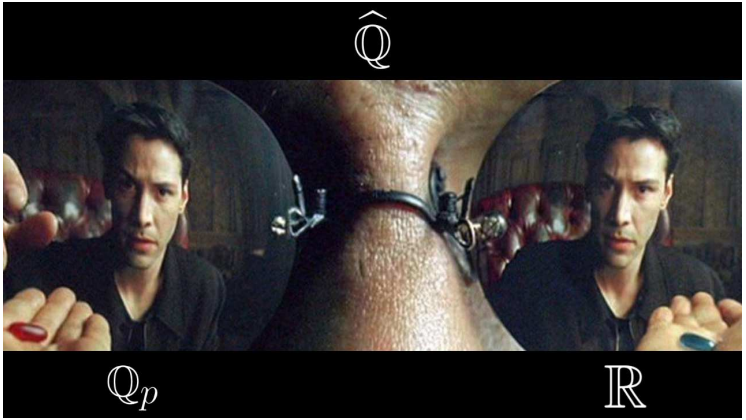
Geometria z Algebrą Liniową II*

Arkadiusz Męcel

WYKŁAD 17, 6.05.2021 r.

Na ostatnim wykładzie:

- przestrzenie metryczne, zbieżność, norma w ciele (i metryka indukowana),
- równoważność norm i tw. Ostrowskiego, konstrukcja uzupełnienia $\widehat{K}$ ciała K,
- wykładnik p-adyczny liczby wymiernej $\mathbb{Q}$, norma p-adyczna na $\mathbb{Q}$,
- ciało liczb p-adycznych $\mathbb{Q}_p$ jako $\widehat{\mathbb{Q}}$ (z normą $|.|_p$), rozwinięcie p-adyczne.



Przypomnienie *analitycznej konstrukcji* elementów $\mathbb{Q}_p$, gdzie p – l. pierwsza.

Przypomnienie *analitycznej konstrukcji* elementów $\mathbb{Q}_p$, gdzie p – l. pierwsza.

- Niech $m < n$ będą całkowite (dodatnie lub ujemne) i dla każdego $m \leq i \leq n$ niech $0 \leq d_i < p$ będzie liczbą całkowitą. Zakładając, że $d_m \neq 0$ nietrudno pokazać, że:

$$\left| \sum_{i=m}^{n} d_i p^i \right|_p = p^{-m}.$$

Przypomnienie *analitycznej konstrukcji* elementów $\mathbb{Q}_p$, gdzie p – l. pierwsza.

- Niech $m < n$ będą całkowite (dodatnie lub ujemne) i dla każdego $m \leq i \leq n$ niech $0 \leq d_i < p$ będzie liczbą całkowitą. Zakładając, że $d_m \neq 0$ nietrudno pokazać, że:

$$\left| \sum_{i=m}^{n} d_i p^i \right|_p = p^{-m}.$$

- Ustalmy $k \in \mathbb{Z}$. Nieskończony ciąg $(d_m, d_{m+1}, \ldots)$, gdzie $d_i \in \{0, 1, \ldots, p-1\}$, dla każdego $i \geq m$, oraz $d_m \neq 0$ wyznacza jednoznacznie nieskończony ciąg Cauchy'ego w $(\mathbb{Q}, |.|_p)$:

$$(\spadesuit) \qquad \begin{aligned} A_1 &= d_m p^m \\ A_2 &= d_m p^m + d_{m+1} p^{m+1} \\ A_3 &= d_m p^m + d_{m+1} p^{m+1} + d_{m+2} p^{m+2} \\ &\vdots \end{aligned}$$

Przypomnienie *analitycznej konstrukcji* elementów $\mathbb{Q}_p$, gdzie p – l. pierwsza.

- Pokazaliśmy, że każdy ciąg Cauchy'ego w $(\mathbb{Q}, |.|_p)$ jest równoważny do dokładnie jednego ciągu $(A_1, A_2, \ldots)$ postaci (♠) i w związku z tym każdy element $\mathbb{Q}_p$ traktować można jako szereg postaci:

$$A = \lim_{i \to \infty} A_i = d_m p^m + d_{m+1} p^{m+1} + d_{m+2} p^{m+2} + \ldots . \quad (\dagger)$$

  Co więcej, normę p-adyczną można rozszerzyć w sposób ciągły z $\mathbb{Q}$ do $\mathbb{Q}_p$.

