p-adic Numbers 강의록

Donghyun Park

January 13, 2026

1 5강. Hensel's lemma and Local-Global Principal

1.1 Hensel's Lemma

Let the polynomial $F(X) = a_0 + a_1X + \cdots + a_nX^n$ with coefficients $a_i \in R$. The formal derivative is defined

$$F'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$$

Theorem 1 ([Gou20] Theorem 4.5.2)**.** *$F(X)$ a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that*

$$F(\alpha_1) \equiv 0(mod\, p\mathbb{Z}_p)$$

$$F'(\alpha_1) \not\equiv 0(mod\, p\mathbb{Z}_p)$$

Then there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1(mod\, p\mathbb{Z}_p)$ and $F(\alpha) = 0$

Proof. We construct Cauchy sequence $\alpha_1, \alpha_2, \cdots$ that satisfies
(a) $F(\alpha_n) \equiv 0(mod\, p^n)$
(b) $\alpha_{n+1} \equiv \alpha_n(mod\, p^n)$
How to do that? α_1 is given. $\alpha_{n+1} = \alpha_n + b_np^n$
$F(\alpha_{n+1}) = F(\alpha_n + b_np^n) = F(\alpha_n) + F'(\alpha_n)b_np^n + \cdots$
By the Taylor formula (Is this true? True! for polynomials)
So we have b_n chosen to make $F(\alpha_n)+F'(\alpha_n)b_np^n$ divisible by p^{n+1}...
(Need more... $F'(\alpha_n)$ also not divisible by p? The same logic!) □

In other language

Theorem 2. *$F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. If there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that $|F(\alpha_1)| < 1$ and $|F'(\alpha_1)| = 1$. Setting*

$$\alpha_{n+1} = \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)}$$

defines a convergent sequence whose limit $\alpha \in \mathbb{Z}_p$ is the unique p-adic integer such that $|\alpha - \alpha_1| < 1$ and $F(\alpha) = 0$

Stronger version of Hensel's lemma.

Theorem 3. *$F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. If there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that $|F(\alpha_1)| < |F'(\alpha_1)|^2$. Then there exists an unique p-adic integer α such that $|\alpha - \alpha_1| < p^{v_p(F(\alpha_1)) - v_p(F'(\alpha_1))}$ and $F(\alpha) = 0$*

1.2 Application of Hensel's Lemma

We call m-th root of unity if it is root of $F(X) = X^m - 1$. Primitive m-th root of unity is m-th root of unity that does not satisfy $\zeta^n = 1$ for $1 \leq n \leq m-1$

Remark 1. *Root of unity (if exists) is always p-adic integer*

Proposition 1 ([Gou20] Proposition 4.6.1)**.** *For any prime p and any positive integer m not divisible by p, there exists a primitive m-th root of unity in $\mathbb{Q}_p$ if and only if $m \mid p-1$*

Proof. $F'(\lambda) = m\lambda^{m-1}$ so if $p \nmid m$ then $F'(\alpha_1) \not\equiv 0(mod\, p)$ if $\alpha_1 \not\equiv 0(mod\, p)$.
So we want to find $\alpha_1^m \equiv 1(mod\, p)$ then by Hensel's lemma, it lifts to the root in $\mathbb{Q}_p$.
Now, $m \mid p-1$, we can find m incongruent roots of $X^m-1 \equiv 0(mod\, p)$.
There are no other roots of unity. $\zeta^k = 1$ and $p \nmid k$ then as modulo p, k must divide $p-1$ or $k = 1$. □

Remark 2. *1. (p-1)-roots of unity are all noncongruent modulo p ($p-1$ root of unity 중 1와 congruent한 것은 1 뿐이므로! Hensel lemma)*
2. The structure of $\mathbb{Z}_p^\times$ as a multiplicative group, is $V \times U_1$ where V is (p-1) roots of unity and $U_1 = 1 + p\mathbb{Z}_p$.

