed to show convergence). □

This shows the convergence to α. The uniqueness isn't hard: just consider the difference between two hypothetical solutions. □

Example 2.22. We compute $\sqrt{1+p} \in \mathbb{Z}_p$. We can see this via Hensel's lemma $f(x) = x^2 - (1+p)$ has root $\alpha_0 = 1$. Then $f(\alpha_0) = -p, f'(1) = 2$.

Example 2.23. Another example is $x^{p-1} - 1$. This is the minimal polynomial of the $(p-1)$-th roots of unity. For any $n \in \mathbb{Z}$, if $p \nmid n$, $|f(n)| < 1$. Further, the derivative at n will also not be divisible by p, so we can lift.

3. Lecture 3

Question 3.1. WHen is $x \in \mathbb{Q}_p^\times$ a square?

We have that

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \cong \oplus_{p \text{ prime}} \mathbb{F}_2 \oplus \mathbb{F}_2$$

because each element squared is 0 and we have a map

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \to \oplus_{p \text{ prime}} \mathbb{F}_2$$

via $x \mapsto v_p(x) \pmod 2$ and the extra $\mathbb{F}_2$ is from the sign. Similarly, $\mathbb{R}^\times/\mathbb{R}^{\times 2} \cong \mathbb{F}_2$. We hope that the p-adic version is like this too.

We want to use a similar result as in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, except here we have no sign nor other primes. So we have that

$$v_p : \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to \mathbb{F}_2.$$

Our first criterion is that the p-adic valuation has to be even. Another obstruction is from $x \in \mathbb{Z}_p^\times$ (i.e. $v_p(x) = 0$). Here x also needs to be a square in $\mathbb{Z}_p^\times$ if it is a square $\mathbb{Q}_p^\times$.

Aside: Over $\mathbb{R}$, we have a natural ordering from the squares always being positive. But over $\mathbb{Q}_p$, any element is a sum of 4 squares.

Claim 3.1. *For $p > 2$,*

$$\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} = \mathbb{F}_2 \oplus \mathbb{F}_2.$$

Proof. It is enough to show that if $x \in \mathbb{Z}_p^\times$ is a square mod p, then x is a square.

Consider $f(y) = y^2 - x$. This has a root mod p if x is a square mod p, say α_0. Then to meet the criterion for Hensel's lemma, we also check that $f'(\alpha_0) = 2\alpha_0$ is a unit, which checks out because $2\alpha_0 \in \mathbb{Z}_p^\times$ because $p \neq 2$. □

Proposition 3.1. *$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \cong \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2$. Moreover, anything in $\mathbb{Z}_2^\times$ that is congruent 1 mod 8 is a square in $\mathbb{Z}_2$.*

Proof. The first factor records the 2-adic valuation. Then because $\mathbb{Z}_2^\times \to (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} = \mathbb{F}_2 \oplus \mathbb{F}_2$. Now all we need to check is that if $x \in \mathbb{Z}_2$ is such that $x \equiv 1 \pmod 8$, then x is a square. We want to use Hensels, but the derivative will create issues.

We change variables: let $y = 1 + 2z, y^2 = x$. Then we have $4z^2 + 4z + 1 = x$ and $z^2 + z = \frac{x-1}{4} \equiv 0 \pmod 2$. Then $f(z) = z^2 + z + \frac{x-1}{4}$. Here, $f'(\alpha_0) = 2\alpha_0 + 1$, showing that Hensel's lemma applies. □

In some cases, one can hope to solve an equation over $\mathbb{Q}$ by solving over $\mathbb{Q}_p, \mathbb{R}$. We can see this with the rationals. The decomposition into a direct sum shows that a rational over $\mathbb{Q}$ is a square iff it is a square in $\mathbb{Q}_p, \mathbb{R}$ for all p.

Theorem 3.2 (Hasse-Minkowski)**.** *A quadratic form over $\mathbb{Q}$ (i.e. of the form $\sum a_{ij} x_i x_j$ with variables x_i) has a non-trivial root iff it has a non-trivial zero in each $\mathbb{Q}_p, \mathbb{R}$.*

Remark 3.3. The analogue fails for higher degree polynomials.