Przypomnienie *analitycznej konstrukcji* elementów $\mathbb{Q}_p$, gdzie p – l. pierwsza.

- Pokazaliśmy, że każdy ciąg Cauchy'ego w $(\mathbb{Q}, |.|_p)$ jest równoważny do dokładnie jednego ciągu $(A_1, A_2, \ldots)$ postaci (♠) i w związku z tym każdy element $\mathbb{Q}_p$ traktować można jako szereg postaci:

$$A = \lim_{i \to \infty} A_i = d_m p^m + d_{m+1} p^{m+1} + d_{m+2} p^{m+2} + \ldots . \quad (\dagger)$$

  Co więcej, normę p-adyczną można rozszerzyć w sposób ciągły z $\mathbb{Q}$ do $\mathbb{Q}_p$.

- W związku z tym każda liczba $A \in \mathbb{Q}_p$ postaci (†) ma jednoznaczne rozwinięcie p-adyczne postaci:

$$A = \begin{cases} \ldots d_1 d_0, d_{-1} \ldots d_m & , \text{ dla } m \leq 0, \\ \ldots d_{m+1} d_m \underbrace{0 \ldots 0}_{m-1} & , \text{ dla } m > 0 \end{cases}$$

Przypomnienie *analitycznej konstrukcji* elementów $\mathbb{Q}_p$, gdzie p – l. pierwsza.

- Pokazaliśmy, że każdy ciąg Cauchy'ego w $(\mathbb{Q}, |.|_p)$ jest równoważny do dokładnie jednego ciągu $(A_1, A_2, \ldots)$ postaci (♠) i w związku z tym każdy element $\mathbb{Q}_p$ traktować można jako szereg postaci:

$$A = \lim_{i \to \infty} A_i = d_m p^m + d_{m+1} p^{m+1} + d_{m+2} p^{m+2} + \ldots . \quad (\dagger)$$

  Co więcej, normę p-adyczną można rozszerzyć w sposób ciągły z $\mathbb{Q}$ do $\mathbb{Q}_p$.

- W związku z tym każda liczba $A \in \mathbb{Q}_p$ postaci (†) ma jednoznaczne rozwinięcie p-adyczne postaci:

$$A = \begin{cases} \ldots d_1 d_0, d_{-1} \ldots d_m & , \text{ dla } m \leq 0, \\ \ldots d_{m+1} d_m \underbrace{0 \ldots 0}_{m-1} & , \text{ dla } m > 0 \end{cases}$$

- Analiza w $\mathbb{Q}_p$ wygląda zgoła inaczej, niż w $\mathbb{Q}$. Na przykład dla każdej liczby pierwszej p mamy (w $\mathbb{Q}_p$): $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \ldots$

Uwaga (dobra nowina nad $\mathbb{Q}_p$?)

Niech $A_1, A_2, \ldots \in \mathbb{Q}_p$. Wówczas szereg $\sum_k A_k$ jest zbieżny wtedy i tylko wtedy, gdy ciąg A_k jest zbieżny do zera w normie $|.|_p$.

Uwaga (dobra nowina nad $\mathbb{Q}_p$?)

Niech $A_1, A_2, \ldots \in \mathbb{Q}_p$. Wówczas szereg $\sum_k A_k$ jest zbieżny wtedy i tylko wtedy, gdy ciąg A_k jest zbieżny do zera w normie $|.|_p$.