나중에 analysis를 하고 돌아옵시다!
3. Containing n-th root of unity is an important feature! Especially in the field theory, ***Kummer Theory***

Next application is analyzing the multiplicative group $\mathbb{Q}_p^\times$, quotient group $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$
First $p \neq 2$ prime.

Proposition 2. *$b \in \mathbb{Z}_p^\times$ If there exists an $\alpha_1 \in \mathbb{Z}_p$ such that $\alpha_1^2 \equiv b(mod\, p\mathbb{Z}_p)$ then b is a square on the element of $\mathbb{Z}_p^\times$*

Proof. Hensel's lemma on $X^2 - b$ □

Corollary 1. *$p \neq 2$ the $x \in \mathbb{Q}_p$ is a square if and only if it can be written as $x = p^{2n}y^2$ for $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^\times$. Thus $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Coset representation $\{1, p, c, cp\}$*

If $p = 2$ prime. Then we apply the strong hensel's lemma. 2-adic unit is square if and only if it is congruent to 1 modulo 8. $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ has order 8. Coset representative $\{1, -1, 5, -5, 2, -2, 10, -10\}$
More detail: $f(X) = X^2 - b$, $f'(X) = 2X$. For $X \equiv 1(mod\ 2)$, $|f'(x)|^2 = \frac{1}{4}$ and $\frac{1}{4} < |x^2 - b|$ for $x \in \mathbb{Z}^\times$ if $x^2 \equiv b(mod\, 8)$. $x = 1 + 2y$, $y \in \mathbb{Z}_2$ so $x^2 = 1 + 4y + 4y^2 \equiv 1(mod\, 8)$ so if and only if $b \equiv 1(mod\, 8)$.
$x \in \mathbb{Q}_2$ is a square if and only if it can be written as $x = 2^{2n}y$ for $y \in 1 + 8\mathbb{Z}_2$.

1.3 Hensel's Lemma for Polynomials

$g(X), h(X) \in \mathbb{Z}_p[X]$. $\bar{g}(X), \bar{h}(X) \in \mathbb{F}_p[X]$ a polynomials obtained by reducing the coefficients modulo p. $g(X)$ and $h(X)$ are relatively prime modulo p if $gcd(\bar{g}, \bar{h}) = 1$ in $\mathbb{F}_p[X]$

Theorem 4 (Theorem 4.7.2 (Hensel's Lemma for Polynomials))**.** *$f(X) \in \mathbb{Z}_p[X]$ a polynomial and assume $g_1(X), h_1(X) \in \mathbb{Z}_p[X]$ such that*
- $g_1(X)$ monic
- $g_1(X)$ and $h_1(X)$ reduced into polynomial in $\mathbb{F}_p[X]$ by modulo p for each coefficients, then is relatively prime modulo p
- $f(X) \equiv g_1(X)h_1(X) (\mathrm{mod}\, p)$ coefficient-wise

Then there exists $g(X), h(X) \in \mathbb{Z}_p[X]$ that
- $g(X)$ monic
- $g(X) \equiv g_1(X) (\mathrm{mod}\, p)$ and $h(X) \equiv h_1(X) (\mathrm{mod}\, p)$
- $f(X) = g(X)h(X)$

Proof. Construct the sequence of polynomials $g_n(X)$, $h_n(X)$ satisfying
- $g_n(X)$ monic, degree equal to $g_1(X)$
- $g_{n+1}(X) \equiv g_n(X)(mod\ p^n)$ and $h_{n+1}(X) \equiv h_n(X)(mod\ p^n)$
- $f(X) \equiv g_n(X)h_n(X)(mod\ p^n)$

All coefficient wise.

