p-adic numbers

Dongryul Kim

제 1 장 p-adic order

이 장에서는 p-adic order의 기본적인 내용에 대해 살펴봅시다. 먼저 p-adic order의 정의와 관련된 식들을 알아보고, 그 다음 유명한 "Lifting the Exponent" 정리를 증명할 것입니다. 올림피아드 문제에서 어떻게 p-adic order가 사용되는지, 그리고 어떤 테크닉들이 있는지 함께 문제를 풀며 공부해봅시다.

§1. p-adic order의 정의

양의 정수는 소수들로 유일하게 소인수분해 된다. 이것은 산술의 기본 정리(Fundamental Theorem of Arithmetic)가 말하는 내용이다. 이것을 수식으로 표현하자면 다음과 같다. 임의의 0이 아닌 정수 n에 대해, $n=\pm p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$이 성립하는 소수들 $p_1<p_2<\cdots<p_k$와 양의 정수들 $e_1,e_2,\cdots,e_k$가 유일하게 존재한다.

조금 더 가보자. 이것을 사용하면 다음과 같은 사실도 알 수 있다. 임의의 0이 아닌 유리수 q에 대해, $q=\pm p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$이 성립하는 소수들 $p_1<p_2<\cdots<p_k$와 정수들 $e_1,e_2,\cdots,e_k$가 유일하게 존재한다. 이것은 임의의 0이 아닌 유리수가 서로소인 두 정수의 비로 (거의) 유일하게 표현된다는 것으로부터 쉽게 증명할 수 있는 사실이다. 벌써 우리는 p-adic order의 정의를 받아들일 준비가 되었다.

임의의 소수 p를 생각하자. 이때 정수 n의 **p-adic order** $\nu_p(n)$은 n을 소인수분해 하였을 때 p의 지수로 정의한다. 또한 편의상 $\nu_p(0)=\infty$라 한다. 즉, 엄밀하게 정의하면 함수 $\nu_p:\mathbb{Z}\to\mathbb{Z}_{\geq 0}\cup\{\infty\}$는

$$\nu_p(n)=\max\{0\leq k\in\mathbb{Z}:p^k|n\}$$

와 같이 표현된다.

위에서 소인수분해를 유리수 범위까지 확장한 것과 마찬가지로, p-adic order의 정의도 유리수의 범위까지 확장할 수 있다. 유리수를 소인수분해 하였을 때 p의 지수를 $\nu_p(q)$로 정의하는 것이다. 유리수 q를 기약분수로 나타내었을 때 $q=b/a$라 한다면, q의 **p-adic order**은

$$\nu_p(b/a)=\nu_p(b)-\nu_p(a)$$

이 된다. 이때 ν_p는 $\mathbb{Q}\to\mathbb{Z}\cup\{\infty\}$가 된다.

물론 올림피아드 정수론에서 유리수를 다루는 일은 매우 드물고, 유리수를 다루느니 정수를 곱한 후 정수를 다루는 것이 머리가 덜 아픈 경우가 대부분이다. 때문에 유리수 범위에서 정의된 p-adic order은 사용할 일이 거의 없을 것이다. 하지만 2장에서 나올 내용들 때문에 밑밥을 깔아야만 한다는 것을 이해해주길 바란다.

Example. 임의의 소수 p에 대해, $\nu_p(1)=0$이고, $\nu_p(p)=1$, $\nu_p(1/p)=-1$이다. 또한 예를 들어 $q=10/9$라 하면, $\nu_2(q)=1$, $\nu_5(q)=1$, $\nu_3(q)=-2$가 되며 임의의 다른 소수 p에 대해서는 $\nu_p(q)=0$이다.

p-adic order은 다음과 같은 기본적인 성질들을 가지고 있다. 증명은 간단하므로 독자에게 맡기겠다.

Proposition 1.1.

(i) 어떤 유리수 q가 정수일 필요충분조건은 임의의 소수 p에 대해 $\nu_p(q)\geq 0$인 것이다. 또한 두 정수 m과 n에 대해 m이 n을 나눌 필요충분조건은 임의의 소수 p에 대해 $\nu_p(m)\geq\nu_p(n)$인 것이다.

(ii) 임의의 유리수 m과 n에 대해 $\nu_p(mn)=\nu_p(m)+\nu_p(n)$이다.

(iii) 임의의 유리수 m과 n에 대해 $\nu_p(m+n)\geq\min\{\nu_p(m),\nu_p(n)\}$이다.

(iv) 유리수 m과 n에 대해 $\nu_p(m)\neq\nu_p(n)$이라면 $\nu_p(m+n)=\min\{\nu_p(m),\nu_p(n)\}$이다.

(v) 임의의 유리수 $m\neq 0$에 대해 다음이 성립한다.

$$m=\prod_p p^{\nu_p(m)}$$

(vi) 양의 정수 n에 대해 다음이 성립한다.

$$\nu_p(n!)=\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor$$

(vii) 양의 정수들 $a_1,\cdots,a_k$에 대해 $\nu_p(\gcd\{a_1,\cdots,a_k\})=\min\{\nu_p(a_1),\cdots,\nu_p(a_k)\}$이다.

(viii) 양의 정수들 $a_1,\cdots,a_k$에 대해 $\nu_p(lcm\{a_1,\cdots,a_k\})=\max\{\nu_p(a_1),\cdots,\nu_p(a_k)\}$이다.

별것 없는 것처럼 보이겠지만, Proposition 1.1.의 내용들만 가지고도 정말 많은 문제를 풀 수 있다. 예제들 몇 개만 살펴보자. 풀이를 먼저 보는 것은 실력 향상에 도움이 되지 않음을 명심하고 예제더라도 꼭 풀어본 후에 풀이를 보도록 하자!

Problem 1.2. *임의의 양의 정수 n에 대해 $n!$이*

$$\prod_{k=0}^{n-1}(2^n-2^k)$$

를 나눔을 보여라.

Solution. 앞에서 보인 Proposition 1.1.의 (i)에 의해 임의의 소수 p에 대해

$$\nu_p(n!)\leq\nu_p\left(\prod_{k=0}^{n-1}(2^n-2^k)\right)=\sum_{k=0}^{n-1}\nu_p(2^n-2^k)$$

임을 보이면 충분하다. 이때 Proposition 1.1.의 (vi)에 의해

$$\nu_p(n!)=\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor\leq\sum_{i=1}^{\infty}\frac{n}{p^i}=\frac{n}{p-1}$$

이므로

$$\left\lfloor \frac{n}{p-1} \right\rfloor \le \sum_{k=0}^{n-1} \nu_p(2^n - 2^k)$$

임을 보이면 된다.

우선 $p=2$인 경우 $\nu_2(2^n-2^k)=k$이므로 우변은 $n(n-1)/2$인 반면 좌변은 n이다. 그러므로 $n \ge 3$인 경우에 성립함을 알 수 있고, $n=1,2$인 경우는 따로 확인해줄 수 있다.

p가 홀수인 경우를 생각해보자. $2^{t(p-1)}-1$은 p의 배수이므로 $\nu_p(2^n - 2^{n-t(p-1)}) \ge 1$이다. 그러므로

$$\sum_{k=0}^{n-1} \nu_p(2^n-2^k) \ge \sum_{t=1}^{\lfloor n/(p-1) \rfloor} \nu_p(2^n - 2^{n-t(p-1)}) \ge \left\lfloor \frac{n}{p-1} \right\rfloor$$

이 성립한다. 두 경우 모두에 대해 부등식이 증명되었다.

□

Problem 1.3. *양의 정수 n을 p진법으로 나타내었을 때 각 자릿수의 합을 $s_p(n)$으로 표기하자. 임의의 양의 정수 n과 n보다 작은 양의 정수들 a와 b에 대해, 소수 p가 존재하여*

$$\min\{s_p(a)+s_p(n-a), s_p(b)+s_p(n-b)\} \ge p-1+s_p(n)$$

이 성립함을 보여라.

Solution. $s_p(n)$을 조금 더 잘 해석할 필요가 있다. 우리는 다음이 성립함을 보일 것이다.

$$\nu_p(n!) = \frac{n-s_p(n)}{p-1}$$

n을 p진법 전개하여 표현하였을 때 $n=a_0+a_1p+\cdots+a_kp^k$이라 하자. 이때 Proposition 1.1. 의 (vi)에 의해

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^{k}\sum_{j=i}^{k} a_j p^{j-i} = \sum_{j=1}^{k} \left(a_j \sum_{i=1}^{j} p^{j-i} \right) = \sum_{j=1}^{k} a_j \frac{p^j-1}{p-1} = \frac{n-s_p(n)}{p-1}$$

임을 알 수 있다.

이제 이 식을 사용하여 $s_p(a)+s_p(n-a)-s_p(n)$를 정리해보면,

$$\begin{aligned} & s_p(a)+s_p(n-a)-s_p(n) \\ &= \{a-(p-1)\nu_p(a!)\}+\{n-a-(p-1)\nu_p((n-a)!)\}-\{n-(p-1)\nu_p(n!)\} \\ &= (p-1)\{\nu_p(n!)-\nu_p(a!)-\nu_p((n-a)!)\} \\ &= (p-1)\nu_p\left(\binom{n}{a}\right) \end{aligned}$$

이 된다. 즉, $s_p(a)+s_p(n-a) \ge p-1+s_p(n)$은 결국 $\binom{n}{a}$가 p의 배수인 것이랑 동치이다. 문제에서 물어보는 것은 $\binom{n}{a}$와 $\binom{n}{b}$를 동시에 나누는 소수 p가 존재함을 보이는 것이므로 우리는 두 수가 서로소가 아님을 보여야 한다.

우선 $\binom{n}{a}$와 $\binom{n}{n-a}$는 같으므로 편의상 $a \le n/2$라 가정할 수 있다. 마찬가지로 $b \le n/2$라 하자. 만약 $\binom{n}{a}$와 $\binom{n}{b}$가 서로소라면, 등식

$$\binom{n}{a}\binom{n-a}{b} = \frac{n!}{a!b!(n-a-b)!} = \binom{n}{b}\binom{n-b}{a}$$

에서 $\binom{n}{a}$이 $\binom{n-b}{a}$를 나누어야 하는데, 둘 다 0이 아니고, $\binom{n}{a}$이 $\binom{n-b}{a}$보다 당연히 크므로 모순이다. 즉, $\binom{n}{a}$와 $\binom{n}{b}$는 서로소가 아니고, 둘을 동시에 나누는 소수 p가 존재한다.

□

다음 문제는 1984년에 Miklós Schweitzer 경시대회에 출제되었던 적이 있는 문제이다. 당시 Erdős는 Sylvester과 Schur의 $n \geq 2k$이면 $n(n-1)\cdots(n-k+1)/k!$을 나누는 k 보다 큰 소수가 항상 존재한다는 정리를 사용하여 증명하였다. 그런데 3년 후에 Szegedi라는 사람이 이 문제의 초등적인 풀이를 제시하였다. 매우 어려운 문제이나 그래도 최소 두세 시간 정도는 투자해본 후 풀이를 읽기를 바란다.