Dowód. Dla $m \geq n$ stosujemy fakt, że $|.|_p$ jest niearchimedesowska (także w $\mathbb{Q}_p$):

$$\left| \sum_{k=1}^{m} A_k - \sum_{k=1}^{n} A_k \right|_p = \left| \sum_{k=n+1}^{m} A_k \right|_p \leq \max_{n<k\leq m} |A_k|_p$$

Skoro $A_k \to 0$, to ciąg sum częściowych szeregu $\sum_k A_k$ jest Cauchy'ego w $|.|_p$.
To znaczy, że ciąg ten ma granicę ($\mathbb{Q}_p$ jest, zgodnie z konstrukcją, zupełna).
W drugą stronę stosujemy standardowe argumenty znane z analizy rzeczywistej.

* * *

Niestety niektóre *porządne* funkcje nad $\mathbb{R}$ (określone na całej prostej lub półprostej) określone analogicznymi szeregami w $\mathbb{Q}_p$ mają zupełnie inne promienie zbieżności. Więcej: S. Katok: *p-adic Analysis Compared with Real*.

Uwaga (dobra nowina nad $\mathbb{Q}_p$?)

Niech $A_1, A_2, \ldots \in \mathbb{Q}_p$. Wówczas szereg $\sum_k A_k$ jest zbieżny wtedy i tylko wtedy, gdy ciąg A_k jest zbieżny do zera w normie $|.|_p$.

Przykłady. Niech $x \in \mathbb{Q}_p$ oraz $|x|_p = p^{-v_p(x)}$ (to definicja v_p na $\mathbb{Q}_p$).

- (Bolesne) Poniższy szereg jest zbieżny wtedy i tylko wtedy, gdy $v_p(x) > \frac{1}{p-1}$:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$$

- (Radosne) Poniższy szereg jest zbieżny wtedy i tylko wtedy, gdy $v_p(x) > 0$:

$$\ln(1+x) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{x^k}{k} = x - \frac{x^2}{2} + \frac{x^3}{3} \ldots$$

Uwaga (dobra nowina nad $\mathbb{Q}_p$?)

Niech $A_1, A_2, \ldots \in \mathbb{Q}_p$. Wówczas szereg $\sum_k A_k$ jest zbieżny wtedy i tylko wtedy, gdy ciąg A_k jest zbieżny do zera w normie $|.|_p$.

Przykłady (teraz coś pocieszającego dla Olimpijczyków).

- Zostańmy jeszcze przy

$$\ln(1+x) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{x^k}{k} = x - \frac{x^2}{2} + \frac{x^3}{3} \ldots, \quad v_p(x) > 0$$

  i weźmy $p = 2$ oraz $x = -2$. Mamy też $v_2(-2) = 2^{-v_2(-2)} = \frac{1}{2}$, czyli jesteśmy w promieniu zbieżności szeregu $\ln(1+x)$.

Uwaga (dobra nowina nad $\mathbb{Q}_p$?)

Niech $A_1, A_2, \ldots \in \mathbb{Q}_p$. Wówczas szereg $\sum_k A_k$ jest zbieżny wtedy i tylko wtedy, gdy ciąg A_k jest zbieżny do zera w normie $|.|_p$.

Przykłady (teraz coś pocieszającego dla Olimpijczyków).

- Zostańmy jeszcze przy

$$\ln(1+x) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{x^k}{k} = x - \frac{x^2}{2} + \frac{x^3}{3} \ldots, \quad v_p(x) > 0$$

i weźmy $p = 2$ oraz $x = -2$. Mamy też $v_2(-2) = 2^{-v_2(-2)} = \frac{1}{2}$, czyli jesteśmy w promieniu zbieżności szeregu $\ln(1+x)$.

$$\ln(-1) = \ln(1-2) = -\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \ldots\right)$$

W $\mathbb{Q}_2$ mają też sens rachunki: $2\ln(-1) = \ln((-1)^2) = \ln(1) = 0$.

Uwaga (dobra nowina nad $\mathbb{Q}_p$?)

Niech $A_1, A_2, \ldots \in \mathbb{Q}_p$. Wówczas szereg $\sum_k A_k$ jest zbieżny wtedy i tylko wtedy, gdy ciąg A_k jest zbieżny do zera w normie $|.|_p$.

Przykłady (teraz coś pocieszającego dla Olimpijczyków).