$g_2(X) = g_1(X) + pr_1(X)$, $h_2(X) = h_1(X) + ps_1(X)$.
Then we are finding $r_1(X)h_1(X) + s_1(X)g_1(X) \equiv (f(X) - g_1(X)h_1(X))/p = k_1(X)(mod\ p)$.
By relatively prime modulo p condition, $a(X), b(X) \in \mathbb{Z}_p[X]$ such that $a(X)g_1(X) + b(X)h_1(X) \equiv 1(mod\ p)$. Define $\tilde{r}_1(X) = b(X)k_1(X)$, $\tilde{s}_1(X) = a(X)k_1(X)$ □

1.4 Local-Global Principle

We will use $\mathbb{Q}_p$ to analyze Diophantine equation. The existence of solutions in $\mathbb{Q}$ can be detected by studying roots on $\mathbb{Q}_p$ which are local solutions.

Easy direction: If the equation has $\mathbb{Q}$ solution then it does in $\mathbb{Q}_p$, $p \leq \infty$ because $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.
Instances:
- $X^2 + Y^2 + Z^2 = 0$ in $\mathbb{Q}_\infty = \mathbb{R}$; only $(0, 0, 0)$ can be a solution
- $X^2 - 3Y^2 = 0$ in $\mathbb{Q}_7$; only $(0, 0)$ can be a solution
- $X^2 - 37Y^2 = 0$ in $\mathbb{Q}_5$; only $(0, 0)$ can be a solution

$\mathbb{Q}_p$ is "local" information near the prime p. "global" means for $\mathbb{Q}$. The Local-Global Principle is

Local-Global Principle: The existence or non-existence of solutions in $\mathbb{Q}$ of a diophantine equation can be detected by studying, for each $p \leq \infty$ the solutions of the equation in $\mathbb{Q}_p$ (local solutions)

Easy example

Proposition 3 ([Gou20] Proposition 4.8.1)**.** *A number $x \in \mathbb{Q}$ is a square if and only if it is a square in every $\mathbb{Q}_p$, $p \leq \infty$*

Proof.
$$x = \pm \prod_{p<\infty} p^{v_p(x)}$$

If x is square in every $\mathbb{Q}_p$, then $v_p(x)$ must be even, and x is positive number. Thus is square in $\mathbb{Q}$ □

We can interpret proposition as $f(X) = X^2 - a$, $a \in \mathbb{Q}$, $f(X)$ has a solution in $\mathbb{Q}$ if and only if it has a solution in each $\mathbb{Q}_p$. (Local-Global Principle)

Local-Global Principle might fail :
- $(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$ has roots in $\mathbb{Q}_p$ but not in $\mathbb{Q}$

Remark 3. *$p = 2, 17$ holds since $X^2 - 17 = 0$, $X^2 - 2$ is solvable in $\mathbb{Q}_2$, $\mathbb{Q}_{17}$*
$p \neq 2, 17$ then one of the three equation is solvable. (Legendre symbol..!)

- $X^4 - 17 = 2Y^2$ has roots in $\mathbb{Q}_p$ but not in $\mathbb{Q}$.

Theorem 5 (Theorem 4.8.2 (Hasse-Minkowski))**.** *For the quadratic form*

$$F(X_1, \cdots, X_n) = \sum_{i,j} c_{ij} X_i X_j \in \mathbb{Q}[X_1, \cdots, X_n]$$

the equation $F(X_1, \cdots, X_n) = 0$ has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for $p \leq \infty$.

1.5 Hasse-Minkowski Application

Let us consider

$$aX^2 + bY^2 + cZ^2 = 0$$

a, b, c are pairwise-relatively prime integers with no square factors.
We can find the solution in $\mathbb{Q}_p$ if
- $p = \infty$ **:** a, b, c **do not have the same sign**
- p **odd prime :** $p \nmid abc$ **or** $p \mid a$ **then** $b + r^2 c \equiv 0 (\mathrm{mod}\, p)$ **for some** $r \in \mathbb{Z}$

Theorem 6 (Chevalley-Warning Theorem)**.** *Let $f_\alpha \in \mathbb{F}_p[X_1, \cdots, X_n]$ a family of polynomials that satisfy $\sum_\alpha \deg f_\alpha < n$. If V be their common zeros in K^n then*

$$Card(V) \equiv 0(mod\ p)$$

Lemma 1. *Let $u \geq 0$ be an integer. Then*

$$\sum_{x \in \mathbb{F}_p} x^u = \begin{cases} -1 & u \geq 1, p-1 \mid u \\ 0 & o.w. \end{cases}$$