Problem 1.4. *양의 정수 a와 b가 주어져있다. 임의의 소수 p에 대해 a를 p로 나눈 나머지가 b를 p로 나눈 나머지 이하라면 $a=b$임을 보여라.*

Solution. a를 p로 나눈 나머지를 $a\%p$로 표기하자. 우선 충분히 큰 소수 p에 대해 조건을 적용하면 $a \leq b$임은 쉽게 알 수 있다. 결론을 부정하여 $a<b$라고 가정해보자.
만일 $b/2 < a < b$라면, $b-a=c$라 하자. 자명히 $c<b/2$가 되고, $c\%p \equiv b\%p - a\%p \pmod{p}$인데, $0 \leq b\%p - a\%p < p$이므로 $c\%p = b\%p - a\%p \leq b\%p$이다. 즉, a를 c로 대체해도 문제의 조건이 성립하므로 $a \leq b/2$인 경우에만 모순을 이끌어내도 충분하다.
우리는 $\binom{b}{a}$의 p-adic order을 관찰할 것이다. 우선 $p>a$인 경우를 살펴보자. 조건에 의해 $a=a\%p \leq b\%p$이므로 $b, b-1, \cdots, b-a+1$들 중 p의 배수는 존재하지 않는다. 즉, $\binom{b}{a}$는 절대로 p의 배수가 될 수 없다.
이번에는 $p \leq a$인 경우를 살펴보자. 편의상 $m(p) = \lfloor \log_p b \rfloor$ 라 하면,

$$\begin{aligned}\nu_p\left(\binom{b}{a}\right) &= \sum_{i=1}^{\infty}\left(\left\lfloor \frac{b}{p^i} \right\rfloor - \left\lfloor \frac{a}{p^i} \right\rfloor - \left\lfloor \frac{b-a}{p^i} \right\rfloor \right) \\ &= \sum_{i=1}^{m(p)}\left(\left\lfloor \frac{b}{p^i} \right\rfloor - \left\lfloor \frac{a}{p^i} \right\rfloor - \left\lfloor \frac{b-a}{p^i} \right\rfloor \right)\end{aligned}$$

임을 알 수 있다. 이때, 조건에서 $b\%p = a\%p + (b-a)\%p$이므로 우변에서 $i=1$인 항의 값은 무조건 0이 되어야 한다. 또한 우변의 각 항은 0 또는 1이다. 그러므로 우변의 최댓값은

$$\nu_p\left(\binom{b}{a}\right) = \sum_{i=2}^{m(p)}\left(\left\lfloor \frac{b}{p^i} \right\rfloor - \left\lfloor \frac{a}{p^i} \right\rfloor - \left\lfloor \frac{b-a}{p^i} \right\rfloor \right) \leq m(p)-1$$

이 된다.
Proposition 1.1.의 (v)에 의해

$$\binom{b}{a} = \frac{b(b-1)\cdots(b-a+1)}{a!} = \prod_{p \leq a} p^{\nu_p\left(\binom{b}{a}\right)} \leq \prod_{p \leq a} p^{m(p)-1}$$

임을 알 수 있다. 이때,

$$\frac{a!}{\prod_{p \leq a} p} < a^{a-\pi(a)} \leq (b-a)^{a-\pi(a)} < \frac{(b-a+1)\cdots(b-1)b}{\prod_{p \leq a} p^{m(p)}}$$

이므로 모순이다. (마지막 부등식은 $p^{m(p)}$들이 b 이하의 서로 다른 수들이기 때문에 성립한다.) 그러므로 $a=b$가 성립해야 한다.

□

마지막으로 연습문제들을 풀면서 실력을 다져보자.

< 연습문제 >

1. 임의의 양의 정수 n에 대해 $n!$이

$$\prod_{k=0}^{n-1}(2^n-2^k)$$

를 나눔을 보여라.

2. 임의의 정수들 $a_1,a_2,\cdots,a_n$에 대해

$$\prod_{1\le i<j\le n}\frac{a_i-a_j}{i-j}$$

는 정수임을 보여라.

3. 임의의 $n>1$에 대해 $2^{n-1}+1$은 n의 배수가 될 수 없음을 보여라.

4. 양의 정수들의 무한수열 $a_1,a_2,\cdots$이 임의의 정수 m과 n에 대해 $\gcd(a_m,a_n)=a_{\gcd(m,n)}$을 만족시킨다. 이때 임의의 n에 대해 $a_n=\prod_{d|n}b_d$이 성립하는 정수들의 무한수열 $b_1,b_2,\cdots$이 존재함을 증명하여라.

5. 다음 조건을 만족하는 양의 정수들 n과 $n_1<n_2<\cdots<n_k$는 존재하지 않음을 증명하여라.

$$\frac{1}{10^n}=\frac{1}{n_1!}+\frac{1}{n_2!}+\cdots+\frac{1}{n_k!}$$

6. 임의의 양수 $c>0$에 대해, n^2+1의 최대 소인수가 cn보다 크게 되는 양의 정수 n이 무한히 많이 존재함을 보여라.

7. (Tuymaada 2004) 양의 정수 n에 대해, $m+1,m+2,\cdots,m+n$이 모두 합성수가 되는 $m>n^{n-1}$을 생각하자. 이때 서로 다른 소수들 $p_1,p_2,\cdots,p_n$이 존재하여 임의의 $1\le k\le n$에 대해 p_k가 $m+k$를 나누게 됨을 증명하여라.

8. 양의 정수 $1<a<b<n$이 $a!b!=n!$을 만족시킨다고 하자. 이때 $n<b+1000\log\log n$임을 보여라.

9. 소수 p와 정수 $n>s+1$이 주어져있다. $d=\lfloor (n-s-1)/(p-1)\rfloor$이라 할 때,

$$\sum_{p|k,0\le k\le n}(-1)^k k^s\binom{n}{k}$$

는 p^d의 배수임을 보여라.

§2. Lifting the Exponent

2절에서는 Lifting the Exponent(줄여서 LTE)라는 보조정리를 다룰 것이다. LTE는 기본적으로 두 거듭제곱수의 차나 합의 p-지수를 계산하는 보조정리이다. LTE를 알고 있다면, 예를 들어 "$3^{2^n}-1$의 2-지수는 얼마일까?"라는 질문에 대한 답을 바로 할 수 있다. 정리의 statement 자체는 매우 간단하지만 유용하게 쓰일 수 있어 알고 있다면 많은 경우에서 우리의 생각을 덜어줄 수 있다. 본격적으로 정리를 증명하기에 앞서 정리의 일부분인 다음 보조정리들을 증명하자.

Lemma 2.1. *양의 정수 n과 서로 다른 정수 x와 y를 생각하자. 어떤 소수 p가 x와 y 둘 모두와 서로소인데, $x-y$를 나눈다고 하자. 만약 p와 n도 서로소라면,*

$$\nu_p(x^n-y^n)=\nu_p(x-y)$$

이 성립한다.

Proof. $(x^n-y^n)/(x-y)$가 p의 배수가 아님을 보이면 된다. 실제로 $x\equiv y\,(\mathrm{mod}p)$이므로

$$\frac{x^n-y^n}{x-y}=x^{n-1}+x^{n-2}y+\cdots+y^{n-1}\equiv nx^{n-1}\,(\mathrm{mod}p)$$

인데, n은 p의 배수가 아니고, x도 p의 배수가 아니므로 좌변도 p의 배수가 아니다. 즉, $\nu_p(x^n-y^n)=\nu_p(x-y)$이 된다.

□

Lemma 2.2. 홀수인 소수 p와 서로 다른 정수 x와 y를 생각하자. p가 x와 y 둘 모두와 서로소인데, $x-y$를 나눈다고 할 때,

$$\nu_p(x^p-y^p)=\nu_p(x-y)+1$$

이 성립한다.

Proof. $\nu_p((x^p-y^p)/(x-y))=1$임을 보여야 한다. 즉, $(x^p-y^p)/(x-y)$는 p의 배수인데, p^2의 배수는 아님을 보여야 한다.
우선 $y=x+kp$라 하고 $x^{p-1-i}y^i$를 $\mathrm{mod}p^2$으로 살펴보자.

$$\begin{aligned}x^{p-1-i}y^i=x^{p-1-i}(x+kp)^i&=x^{p-1-i}\sum_{j=0}^{i}\binom{i}{j}x^{i-j}(kp)^j\\&\equiv x^{p-1-i}(x^i+ix^{i-1}(kp))\\&=x^{p-1}+ix^{p-2}kp\ \ (\mathrm{mod}p^2)\end{aligned}$$

이므로

$$\begin{aligned}\frac{x^p-y^p}{x-y}&=x^{p-1}+x^{p-2}y+\cdots+y^{p-1}\\&\equiv px^{p-1}+\frac{p(p-1)}{2}x^{p-2}kp\\&\equiv px^{p-1}\ \ (\mathrm{mod}p^2)\end{aligned}$$

이다. x는 p와 서로소이므로 $(x^p-y^p)/(x-y)$는 p의 배수가 되지만 p^2의 배수은 안 된다. 그러므로 $\nu_p((x^p-y^p)/(x-y))=1$이다.

□

이제 이 두 보조정리를 이용하면 다음의 정리를 바로 증명할 수 있다.

Theorem 2.3. (First Form of LTE) *양의 정수 n과 서로 다른 정수 x와 y를 생각하자. 어떤 <u>홀수</u> 소수 p가 x와 y 둘 모두와 서로소인데, $x-y$를 나눈다고 하자. 이때*

$$\nu_p(x^n-y^n)=\nu_p(x-y)+\nu_p(n)$$

이 성립한다.

Proof. $n=p^ek$라 하자. (단, k는 p와 서로소인 수다.) 자명히 $e=\nu_p(n)$이 될 것이다.
우선 Lemma 2.2.에 의해 $\nu_p\left(x^{p^{i+1}}-y^{p^{i+1}}\right)=\nu_p\left(x^{p^i}-y^{p^i}\right)+1$이므로 이 식을 연속적으로 적용시키면 $\nu_p\left(x^{p^e}-y^{p^e}\right)=\nu_p(x-y)+e$임을 알 수 있다. 한편, Lemma 2.1.에 의해

$$\nu_p(x^n-y^n)=\nu_p\left(x^{p^ek}-y^{p^ek}\right)=\nu_p\left(x^{p^e}-y^{p^e}\right)$$

이므로 결과적으로

$$\nu_p(x^n-y^n)=\nu_p\left(x^{p^e}-y^{p^e}\right)=\nu_p(x-y)+e=\nu_p(x-y)+\nu_p(n)$$

이 성립한다.

□

Corollary 2.4. (Second Form of LTE) *양의 <u>홀수</u> n과 서로 다른 정수 x와 y를 생각하자. 어떤 <u>홀수</u> 소수 p가 x와 y 둘 모두와 서로소인데, $x+y$를 나눈다고 하자. 이때*

$$\nu_p(x^n+y^n)=\nu_p(x+y)+\nu_p(n)$$

이 성립한다.

Proof. Theorem 2.3.에서 y에 $-y$를 대입하자. 그러면

$$\nu_p(x^n+y^n)=\nu_p(x^n-(-y)^n)=\nu_p(x-(-y))+\nu_p(n)=\nu_p(x+y)+\nu_p(n)$$

임을 알 수 있다.

□

LTE를 이용함에 있어 학생들이 주로 저지르는 실수는 크게 두 가지가 있다. 첫 번째로, $x\pm y$가 p의 배수임을 확인하지 않은 채 사용하는 것이다. 이 경우 대부분 말도 되지 않는 결과가 나오게 된다. 두 번째는 $p=2$일 때 정리를 사용하는 것이다. 안타깝게도 우리가 증명한 정리들은 $p=2$를 예외로 둔다. 예를 들어 $\nu_2(3^2-1^2)=3\neq 2=\nu_2(3-1)+\nu(2)$이다. 문제가 어디서 발생했는지를 찾아보면, Lemma 2.2.에서 x와 y가 홀수일 경우 $x+y$가 4의 배수가 아니라는 보장을 하지 못해 성립하지 않게 되었다. 하지만 이것은 $x-y$가 4의 배수라는 추가적인 조건을 가정해줌으로써 해결된다. 실제로 다음 정리가 성립한다.

Theorem 2.5. (LTE for the case $p=2$) *양의 정수 n과 서로 다른 홀수 x와 y를 생각하자. 4가 $x-y$를 나눈다고 할 때,*

$$\nu_2(x^n-y^n)=\nu_2(x-y)+\nu_2(n)$$

이 성립한다.

세부적인 증명 과정은 독자들이 한 번 메워보기를 바란다. (사실 다 말해준 것 같다.) 여기서 n이 짝수라면 다음 따름정리가 성립한다.

Corollary 2.6. *양의 짝수 n과 서로 다른 홀수 x와 y를 생각하자. 이때*

$$\nu_2(x^n-y^n)=\nu_2(x-y)+\nu_2(x+y)+\nu_2(n)-1$$

이 성립한다.

Proof. x와 y가 홀수이므로 x^2-y^2는 4의 배수이다. 즉, Theorem 2.5.에 의해

$$\nu_2(x^n-y^n)=\nu_2(x^2-y^2)+\nu(n/2)=\nu_2(x-y)+\nu_2(x+y)+\nu_2(n)-1$$

이다.

