

Cauchy Sequences

Definition A sequence of p -adic numbers $\{x_n\}$ is Cauchy if for any $\epsilon > 0$, there exists an $N > 0$ such that $|x_m - x_n|_p < \epsilon$ whenever $m, n \geq N$.

In words, the distances between *arbitrarily* chosen points past a certain point will grow arbitrarily small.

In the p -adics numbers, we have an equivalent condition, proven on the homework:

Theorem A sequence of p -adic numbers $\{x_n\}$ is Cauchy if for any $\epsilon > 0$, there exists an $N > 0$ such that $|x_{n+1} - x_n|_p < \epsilon$ whenever $n \geq N$.

The difference here is that it suffices that distances between *consecutive* points past a certain point will grow arbitrarily small. This is a highly useful fact for checking whether certain sequences are Cauchy or not.

Example Is the sequence $\{x_n\}$ defined by $x_n = n$ a Cauchy sequence? It is enough to determine whether $|x_{n+1} - x_n|_p$ grows arbitrarily small. In this case, $|x_{n+1} - x_n|_p = |(n+1) - n|_p = |1|_p = 1$, so the answer is **no**.

Since the p -adics are complete, every Cauchy sequence is a convergent sequence. If a sequence is Cauchy, then one should be able to determine what the sequence converges to.

Example The sequence $x_1 = 1, x_2 = 1 + p, x_3 = 1 + p + p^2$, etc. is a Cauchy sequence, since $|x_{n+1} - x_n|_p = |p^n|_p = \frac{1}{p^n}$ grows arbitrarily small as n tends to infinity. The sequence $\{x_n\}$ converges to the p -adic number $x = 1 + p + p^2 + p^3 + \dots = \frac{1}{1-p}$.

Review Problems

1. Determine whether the sequence $\{n^2\}$ is a Cauchy sequence in \mathbb{Q}_p . If so, what does it converge to?
2. Determine whether the sequence $\{n!\}$ is a Cauchy sequence in \mathbb{Q}_p . If so, what does it converge to?
3. (*Challenge Problem*) Determine whether the sequence $\{\frac{p^n}{n!}\}$ is a Cauchy sequence in \mathbb{Q}_p . If so, what does it converge to? (Hint: $p = 2$ is a special case.)

Hensel's Lemma

Hensel's Lemma tells us when a root of a polynomial modulo p extends to a root in \mathbb{Q}_p .

Hensel's Lemma Let $f(x)$ be a polynomial with coefficients in \mathbb{Z}_p . Suppose there is an α_1 such that $f(\alpha_1) \equiv 0 \pmod{p}$ and $f'(\alpha_1) \not\equiv 0 \pmod{p}$. Then there exists an $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$, and α is uniquely determined by $\alpha \equiv \alpha_1 \pmod{p}$.

Example For an odd prime p , $f(x) = x^2 + 1$ has a root modulo p if and only if -1 is a square modulo p , i.e., if $p \equiv 1 \pmod{4}$. Suppose a_0 is the solution to $a_0^2 + 1 \equiv 0 \pmod{p}$. Since a_0 cannot be divisible by p , the derivative $f'(a_0) = 2a_0$ cannot be zero modulo p . By Hensel's Lemma, there is a unique root α in \mathbb{Q}_p that extends the root a_0 (i.e., $\alpha \equiv a_0 \pmod{p}$).

For a given p , the proof of Hensel's Lemma shows how to explicitly construct the digits of the roots. Suppose $\alpha_n = a_0 + a_1p + \dots + a_{n-1}p^{n-1}$ is a solution to $f(\alpha_n) \equiv 0 \pmod{p^n}$, and one wishes to find $\alpha_{n+1} = a_0 + a_1p + \dots + a_{n-1}p^{n-1} + a_np^n$ which is a solution to $f(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}}$. Then a_n is given by the equation

$$a_n \equiv -\left(\frac{f(\alpha_n)}{p^n}\right) \cdot [f'(a_0)]^{-1} \pmod{p}$$

Example Applying this to the equation to $p = 5$ and $f(x) = x^2 + 1$, one can show that two roots of this polynomial have the following p -adic expansions:

$$\begin{aligned}\alpha &= 2 + p + 2p^2 + p^3 + 3p^4 + \dots \\ \beta &= 3 + 3p + 2p^2 + 3p^3 + p^4 + \dots\end{aligned}$$

Review Problems

- Show that the roots of $f(x) = x^2 + 1$ have the expansions listed above.
- Determine the odd primes p for which $g(x) = x^2 - x - 1$ has roots in \mathbb{Q}_p .

