p-adic Numbers 강의록

Donghyun Park

January 15, 2026

0.1 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. 이 방정식의 유리수 solution이 존재하는 지를 알고 싶다. 그런데 Hasse-Minkowski에 의해 각 $\mathbb{Q}_p$에서 solution이 존재하는지 여부를 알아보면 된다.

- $p = \infty$ **:** a, b, c **do not have the same sign** (증명은 자명)
- p **odd prime :** $p \nmid abc$ **or** $p \mid a$ **then** $b + r^2c \equiv 0 (\mathrm{mod}\, p)$ **for some** $r \in \mathbb{Z}$

증명을 해봅시다.

Theorem 1 (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 1. *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 2. *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. 왜냐하면 Corollary 2에 의해 nontrivial zero on $\mathbb{F}_p^3$이 존재하는데, $x, y, z \in \mathbb{F}_p^3$ 중에 0이 아닌 값이 존재할 때, 해당 변수에 대한 식으로 (예를 들면 $x \neq 0$인 solution이 있다면 $f(X) = aX^2 + by^2 + cz^2$가 mod p solution을 가지고, 미분한 것은 mod p로 0이 아니므로 y, z는 고정한 채 $x \in \mathbb{Q}_p$ solution이 존재한다.

In the case $p \mid a$ and b, c coprime to a. 위에서의 논리가 똑같이 적용된다. mod p로 셋 다 0이 아닌 solution이 있으면 되는데, 이것이 $b + r^2c \equiv 0 (mod\ p)$ 이다.
- $p = 2$ **:** 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**

Strong Hensel lemma에 의해서 mod 8로 solution이 존재하고 홀수인 변수가 있다면 solution in $\mathbb{Q}_2$가 존재한다.
첫 번째로 a, b, c all odd. 그러면 two y, z should be odd and x should be even.
$a(4x') + b(1 + 4y') + c(1 + 4z') = 0$ so $b + c \equiv 0 (mod\ 4)$.
이제 mod 8로 식을 바라보면
- $b + c \equiv 0 (mod\ 8)$ then let x divisible by 4, y, z odd gives solution modulo 8.
- $b + c \equiv 4 (mod\ 8)$ then let x is form $4k + 2$, y, z odd gives solution modulo 8

이므로 두 경우에 대해 모두 solution이 존재함을 확인할 수 있다.

$2 \mid a$ then solution look at modulo 8... (위 과정을 반복)

0.2 Sum of three squares

Theorem 2. *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 solution을 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 solution이 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 1. *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)**.** *$f(X) = \sum_{i,j=1}^n a_{ij}X_iX_j$ 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 $x \cdot y = \sum_{i,j} a_{ij}x_iy_j$ 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 $t^2m = x \cdot x$, $x \in \mathbb{Z}^p$. 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 $x' \cdot x' = t'^2m$ and $tt' = t^2z \cdot z$ 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.

1 6강. Analysis on p-adic numbers 2

1.1 Functions Defined by Power series(Conti)

Proposition 1 ([Gou20] Proposition 5.5.4)**.** *$f(X), g(X)$ be a formal power series, and suppose there is a non-stationary sequence(결국 같은 값만 계속 나오는) $x_m \in \mathbb{Q}_p$ converging to zero in $\mathbb{Q}_p$ and $f(x_m) = g(x_m)$ for every m. Then $f(X) = g(X)$*

Proof. $h(X) = f(X) - g(X)$, $h(x_m) = 0$ for every m.
만약 $h(X)$가 0이 아니라면
$h(X) = X^r(a_r + a_{r+1}X + \cdots) = X^rh_1(X)$, $h_1(0) \neq 0$. h_1 은 region of convergence에서 continuous이고, $h_1(x_m) \to a_r$ 그러면 $h(x_m)$은 nonzero일 수밖에 없다. (큰 m에 대해서) □