Example 3.4. $x^4 - 17 = 2y^2$ has solutions over $\mathbb{Q}_p, \mathbb{R}$ but not over $\mathbb{Q}$.

Question 3.2. Let $G \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a finite subgroup. How large can G be?

Example 3.5. The signed permutation matrices have $2^n \cdot n!$. This is the best possible in most cases.

We have a bound for the size, but also the order.

Theorem 3.6 (Minkowski)**.**

$$v_\ell(|G|) \leq \left\lfloor \frac{n}{\ell - 1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-2)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots .$$

This gives us a bound on $|G|$ because there are a finite number of primes and these terms eventually die.

Proposition 3.7. *With $p > 2$, let $A \in GL_n(\mathbb{Z}_p)$ such that $A \equiv 1 \pmod p$. Then A has infinite order if $A \neq 1$.*

Proof. Suppose FTSOC that we have a counter-example matrix A with finite order. WLOG, we may assume that the order of A is prime, say ℓ. Let M be the matrix $A - 1$, which by assumption doesn't equal 0. But $(1 + M)^\ell = 1$. Expanding this out, we get

$$1 + \ell M + \binom{\ell}{2} M^2 + \cdots + M^\ell = 1 \iff \ell M + \cdots + M^\ell = 0. \tag{3.8}$$

Finally, to get a contradiction, we can realize that if B is any matrix (b_{ij}), then define $|B| = \max(|B_{ij}|)$. Next observe that $|BB'| \leq |B| \cdot |B'|$ (by the non-Archmedean property). Then *Equation* (3.8) gives us that $\ell M = \sum_{j=2}^{\ell} \binom{\ell}{j} M^j$. Suppose that $|M| = \eta < 1$. If $\ell \neq p$, then $|\ell M| = \eta$, but the RHS has absolute value $\leq \eta^2$.

If $\ell = p$, then the LHS has absolute value $|pM| = \frac{1}{p}|M|$. Then the RHS is $\binom{p}{2} M^2 + \binom{p}{3} M^3 + \cdots + M^p$, which is at most either $\frac{1}{p}|M^2|$ or $|M^p|$. Because $p > 2$, $|M^p| \leq |M| \cdot |M|^2 \leq \frac{1}{p^2}|M|$. □

There's a similar proof using Lie algebras.

Corollary 3.9. *With $p > 2$ a prime and $G \subseteq GL_n(\mathbb{Z}_p)$ is finite, then*

$$G \rightarrowtail GL_n(\mathbb{F}_p).$$

So $|G| \mid |GL_n(\mathbb{F}_p)|$.

Proposition 3.10. $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Proof. It suffices to pick n linearly independent vectors over $\mathbb{F}_p$ because we just need to send the canonical basis to another basis as this is what invertible matrices do. □

Proof of Minkowski's Theorem. Let $G \subseteq \mathrm{GL}_n(\mathbb{Q})$ be finite.

Observation 3.11. G preserves a lattice Λ in $\mathbb{Q}^n$ (pick any Λ_0 and then define $\sum_{g \in G} g\Lambda_0$). We have that G has a conjugate in $\mathrm{GL}_n(\mathbb{Z})$. WLOG let $G \subseteq \mathrm{GL}_n(\mathbb{Z})$. The corollary implies that $v_\ell(|G|) \leq v_\ell(|\mathrm{GL}_n(\mathbb{F}_p)|)$. Now choose p that minimizes the RHS.

Given ℓ, we want p to minimize $\sum_{i=0}^{n-1} v_\ell(p^n - p^i)$. Claim is that it gives the RHS.

In fact, with $p \neq \ell$, this is just

$$\sum_{j=1}^{n} v_\ell(p^j - 1).$$

We want to choose p that minimizes this.

For j such that $\ell - 1 | j$, by Fermat's Little Theorem we get an unavoidable factor of ℓ. In fact, we want to pick p such that p is a primitive root mod ℓ so that $v_\ell(p^j - 1) > 0 \iff \ell - 1 | j$. But also, we want $v_\ell(p^{\ell-1} - 1) = 1$ on the nose.