□

같이 문제 몇 개를 살펴보며 LTE의 강력함을 몸소 느껴보자.

Problem 2.7. (Romania TST 2004) *정수 $m\geq 2$가 주어져있다. 어떤 양의 정수 n과 서로소인 임의의 정수 a에 대해 a^m-1이 항상 n의 배수가 된다고 하자. 이때 $n\leq 4m(2^m-1)$임을 보여라.*

Solution. $n=2^ek$인 음 아닌 정수 e와 홀수 k를 생각하자. 자명히 $e=\nu_2(n)$일 것이다.
$k\pm 2$는 홀수이고, k와 서로소이므로 $\gcd(n,k\pm 2)=1$임을 쉽게 확인할 수 있다. a에 $k+2$를 대입해고, 우선 법 k로 관찰해보면,

$$(k+2)^m-1\equiv 2^m-1\equiv 0 \pmod{k}$$

이므로 k는 2^m-1의 약수가 된다.
또한, $(k+1)(k+3)$과 $(k-1)(k-3)$은 모두 8의 배수인데, 둘 중 16의 배수가 아닌 것이 존재한다. 일반성을 잃지 않고 $\nu_2((k-1)(k-3))=3$이라 가정하고 a에 $k-2$를 대입하면,

$$\begin{aligned}\nu_2(n)&\leq \nu_2((k-2)^m-1)=\nu_2((k-1)(k-3))+\nu_2(m)-1\\&\leq \nu_2(m)+2\end{aligned}$$

임을 보일 수 있다. (m이 홀수여도 성립함은 따로 확인해줄 수 있다.) 즉, $e\leq \nu_2(m)+2$가 되므로 $2^e\leq 4m$이다. 그러므로 $n=2^ek\leq 4m(2^m-1)$이 된다.

□

다음 문제는 3rd Mathlinks Contest의 Round 1에 3번으로 나온 문제이다. 112호에 살았던 친구들이 풀이를 제출하지 않은 문제이기도 하다. (ㅎㅎ) 이 문제도 LTE를 사용하면 어렵지 않게 풀 수 있다.

Problem 2.8. (3rd Mathlinks Contest) *a와 b는 서로 다른 양의 유리수이다. 무한히 많은 양의 정수 n에 대해 a^n-b^n이 정수라고 할 때, a와 b는 정수임을 증명하여라.*

Solution. $a=x/z$, $b=y/z$의 꼴로 나타내자. 여기서 x,y,z는 정수이고, $\gcd(x,y,z)=1$이다. 무한히 많은 n에 대해 $(x^n-y^n)/z^n$이 정수이므로 $z^n|x^n-y^n$이 성립한다. a와 b가 정수가 아니라고, 즉 $z>1$이라고 가정해보자.

z를 나누는 임의의 소수 p를 생각해보자. z^n이 x^n-y^n을 나누려면, $\nu_p(x^n-y^n)\geq n\nu_p(z)$가 반드시 성립해야 한다. 이러한 n이 무한히 많은데, x와 y가 동시에 p의 배수인 것은 $\gcd(x,y,z)=1$에 모순이므로 불가능하다. 그러므로 x와 y는 모두 p와 서로소여야만 한다. 이제 $x^{p-1}-y^{p-1}$는 p의 배수이므로 x^k-y^k이 p의 배수인 최소의 k를 생각할 수 있다. $\nu_p(x^n-y^n)\geq n\nu_p(z)$가 성립하는 모든 n에 대하여 x^n-y^n은 p의 배수여야 하므로 n은 k의 배수여야만 한다. 즉, $n=km$인 m이 존재하고, $x^k=A$, $y^k=B$라 하면 $A-B$는 p의 배수가 된다.

만약 p가 홀수라면, LTE에 의하여

$$\begin{aligned} n\nu_p(z) &\leq \nu_p(x^n-y^n)=\nu_p(A^m-B^m) \\ &= \nu_p(A-B)+\nu_p(m)=\nu_p(A-B)+\nu_p(n) \end{aligned}$$

인 n이 무한히 많다. (k는 $p-1$의 약수이므로 $\nu_p(k)=0$이다.) 하지만, $\nu_p(n)\leq \log_p n+1$이므로 모순이다.

만약 $p=2$라면, 마찬가지로 LTE에 의하여

$$\begin{aligned} n\nu_2(z) &\leq \nu_2(x^n-y^n)=\nu_2(A^m-B^m) \\ &\leq \nu_2(A^2-B^2)+\nu_2(m)-1=\nu_2(A^2-B^2)-1+\nu_2(n) \end{aligned}$$

이다. $\nu_2(n)\leq \log_2 n+1$이므로 마찬가지로 모순이 발생한다. 즉, $z=1$이고 a와 b는 모두 정수이다.

□

다음 연습문제들을 풀어보며 LTE를 확실히 몸에 익혀두자.

< 연습문제 >

1. (Romania TST 2009) 2 이상의 양의 정수 a, k와 $(a-1)^k$를 나누는 양의 정수 n이 주어져있다. 이때 n은 $a^{n-1}+a^{n-2}+\cdots+a+1$을 나눔을 보여라.

2. (Gaussian binomial coefficients) 양의 정수 q가 주어져 있다. 임의의 양의 정수 k에 대해 $[k]_q=1+q+\cdots+q^{k-1}$라 하자. 이때 임의의 $m\geq k$에 대해

$$\binom{m}{r}_q=\frac{[m]_q[m-1]_q\cdots[m-r+1]_q}{[r]_q[r-1]_q\cdots[1]_q}$$

이 정수임을 보여라.

3. (Balkan 1993) 정수 $m \geq 2$와 소수 p가 주어져있다. 방정식

$$\frac{x^p + y^p}{2} = \left(\frac{x+y}{2}\right)^m$$

을 만족하는 해 $(x,y) \neq (1,1)$이 존재할 필요충분조건은 $m = p$인 것임을 보여라.

4. n^{p-1}이 $(p-1)^n + 1$을 나누는 소수 p와 양의 정수 $n > 1$의 순서쌍 (n,p)를 모두 구하여라.

5. 임의의 양의 정수 k에 대하여, n^3이 $2^{kn^2} + 3^{kn^2}$을 나누는 양의 정수 n이 무한히 많음을 보여라.

6. (FKMO 2010) 임의로 주어진 소수 p가 있다. 다음 조건들을 모두 만족하는 양의 정수열 $(n_1, n_2, \cdots, n_k)$가 $k = 1$일 때에는 존재하지 않지만 2 이상의 어떤 양의 정수 k 하나에 대해서라도 존재한다면, 소수 p를 *참한 소수*라고 부르자:

조건 1. 모든 $i = 1,2,\cdots,k$에 대하여 $n_i \geq (p+1)/2$

조건 2. 모든 $i = 1,2,\cdots,k$에 대하여 $p^{n_i} - 1$은 n_{i+1}의 배수이고, $(p^{n_i} - 1)/n_{i+1}$과 n_{i+1}은 서로소이다. 단, $n_{k+1} = n_1$이다.

2는 참한 소수가 아니지만 그 외의 모든 소수는 참한 소수임을 보여라.

7. 서로 소인 두 양의 정수 x와 y가 주어져있다. 이때 $\nu_p(x^{p-1} - y^{p-1})$가 홀수인 소수 p가 무한히 많이 존재함을 증명하여라.

제 2 장 p-adic numbers

지금까지가 준비과정이었다면, 이제 본격적으로 p-adic이 어떠한 것인지에 대해 알아봅시다. 먼저 p-adic number는 정말 어려운 내용입니다. 해석적으로 혹은 대수적으로 깊이 파고들려면 정말 정말 어려운 수학이 많이 쓰입니다. 따라서 우리는 p-adic이 대략적으로 어떠한 개념인지, 그리고 문제를 푸는데 있어 그것을 어떻게 사용할 수 있는지에 대해서만 간략하게 살펴볼 것입니다.

§1. p-adic norm

p-adic norm을 설명하기에 앞서, norm이 무엇인지 모르는 학생들을 위해 norm의 정의를 설명해야할 것 같다. 어떤 field[1] K에 대해, 다음 세 조건을 만족하는 실함수 $|\cdot|_v : K \to \mathbb{R}$을 **norm** 또는 **absolute value**라고 부른다.

AV 1. 임의의 $x \in K$에 대해, $|x|_v \geq 0$이며, $|x|_v = 0$일 필요충분조건은 $x = 0$인 것이다.
AV 2. 임의의 $x, y \in K$에 대해, $|xy|_v = |x|_v |y|_v$가 성립한다.
AV 3. 임의의 $x, y \in K$에 대해, 삼각부등식 $|x+y|_v \leq |x|_v + |y|_v$가 성립한다.

만약, **AV 3.**이 다음과 같은 더 강한 조건으로 대체된다고 하면,

AV 4. 임의의 $x, y \in K$에 대해, 삼각부등식 $|x+y|_v \leq \max\{|x|_v, |y|_v\}$가 성립한다.

이때 $|\cdot|$을 **non-Archimedean norm** 혹은 **valuation**이라고 부를 것이다.

1장의 1절에서 우리는 p-adic order을 정의하였다. 이것을 이용하여 $\mathbb{Q}$ 위에서의 p-adic norm을 다음과 같이 정의할 수 있다.

$$|x|_p = p^{-\nu_p(x)}$$

여기서 $x = 0$인 경우에 $|0|_p = p^{-\nu_p(0)} = p^{-\infty} = 0$으로 정의할 것이다.

이것이 실제로 norm이 된다는 사실을 1장의 Proposition 1.1.을 사용하면 쉽게 확인할 수 있다. 심지어 p-adic norm은 non-Archimedean norm이기도 하다. 이것 역시 증명은 독자들에게 맡긴다.

---

1) **Field** 혹은 **체**는 덧셈, 뺄셈, 곱셈, 나눗셈이 잘 정의된 집합이라고 생각하면 된다. 예를 들자면 유리수 집합, 실수 집합, 복소수 집합은 모두 field이다. 하지만 정수 집합에서는 나눗셈이 잘 정의가 되지 않으므로 정수 집합은 field가 아니다. 양의 실수들의 집합에서도 뺄셈이 잘 정의되지 않으므로 이 경우도 field가 되지 않는다. 한편 $\{a+bi : a, b \in \mathbb{Q}\} \subset \mathbb{C}$은 field가 된다.

이쯤에서 $\mathbb{Q}$ 위에서 정의된 다른 norm에는 어떤 것이 있나 궁금할 수도 있다. 이것에 관련된 짤막한 상식 하나를 소개하고자 한다.

Theorem 1.1. (Ostrowski) $\mathbb{Q}$ *위에서 정의된 임의의 norm* $|\cdot|_v$*에 대해, 다음 중 하나가 성립한다.*

(1) 임의의 $x \in \mathbb{Q}$*에 대해* $|x|_v = 1$

(2) 어떤 $c > 0$*가 존재하여 임의의* $x \in \mathbb{Q}$*에 대해* $|x|_v = |x|^c$

(3) 어떤 $c > 0$*와 소수* p*가 존재하여 임의의* $x \in \mathbb{Q}$*에 대해* $|x|_v = |x|_p^c$

이 정리의 증명은 아래에 연습문제로 빼놓겠다. 관심 있다면 증명을 시도해보고, 아니면 그냥 정리의 statement만 눈에 익혀놓고 가자.

< 연습문제 >

1. 임의의 유리수 $x \neq 0$에 대해,

$$\prod_p |x|_p = \frac{1}{|x|}$$

가 성립함을 보여라. (단, 곱은 모든 소수 p에 대한 것이다.)

2. 임의의 non-Archimedean norm $|\cdot|_v$에 대해, $|x|_v \neq |y|_v$라면 $|x+y|_v = \max\{|x|_v, |y|_v\}$가 성립함을 보여라.

3. $\mathbb{Q}$ 위에서 정의된 임의의 norm $|\cdot|_v$를 생각하자. 이때 임의의 정수 $m, n > 1$에 대해

$$|m|_v \leq \max\{1, |n|_v\}^{\log m / \log n}$$

이 성립함을 보여라.