Proposition 2 ([Gou20] Proposition 5.5.5)**.** *$f(X) = \sum a_nX^n$ be a power series with non-zero radius of convergence and $f'(X)$ be a formal derivative. $x \in \mathbb{Q}_p$, if $f(x)$ converges then so does $f'(x)$ and we have*

$$f'(x) = \lim_{h\to 0} \frac{f(x + h) - f(x)}{h}$$

Proof. $f(x)$ converge하는 것과 $a_nx^n \to 0$은 서로 동치.
$|na_{n-1}x^{n-1}| \leq \frac{1}{|x|}|a_nx^n| \to 0$ 이다. ($x = 0$은 자명하게 성립하고..)
이제, $f(X)$가 $|x| \leq \rho_1$에서 converge한다고 생각합시다. $x = 0$ 이라면 $|h| \leq \rho_1$, $x \neq 0$ 이면 $|h| < |x| \leq \rho_1$을 가정.

$$f(x + h) = \sum_{n=0}^\infty a_n \sum_{m=0}^n \binom{n}{m} x^{n-m}h^m$$
$$\frac{f(x + h) - f(x)}{h} = \sum_{n=1}^\infty \sum_{m=1}^n a_n \binom{n}{m} x^{n-m}h^{m-1}$$

Taking limit $h \to 0$, since we have $|a_n\binom{n}{m}x^{n-m}h^{m-1}| \leq |a_n|\rho_1^{n-1}$. Series converges when $|x| = \rho_1$ so $|a_n|\rho_1^n \to 0$
Given $\epsilon > 0$, $m \geq M$ implies $|a_n|\rho_1^{n-1} < \epsilon$. Thus

$$|a_n\binom{n}{m}x^{n-m}h^{m-1}| \leq |a_n|\rho_1^{n-1} < \epsilon$$

uniformly in h.
Finally, below lemma gives the limit can be taken term-by-term.

$$f'(x) = \sum_{n=1}^\infty na_nx^{n-1}$$

□

Lemma 4 ([Gou20] Problem 167)**.** *Suppose for all $|h| \leq r$, $f(h) = \sum_{n=0}^\infty f_n(h)$ and $\lim_{n\to\infty} f_n(h) = 0$ uniformly in h. Then*

$$\lim_{h\to 0} f(h) = \sum_{n=0}^\infty \lim_{h\to 0} f_n(h)$$

Proof. Assume the limit exists, let

$$A = \lim_{h\to 0} f(h), a_n = \lim_{h\to 0} f_n(h)$$

Let $\epsilon > 0$, M such that $m \geq M$ implies $|f_m(h)| < \epsilon$ for all $|h| \leq r$.

$$|f(h) - \sum_{n=0}^M f_n(h)| = |\sum_{n=M+1}^\infty f_n(h)| \leq \max_{n>M} |f_n(h)| < \epsilon$$

For each n, there exists δ_n such that if $|h| < \delta_n$ implies $|f_n(h) - a_n| < \epsilon$. Therefore, $m \geq M$, $|a_m| \leq \max(|f_m(h)|, |a_m - f_m(h)|) < \epsilon$.
Finally, δ exists so that $|h| < \delta$, $|f(h) - A| < \epsilon$.
$|h| < \min(r, \delta, \delta_0, \cdots, \delta_M)$ and $m \geq M$
(a) $|A - f(h)| < \epsilon$
(b) $|f(h) - \sum_{n=0}^M f_n(h)| < \epsilon$
(c) $|\sum_{n=0}^M f_n(h) - \sum_{n=0}^M a_n| < \max_{0\leq n\leq M} |f_n(h) - a_n| < \epsilon$
(d) $\sum_{n=0}^M a_n - \sum_{n=0}^m a_n| \leq \max_{M<n\leq m} |a_n| \leq \epsilon$
Thus,

$$|A - \sum_{n=0}^m a_n| \leq \epsilon$$

□

Corollary 3 ([Gou20] Corollary 5.5.6)**.** *$f(X), g(X)$ are power series, and suppose that both series converge for $|x| < \rho$. If $f'(x) = g'(x)$ for all $|x| < \rho$ then there exists a constant $c \in \mathbb{Q}_p$ such that $f(X) = g(X) + c$ as power series.*