In order to do this, now that $(\mathbb{Z}/\ell^2\mathbb{Z})^\times = \mathbb{Z}/\ell(\ell-1)\mathbb{Z}$, which is a well-known result in number theory. Here, p needs to be a generator of this group so that the order of p in $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ is $\ell(\ell-1)$. This means that $v_\ell(p^j - 1) = 0$ when $\ell - 1 \nmid j$ and $v(j) + 1$ when $\ell - 1 | j$. This gives us the desired bound.

The justification for the existence of the prime number p is via the cyclicity of $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ and Dirichlet's Theorem.

□

Remark 3.12. Some computations:

$$v_\ell(n!) = \left\lfloor \frac{n}{\ell} \right\rfloor + \left\lfloor \frac{n}{\ell^2} \right\rfloor + \cdots .$$

$$\mathbb{Z}_\ell^\times \cong \mu_{\ell-1} \times \mathbb{Z}_\ell$$

with $\ell > 2$ and $\mu_{\ell-1}$ is the $\ell - 1$-th root of unity. The $\mathbb{Z}_\ell$ term is like the units $\equiv 1 \pmod{\ell}$. A proof of this can be seen in Serre's A Course in Arithmetic.

Definition 3.13. The exponential and logarithm functions

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \qquad \log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots .$$

We can try and consider these are functions of a p-adic variable, since we have ideas of convergence. But we have issues of convergence. The $n!$ can cause problems in the p-adics.

Proposition 3.14. $\exp(x)$ *converges when* $|x| < p^{-\frac{1}{p-1}}$. *This defines a continuous function in that neighborhood, and* $\exp(x+y) = \exp(x)\exp(y)$.

Further, this is just a disk of radius $\frac{1}{p}$ *for* $p > 2$ *or* $\frac{1}{4}$ *for* $p = 2$.

Proof. We need that $\frac{x^n}{n!} \to 0$. We have that $|x^n| = |x|^n$. To do this, we note that $v_p(n!) \leq \frac{n}{p-1}$. So $|\frac{1}{n!}| \leq p^{\frac{n}{p-1}}$. Thus $|\frac{x^n}{n!}| \leq |x|^n \cdot p^{\frac{n}{p-1}}$, which is the exact condition we need. □

Proposition 3.15. $\log(1+x)$ *convergences if* $|x| < 1$. *Further,* $\log((1+x)(1+y)) = \log(1+x) + \log(1+y)$. *Then*

$$|\frac{x^n}{n}| \leq |x|^n \cdot n \to 0 \Leftarrow |x| < 1.$$

Proposition 3.16. $\log$ *and* $\exp$ *are inverse where defined.*

Notice that the second part of the computations earlier in a remark is that we have an isomorphism $(1 + \ell\mathbb{Z}_\ell)^\times \cong \ell\mathbb{Z}_\ell$ via log and vice versa via exp.

4. Lecture 4 - Linear Recurrences

Definition 4.1. Let $x_0, x_1, \ldots$ be a sequence in a field F. Say that the sequence has a **linear recurrence** if $\exists d > 0$ and $a_1, \ldots, a_d \in F$ such that $\forall n \geq d, x_n = a_1 x_{n-1} + \cdots + a_d x_{n-d}$.

Example 4.2. The Fibonacci sequence is a famous example: begins with $0, 1$ and $x_n = x_{n-1} + x_{n-2}$.

Question 4.1. Given a linear recurrence, what do its zeros look like?

The decidability of this is an open problem.

Theorem 4.3 (Skolem-Mahler-Lech)**.** *If char$(F) = 0$, the set $\{n : x_n = 0\}$ is a union of a finite set and finitely many arithmetic progressions.*

Proposition 4.4. *Given $p(x) \in F[x]$, $\{p(n)\}_n$ is a linear recurrence.*

Example 4.5. A criterion for linear recurrence: The generating function

$$\sum_{n\geq 0} x_n t^n \in F[[t]]$$

is rational iff x_n is a linear recurrence. Namely, the linear recurrence gives us a polynomial $p(t)$ such that $p(t)\cdot$ generating function has finitely many roots $1-a_1t-a_2t^2-\cdots-a_dt^d$.