4. Ostrowski's theorem을 증명하여라.

---

§2. p-adic numbers

엄밀한 논의를 하기 전에, 우선 p-adic integer가 대충 어떤 것인지에 대한 개념을 잡는 것이 중요할 것 같다. 다음과 같은 시나리오를 생각해보자.

어떤 정수 x가 주어져 있지만 그 값을 실제로 계산하기는 매우 힘든 상황을 가정해보자. x에 대한 관찰을 하고 싶은데, 그 값을 직접 계산할 수 없어 x를 p로 나눈 나머지만 계산해보았다니 $x \equiv 1 (\mathrm{mod} p)$가 나온다. 그런데 갑자기 옆에서 이종원 조교가 오더니 x를 p^2으로 나눈 나머지를 계산해보라고 한다. 어쩔 수 없이 우리는 x를 p^2으로 나눈 나머지를 계산

해본다. 계산을 해보기 전에도 우리는 그 값이 $1, 1+p, \cdots, 1+(p-1)p$들 중 하나라는 사실은 알고 있다. 하지만 이 p개의 값들 중에서 실제로 어떤 것인지를 결정해주어야 하고, 그것이 x를 $\mathrm{mod} p^2$으로 계산하는 것이다. 힘들게 힘들게 계산을 하였더니 $x \equiv 1+p (\mathrm{mod} p^2)$라는 결과가 나온다. 이번에는 주관조교가 와서 x를 p^3으로 나눈 나머지를 알고 싶다고 한다. 구하지 않으면 조교직을 박탈하겠다고 협박한다. 이번에도 $1+p, 1+p+p^2, \cdots, 1+p+(p-1)p^2$들 중에 나머지가 있는 것을 알지만, 어느 것인지를 정확히 알지 못해 결국 나머지를 계산하여 $x \equiv 1+p+p^2 (\mathrm{mod} p^3)$임을 보인다.

시간만 있다면, x를 p^k으로 나눈 나머지를 계속해서 계산해볼 수 있다. 항상 k가 $k+1$이 될 때마다 p가지의 선택지가 있지만, x가 정수라는 조건에서 제약이 생긴다. k가 충분히 크다면, x를 p^k으로 나눈 나머지는 $x \geq 0$일 때 x가, $x < 0$일 때 $p^k - x$가 나온다는 것이다. 그렇지 않다면, x가 존재하지 않게 된다. 예를 들어서 $p > 2$라면 임의의 $k \geq 1$에 대해

$$x \equiv 1+p+ \cdots +p^{k-1} (\mathrm{mod} p^k)$$

인 x는 존재하지 않는다. $\mathrm{mod} p^k$으로 보았을 때는 아무런 모순이 나오지 않음에도 불구하고 말이다.

하지만 $x^2 = -1$이라는 존재하지 않는 수 i를 가지고 실수 집합을 복소수 집합으로 확장한 것처럼 정수 집합도 비슷하게 확장해볼 수는 없을까? 위의 예시를 가져와보자. 이러한 수 x를 생각해보면 $2x$는 p^k으로 나눈 나머지가 $2+2p+ \cdots +2p^{k-1}$이 될 것이다. 조금 더 나아가서 $(p-1)x \equiv -1 (\mathrm{mod} p^k)$이 항상 성립하게 된다. ($x = -1/(p-1)$이라 할 수 없을까라는 생각이 들기 시작할 것이다.) 또한 x를 p진법으로 전개해보면

$$x = \overline{\cdots 11111111_{(p)}}$$

과 같은 꼴이 될 것이다.

이렇게 $\mathrm{mod} p^k$으로 계속해서 볼 수 있는 수들의 집합을 **p-adic integers**라고 부르고, $\mathbb{Z}_p$로 표기한다. 신기한 것은 $\mathbb{Z}_p$ 위에서 덧셈, 뺄셈, 곱셈이 모두 잘 정의된다는 것이다. 예를 들어 $\overline{\cdots 00000_{(3)}} - \overline{\cdots 02110_{(3)}} = \overline{\cdots 20120_{(3)}}$이 된다. 이것은 p^k으로 나눈 나머지들 사이에서 덧셈, 뺄셈, 곱셈이 잘 정의되기 때문이다. 하지만 나눗셈은 잘 정의되지 않을 수도 있다. (1을 p로 나누는 것은 불가능하다.)

나눗셈이 가능하게 하는 일은 매우 간단하다. 먼저 p의 배수가 아닌 $\mathbb{Z}_p$의 원소로 나누는 일은 가능하다. 문제가 되는 것은 p^k으로 나누는 것이다. 이것은 p진법 전개에서 소수점을 추가해주면 쉽게 해결할 수 있다. 예를 들어 $\overline{\cdots 021120_{(3)}} \div 3^3 = \overline{\cdots 021.120_{(3)}}$으로 정의하는 것이다. 이렇게 소수점을 넣어 확장시킨 수 체계에서는 나눗셈까지 잘 정의되므로 field가 된다. 이러한 수들의 집합을 **p-adic number**라 부르고, $\mathbb{Q}_p$로 표기한다.

이제 p-adic number가 무엇인지에 관한 감을 잡았다면, 엄밀한 논의를 시작해보자. 너무 어렵다 싶은 생각이 드는 독자들은 다음 세 페이지에 나오는 내용을 넘어가도 좋다. 하지만 한 번쯤은 알아두어도 나쁠 것이 없으니 시간이 있으면 읽어보는 것이 좋을 것이다. 천천히

설명할 것이니 잘 따라오기를 바란다.

우리는 $\mathbb{Q}$를 확장하여 $\mathbb{Q}_p$를 정의할 것이다. $\mathbb{Q}$로부터 $\mathbb{R}$을 정의한 것과 똑같이 completion을 사용할 것이다. 우선 필요한 정의들부터 하자.

Definition 2.1. 유리수들의 무한수열 (a_n)과 유리수 ℓ을 생각하자. 만약 임의의 $\epsilon > 0$에 대해 충분히 큰 정수 M이 존재하여 임의의 정수 $n > M$에 대해

$$|a_n - \ell|_p < \epsilon$$

이 성립한다면, 수열 (a_n)이 **ℓ에 수렴한다**고 하고,

$$\lim_{n\to\infty}{}^{(p)} a_n = \ell$$

으로 표기하자.

Example. 수열 $a_n = n!$을 생각해보자. 임의의 n에 대해 $\nu_p(n!) > n/(p-1) - \log_p n - 1$이 성립하므로 충분히 큰 n에 대해서는 $\nu_p(n) > n/2p$가 성립한다. 즉, $|n! - 0|_p < p^{-n/2p}$이 되어 임의의 ϵ에 대해 $n > 2p\log_p(1/\epsilon)$이면 $|n! - 0|_p < \epsilon$이다. 즉, p-adic 체계에서

$$\lim_{n\to\infty}{}^{(p)} n! = 0$$

이다.

Example. 수열 $a_n = 1 + p + \cdots + p^n$을 생각해보자. $(p-1)a_n + 1 = p^{n+1}$이므로

$$\nu_p\left(a_n + \frac{1}{p-1}\right) = n+1$$

이다. 즉, (a_n)은 $-1/(p-1)$로 수렴한다.

Definition 2.2. 유리수들의 무한수열 (a_n)을 생각하자. 만약 임의의 $\epsilon > 0$에 대해 충분히 큰 정수 M이 존재하여 임의의 정수 $m, n > M$에 대해

$$|a_m - a_n|_p < \epsilon$$

이 성립한다면, 수열 (a_n)을 **Cauchy sequence**라 하자.

Definition 2.3. 어떤 무한 유리수 수열 (a_n)에 대해,

$$\lim_{n\to\infty}{}^{(p)} a_n = 0$$

이라면, (a_n)을 **null sequence**라 부르자.

유리수에서 정의된 p-adic norm이 아니더라도 일반적인 field에서 정의된 norm에서 항상 성립하는 몇 가지 성질들이 있다. 다음 Proposition을 통해 극한이나 코시 수열과 관련된 성질들은 어떠한 것이 있는지 알아보자.

Proposition 2.4.

(i) 무한 유리수 수열 (a_n)과 (b_n)이 각각 ℓ_a와 ℓ_b로 수렴한다면, 수열 $(a_n + b_n)$은

$\ell_a+\ell_b$로 수렴한다.

(ii) 무한 유리수 수열 (a_n)과 (b_n)이 각각 ℓ_a와 ℓ_b로 수렴한다면, 수열 (a_nb_n)은 $\ell_a\ell_b$로 수렴한다.

(iii) 무한 유리수 수열 (a_n)과 (b_n)이 각각 ℓ_a와 $\ell_b\neq 0$로 수렴한다면, 수열 (a_n/b_n)은 ℓ_a/ℓ_b로 수렴한다.

(iv) 무한 유리수 수열 (a_n)이 수렴한다면, (a_n)은 Cauchy sequence이다.

(v) 무한 유리수 수열 (a_n)과 (b_n)이 Cauchy sequence라면, 수열 (a_n+b_n)도 Cauchy sequence이다.

(vi) 무한 유리수 수열 (a_n)과 (b_n)이 Cauchy sequence라면, 수열 (a_nb_n)도 Cauchy sequence이다.

(vii) 무한 유리수 수열 (a_n)이 Cauchy sequence이고, (b_n)이 null sequence라면, 수열 (a_nb_n)도 null sequence이다.

(viii) 무한 유리수 수열 (a_n)과 (b_n)이 Cauchy sequence이고, (b_n)이 null sequence은 아니라고 할 때, 수열 (a_n/b_n)도 Cauchy sequence이다.

Proof. (i) 정의에 의해 임의의 $\epsilon>0$에 대해 어떤 M_a와 M_b가 존재하여 임의의 $n>M_a$에 대해 $|a_n-\ell_a|_p<\epsilon$이고 임의의 $n>M_b$에 대해 $|b_n-\ell_b|_p<\epsilon$이다. 그러므로 임의의 정수 $n>\max\{M_a,M_b\}$에 대해

$$|a_n+b_n-(\ell_a+\ell_b)|_p\le\max\{|a_n-\ell_a|_p,|b_n-\ell_b|_p\}<\epsilon$$

이 성립한다. 즉, (a_n+b_n)은 $\ell_a+\ell_b$로 수렴한다.

(ii) 우선 충분히 큰 임의의 n에 대해 $|a_n-\ell_a|_p<1$이므로 $|a_n|_p<|\ell_a|_p+1$이다. 임의의 $\epsilon>0$에 대해 어떤 M이 존재하여 임의의 정수 $n>M$에 대해 $|a_n-\ell_a|_p<\epsilon/(|\ell_a|_p+1)$이며 $|b_n-\ell_b|_p<\epsilon/(|\ell_b|_p+1)$이다. 이때

$$\begin{aligned}|a_nb_n-\ell_a\ell_b|_p&=|a_n(b_n-\ell_b)+(a_n-\ell_a)\ell_b|_p\\&\le\max\{|a_n|_p|b_n-\ell_b|_p,|a_n-\ell_a|_p|\ell_b|_p\}\\&<\max\left\{\frac{(|\ell_a|_p+1)\epsilon}{|\ell_a|_p+1},\frac{|\ell_b|_p\epsilon}{|\ell_b|_p+1}\right\}=\epsilon\end{aligned}$$

이므로 (a_nb_n)는 $\ell_a\ell_b$에 수렴한다.

(iii) (ii)에 의해 $(1/b_n)$이 $1/\ell_b$로 수렴함을 보이면 충분하다. 수렴성의 정의에 의해 어떤 M이 존재하여 임의의 $n>M$에 대해 $|b_n-\ell_b|_p<\min\{|\ell_b|_p/2,|\ell_b|_p^2\epsilon/2\}$가 성립한다. 이때 일단 $|b_n|\ge|\ell_b|_p-|\ell_b|_p/2=|\ell_b|_p/2$이므로

$$\left|\frac{1}{b_n}-\frac{1}{\ell_b}\right|_p=\frac{|b_n-\ell_b|_p}{|b_n|_p|\ell_b|_p}<\frac{|\ell_b|_p^2\epsilon/2}{|\ell_b|_p^2/2}=\epsilon$$

이다. 즉, $(1/b_n)$이 $1/\ell_b$로 수렴한다.