- Dostaliśmy zatem całkiem poważne zadanie teorioliczbowe:
  dla każdego całkowitego $M > 0$ istnieje liczba n taka, że:

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \ldots + \frac{2^n}{n} \equiv 0 \bmod 2^M.$$

  Rzeczywiście, powyższa suma to suma częściowa szeregu $\ln(1-2)$, który jest zbieżny do 0. A zatem powyższe wyrażenie w normie $|.|_2$ zbiega do zera, czyli dzieli kolejne coraz wyższe potęgi liczby 2, wraz ze wzrostem n.

  Elementarny dowód tej obserwacji jest dość niebanalny (zachęcam do prób!).

Uwaga (dobra nowina nad $\mathbb{Q}_p$?)

Niech $A_1, A_2, \ldots \in \mathbb{Q}_p$. Wówczas szereg $\sum_k A_k$ jest zbieżny wtedy i tylko wtedy, gdy ciąg A_k jest zbieżny do zera w normie $|.|_p$.

Pytania. Skoro $|n!|_p \to 0$ (skorzystaj z formuły na $v_p(n!)$), to szereg

$$\sum_{n=0}^{\infty} n! \qquad (\S)$$

jest zbieżny w $\mathbb{Q}_p$. Od lat 70' są jednak nierozwiązane dwa problemy:

- czy szereg $(\S)$ ma dla jakiegoś p sumę 0?
- czy dla pewnego p ma sumę wymierną w $\mathbb{Q}_p$ (czyli, bez wdawania się w szczegóły: rozwinięcie p-adyczne sumy tego szeregu jest periodyczne)?

Ciekawostka: dla każdego n naturalnego, $n \geq 1$, zachodzi $\prod_{p \in \mathbb{P}} |n!|_p = \frac{1}{n!}$.

Znacznie więcej w pracy (licealistki!) S. Casacuberta: *Open problems in factorials*.

Problemy lokalno-globalne. Wprowadzenie.

- Rozważmy równanie
$$x^3 - 2x + 17 = 0.$$
Aby stwierdzić czy ma ono rozwiązania całkowite wystarczy zauważyć, że modulo 5 równanie to ma postać:
$$x^3 + 3x + 2 = 0$$
i nie ma żadnych rozwiązań w ciele $\mathbb{Z}_5$.

- Stąd (korzystając z prostych argumentów algebraicznych) wnioskuje się, że wyjściowe równanie nie ma rozwiązań całkowitych (ani wymiernych).

- Patrzenie na równanie modulo liczba pierwsza daje następującą intuicję ogólnego postępowania: patrz **lokalnie** (modulo 5), gdy otrzymać wynik **globalny** (w $\mathbb{Z}$). Niestety, gdybyśmy znaleźli rozwiązanie powyższego równania w $\mathbb{Z}_5$, to nie mielibyśmy pewności, że istnieje ono nad $\mathbb{Z}$ czy też $\mathbb{Q}$.

Problemy lokalno-globalne. Wprowadzenie.

Twierdzenie (patrz np. https://arxiv.org/pdf/2102.08379.pdf)

Dana jest liczba całkowita $n \neq 1$ spełniająca warunki:

- n jest niepodzielna przez sześcian liczby pierwszej,
- $n \equiv 1 \pmod 9$,
- jeśli liczba pierwsza q dzieli n, to $q \equiv 1 \pmod 3$.

Wówczas wielomian:

$$(x^3 - n)(x^2 + 3) = 0$$

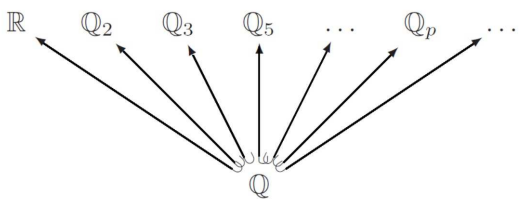
nie ma pierwiastków wymiernych, choć ma rozwiązania w dowolnym ciele $\mathbb{Z}_p$.