Example 4.6. We have $\frac{1}{1-t} = \sum_{n\geq 0} t^n$, the k-th derivative is rational: $\sum_{n\geq 0} n(n-1)\cdots(n-(k-1))t^{n-k}$. So $\{n, n-1, \ldots, (n-(k-1))\}_n$ is a linear recurrence.

Example 4.7. Let $\alpha \in F$. Then α^n is a linear recurrence.

Example 4.8. If $\{x_n\}$ is a linear recurrence, then $\{\alpha^n x_n\}$ is a linear recurrence.

Example 4.9. We have that $\{\alpha^n p(n)\}$ is a linear recurrence (building off the earlier proposition).

Remark 4.10. Over an algebraically closed field, all linear recurrences are linear combinations of $\{\alpha^n p(n)\}$. I.e. we can write the generating function as a sum of $\frac{f(x)}{(1-x\alpha)^n}$.

Observation 4.11. A sum of linear recurrences is a linear recurrence.

Theorem 4.3 is not true in characteristic p because of

Example 4.12. (in $\mathbb{F}_p(t)$), we have the sequence $x_n = (1+t)^n - t^n - 1$. This is a polynomial, so there is a linear recurrence. But the zeros of this are $n =$ powers of p.

If n is a power of p, this is easily seen to be true. But for odd p, if $n \neq p$, then $\binom{2p}{p} \not\equiv 0 \pmod p$. So $(1+t)^{2t} \neq 1 + t^{2p}$.

The outline of the proof of Theorem 4.3 is to get a sequence in the p-adics, show that it is analytic, and finally show that analytic functions have no zeros or finitely many.

4.1. **Analytic Functions.** Let F be a complete, NA field, e.g. $F = \mathbb{Q}_p$. Consider a formal power series $\sum_{i=0}^{\infty} a_i x^i \in F[[x]]$. Suppose we have $r > 0$ such that $|a_i| r^i \to 0$ as $i \to \infty$. Then $f(x)$ defines a function on $\{x \in F || x| \leq r\}$. Such functions are called analytic. Note that this "closed disk" is also open.

Example 4.13.

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} \qquad r < p^{-\frac{1}{p-1}}$$

$$\sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \qquad r < 1.$$

We use this with $r = 1$ for simplicity, so any $a_i \to 0$ in $\mathbb{Q}_p$ defines an analytic function on $\mathbb{Z}_p$.

Theorem 4.14 (Mahler)**.** *Any continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is uniquely expressed as*

$$\sum_{n=0}^{\infty} a_n \binom{x}{n}$$

where $a_n \in \mathbb{Q}_p$ converge to 0.

Recall that over $\mathbb{C}$, analytic functions have isolated zeros.

Theorem 4.15 (Strassmann)**.** *Let $\sum a_i x^i$ be an analytic function on $\mathbb{Z}_p$ (so $a_i \in \mathbb{Q}_p$ converge to 0).*

Proof. Choose N such that $|a_i| \leq |a_N| \forall i$ and $|a_i| < |a_N|, i > N$. Then f has $\leq N$ roots.

We do induction on $N = N(f)$. If $N = 0$, then $|a_i| < |a_0|$ for $i > 0$. Then

$$|\sum_{i=0}^{\infty} a_i x^i| = |a_0| \neq 0 \implies \text{ no roots in } \mathbb{Z}_p.$$

Suppose that $N > 0$, and suppose that $\alpha \in \mathbb{Z}_p$ is a root of f. Then

$$f(\alpha) = \sum a_i \alpha^i = 0$$

and $f(x) = f(x) - f(\alpha) = \sum_{i=0}^{\infty} a_i(x^i - \alpha^i) = (x - \alpha)g(x)$. Then the fact that $g(x)$ is analytic on $\mathbb{Z}_p$ follows from:

Claim 4.1. $N(f) = N(x - \alpha) + N(g)$.