(iv) $\lim_{n\to\infty}^{(p)}a_n=\ell$이라 가정해보자. 임의의 양수 ϵ에 대해 어떤 M이 존재하여 임의의 $n>M$에 대해 $|a_n-\ell|_p<\epsilon$이어야 한다. 이때, $m>M$이라면, $|a_m-\ell|_p<\epsilon$이다. p-adic norm은 non-Archimedean이므로

$$|a_m - a_n|_p = |(a_m - \ell) - (a_n - \ell)| \\ \leq \max\{|a_m - \ell|, |a_n - \ell|\} < \epsilon$$

이 성립한다. 임의의 $m,n > M$에 대해 $|a_m - a_n|_p < \epsilon$이므로 (a_n)은 Cauchy sequence이다. (v), (vi), (vii)과 (viii)의 증명은 (i), (ii)와 (iii)의 증명과 유사하고, 보다시피 재미가 없으니 독자에게 맡긴다.

□

이제 드디어 p-adic numbers를 정의할 수 있게 되었다. 결론적으로 $\mathbb{Q}_p$는 Cauchy sequence들을 null sequence들로 quotient 취한 것이 되지만, 그 과정을 서술하겠다. 임의의 Cauchy sequence (a_n)에 대해, Cauchy sequence들의 집합 $\{a_n\}$을

$$\{a_n\} = \{(a_n + b_n) : b_n \in Null(p)\}$$

으로 정의하자. (이 집합에 Cauchy sequence들의 집합임은 Proposition 2.4.의 (iv)와 (v)에서 자명하다.) Null sequence와 null sequence의 합과 차는 모두 null sequence이므로 두 수열 (a_n)과 (b_n)에 대해 $\{a_n\} = \{b_n\}$일 필요충분조건이 $(b_n) \in \{a_n\}$이 됨을 확인할 수 있다.

$(c_n) \in \{a_n\}$이고 $(d_n) \in \{b_n\}$이라 해보자. 이때 $(c_n) = (a_n) + (x_n)$이고 $(d_n) = (b_n) + (y_n)$인 null sequence들 (x_n)과 (y_n)이 존재한다. 여기서 $(c_n + d_n) = (a_n + b_n) + (x_n + y_n)$인데, Proposition 2.4.의 (i)에 의해 $(x_n + y_n)$이 null sequence이므로 $(c_n + d_n) \in \{a_n + b_n\}$이다. 마찬자기로 $(c_n d_n) = (a_n b_n) + (a_n y_n) + (x_n b_n) + (x_n y_n)$이 성립하는데, Proposition 2.4.의 (i), (iv), (viii)에 의해 $(a_n y_n) + (x_n b_n) + (x_n y_n)$은 null sequence가 된다. 즉, $(c_n d_n) \in \{a_n b_n\}$이며 둘 다 Cauchy sequence가 된다. 뺄셈과 나눗셈에 대해서도 비슷한 사실을 확인할 수 있다. (나눗셈의 경우에는 $\{b_n\} \neq Null(p)$인 경우에만 가능할 것이다.)

이것은 무슨 의미를 가지고 있는지를 생각해보면, $\{a_n\}$과 $\{b_n\}$의 합, 차, 곱, 나눗셈을 모두 정의할 수 있게 된다. 예를 들어보자. 만약 $\{a_n'\} = \{a_n\}$이고 $\{b_n'\} = \{b_n\}$이라고 하면, $(a_n') \in \{a_n\}$이며 $(b_n') \in \{b_n\}$이므로 우리가 위에서 보인 것에 의해 $(a_n' b_n') \in \{a_n b_n\}$이 성립한다. 즉, $\{a_n' b_n'\} = \{a_n b_n\}$이 되어 $\{a_n\}$과 $\{b_n\}$의 곱이 $\{a_n\}\{b_n\} = \{a_n b_n\}$로 잘 정의된다. 같은 방법으로 두 집합 사이에 합이나 차, 나눗셈도 모두 잘 정의할 수 있다. 물론 수열 $(a_n) = (0)$이라면 $\{a_n\} = Null(p)$이 되므로 $\{a_n\}/\{b_n\}$이 정의되지 않을 것이다.

이제 $\{a_n\}$들의 집합을 생각하고, 이 집합을 **p-adic numbers**라 하고, **$\mathbb{Q}_p$**로 표기하자. 우리가 정의한대로 $\mathbb{Q}_p$의 원소들 사이에서는 합, 차, 곱과 나눗셈이 모두 정의되어있다. 즉, $\mathbb{Q}_p$는 field가 된다. $\mathbb{Q}_p$의 원소들 중에 $|x|_p \leq 1$인 x들의 집합을 **p-adic integers**라 부르고, **$\mathbb{Z}_p$**로 표기하자. $\mathbb{Z}_p$는 당연히 $\mathbb{Q}_p$의 부분집합이 될 것이고, 합, 차, 곱에 대해 닫혀있음을 쉽게 확인할 수 있을 것이다.

이로써 3페이지에 걸쳐 p-adic numbers의 엄밀한 정의가 끝났다. 이해가 잘 가지 않는 독자들은 completion of a field를 인터넷에서 검색하여 읽어보기를 바란다. (하지만 아마도 이것보다 과정이 상세하게 나온 글은 찾기 힘들 것이다.)

우리는 $\mathbb{Q}_p$의 원소들을 각각 수열들의 집합으로 정의하였다. 하지만, $x \in \mathbb{Q}_p$라는 표현을 볼 때마다 수열들의 집합을 머릿속에서 연상하는 것은 매우 힘든 일이다. 그러므로 앞으로는 $\mathbb{Q}_p$의 각 원소를 수처럼 생각하는 것이 편할 것이다. 심지어 $\mathbb{Q}_p$의 원소들 사이에 사칙연산까지 정의되었는데 계속 집합을 더하고 뺀다고 생각하는 것만큼 체력을 낭비하는 일도 없다. 정의는 정의일 뿐 수학자가 생각하는 방식이 아님을 명심하자!

또한, 임의의 유리수 q에 대해, q로 수렴하는 유리수들로 이루어진 수열들의 집합에 대응되는 $\mathbb{Q}_p$의 원소가 정확히 하나 있다. 편의상 그 $\mathbb{Q}_p$의 원소를 q로 표기하자. 문자가 중복되며 혼란이 오겠지만, 사실상 $\mathbb{Q}$의 원소 q와 $\mathbb{Q}_p$의 원소 q를 같은 q로 생각해도 된다. 사칙연산이 같게 적용되기 때문이다. 따라서 그냥 $\mathbb{Q}_p \supset \mathbb{Q}$라고 말할 수 있다. 유리수로 수렴하지 않는 수열의 경우에도, 임의의 $x \in \mathbb{Q}_p$에 대해, x에 대응되는 Cauchy sequence들의 집합을 생각하자. 이 집합의 모든 원소들(Cauchy sequence들)은 편의상 x에 수렴한다고 말할 수 있다. 이렇게 정의하여도 우리가 증명한 Proposition 2.4.의 (ⅰ), (ⅱ), (ⅲ)이 모두 성립하게 된다. (그것들이 모두 성립하도록 우리가 잘 정의하였다고 말하는 편이 더 옳을 수도 있겠다.) 유리수로 이루어진 임의의 Cauchy sequence는 어떠한 값에 수렴한다는 이야기까지 할 수 있다.

심지어 $\mathbb{Q}_p$의 원소들에 대해서 p-adic order나 norm도 잘 정의할 수 있다. 우선 다음 명제를 증명하자.

Proposition 2.5. *어떤 Cauchy sequence이며 null sequence는 아닌 수열 (x_n)을 생각하자. 이때 어떤 M이 존재하여 임의의 정수 $m,n > M$에 대해 $|x_m|_p = |x_n|_p$가 성립한다.*

Solution. $\lim_{n\to\infty}|x_n|_p$가 0은 아니므로 어떤 $\epsilon > 0$이 존재하여 무한히 많은 n에 대해 $|x_n|_p > \epsilon$이 성립할 것이다. 한편 (x_n)은 Cauchy sequence이므로 어떤 M이 존재하여 임의의 $m,n > M$에 대해 $|x_m - x_n|_p < \epsilon$이 성립한다. 위에서 $|x_n|_p > \epsilon$인 n이 무한히 많으므로 어떤 $t > M$이 존재하여 $|x_t|_p > \epsilon$이 되고, 임의의 $n > M$에 대해 $|x_n - x_t|_p < \epsilon$이 된다. 이때 항상 $|x_t|_p \neq |x_n - x_t|_p$이므로

$$|x_n|_p = \max\{|x_t|_p, |x_n - x_t|_p\} = |x_t|_p$$

가 된다. 즉, 임의의 $n > M$에 대해 $|x_n|_p$는 일정한 값을 가진다.

□

임의의 $x \in \mathbb{Q}_p$에 대해, x로 수렴하는 유리수 수열 (x_n)이 존재할 것이다. 이때 x의 p-adic order을

$$\nu_p(x) = \lim_{n\to\infty} \nu_p(x_n)$$

으로 정의해보자. (여기서 $\lim$은 $\lim^{(p)}$가 아닌, 우리가 평소에 사용하는 극한임을 주의하자.) 만약 $x \neq 0$이라면, Proposition 2.5.에 의해 어느 이후로 모든 항의 값이 일정해지고,

$x=0$이라면 값이 무한대로 발산한다. 즉 $x\neq 0$이면 $\nu_p(x)<\infty$이도록 p-adic order가 잘 정의된다. 마찬가지로

$$|x|_p = p^{-\nu_p(x)}$$

로 정의할 수 있다. 이렇게 정의하였을 때 유리수에서 성립하였던 p-adic order와 p-adic norm들의 성질이 그대로 성립하게 된다. 증명은 연습문제로 남겨두겠다.

마지막으로, $x\in\mathbb{Z}_p$일 때, x를 $\bmod p^k$으로 보는 것이 관찰하는 것이 가능하다는 말을 하고 싶다. $x\equiv y\,(\bmod p^k)$은 $\nu_p(x-y)\geq k$와 동치인 것으로 정의할 수 있고, 임의의 $x\in\mathbb{Z}_p$은 $0,1,\cdots,p^k-1$들 중 하나와 $\bmod p^k$으로 동일함을 보일 수 있다. 즉, $\mathbb{Z}$의 원소를 다루듯이 비슷하게 $\mathbb{Z}_p$의 원소들도 다룰 수 있다. 단, p^k꼴이 아닌 수로 mod를 관찰하기 힘들다.

< 연습문제 >

1. 임의의 $\mathbb{Q}_p$의 원소 x와 y에 대해 다음을 증명하여라.
   (ⅰ) $\nu_p(xy)=\nu_p(x)+\nu_p(y)$이며 $|xy|_p=|x|_p|y|_p$이다.
   (ⅱ) $\nu_p(x+y)\geq\min\{\nu_p(x),\nu_p(y)\}$이며 $|x+y|_p\leq\max\{|x|_p,|y|_p\}$이다.
   (ⅲ) $\nu_p(x)\neq\nu_p(y)$면 $\nu_p(x+y)=\min\{\nu_p(x),\nu_p(y)\}$이고 $|x+y|_p=\max\{|x|_p+|y|_p\}$이다.

2. 어떤 유리수 수열 (a_n)에 대해 새로운 수열 (s_n)을 $s_n=a_1+\cdots+a_n$으로 정의하자. 이때 (s_n)이 수렴할 필요충분조건은 $\lim_{n\to\infty}^{(p)}a_n=0$임을 보여라.

3. (p-adic LTE) 양의 정수 n과 홀수인 소수 p, 그리고 서로 다른 $\mathbb{Q}_p$의 원소 x와 y를 생각하자. 만약 $\nu_p(x)=\nu_p(y)<\nu_p(x-y)$라고 한다면

$$\nu_p(x^n-y^n)=\nu_p(x-y)+\nu_p(n)+n\nu_p(x)$$

이 성립함을 보여라.

4. 임의의 $\mathbb{Q}_p$의 원소 x,y에 대해 $x=qy$인 $q\in\mathbb{Z}_p$가 존재할 필요충분조건은 $\nu_p(x)\geq\nu_p(y)$인 것임을 보여라. 즉, $\nu_p(x)\geq\nu_p(y)$이기만 하면 y는 x를 나눈다.