Proof. $f'(X) = \sum_{n=1}^\infty na_nx^{n-1}$, $g'(X) = \sum_{n=1}^\infty nb_nx^{n-1}$.
Proposition 5 에 의해 $a_n = b_n$ for $n \geq 1$ □

1.2 Strassman's Theorem

Theorem 3 ([Gou20] Theorem 5.6.1. Strassman's theorem). *Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$ a non-zero power series with coefficients in $\mathbb{Q}_p$ and suppose $\lim_{n\to\infty} a_n = 0$ so $f(x)$ converges for all $x \in \mathbb{Z}_p$. Let N be the integer defined by the two conditions:*

$$|a_N| = \max_n |a_n|$$

$$|a_n| < |a_N|$$

for $n > N$
Then the function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ defined by $x \mapsto f(x)$ has at most N zeros.

Proof. Induction on N.
$N = 0$ case: $|a_0| > |a_n|$ for $n \geq 1$
If f has zero, $|a_0| = |a_1 x + a_2 x^2 + \cdots| \leq \max_{n\geq 1} |a_n|$ contradiction.
Inductive step: suppose $|a_N| = \max_n |a_n|$ and $|a_n| < |a_N|$ for $n > N$, $f(\alpha) = 0$ for $\alpha \in \mathbb{Z}_p$.
Then

$$f(x) = f(x) - f(\alpha) = \sum_{n\geq 1} a_n(x^n - \alpha^n)$$

$$= (x-\alpha) \sum_{n\geq 1} \sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}$$

This double series are exchangable, (check!)

$$f(x) = (x-\alpha) \sum_{j=0}^{\infty} b_j x^j$$

$b_j = \sum_{k=0}^{\infty} a_{j+1+k}\alpha^k$ satisfies $b_j \to 0$, $\sum b_j X^j$ is clearly nonzero. Finally,

$$|b_j| \leq \max_{k\geq 0} |a_{j+1+k}| < |a_N|$$

for $j \geq N$

$$|b_{N-1}| = |a_N + a_{N+1}\alpha + \cdots| = |a_N|$$

Strassman theorem applied to $g(X) = \sum_{j=0}^{\infty} b_j X^j$ has at most $N-1$ roots. □

Corollary 4 ([Gou20] Corollary 5.6.2). *Let $f(X) = \sum a_n X^n$ be a non-zero power series which converges on $\mathbb{Z}_p$, and $\alpha_1, \cdots, \alpha_m$ be the roots of $f(X)$ in $\mathbb{Z}_p$. Then we can find a power series $g(X)$ which converges on $\mathbb{Z}_p$ but has no zeros in $\mathbb{Z}_p$, for which*

$$f(X) = (X-\alpha_1)\cdots(X-\alpha_m)g(X)$$

Corollary 5 ([Gou20] Corollary 5.6.6). *$f(X) = \sum_n a_n X^n$ be a p-adic power series, and suppose that $f(X)$ is entire, that $f(x)$ converges for every $x \in \mathbb{Q}_p$. Then $f(X)$ has at most countably many zeros. Furthermore, if the set of zeros is not finite then zeros form a sequence α_n with $|\alpha_n| \to \infty$*

Proof. Think at each bounded disk $p^m\mathbb{Z}_p$ □

그러면 이런 표현이 가능하면 좋을 것 같다..

$$f(X) = h(X) \prod (1 - \alpha^{-1}X)$$

$h(X)$ do not have zero... α ranges over all zeros.

Remark 2. *In complex analysis, there is a Hadamard's factorization theorem.*
f be a entire function with growth order ρ_0. If f has (non-zero) zeros of f, $a_1, a_2, \cdots$ then

$$f(z) = e^{P(z)} z^m \prod_{n=1}^{\infty} E_k(z/a_n)$$

where P is a polynomial of degree less or equal than k.
Here, $E_k(z) = (1-z)e^{z+z^2+\cdots+z^k/k}$
그리고, Weierstrass construction이라고 불리우는, $a_n \in \mathbb{C}$ that $|a_n| \to \infty$ then there exists an entire function that vanishes precisely at $z = a_n$.