Istnienie wielomianów o współczynnikach w $\mathbb{Z}$ takich jak powyższe przeczy prawdziwości *zasady lokalno-globalnej* dla dowolnego równania $f = 0$, $f \in \mathbb{Q}[x]$. Pytanie: czy po ograniczeniu do pewnych klas równań zasada ta może działać (i jak ją dokładnie sformułować)? To jedno z centralnych zagadnień teorii liczb.

Zasada lokalno-globalna (Hasse-Minkowski), 1921

Niech q będzie formą kwadratową na skończenie wymiarowej przestrzeni nad ciałem $\mathbb{Q}$ oraz niech q_p oznacza formę q rozważaną[a] nad $\mathbb{Q}_p$, gdzie $p \in \mathbb{P}$ lub $p = \infty$ (konwencja: $\mathbb{Q}_\infty = \mathbb{R}$). Wówczas q reprezentuje 0 (jest izotropowa) wtedy i tylko wtedy, gdy forma kwadratowa q_p reprezentuje 0, dla każdego $p \in \mathbb{P} \cup \{\infty\}$.

[a] Ma to sens, bo dla każdego p mamy $\mathbb{Q} \subset \mathbb{Q}_p$.



Jasne jest, że dowód wystarczy przeprowadzić dla form kwadratowych postaci: $a_1 x_1^2 + \ldots + a_n x_n^2$, gdzie $a_1, \ldots, a_n \in \mathbb{Q}$ (ale to niewiele ułatwia...)

Lemat

Liczba $x \in \mathbb{Q}$ jest n-tą potęgą liczby wymiernej wtedy i tylko wtedy, gdy jest n-tą potęgą w $\mathbb{Q}_p$, dla każdego $p \leq \infty$.

Dowód. Dla każdego $x \in \mathbb{Q}$ mamy po prostu:

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

Jeśli x jest n-tą potęgą w $\mathbb{R}$ to wyznacza znak powyższego wyrażenia. Jeśli zaś jest n-tą potęgą w $\mathbb{Q}_p$, to oczywiście $v_p(x)$ jest podzielne przez n. Stąd już łatwo wynika, że x jest n-tą potęgą w $\mathbb{Q}$.

* * *

Lemat jest prosty, ale kluczowa idea jest taka, że korzystając z zasady lokalno-globalnej w praktyce sprawdzić musimy reprezentowalność formy q_p jedynie w skończenie wielu $\mathbb{Q}_p$ (tylko trzeba wiedzieć w których).

Dowodzimy tw. H-M dla $q : \mathbb{Q}^2 \to \mathbb{Q}$. Niech $q(x_1, x_2) = a_1 x_1^2 + a_2 x_2^2$.

- Oczywiście twierdzenie jest prawdziwe dla f wtw, gdy jest prawdziwe dla $a_1 f$ (jeśli $a_1 = 0$, to teza jest oczywista). Więc można zakładać, że $q(x_1, x_2) = x_1 + a x_2^2$.

Dowodzimy tw. H-M dla $q : \mathbb{Q}^2 \to \mathbb{Q}$. Niech $q(x_1, x_2) = a_1 x_1^2 + a_2 x_2^2$.

- Oczywiście twierdzenie jest prawdziwe dla f wtw, gdy jest prawdziwe dla $a_1 f$ (jeśli $a_1 = 0$, to teza jest oczywista). Więc można zakładać, że $q(x_1, x_2) = x_1 + a x_2^2$.
- Skoro $q_\infty(x, y) = 0$, dla pewnego niezerowego (x, y), to możemy założyć, że $q(x_1, x_2) = x_1 - a x_2$, dla pewnego $a > 0$.

Dowodzimy tw. H-M dla $q : \mathbb{Q}^2 \to \mathbb{Q}$. Niech $q(x_1, x_2) = a_1 x_1^2 + a_2 x_2^2$.