Proof. If $p - 1 \mid u$, by fermat's little theorem, $x^{p-1} = 1$ in $\mathbb{F}_p$ for $x \neq 0$ so $\sum_{x \in \mathbb{F}_p} x^u = p - 1 = -1$
Else, let y be an integer $y^u = 1$ then $\sum_{x \in \mathbb{F}_p} x^u = \sum_{x \in \mathbb{F}_p} x^u y^u = 0$ □

Proof of the Chevalley-Warning Theorem. Define $P = \prod_\alpha (1 - f_\alpha^{p-1})$. Then $x \in V$ if and only if $P(x) = 1$.
Claim:
$$\sum_{x \in \mathbb{F}_p^n} P(x) = 0$$

Since $\deg P < n(p-1)$, every monomial has some variable of degree less than $p-1$. For example $x_1^{b_1} \cdots x_n^{b_n}$, $b_n < p-1$. Summing over x_n becomes 0. □

Corollary 2. *In the same setting of the Chevalley-Warning theorem and assume f_α does not have a constant term. Then the system of equation $f_\alpha = 0$ have a nontrivial common solution*

Proof. $0 \in V$ □

Corollary 3. *The quadratic form with more than 3 variables (Only one $f \in \mathbb{F}_p[X_1, \cdots, X_n]$ with $n \geq 3$) have a nontrivial zero.*

Applied to $p \nmid abc$, solves the case.
In the case $p \mid a$, b, c coprime to a. Thus Hensel's lemma is applicable. The problem reduced to the existence of solution reduced to modulo p.
- $p = 2$ **:** a, b, c **all odd then two sum must be divisible by 4, and if** a **even then** $b + c$ **or** $a + b + c$ **divisible by 8**
a, b, c all odd. Two y, z should be odd and x should be even. $a(4x') + b(1 + 4y') + c(1 + 4z') = 0$ so $b + c \equiv 0(mod\ 4)$.
Conversely, look at the solution modulo 8.
- $b + c \equiv 0(mod\ 8)$ then let x divisible by 4, y, z odd gives solution modulo 8. Now Strong Hensel's lemma
- $b + c \equiv 4(mod\ 8)$ then let x is form $4k + 2$, repeat.
$2 \mid a$ then solution look at modulo 8... (the same)
By Hasse-Minkowski, if above condition guarantees solution in $\mathbb{Q}$.

1.6 Sum of three squares

Theorem 7. *An $n \in \mathbb{N}$ is sum of three squares if and only if n is not a form of $4^a(8b - 1)$*

Consider 동차 이차식 $x^2 + y^2 + z^2 - nw^2 = 0$

Lemma 2. *$f(X) = 0$ 의 non-trivial 유리수 해가 존재할 조건은 $-n$ 이 $\mathbb{Q}_2$의 제곱수가 아닌 것. 그리고 이 필요충분 조건은 n 이 $4^a(8b - 1)$ 꼴이 아닌 것.*

Proof. Hasse-Minkowski에 의해 유리수 해가 존재하는 것은 $\mathbb{R}, \mathbb{Q}_p$에서 근이 존재하는 것과 동치. 실수는 일단 됐고.
$\mathbb{Q}_p$, $p \neq 2$를 보자.
Case 1. $p \nmid n$ $w = 1, z = 0$. $x^2 + y^2 \equiv n(mod\ p)$ solution 존재?
$S = \{x^2 \mid x \in \mathbb{F}_p\}$ 원소 개수 $(p+1)/2$. $T = \{n - y^2 \mid y \in \mathbb{F}_p\}$ 원소 개수 $(p+1)/2$. 공통원소 존재. 따라서 mod p 해가 존재.
Hansel's condition.