가능하긴 한데... 의미 없는 경우들도 존재한다. $\mathbb{Q}_5$, $X^2 - 2$ 같은... 근이 없으면 딱히 아무것도 할 수 있는게 없다... 실수에서 대응되는 복소수처럼 모든 다항식이 근을 가지는 그런 공간이면 좋을텐데... $\mathbb{Q}_p$ 도 이러한 수체계가 존재할까? 추후에 이것에 대한 대답을 할 수 있게 된다 ($\mathbb{C}_p$)

1.3 Logarithm and Exponential Functions

이렇게 power series에 대해 많이 논의했는데, 그 결과 꽤 유용한 함수들을 얻게 된다.
Define the logarithm

$$\log(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} + \cdots$$

this function is defined for all prime p
Radius of convergence? $a_n = \frac{(-1)^n}{n}$ so $|a_n| = p^{v_p(n)}$, $\sqrt[n]{|a_n|} \to 1$, $\rho = 1$.
For $|x| = 1$, the $|a_n|$ do not tend to zero so

Lemma 5 ([Gou20] Lemma 5.7.1). *The series*

$$f(X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} + \cdots$$

converges for $|x| < 1$ and diverges otherwise.

We define p-adic logarithm $\log_p : 1 + p\mathbb{Z}_p \to \mathbb{Q}_p$ by

$$\log_p(x) = \log(1 + (x-1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}$$

Proposition 3 ([Gou20] Proposition 5.7.3). *Suppose $a, b \in 1 + p\mathbb{Z}_p$ then*

$$\log_p(ab) = \log_p(a) + \log_p(b)$$

Proof. Let $a = 1+x, b = 1+y$ then we let $f(x) = \log_p(1+x)$, by Proposition 6 $f'(x) = \sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1+x}$
Fixing y, define $g(x) = \log_p((1+x)(1+y))$ converges for $|x| < 1$. Then

$$g'(x) = (1+y)f'(y + (1+y)x) = \frac{1+y}{1+y+(1+y)x} = \frac{1}{1+x}$$

(Note: 미분의 연쇄법칙은 성립한다!)
So $g'(x) = f'(x)$, they are both defined by power series, converge for $|x| < 1$. $g(x) = f(x) + c$ by Corollary 3. $c = g(0) - f(0) = f(y)$. Thus $g(x) = f(x) + f(y)$ □

Problem 1.1 ([Gou20] Problem 176, 177, 178). *We know from Chapter 4, that the p-adic number has mth-root of unity (in the case $p \nmid m$) if and only if $m \mid p-1$. Now we consider the case $p \mid m$*
(a) $p \neq 2$
Let $x = 1 + py$ where $y \in \mathbb{Z}_p$, then

$$\log_p(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} p^n y^n = g(y)$$

Then $g(y)$ satisfies Strassman's theorem assumption with $N = 1$. Thus, $\log_p(x) = 0$ if and only if $x = 1$.
Thus if $x^p = 1$ for $x \in \mathbb{Q}_p$ then $x \in \mathbb{Z}_p$ so $x \equiv 1 (mod\ p)$.
$p \log_p(x) = \log_p(1) = 0$ so $\log_p(x) = 0$, $x = 1$...
$p \neq 2$ then there does not exist such root of unity
(b) $p = 2$
Similarly, $x = 1 + 2y$ and

$$\log_2(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} 2^n y^n = g(y)$$

$g(y) = 2y - 2y^2 + \frac{8}{3}y^2 + \cdots$ 이므로 $N = 2$, Strassman theorem gives $\log_2(x) = 0$ has at most two roots, and it is $x = \pm 1$.
So primitive 2-root of unity exists (and it is -1), but if $x^4 = 1$ then $4 \log_2(x) = 0$ so $x = \pm 1$.