5. (Teichmüller character) 함수 $\omega:\mathbb{Z}_p\to\mathbb{Z}_p$를 다음과 같이 정의하자.

$$\omega(a)=\lim_{n\to\infty}^{(p)}a^{p^n}$$

이때 다음을 보여라.
   (ⅰ) 임의의 a에 대해 $\omega(a)$가 잘 정의된다. 즉, 수열 (a^{p^n})이 수렴한다.
   (ⅱ) 임의의 a와 b에 대해 $\omega(ab)=\omega(a)\omega(b)$가 성립한다.
   (ⅲ) 임의의 a에 대해 $\omega(a)^{p-1}=1$가 성립한다.
   (ⅳ) 임의의 a와 b에 대해 $\nu_p(a-b)\geq 1$이면 $\omega(a)=\omega(b)$이다.
   (ⅴ) 임의의 a에 대해 $\omega(a)^{(p-1)/2}$는 르장드르 기호 (a/p)와 값이 같다.

6. 우리가 앞에서 직관적으로 정의한 $\mathbb{Q}_p$와 뒤에서 엄밀하게 정의한 $\mathbb{Q}_p$가 일치함을 증명하여라. 즉, 임의의 p-adic number $x \neq 0$에 대해 다음을 만족하는 정수 k와 $i = k, k+1, \cdots$에 대한 정수들 $0 \leq a_i < p$이 유일하게 존재함을 보여라. (단, $a_k \neq 0$이다.)

$$x = \sum_{i=k}^{\infty} a_i p^i$$

x를 이렇게 표현한 것을 **p-adic expansion**이라 한다.

7. $\mathbb{Q}_p$의 원소들 사이에서 p-adic norm이 정의되었으므로 $\mathbb{Q}_p$의 원소들로 이루어진 Cauchy sequence를 정의할 수 있다. 이때 $\mathbb{Q}_p$의 원소들로 이루어진 임의의 Cauchy sequence는 어떤 $\mathbb{Q}_p$의 원소로 항상 수렴함을 보여라. (해석학에서는 이러한 공간을 complete metric space라고 한다.)

8. (Hensel's lemma) 모든 계수가 $\mathbb{Z}_p$의 원소인 다항식 $f \in \mathbb{Z}_p[x]$이 주어져 있다. 만약 어떤 $a_0 \in \mathbb{Z}_p$에 대해 $|f(a_0)|_p < |f'(a_0)|_p^2$이 성립한다면, 어떤 $f(a) = 0$인 $a \in \mathbb{Z}_p$가 존재하여

$$|a - a_0|_p \leq \left| \frac{f(a_0)}{f'(a_0)} \right|_p$$

이 성립함을 증명하여라.

§3. Infinite series

이번 절에서는 p-adic numbers에서 정의되는 함수에 대해 살펴볼 생각이다. p-adic에서 무한급수를 생각할 수 있을까? 답부터 말하자면, 있다. 이것이 어떻게 정의되는지, 그리고 정의를 하면 어떠한 점이 좋은지 알아보자.

우선 2절 연습문제에도 있는 다음 명제가 가장 많이 쓰인다. 증명은 독자들에게 맡기겠다.

Theorem 3.1. *어떤 $\mathbb{Q}_p$의 원소들로 이루어진 수열 (a_n)에 대해 새로운 수열 (s_n)을 $s_n = a_1 + \cdots + a_n$으로 정의하자. 이때 (s_n)이 수렴할 필요충분조건은 $\lim_{n\to\infty}^{(p)} a_n = 0$인 것이다.*

이 정리가 좋은 이유는, non-archimedean norm에서는 어떤 무한급수가 수렴함을 보이기가 훨씬 쉬워지기 때문이다. 일반적으로 실수에서는 절대수렴하지 않는 급수가 수렴할 수 있었는데, p-adic norm에서는 그런 일이 절대로 일어나지 않는다.

다음과 같은 무한급수를 생각해보자.

$$\sum_{k=0}^{\infty}\frac{x^k}{k!}$$

Theorem 3.1.에 의해 이 급수가 수렴할 필요충분조건은 $\lim_{k\to\infty}(\nu_p(x^k)-\nu_p(k!))=\infty$인 것이다. 이때, $\nu_p(k!)=(k-s)/(p-1)$이므로 저 값이 ∞로 발산할 필요충분조건은 $\nu_p(x)>1/(p-1)$인 것이다. 이것을 norm으로 바꾸면 $|x|_p<p^{-1/(p-1)}$이 된다. 즉, x의 p-adic norm이 특정한 수보다 작을 때에만 무한급수가 수렴하게 된다. (우리가 일반적으로 말하는 수렴반경과 같은 의미일 것이다.)

이제 $|x|_p<p^{-1/(p-1)}$인 임의의 $x\in\mathbb{Q}_p$에 대해서, 다음과 같이 지수함수 $\exp_p(x)$를 정의할 수 있게 된다.

$$\exp_p(x)=\sum_{k=0}^{\infty}\frac{x^k}{k!}$$

마찬가지로, 로그함수 $\log_p(x)$도

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

으로 정의하자. 이때 급수가 수렴하려면 $\lim_{n\to\infty}(n\nu_p(x)-\nu_p(n))=\infty$가 되어야 하므로 $|x|_p<1$이기만 하면 항상 수렴한다. 즉, 수렴반경은 1이 된다.

사실 가장 중요한 사실은 $\exp_p$와 $\log_p$에 대해 실수에서 가지고 있는 많은 성질들이 똑같이 성립한다는 것이다. 다음 Proposition을 살펴보자.

Proposition 3.2.

(i) 임의의 $x,y\in\mathbb{Q}_p$에 대해, $\exp_p(x)$와 $\exp_p(y)$가 정의된다면

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

가 성립한다.

(ii) 임의의 $x,y\in\mathbb{Q}_p$에 대해, $\log_p(1+x)$와 $\log_p(1+y)$가 정의된다면

$$\log_p(1+x+y+xy)=\log_p(1+x)+\log_p(1+y)$$

가 성립한다.

(iii) 임의의 $x\in\mathbb{Q}_p$에 대해, $|x|_p<p^{-1/(p-1)}$이라면

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

가 성립한다.

Proof. (i) 기본적으로 모두 전개를 해서 양 변의 전개식이 같음을 보이는 것이다. 예를 들어,

$$\exp_p(x+y)=\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}a_{(i,j)}x^iy^j,\qquad \exp_p(x)\exp_p(y)=\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}b_{(i,j)}x^iy^j$$

인 $a_{(i,j)}$와 $b_{(i,j)}$들이 존재할 것이다. 여기서 임의의 (i,j)에 대해 $a_{(i,j)}=b_{(i,j)}$임을 보이면 결국 $\exp_p(x+y)=\exp_p(x)\exp_p(y)$을 증명한 셈이 되는 것이다. 그런데 우리는 실수에서 같은

식 $e^{x+y}=e^x e^y$이 성립함을 아주 잘 알고 있다. 또한, e^{x+y}의 전개식도 $x^i y^j$의 계수가 $a_{(i,j)}$이며, $e^x e^y$의 전개식에서 $x^i y^j$의 계수도 $b_{(i,j)}$가 될 것이다. 즉, $a_{(i,j)}=b_{(i,j)}$가 됨을 알 수 있고, 이때 $\exp_p(x+y)=\exp_p(x)\exp_p(y)$도 성립할 것이다. 여기서 수렴에 관련된 문제들을 해결해주어야 하지만, 실제로 $|x+y|_p < p^{-1/(p-1)}$이므로 $\exp_p(x+y)$도 수렴하므로 큰 문제가 되지 않는다.
(ii)와 (iii)에 대해서도 식만 바꿔주면 동일하게 성립한다. 시간이 없으므로 쓰지는 않겠다.

□

신기하게도 이것을 이용하여 풀 수 있는 올림피아드 문제가 있다.

Problem 3.3. *임의의 자연수 n에 대해*

$$\frac{2^1}{1}+\frac{2^2}{2}+\cdots+\frac{2^n}{n}=\frac{p_n}{q_n}$$

인 서로소인 두 수 p_n과 q_n을 생각하자. 이때 $\lim_{n\to\infty}\nu_2(p_n)=\infty$ 임을 보여라.

Solution. $|-2|_2=2^{-1}$이므로 $\log_2(-1)$은 $\mathbb{Q}_2$에서 잘 정의된다. 이때 $2\log_2(-1)=\log_2(1)$이고, $\log_2(1)=0$이므로 $\log_2(-1)=0/2=0$이 된다.
한편, $\log_2(-1)$을 급수로 전개해보면,

$$-\log_2(-1)=\frac{2^1}{1}+\frac{2^2}{2}+\frac{2^3}{3}+\cdots$$

임을 쉽게 확인할 수 있다. 이 급수가 0으로 수렴하므로 부분합 p_n/q_n의 2-adic norm도 당연히 0에 수렴할 것이다. 즉, $\lim_{n\to\infty}2^{-\nu_2(p_n)}=0$이 되어 $\lim_{n\to\infty}\nu_2(p_n)=\infty$이다.

□

< 연습문제 >

1. $|x-1|_p<1$인 임의의 $x\in\mathbb{Z}_p$에 대해

$$\log x=\lim_{n\to\infty}\frac{x^{p^n}-1}{p^n}$$

임을 증명하여라.

제 3 장 Applications of p-adic numbers

이제 p-adic numbers가 어떠한 수들이고, 어떻게 정의되는지 알았으니 어떻게 쓰이는지를 배워볼 차례입니다. 예상 외로 p-adic numbers가 이곳저곳에 많이 쓰이기 때문에 설명할 것은 많으나 시간이 부족하여 몇 가지의 주제만 선별하였습니다. 수학은 독학에 바탕을 두고 있으므로 관심이 있으신 분들은 꼭 인터넷에서 자료를 찾거나 해서 (혹은 주관조교에게 연락을 해서) 공부를 해보시길 바랍니다.

§1. Schur derivatives

1933년에 I. Schur는 페르마의 작은 정리의 초등적인 일반화를 증명하였다. 그는 다음과 같이 소수 p에 대한 수열 (a_n)의 미분 (a_n')을 정의하였다.

Definition 1.1. 수열 (a_n)이 있을 때, 이 수열의 **Schur derivative** $(a_n') = \Delta(a_n)$을

$$a_n' = \frac{a_{n+1} - a_n}{p^{n+1}}$$

으로 정의하자.

이 수열에 $a_n = a^{p^n}$을 대입하면, a_n'이 정수임은 LTE를 이용하면 쉽게 확인할 수 있다. 이때 Schur는 더 나아가 a가 p와 서로소일 때 수열 (a^{p^n})의 $p-1$번째 미분까지 모두 정수 수열임을 증명하였다.
Schur가 이것에 대한 논문을 출판한 이후 Rothgiesser는 귀납법을 사용하여 이 정리를 새롭게 증명하였고, Zorn은 1936년에 p-adic analysis를 사용하여 증명하였다. 이 절에서 우리는 Zorn의 증명을 함께 살펴볼 것이다.

$p=2$일 때는 따로 처리하고, 편의상 $p>2$인 경우만 다루자. 우선 $|x-1|_p < 1$인 x에 대해,

$$X_n = \frac{x^{p^n}-1}{p^{n+1}}$$

으로 정의하자. 이때, $\left|x^{p^n}-1\right| < 1$이므로

$$\begin{aligned} X_n &= \frac{x^{p^n}-1}{p^{n+1}} = \frac{1}{p^{n+1}}\left\{\exp(\log x^{p^n})-1\right\} \\ &= \frac{1}{p^{n+1}}\sum_{k=1}^{\infty}\frac{(p^n\log x)^k}{k!} = \sum_{k=1}^{\infty}\frac{p^{nk-n-1}}{k!}(\log x)^k \\ &= \sum_{k=1}^{\infty} p^{(n+1)(k-1)}\frac{(\log x/p)^k}{k!} \end{aligned}$$

이 성립한다. 여기서 $|x-1|_p < 1$이므로 $\log x/p \in \mathbb{Z}_p$임을 확인할 수 있다. 이제 $\Delta^r X_n$을 관찰하기 위해서는 $\Delta^r p^{(n+1)(k-1)}$을 계산하면 됨을 알 수 있다.