- Oczywiście twierdzenie jest prawdziwe dla f wtw, gdy jest prawdziwe dla $a_1 f$ (jeśli $a_1 = 0$, to teza jest oczywista). Więc można zakładać, że $q(x_1, x_2) = x_1 + a x_2^2$.
- Skoro $q_\infty(x, y) = 0$, dla pewnego niezerowego (x, y), to możemy założyć, że $q(x_1, x_2) = x_1 - a x_2$, dla pewnego $a > 0$.
- Skoro q_p reprezentuje 0, czyli jest izotropowa, to zgodnie z lematem sprzed dwóch wykładów (lub ze zwykłej obserwacji wynika), że forma $q(x) = x_1^2$ reprezentuje a. Czyli a jako element każdego z $\mathbb{Q}_p$ jest kwadratem.

Dowodzimy tw. H-M dla $q : \mathbb{Q}^2 \to \mathbb{Q}$. Niech $q(x_1, x_2) = a_1 x_1^2 + a_2 x_2^2$.

- Oczywiście twierdzenie jest prawdziwe dla f wtw, gdy jest prawdziwe dla $a_1 f$ (jeśli $a_1 = 0$, to teza jest oczywista). Więc można zakładać, że $q(x_1, x_2) = x_1 + a x_2^2$.
- Skoro $q_\infty(x, y) = 0$, dla pewnego niezerowego (x, y), to możemy założyć, że $q(x_1, x_2) = x_1 - a x_2$, dla pewnego $a > 0$.
- Skoro q_p reprezentuje 0, czyli jest izotropowa, to zgodnie z lematem sprzed dwóch wykładów (lub ze zwykłej obserwacji wynika), że forma $q(x) = x_1^2$ reprezentuje a. Czyli a jako element każdego z $\mathbb{Q}_p$ jest kwadratem.
- Mamy jednak
$$a = \prod_{p<\infty} p^{v_p(a)}.$$
Stąd $v_p(a)$ jest parzyste, dla każdego p, czyli liczba a jest kwadratem w $\mathbb{Q}$, a więc q reprezentuje 0 w $\mathbb{Q}$.

Dla form na $\mathbb{Q}^3$ twierdzenie H-M wynika z następującego twierdzenia.

Twierdzenie (Legendre), 1785

Niech a, b, c będą niezerowymi, bezkwadratowymi liczbami całkowitymi parami względnie pierwszymi. Wówczas następujące warunki są równoważne:

- równanie $ax^2 + by^2 + cz^2 = 0$ ma niezerowe rozwiązanie,
- nie wszystkie z liczb a, b, c mają ten sam znak, oraz liczby $-bc, -ca, -ab$ są resztami kwadratowymi odpowiednio modulo a, b, c.

Dla form na $\mathbb{Q}^3$ twierdzenie H-M wynika z następującego twierdzenia.

Twierdzenie (Legendre), 1785

Niech a, b, c będą niezerowymi, bezkwadratowymi liczbami całkowitymi parami względnie pierwszymi. Wówczas następujące warunki są równoważne:

- równanie $ax^2 + by^2 + cz^2 = 0$ ma niezerowe rozwiązanie,
- nie wszystkie z liczb a, b, c mają ten sam znak, oraz liczby $-bc, -ca, -ab$ są resztami kwadratowymi odpowiednio modulo a, b, c.

Jeśli chcemy reprezentowalności 0 dla formy $ax^2 + by^2 + cz^2$, to:

- jeśli którakolwiek z liczb a, b, c wynosi 0, to oczywiście mamy, co chcemy,
- to, że wystarczy sprawdzić tezę gdy a, b, c są względnie pierwsze jest jasne, a tak naprawdę można pokazać, że abc musi być bezkwadratowe (jw.),
- liczby a, b, c muszą być różnych znaków (reprezentowalność 0 w $\mathbb{Q}_\infty = \mathbb{R}$),
- a dalej... używa się Lematu Hensela.

Definicja

Liczbę p-adyczną $A \in \mathbb{Q}_p$ nazywamy **całkowitą** liczbą p-adyczną, jeśli jej rozwinięcie zawiera jedynie nieujemne potęgi p (równoważnie $|A|_p \leq 1$). Oznaczenie: $\mathbb{Z}_p$.