As a conclusion $\mathbb{Q}_p$,
For $p = 2$ the only roots of unity in $\mathbb{Q}_p$ are ± 1
For $p \neq 2$, $\mathbb{Q}_p$ contains all the $(p-1)$st roots of unity and no others.

Exponential을 살펴봅시다.

$$exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$$

Region of convergence?

Lemma 6 ([Gou20] Lemma 5.7.4). *Let p be a prime, then*

$$v_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor < \frac{n}{p-1}$$

Lemma 7 ([Gou20] Lemma 5.7.5). *Let $g(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$ then $g(x)$ converges if and only if $|x| < p^{-1/(p-1)}$*

Proof. By previous lemma, $\rho \geq p^{-1/(p-1)}$ so series converges for $|x| < p^{-1/(p-1)}$.
For $|x| = p^{-1/(p-1)}$, $n = p^m$ then

$$v_p(n!) = \frac{p^m - 1}{p-1}$$

$$v_p(\frac{x^n}{n!}) = \frac{p^m}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}$$

so does not tend to zero, do not converges □

For $p \neq 2$, above is equivalent to $|x| < 1$ so $p\mathbb{Z}_p$. But for $p = 2$, above region is $|x| < 1/2$, so $4\mathbb{Z}_2$.
We define $exp_p : D \to \mathbb{Q}_p$ as above for $D = B(0, p^{-1/(p-1)})$.

Proposition 4 ([Gou20] Proposition 5.7.7). *If $x, y \in D$ we have $x + y \in D$ and*

$$\exp_p(x+y) = \exp_p(x)\exp_p(y)$$

Proof. Double seires의 교환으로부터

$$\begin{aligned} \exp_p(x+y) &= \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{(n-k)!k!} x^{n-k} y^k \\ &= \Big(\sum_{m=0}^{\infty} \frac{x^m}{m!} \Big) \Big(\sum_{k=0}^{\infty} \frac{y^k}{k!} \Big) \end{aligned}$$

□

마지막으로, log와 exp에 대해 저희가 기대하는 그 것도 성립합니다.

Proposition 5 ([Gou20] Proposition 5.7.8). *Let $x \in \mathbb{Z}_p$, $|x| < p^{-1/(p-1)}$ then we have*

$$|\exp_p(x) - 1| < 1$$

and

$$\log_p(\exp_p(x)) = x$$

Conversely, if $|x| < p^{-1/(p-1)}$ we have

$$|\log_p(1+x)| < p^{-1/(p-1)}$$

and

$$\exp_p(\log_p(1+x)) = 1 + x$$

Proof. 합성함수에 대한 정리. $x = 0$은 자명하게 성립한다.

$$|\frac{x^n}{n!}| = |x|^n \cdot p^{v_p(n!)} < |x|^n p^{n/(p-1)}$$

만약 $|x| < p^{-1/(p-1)}$,

$$|\exp_p(x) - 1| = |\sum_{n=1}^{\infty} \frac{x^n}{n!}| < 1$$

조금 더 좋은 estimate으로, $n \geq 2$일 때

$$v_p(\frac{x^{n-1}}{n!}) = (n-1)v_p(x) - v_p(n!) > \frac{n-1}{p-1} - \frac{n-s}{p-1} = \frac{s-1}{p-1} \geq 0$$

where if $n = a_0 + a_1 p + \cdots + a_k p^k$, $s = a_0 + a_1 + \cdots a_k$...
(In fact, $v_p(n!) = \frac{n-s}{p-1}$)
Thus, $|x^n/n!| < |x|$ for $n \geq 2$, $|\exp_p(x) - 1| = |x|$. 이제 Theorem 1 (혹은 Theorem 5.4.3)에서 $f(X) = \log_p(1+X)$, $g(X) = \exp_p(X) - 1$이라 둘 때 (a), (b)와 더불어 (c)의