Lemma 1.2. *$\Delta^r p^{(n+1)(k-1)}$은 다음과 같이 계산할 수 있다.*

$$\Delta^r p^{(n+1)(k-1)} = p^{(k-r-1)(n+1)}(p^{k-r}-1)(p^{k-r+1}-1)\cdots(p^{k-1}-1)$$

Proof. 우선 $r=0$이면 자명하다. 이제 $r-1$일 때 성립한다고 가정해보자.
이때 $\Delta^r p^{(n+1)(k-1)}$을 계산해보면,

$$\begin{aligned}\Delta(\Delta^{r-1}p^{(n+1)(k-1)}) &= p^{-n-1}(p^{(n+2)(k-r)}(p^{k-r+1}-1)\cdots(p^{k-1}-1)\\ &\quad -p^{(n+1)(k-r)}(p^{k-r+1}-1)\cdots(p^{k-1}-1))\\ &= p^{(n+1)(k-r-1)}(p^{k-r}-1)\cdots(p^{k-1}-1)\end{aligned}$$

이 된다. 즉, 임의의 r에 대해 위 식이 성립한다.

□

위의 Lemma를 사용하면 $\Delta^r X_n$을 계산할 수 있게 된다.

$$\Delta^r X_n = \sum_{k=r+1}^{\infty} p^{(k-r-1)(n+1)}\frac{(p^{k-r}-1)\cdots(p^{k-1}-1)}{k!}\left(\frac{\log x}{p}\right)^k$$

그리고 이 식을 이용하여 다음 정리들을 증명할 수 있다. (여기서 $k \le r$이면 항이 0이 되므로 $k \ge r+1$인 경우만 더해주어도 무방하다.)

Theorem 1.3. *x를 $x-1$이 p의 배수가 정수라 하자. 이때 다음이 성립한다.*

(i) $|x-1|_p \le p^{-2}$라면 임의의 r과 n에 대해 $\Delta^r X_n$은 정수이다.

(ii) $|x-1|_p > p^{-2}$라면 임의의 n에 대해 $\nu_p(\Delta^{p-1}X_n) = -1$이다.

(iii) 임의의 n에 대해 $\Delta X_n, \Delta^2 X_n, \cdots, \Delta^{p-2}X_n$은 정수이다.

Proof. (i) 우선 임의의 $k>0$에 대해 $\nu_p(k!) \le k-1$가 성립한다. 또한, 임의의 x에 대해 $|\log x|_p \le |x-1|_p$이므로 여기서 $\nu_p(\log x/p) \ge 1$이다. 즉, $1/k!\,(\log x/p)^k$이 $\mathbb{Z}_p$의 원소가 되므로 그것들을 합한 $\Delta^r X_n$도 $\mathbb{Z}_p$의 원소가 된다. 한편, $\Delta^r X_n$을 계산할 때 분모에는 p의 거듭제곱 밖에 나타나지 않으므로 $\Delta^r X_n$은 정수가 된다.

(ii) $x-1$이 p^2의 배수가 아니므로 $\nu_p(\log x) = 1$이 된다. 즉, $\nu_p(\log x/p) = 0$이 된다. 이제 $\Delta^{p-1}X_n$을 계산할 때, 각 항의 p-adic order은 $(k-p)(n+1) - \nu_p(k!)$이다. 이때 $k=p$라면 $\nu_p(p!)=1$이므로 그 값은 -1이 되고, $k \ge p+1$이라면 $(k-p)(n+1) \ge k-p \ge \nu_p(k!)$이 되어 항상 0 이상이다. 즉, 하나의 항만이 p-adic order가 -1이고 나머지는 모두 p-adic order가 0 이상므로 $\nu_p(\Delta^{p-1}X_n) = -1$이다.

(iii) $r \le p-2$일 때 각 항의 p-adic order의 값이 0 이상임을 보일 것이다. 우선 $k \le p-1$이라면 항에서 분모인 $k!$의 p-adic order가 0이므로 당연히 전체 항은 $\mathbb{Z}_p$에 속한다. 한편, $k \ge p$인 경우에는 항의 p-adic order는 $(k-r+1)(n+1) - \nu_p(k!) \ge k-p+1-\nu_p(k!) \ge 0$ 이상이 된다. 즉, 모든 경우에 항의 p-adic order가 0 이상이므로 $r \le p-2$에 대해 $\Delta^r X_n$은 정수이다.

□

이제 본격적으로 $\Delta^r a^{p^n}$에 관한 이야기를 시작해보자. L_n을

$$L_n = \frac{a^{(p-1)p^n}-1}{p^{n+1}}$$

으로 정의하면, $x = a^{p-1}$이라 할 때 $L_n = X_n$이다. 즉, Theorem 1.3.을 L_n에서 적용할 수 있게 된다. 또한, $\Delta a^{p^n} = (a^{p^{n+1}} - a^{p^n})/p^{n+1} = a^{p^n} L_n$이 된다.
드디어 다음 정리를 증명할 수 있게 되었다.

Theorem 1.4. (Schur, 1933) p가 홀수인 소수이고, a는 p와 서로소인 정수라고 하자. 이때 $\Delta^r a^{p^n}$에 관해서 다음이 성립한다.

(i) 임의의 n에 대해 $\Delta a^{p^n}, \Delta^2 a^{p^n}, \cdots, \Delta^{p-1} a^{p^n}$은 모두 정수이다.

(ii) $a^{p-1}-1$이 p^2의 배수라면 임의의 r과 n에 대해 $\Delta^r a^{p^n}$은 정수이다.

(iii) $a^{p-1}-1$이 p^2의 배수가 아니라면 임의의 n에 대해 $\nu_p(\Delta^p a^{p^n}) = -1$이다.

Proof. 우선, 임의의 r에 대해

$$\Delta^r a^{p^n} = a^{p^n}(\Delta^{r-1} L_n + P_n)$$

의 꼴로 나타내어짐을 보이자. (여기서 P_n는 $r' \le r-2$에 대해 $\Delta^{r'} L_{n+\mu}$꼴들로 이루어진 정수계수 다항식이다.)
예를 들어서 $r=1$일 때는 $\Delta a^{p^n} = a^{p^n} L_n(a)$이므로 $P_n = 0$으로 성립한다. $r=2$일 때는 임의의 수열 a_n과 b_n에 대해 $\Delta(a_n b_n) = a_n(\Delta b_n) + (\Delta a_n) b_{n+1}$임에 착안하면

$$\Delta^2 a^{p^n} = \Delta(a^{p^n} L_n) = a^{p^n}(\Delta L_n + L_n L_{n+1})$$

임을 보일 수 있다. 즉, $P_n = L_n L_{n+1}$이 되며 성립하게 된다.
$r-1$일 때 성립한다고 가정해보자. 이때

$$\Delta^r a^{p^n} = \Delta(a^{p^n}(\Delta^{r-2} L_n + P_n)) = a^{p^n}(\Delta^{r-1} L_n + \Delta P_n + L_n(\Delta^{r-2} L_{n+1} + P_{n+1}))$$

이 되는데, $\Delta P_n + L_n(\Delta^{r-2} L_{n+1} + P_{n+1})$이 우리가 원하는 꼴의 다항식임을 쉽게 확인할 수 있다. 즉, 임의의 r에 대해 성립하게 된다.
이제 명제들을 각각 증명해보자.
(i) $r \le p-1$이라면, $r' \le r-1$에 대해 $\Delta^{r'} L_n$은 항상 정수인데, $\Delta^r a^{p^n}$은 $\Delta^{r'} L_n$들을 곱하고 더해서 나타낼 수 있으므로 $\Delta^r a^{p^n}$도 정수가 된다.
(ii) $a^{p-1}-1$이 p^2의 배수라면 $\Delta^r L_n$은 항상 정수이므로 자명히 $\Delta^r a^{p^n}$도 정수가 된다.
(iii) $a^{p-1}-1$이 p^2의 배수가 아니라면 $\Delta L_n, \cdots, \Delta^{p-2} L_n$은 정수인데, $\Delta^{p-1} L_n$은 p-adic order가 -1이다. 그러므로 $\Delta^p a^{p^n}$도 p-adic order가 -1이 된다.

□

§2. p-adic continuous functions

이번 절에서는 p-adic numbers에서 정의되는 연속함수에 대해 살펴보자. $\mathbb{Z}_p$에서 $\mathbb{Q}_p$로 가는 함수의 연속성은 다음과 같이 정의된다.

Definition 2.1. 어떤 함수 $f:\mathbb{Z}_p\to\mathbb{Q}_p$와 $x_0\in\mathbb{Z}_p$를 생각하자. 임의의 $\epsilon>0$에 대해 어떤 $\delta>0$이 존재하여, $|x-x_0|_p<\delta$인 모든 x에 대해 $|f(x)-f(x_0)|_p<\epsilon$이 성립한다고 하자. 이 때 **f가 x_0에서 연속**이라고 하자. 또한 임의의 x_0에 대해 f가 x_0에서 연속이면 f를 **연속함수**라고 부르자.

우선 다항식은 항상 연속함수임을 쉽게 보일 수 있다. 그것은 $|f(x)-f(y)|_p\le|x-y|_p$가 항상 성립하기 때문이다. 또한,

$$\binom{x}{n}=\frac{x(x-1)\cdots(x-n+1)}{n!}$$

으로 정의하면, 이것도 $\mathbb{Z}_p$에서 $\mathbb{Z}_p$로 가는 함수이며, $|f(x)-f(y)|_p\le|x-y|_p/|n!|_p$이므로 이 함수 역시 연속함수임을 쉽게 알 수 있다.

Mahler는 1958년에 p-adic 연속함수들이 어떠한 꼴로 나타내어질 수 있는지를 증명하였다. 하지만 우리는 Mahler의 증명보다 조금 간단한 Bojanic의 증명을 따라갈 것이다. 우선 함수 f에 대해 $a_n(m)$을

$$a_n(m)=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(m+k)$$

으로 정의하자. 이때 다음 등식이 성립함을 확인할 수 있다.

Lemma 2.2. *임의의 $m,n\ge0$에 대해*

$$\sum_{j=0}^{m}\binom{m}{j}a_{n+j}(0)=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(m+k)$$

이 성립한다.

Proof a_{n+j}의 값을 알고 있으므로 대입해보면,

$$\begin{aligned}\sum_{j=0}^{m}\binom{m}{j}\sum_{k=0}^{n+j}(-1)^{n+j-k}\binom{n+j}{k}f(k)&=\sum_{k=0}^{n+m}(-1)^{n-k}f(k)\sum_{j=\max\{k-n,0\}}^{m}(-1)^{j}\binom{n+j}{k}\binom{m}{j}\\&=\sum_{k=0}^{n+m}(-1)^{n-k}f(k)\sum_{j=0}^{m}(-1)^{j}\binom{n+j}{k}\binom{m}{j}\end{aligned}$$

가 성립함을 알 수 있다. 이때

$$\sum_{j=0}^{m}(-1)^{j}\binom{m}{j}\binom{n+j}{k}=(-1)^{m}\binom{n}{k-m}$$

임이 잘 알려져 있다. (단, $k<m$이면 우변은 0이 되는 것이다.) 이 식을 대입하면

$$\sum_{j=0}^{m}\binom{m}{j}a_{n+j}(0)=\sum_{k=0}^{n+m}(-1)^{n-k}f(k)(-1)^{m}\binom{n}{k-m}$$
$$=\sum_{k=0}^{n}(-1)^{n-k}f(k+m)\binom{n}{k}$$

을 얻는다.

□

이제 이 Lemma를 이용하여 Mahler의 정리를 증명해보자.

Theorem 2.3. (Mahler, 1958) *연속함수 $f:\mathbb{Z}_p\to\mathbb{Z}_p$에 대해, $\mathbb{Z}_p$의 원소들로 이루어진 어떤 수열 (β_n)가 존재하여 $\lim_{n\to\infty}^{(p)}\beta_n=0$이고, 임의의 x에 대해*

$$f(x)=\sum_{n=0}^{\infty}\beta_n\binom{x}{n}$$

이 성립하게 된다.