Strong Version of Hensel's Lemma Let $f(x)$ be a polynomial with coefficients in \mathbb{Z}_p . Suppose there is an α_1 such that $f(\alpha_1) \equiv 0 \pmod{p^x}$ and $p^y \parallel f'(\alpha_1)$. If $x \geq 2y + 1$, then there exists an $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_1 \pmod{p^{x-y}}$, and α is uniquely determined.

This strong version is needed when the first derivative is zero modulo p . Recall that $p^y \parallel f'(\alpha_1)$ stands for "exactly divides," that is, p^y divides $f'(\alpha_1)$ but p^{y+1} does not.

Example Let $p = 2$ and $f(x) = x^2 - m$, where m is any 2-adic integer. If $m \equiv 1 \pmod{8}$, then $f(x)$ has a root in \mathbb{Z}_2 . To see this, let $\alpha_1 = 1$. Then $f(1) = 1 - m \equiv 0 \pmod{2^3}$ and $2^1 \parallel f'(1) = 2$. Since $x = 3$, $y = 1$ satisfy the equation $x \geq 2y + 1$, there is a root by the Strong Version of Hensel's Lemma.

Review Problems

- Is there a root of $f(x) = x^4 - 17$ in \mathbb{Z}_2 ? Justify.
- Is there a root of $f(x) = x^3 - 10$ in \mathbb{Z}_3 ? Justify.

Roots of Unity in \mathbb{Q}_p

By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$ for $a = 1, 2, \dots, p-1$. Applying Hensel's Lemma to the equation $f(x) = x^{p-1} - 1$ shows that there are exactly $p-1$ roots in \mathbb{Z}_p corresponding to the distinct first digits $1, 2, \dots, p-1$. It was shown in class that these are the only roots of unity in \mathbb{Q}_p (except when $p = 2$, in which there are the roots 1 and -1).

The roots of unity in \mathbb{Q}_p form a cyclic group of size $p - 1$, meaning that every root of unity is the power of one particular root of unity ζ . Such a root of unity is called *primitive*. It has order $p - 1$, i.e., $\zeta^{p-1} = 1$ but $\zeta^k \neq 1$ for $1 \leq k < p - 1$. By the formula

$$\text{ord}(\zeta^k) = \frac{\text{ord}(\zeta)}{\text{gcd}(\text{ord}(\zeta), k)}$$

there are exactly $\phi(p - 1)$, the number of relatively prime numbers to $p - 1$ between 1 and $p - 1$. If ζ is a primitive root of unity, then ζ^k is primitive if and only if $\text{gcd}(\text{ord}(\zeta), k) = 1$.

There is an important link between the integers modulo p under multiplication and the roots of unity in \mathbb{Q}_p , namely that there is an “isomorphism” between the two groups. If a root of unity ζ has first digit a_0 , then $\text{ord}(\zeta) = \text{ord}_p(a_0)$. This will allow us to determine the order of a root of unity, simply by computing the order of the first digit modulo p .

Example Let $p = 5$. Using Hensel’s Lemma, we can compute the four roots of the equation $f(x) = x^4 - 1$:

$$\begin{aligned}\zeta_1 &= 1 + 0p + 0p^2 + 0p^3 + 0p^4 + \dots \\ \zeta_2 &= 2 + p + 2p^2 + p^3 + 3p^4 + \dots \\ \zeta_3 &= 3 + 3p + 2p^2 + 3p^3 + p^4 + \dots \\ \zeta_4 &= 4 + 4p + 4p^2 + 4p^3 + 4p^4 + \dots\end{aligned}$$

Notice that $\zeta_1 = 1$ and $\zeta_4 = -1$ in \mathbb{Z}_5 . These will be in \mathbb{Q}_p no matter what p is.

We can determine the n for which each ζ_k is a primitive n^{th} root of unity by computing the order of the first digit modulo 5. $a_0 = 1$ has order 1, so ζ_1 is a primitive 1st root of unity. $a_0 = 2, 3$ both have order 4, so ζ_2 and ζ_3 are primitive 4th roots of unity. Finally, $a_0 = 4$ has order 2, so ζ_4 is a primitive 2nd root of unity.