$$|\frac{x^n}{n!}| \leq |\exp_p(x) - 1| = |x|$$

가 성립하므로, $\log_p(\exp_p(x)) = x$

반대 방향.. $f(X) = \exp_p(X)$, $g(X) = \log_p(1+X)$를 적용시키려 한다.
$|\frac{x^n}{n}| \leq |\frac{x^n}{n!}| < |x|$ for $n \geq 2$
따라서 $|\log_p(1+x)| = |x| < p^{-1/(p-1)}$이 성립하고, (a),(b),(c)가 모두 만족되므로

$$\exp_p(\log_p(1+x)) = 1 + x$$

□

1.4 Application : Multiplicative Structure of $\mathbb{Z}_p^\times$

$\mathbb{Z}_p^\times$를 분석하고 싶다. Hensel Lemma로부터 $\mathbb{Z}_p^\times$ contains the $(p-1)$ the roots of unity.

$$U_1 = \{x \in \mathbb{Z}_p^\times : |x-1| < 1\} = 1 + p\mathbb{Z}_p$$

$$U_p = \{x \in \mathbb{Z}_p^\times : |x-1| < p^{-1/(p-1)}\} = 1 + q\mathbb{Z}_p$$

$q = 4$ if $p = 2$, $q = p$ if p odd.
- U_1, U_p are subgroups of $\mathbb{Z}_p^\times$

Proposition 6 ([Gou20] Proposition 5.8.1)**.** *Let* $\mathbb{Z}_p^+ = (\mathbb{Z}_p, +)$ *additive group and*

$$W = \{x \in \mathbb{Z}_p : |x| < p^{-1/(p-1)}\} = q\mathbb{Z}_p$$

considered as a subgroup of $\mathbb{Z}_p^+$
(a) p-adic logarithm defines homomorphism of groups

$$\log_p : U_1 \to \mathbb{Z}_p^+$$

and the image is contained in $p\mathbb{Z}_p$
(b) p-adic logarithm defines an isometric isomorphism of groups

$$\log_p : U_p \to W$$

with inverse $\exp_p$*. In particular* U_p *is torsion-free*

Proof. $\log_p$가 homomorphism인 것은... 우리가 알고.. $\exp_p$ 역시 homomorphism... (b)의 isomorphism 역시 이미 한 내용이다...
$p \neq 2$이면, $W = p\mathbb{Z}_p$이므로 (a),(b)는 동치다.
$p = 2$ 이면, $\log_2(U_1) = W = 4\mathbb{Z}_2$인 것을 보일 수 있다.
마지막으로 torsion-free까지... □

Corollary 6 ([Gou20] Corollary 5.8.2)**.** *For any prime* p*, we have an isomorphism*

$$\mathbb{Z}_p^\times \cong V \times U_p$$

(a) V *is the set of roots of unity in* $\mathbb{Q}_p$ *which forms a subgroup of* $\mathbb{Z}_p^\times$
(b) $V \cong (\mathbb{Z}/q\mathbb{Z})^\times$ *so cyclic group of order* $\varphi(q)$
We also know that U_p *is torsion-free group and* V *is the torsion part.*

Proof. $\mathbb{Z}_p^\times$ 가 roots of unity를 포함하는 것은 알고 있다. (Cyclic group of order $p-1$ when p is odd, order 2 when $p = 2$) 그리고 각 root of unity는 modulo q 로 Noncongruent ($p = 2$: $-1, 1$이었고, $p \neq 2$: 각 $1, 2, \cdots, p-1$마다 하나씩..
따라서 $\mathbb{Z}_p^\times$의 각 원소는 $U_p \times V$ 꼴로 unique하게 적힘. 그리고 곱셈구조를 보존하므로... isomorphic하다. □

즉, logarithm을 통하여 $\mathbb{Z}_p^\times$의 구조는 roots of unity에 U_p를 곱한 형태인데,
roots of unity는 cyclic group을 이루고
U_p 라 불리우는 것은 사실은 $\mathbb{Z}_p^+$, 즉 덧셈 구조와 똑같은 모습으로 생겼다고 결론지을 수 있겠습니다.

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.