The former term is 1, so

$$N(f_1 f_2) = N(f_1) + N(f_2).$$

This implies the theorem because by induction, g has at most $N(g) = N(f) - 1$ roots in $\mathbb{Z}_p$.

Proof of Claim. This is basically Gauss' Lemma: WLOG we can assume that f_1, f_2 is in $\mathbb{Z}_p[[x]] \setminus p\mathbb{Z}_p[[x]]$. Then $N(f_1) = \deg \overline{f_1}$ and $\deg(\overline{f_1 f_2}) = \deg \overline{f_1} + \overline{f}_2$. □

Now suppose we have $x_0, x_1, \cdots$ a linear recurrence with $x_n = a_1 x_{n-1} + \cdots + a_d x_{n-d}$. WLOG, assume $a_d \neq 0$.

Observation 4.16. There is a linear operator on the sequence $y_1, \cdots, y_d$ such that

$$A(x_{n-1}, \ldots, x_{n-d}) = (x_n, \cdots, x_{n-d-1}).$$

So $x_n = wA^n v$, where v captures the initial condition. The idea is that we can interpolate this to a p-adic analytic function. First choose odd $p >> 0$ such that $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ and $M > 0$ such that $A^M \equiv 0 \pmod{p}$.

Claim 4.2. *The sequence $\{A^{a+bM}\}_b$ extends to a p-adic analytic function in $b \in \mathbb{Z}_p$. As such, the sequence $\{x_{a+bM}\} : \mathbb{N} \to \mathbb{Q}$ extends uniquely to an analyic function $\mathbb{Z}_p \to \mathbb{Q}_p$. As a result, it's either identitally 0, or has finitely many zeros.*

Proof.

Proposition 4.17. *Let $p > 2$ and let $B \in GL_n(\mathbb{Z}_p)$ such that $B \equiv 1 \pmod{p}$. Then $m \mapsto B^m$ extends to a p-adic analytic function.*

Proof. Notice that $B^m = (1 + (B-1))^m = \sum_{i=0}^{\infty} \binom{m}{i}(B-1)^i$. We want to show that this extends to an analytic function of $m \in \mathbb{Z}_p$. We use this formula as the extended function in $\mathbb{Z}_p$. But we still need to show that it is analytic. This function will be

$$f(x) = \lim_{N\to\infty} \sum_{i=0}^{N} \binom{m}{i}(B-1)^i.$$

In order for this to converge to an analytic function, it needs to converge in Gauss norm (max of norm of coefficients).

I.e. we need $\binom{x}{i}(B-1)^i \to 0$. The Gauss norm is at most $|\frac{1}{i!}| \cdot |B-1|^i$. But $|\frac{1}{i!}| \le p^{\frac{i}{p-1}}$. Because $B - 1 \equiv 0 \pmod{p}, |(B-1)^i| \le p^{-i}$. Hence the Gauss norm goes to 0, showing that it is analytic. □

□

□

Remark 4.18. We can see that $B^m = \exp(m \log B)$. Interpolate this to $x \mapsto \exp(x \cdot \log B)$. Because $B \equiv 1 \pmod{p}$, $\log B$ converges for odd p. Recall that exp is defined on input of size $< p^{-\frac{1}{p-1}}$. But for $p = 2$, we need B to be equivalent to 1 mod 4.

Example 4.19. Consider $f(x) = 0$ a function $\mathbb{Z}_p \to \mathbb{Z}_p$ if $p|x$ and 1 if $p \nmid x$. Here this has infinitely many zeros, but isn't analytic.

Theorem 4.20. *If K is any finitely generated field of characteristic 0 and $S \subseteq K^\times$ is finite, then $\exists p$ such that $K \hookrightarrow \mathbb{Q}_p$ such that $S \hookrightarrow \mathbb{Z}_p^\times$.*

Given a linear recurrence sequence of the form wA^nv over K, we can embed $K \hookrightarrow \mathbb{Q}_p$ such that A maps into $\mathrm{GL}_n(\mathbb{Z}_p)$.

For a reference, see Cassels, Local Fields. A useful blog post is by Terry Tao.