Proof. 임의의 n에 대해 $\beta_n=a_n(0)$으로 정의하자. $\beta_n\in\mathbb{Z}_p$는 성립하므로 $\lim_{n\to\infty}^{(p)}\beta_n=0$임을 증명해보자.

우선 f는 연속함수이므로 임의의 양의 정수 s에 대해, 어떤 t가 존재하여 $|x-y|_p\le p^{-t}$이면 $|f(x)-f(y)|_p\le p^{-s}$가 성립하게 된다. 즉, $|f(x+p^t)-f(x)|_p\le p^{-s}$가 임의의 $x\in\mathbb{Z}_p$에 대해 성립한다.

이때 Lemma 2.2.에 의해

$$\beta_{n+p^t}=a_{n+p^t}(0)=-\sum_{j=1}^{p^t-1}\binom{p^t}{j}a_{n+j}(0)+\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}(f(k+p^t)-f(k))$$

이며, 임의의 $1\le j\le p^t-1$에 대해 p는 $\binom{p^t}{j}$를 나누므로 임의의 $n\ge p^t$에 대해 $|\beta_n|_p\le p^{-1}$임을 알 수 있다. 또한 이것을 이용하면 다시 임의의 $n\ge 2p^t$에 대해 $|\beta_n|\le p^{-2}$임을 보일 수 있고, 계속 반복하면 $n\ge sp^t$에 대해 $|\beta_n|_p\le p^{-s}$임을 보일 수 있다. s는 충분히 크게 설정할 수 있으므로 수열 (β_n)은 반드시 0에 수렴하게 된다.

임의의 x에 대해 급수

$$g(x)=\sum_{n=0}^{\infty}\beta_n\binom{x}{n}$$

는 수렴하므로 위와 같은 함수 $g:\mathbb{Z}_p\to\mathbb{Z}_p$를 생각해볼 수 있다. 우선 $\lim_{n\to\infty}^{(p)}\beta_n=0$이므로 $g(x)$는 연속함수임을 쉽게 증명할 수 있다. 또한, 임의의 $x\in\mathbb{Z}_{\ge 0}$에 대해

$$g(x)=\sum_{i=0}^{x}a_i(0)f(i)=f(x)$$

임을 Lemma 2.2.로부터 알 수 있다. 즉 임의의 x에 대해 $f(x)=g(x)$이다. 한편, 임의의 $x\in\mathbb{Z}_p$에 대해 x로 수렴하는 양의 정수들의 수열 (x_k)를 잡을 수 있다. f와 g는 연속함수이고, 임의의 k에 대해 $f(x_k)=g(x_k)$일 것이므로

$$f(x)=f\left(\lim_{k\to\infty}^{(p)}x_k\right)=\lim_{k\to\infty}^{(p)}f(x_k)=\lim_{k\to\infty}^{(p)}g(x_k)=g\left(\lim_{k\to\infty}^{(p)}x_k\right)=g(x)$$

이다. 즉, $f=g$가 되며,

$$f(x)=\sum_{n=0}^{\infty}\beta_n\binom{x}{n}$$

임을 알 수 있다.

□

이 정리를 사용하여 다음 문제를 풀어보자.

Problem 2.4. (USA TST 2011) *p는 소수이다. 어떤 수열 $\{z_n\}_{n=0}^{\infty}$에서 임의의 $e\geq 0$에 대해 어떤 $N\geq 0$이 존재하여 $m\geq N$이면 p^e이*

$$\sum_{k=0}^{m}(-1)^k\binom{m}{k}z_k$$

를 나눈다고 할 때, 이 수열을 p-pod라 하자. 만약 수열 $\{x_n\}_{n=0}^{\infty}$와 $\{y_n\}_{n=0}^{\infty}$가 모두 p-pod라고 한다면, 수열 $\{x_ny_n\}_{n=0}^{\infty}$도 p-pod임을 증명하여라.

Solution. 수열 $\{z_n\}$에 대해

$$Z_m=\sum_{k=0}^{m}(-1)^k\binom{m}{k}z_k$$

로 정의한다면, 임의의 k에 대해

$$z_k=\sum_{i=0}^{k}Z_i\binom{k}{i}$$

가 성립한다. $\{x_n\}$과 $\{y_n\}$이 모두 p-pod이므로 $\lim_{m\to\infty}^{(p)}X_m=0$이 되고, 따라서

$$f(x)=\sum_{k=0}^{\infty}X_k\binom{x}{k},\ g(x)=\sum_{k=0}^{\infty}Y_k\binom{y}{k}$$

으로 정의된 함수 $f,g:\mathbb{Z}_p\to\mathbb{Z}_p$는 모두 연속함수가 된다. 연속함수의 곱은 연속함수이므로 $f(x)g(x)$도 연속함수가 되어 Theorem 2.3.에 의해

$$f(x)g(x)=\sum_{k=0}^{\infty}T_k\binom{x}{k}$$

인 0으로 수렴하는 수열 T_k가 존재한다. 이때, $\{x_ny_n\}$이 p-pod일 필요충분조건은 T_k가 0으로 수렴하는 것이므로 자명히 $\{x_ny_n\}$은 p-pod가 된다.

□

§3. Other applications of p-adic numbers

지금까지 p-adic numbers가 어떻게 다른 곳에 사용될 수 있는지 두 가지의 예시를 통해 알아보았다. 하지만 p-adic이 응용되는 분야는 무궁무진하다. 마지막으로, 여기에 싣지는 못하

지만 따로 공부해볼 가치는 있는 기타 잡다한 주제들을 나열만 해놓겠다.

Definition 3.1. 다음 생성함수를 생각해보자.

$$\frac{t}{e^t-1}=\sum_{m=0}^{\infty}B_m\frac{t^m}{m!}$$

여기서 B_m을 m번째 **Bernoulli number**이라고 한다.

항들을 계산해보면 알겠지만, $n>1$인 임의의 홀수 n에 대해 $B_n=0$이라는 사실을 관찰할 수 있다. 이제 n이 짝수일 때 B_n에 관한 정보를 얻고 싶은 마음이 생기는데, 다음이 성립함이 알려져 있다. Witt는 이 정리의 p-adic numbers를 사용한 증명을 발견하였다.

Theorem 3.2. (Von Staudt-Clausen theorem) *임의의 양의 정수 n에 대해,*

$$B_{2n}+\sum_{(p-1)|2n}\frac{1}{p}$$

는 정수다. (여기서 p는 소수이다.)

다음 정리는 모양은 아주 초등적으로 보이지만, 실제로 p-adic 해석학을 사용하지 않은 풀이가 알려져 있지 않은 정리이다.

Theorem 3.3. (Skolem-Mahler-Lech theorem) *어떤 수열 (x_n)에 대해, 정수들 $a_1,a_2,\cdots,a_d$가 존재하여 임의의 $n\geq 0$에 대해*

$$x_{n+d}=a_1x_{n+d-1}+a_2x_{n+d-2}+\cdots+a_dx_n$$

을 만족시킨다. 이때 어떤 유한집합 S와 정수들 $c_1,\cdots,c_N,d_1,\cdots,d_N$이 존재하여

$$\{n\geq 0:x_n=0\}=S\cup(c_1+d_1\mathbb{N})\cup\cdots\cup(c_N+d_N\mathbb{N})$$

이 성립한다. 즉, x_n의 해가 유한집합과 몇 개의 등차수열의 합집합이 된다.

마지막으로 Hasse의 local-global principle에 대해 잠깐 소개하겠다.

Hasse's local-global principle. 어떠한 사실이 모든 소수 p에 대해 $\mathbb{Q}_p$ 위에서 성립하고, $\mathbb{R}$ 위에서도 성립한다면, $\mathbb{Q}$ 위에서도 성립한다.

즉, 모든 소수 p에 대해 $\mathbb{Q}_p$ 위에서 local하게 어떤 명제가 성립한다면 $\mathbb{Q}$ 위에서 global하게도 성립한다는 것이다. 이것은 엄밀한 정리는 아니고, 실제로 반례도 존재하기는 합니다. 하지만 이것과 관련되어 다음 정리는 성립한다.

Theorem 3.4. (Hasse-Minkowski theorem) *유리수들 a_{ij}에 대해*

$$\sum_{1\leq i<j\leq n}a_{ij}x_ix_j=0$$

이 모두 0은 아닌 해 $(x_1,\cdots,x_n)$을 임의의 소수 p에 대해 $\mathbb{Q}_p$ 위에서 갖고, $\mathbb{R}$ 위에서도 갖는다고 하자. 이때 $\mathbb{Q}$ 위에서도 모두 0은 아닌 해 $(x_1,\cdots,x_n)$을 갖는다.

이 정리를 이용하면 다음을 어렵지 않게 증명할 수 있다.

Theorem 3.5. *임의의 $4^t(8k+7)$의 꼴이 아닌 양의 정수 n을 생각하자. 이때 방정식*

$$x^2+y^2+z^2=n$$

은 유리수 해를 갖는다.

또한 다음 (p-adic과 관계가 없는) 정리가 있다.

Theorem 3.6. (Davenport-Cassels theorem) *어떤 양의 정수 n이 세 유리수의 제곱의 합으로 표현 가능하다면, 세 정수의 제곱의 합으로도 표현이 가능하다.*

Theorem 3.5.과 Theorem 3.6.를 조합하면 다음이 증명된다.

Theorem 3.7. (Legendre's three-square theorem) *임의의 $4^t(8k+7)$의 꼴이 아닌 양의 정수 n을 생각하자. 이때 방정식*

$$x^2+y^2+z^2=n$$

은 정수 해를 갖는다.

This page has been intentionally left blank.

This page has been intentionally left blank.

This page has been intentionally left blank.

◇◇◇ 금주의 문제 ◇◇◇

(중등부)

1. c**가** $a^c - b^c$**을 나누는 임의의 양의 정수** a, b, c**에 대해** c**가** $(a^c - b^c)/(a-b)$**를 나눔을 보여라.**

2. 임의의 양의 정수 $n \geq s$**에 대해,** $(n)_s = n!/(n-s)!$**으로 정의하자. 이때**

$$\gcd\{(n)_s, (n+s)_s\} \mid (2s-1)_{\lfloor 4s/3 \rfloor}$$

음을 증명하여라.

3. 소수 $p > 2$**와 정수** $a_0, a_1, \cdots$**가 무한히 많은 양의 정수** n**에 대해**

$$\sum_{k=0}^{n} p^k \binom{n}{k} a_k = 0$$

을 만족시킨다고 가정하자. 이때 모든 n**에 대해** $a_n = 0$**임을 보여라.** [2)]

---

2) 기존의 문제에는 $p > 2$라는 조건이 없었으나, 검토 중 $p = 2$이고 $a_0 = 0$, $a_k = (-1)^k$인 경우 임의의 짝수 n에 대해 조건식이 성립한다는 사실을 발견하여 문제를 수정하게 되었습니다. 이 점에 대해 양해를 구합니다.

◇◇◇ 금주의 문제 ◇◇◇

(고등부)

1. 임의의 양의 정수 $n \geq s$에 대해, $(n)_s = n!/(n-s)!$으로 정의하자. 이때

$$\gcd\{(n)_s, (n+s)_s\} \mid (2s-1)_{\lfloor 4s/3 \rfloor}$$

음을 증명하여라.

2. 소수 $p > 2$와 정수 $a_0, a_1, \cdots$가 무한히 많은 양의 정수 n에 대해

$$\sum_{k=0}^{n} p^k \binom{n}{k} a_k = 0$$

을 만족시킨다고 가정하자. 이때 모든 n에 대해 $a_n = 0$임을 보여라. 3)

3. 단위 정사각형이 넓이가 같은 n개의 삼각형으로 분할되었다. 만약 모든 삼각형의 꼭짓점이 유리수 좌표를 갖는다면, n이 짝수임을 증명하여라.

3) 기존의 문제에는 $p > 2$라는 조건이 없었으나, 검토 중 $p = 2$이고 $a_0 = 0$, $a_k = (-1)^k$인 경우 임의의 짝수 n에 대해 조건식이 성립한다는 사실을 발견하여 문제를 수정하게 되었습니다. 이 점에 대해 양해를 구합니다.