$$\frac{\partial F}{\partial x} = 2x, \frac{\partial F}{\partial y} = 2y, \frac{\partial F}{\partial z} = 2z, \frac{\partial F}{\partial w} = -2nw$$

$(x_0, y_0, 0, 1)$ 에서 위의 x, y 중 하나는 0이 아님. Lifting 가능.
Case 2. $p \mid n$
mod p solution: $x^2 + y^2 + z^2 \equiv 0(mod\ p)$ nontrivial solution 을 찾을 수 있나. Chevalley Warning theorem. Lifting은 자명
그러면 이제 $p = 2$를 들여다보자. $-n$ be square이면 $\mathbb{Q}_2$에서 주어진 이차식은 $x^2 + y^2 + z^2 + W^2 = 0$. 위의 solution 이 존재한다면 mod 8로 바라보았을 때 모든 수가 짝수여야... 무한강하.
$-n$ not a square. Consider $x^2 = n - y^2 - z^2$ polynomial. We shall appropriately choose y, z so $f(x) = x^2 - A$ applied strong hensel.
$f'(x) = 2x$ so we want to find $|f(x_0)|_2 < |f'(x_0)|_2^2$. If x_0 is unit, then $|x_0^2 - A|_2 < 1/4$ or $x_0^2 \equiv A(mod\ 8)$ but $x_0 \equiv 1(mod\ 2)$
Mod 8로 식을 바라봅시다. $-n$ is not square is equivalent to n not 7 mod 8. 그 외에는 항상 해를 찾을 수 있죠..

$$1 + 0 + 0 = 1$$
$$1 + 1 + 0 = 2$$
$$1 + 1 + 1 = 3$$
$$1 + 4 + 0 = 5$$
$$1 + 4 + 1 = 6$$

따라서 lifting이 존재하고... QED ☐

Remark 4. *Quadratic form 에 대해 더 깊이 공부하면 조금 더 다이렉트한 방법으로 $\mathbb{Q}_2$의 제곱수 조건이 튀어나오게 됩니다... 참고문헌 A coure in Arithmetic, J.P.Serre Chapter 1 to 4.*

Lemma 3 (Davenport-Cassels)**.** *$f(X) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$ positive definite quadratic form $a_{ij} = a_{ji} \in \mathbb{Z}$. If*
(H) $\forall x = (x_1, \cdots, x_n) \in \mathbb{Q}^n$,$\exists y = (y_1, \cdots, y_n) \in \mathbb{Z}^p$ that $f(x - y) < 1$
Then if $f(X) = m$ in $\mathbb{Q}^n$ has a solution, then so does in $\mathbb{Z}$

Proof. Let $x \cdot y = \sum_{i,j} a_{ij} x_i y_j$ for $x, y \in \mathbb{Q}^n$. If $f(X) = m$ has solution in $\mathbb{Q}^n$, then there exists $t > 0$ integer such that $t^2 m = x \cdot x$, $x \in \mathbb{Z}^p$. Let t be the integer smallest among the all solutions $f(x) = m$
$\frac{x}{t} = y + z$, $y \in \mathbb{Z}^n$ with $z \cdot z < 1$ exists by (H).
Now if $z \cdot z = 0$ then t must be 1... this leads to conclusion.
Else $z \cdot z \neq 0$ then let $a = y \cdot y - m$, $b = 2(mt - x \cdot y)$, $t' = at + b$, $x' = ax + by$.
Then $x' \cdot x' = t'^2 m$ and $tt' = t^2 z \cdot z$ so $t' = t(z \cdot z) < t$ contradiction. ☐

For the quadratic form $f(X) = X_1^2 + X_2^2 + X_3^2$ satisfies (H) because choosing $|x_i - y_i| \leq \frac{1}{2}$ can be chosen. Thus completing the Sum of three squares.

References

[Gou20] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction.* 3rd. Universitext. Springer, 2020. ISBN: 978-3-030-47295-5. DOI: 10.1007/978-3-030-47295-5.