Review Problems

8. How many primitive 6th roots of unity are there in \mathbb{Q}_7 ? What are their beginning digits?
9. How many primitive 5th roots of unity are there in \mathbb{Q}_{11} ? What are their beginning digits?

Local-Global Principle

The main application of p -adic numbers is the Local-Global Principle. It is clear that if an equation has a solution in the rationals, then it has a solution in \mathbb{Q}_p for all $p \leq \infty$, since the rationals are always contained in \mathbb{Q}_p . (Recall that \mathbb{Q}_∞ means the real numbers.) The Local-Global Principle states that the converse should also be true:

Local-Global Principle If an equation has a nontrivial solution in \mathbb{Q}_p for all $p \leq \infty$, then it has a nontrivial solution in \mathbb{Q} .

Unfortunately, the Local-Global Principle doesn’t always hold true.. There are many examples where there are solutions in \mathbb{Q}_p for all $p \leq \infty$ but not in \mathbb{Q} . However, it is a guiding principle that holds in some important cases. The most famous application is the following theorem:

Hasse-Minkowski Theorem Let

$$f(x_1, x_2, \dots, x_n) = \sum_{1 \leq i \leq n} a_i x_i^2 + \sum_{1 \leq i < j \leq n} b_{ij} x_i x_j$$

be a quadratic form with integer coefficients a_i and b_{ij} . If $f(x_1, x_2, \dots, x_n) = 0$ has nontrivial solutions in \mathbb{Q}_p for all $p \leq \infty$, then it has a nontrivial solution in \mathbb{Q} .

This is a generalization of Legendre's Theorem, which we proved at the end of last quarter for $f(x, y, z) = ax^2 + by^2 - cz^2 = 0$.

Example A simple case of Hasse-Minkowski's Theorem is $f(x, y, z) = x^2 + y^2 - z^2 = 0$. This has nontrivial solutions modulo p for all primes p , since by the pigeonhole principle, there must be two nonzero squares whose sum will be a nonzero square modulo p . By Hensel's Lemma, there is a solution in \mathbb{Q}_p for all p . In the reals, there is a solution for z for any given x and y . Hence, there must be solution in the rationals. It is well known that there are many such solutions by the Pythagorean Theorem.

Counterexample The basic philosophy behind producing counterexamples to the Local-Global Principle is to find a set of conditions, one of which must hold for any given prime (maybe with a few exceptions). Using the Legendre symbol is a common trick. By plugging in specific values for all but one variable, one can often say there is a solution modulo p if a certain Legendre symbol is equal to 1. By plugging in the right values, one may be able to come up with a set of three Legendre symbols, one of which will be equal to 1 for every prime (with a few exceptions).

Consider the equation $x^4 - 17 = 2y^2$. Let $x = 5$. Solving for y^2 , we have $y^2 = 304 = 2^4 \cdot 19$. This has a solution for y modulo p if and only if $\left(\frac{19}{p}\right) = 1$. Now let $y = 4$. Solving for x^4 , we have $x^4 = 49$, or equivalently, $x^2 = 7$. This has a solution for x modulo p if and only if $\left(\frac{7}{p}\right) = 1$. Finally, let $y = 94$. Solving for x^4 , we have $x^4 = 17689 = 133^2$, or equivalently, $x^2 = 133 = 7 \cdot 19$. This has a solution for x modulo p if and only if $\left(\frac{133}{p}\right) = 1$. If 7 or 19 are squares modulo p , then we have a solution in \mathbb{Q}_p by Hensel's Lemma. If 7 and 19 are both nonsquares modulo p , then $133 = 7 \cdot 19$ is a square modulo p . Again by Hensel's Lemma, there is solution in \mathbb{Q}_p .

The exceptional cases are when the Legendre symbol doesn't make sense. This is when $p = 7$, $p = 19$, $p = 2$, and $p = \infty$. A solution for each of these cases must be found separately. Solutions for these problems can be found by plugging in $x = 3$, $x = 2$, $x = 11$, and $y = 0$, respectively.

Review Problems

10. Show that $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$ has a solution in \mathbb{Q}_p for all $p \leq \infty$ but not in \mathbb{Q} .
11. Show that $(x^2 + 5y^2 - 3)(x^2 + 3y^2 - 17) = 0$ has a solution in \mathbb{Q}_p for all $p \leq \infty$ but not in \mathbb{Q} . (*Hint: You only need to plug in small values for x in either equation, though there may be other ways.*)