Widzimy niefortunną kolizję oznaczeń: dlatego wielu autorów jednak stosuje dla ciał notację $\mathbb{F}_p$ (nie tylko dlatego: F – Field, Z – Zahl). Dlatego do końca **tego** wykładu (i tylko tego) ciało p-elementowe oznaczamy (jednak) przez $\mathbb{F}_p$.

Definicja

Niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$, gdzie K jest dowolnym[a] pierścieniem. **Formalną pochodną** wielomianu f nazywamy wielomian postaci:

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + 2 a_2 x + a_1.$$

[a] Na nasze potrzeby: $\mathbb{Z}$ lub $\mathbb{Z}_p$, ale oczywiście definicja jest ogólna.

O czym mówi ten Lemat Hensela?

- Dane: wielomian $q \in \mathbb{Z}[x]$, który rozważamy jako wielomian $q_p \in \mathbb{Z}_p[x]$ i pytamy, czy q_p ma pierwiastek w $\mathbb{Q}_p$. Tego bowiem potrzebujemy do praktycznego korzystania (np.) z twierdzenia Hassego-Minkowskiego.

O czym mówi ten Lemat Hensela?

- Dane: wielomian $q \in \mathbb{Z}[x]$, który rozważamy jako wielomian $q_p \in \mathbb{Z}_p[x]$ i pytamy, czy q_p ma pierwiastek w $\mathbb{Q}_p$. Tego bowiem potrzebujemy do praktycznego korzystania (np.) z twierdzenia Hassego-Minkowskiego.
- Mamy też możliwość redukcji wielomianu q modulo p do wielomianu $\overline{q}_p$ i tu (czyli w $\mathbb{F}_p$) jest łatwo szukać pierwiastków.

O czym mówi ten Lemat Hensela?

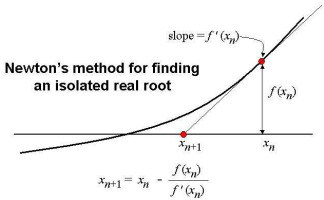
- Dane: wielomian $q \in \mathbb{Z}[x]$, który rozważamy jako wielomian $q_p \in \mathbb{Z}_p[x]$ i pytamy, czy q_p ma pierwiastek w $\mathbb{Q}_p$. Tego bowiem potrzebujemy do praktycznego korzystania (np.) z twierdzenia Hassego-Minkowskiego.
- Mamy też możliwość redukcji wielomianu q modulo p do wielomianu $\overline{q}_p$ i tu (czyli w $\mathbb{F}_p$) jest łatwo szukać pierwiastków.
- Lemat Hensela gwarantuje, że jesli znajdziemy pierwiastek a wielomianu $\overline{q}_p$ i upewnimy się, że nie jest on pierwiastkiem $\overline{q'_p}$ to mamy gwarancję istnienia pierwiastka w $q_p \in \mathbb{Z}_p[x]$, który jest **podniesieniem pierwiastka** a z $\mathbb{F}_p$. Co to znaczy? Zobaczymy zaraz na przykładzie.

O czym mówi ten Lemat Hensela?

- Dane: wielomian $q \in \mathbb{Z}[x]$, który rozważamy jako wielomian $q_p \in \mathbb{Z}_p[x]$ i pytamy, czy q_p ma pierwiastek w $\mathbb{Q}_p$. Tego bowiem potrzebujemy do praktycznego korzystania (np.) z twierdzenia Hassego-Minkowskiego.
- Mamy też możliwość redukcji wielomianu q modulo p do wielomianu $\overline{q}_p$ i tu (czyli w $\mathbb{F}_p$) jest łatwo szukać pierwiastków.
- Lemat Hensela gwarantuje, że jesli znajdziemy pierwiastek a wielomianu $\overline{q}_p$ i upewnimy się, że nie jest on pierwiastkiem $\overline{q'_p}$ to mamy gwarancję istnienia pierwiastka w $q_p \in \mathbb{Z}_p[x]$, który jest **podniesieniem pierwiastka** a z $\mathbb{F}_p$. Co to znaczy? Zobaczymy zaraz na przykładzie.
- Co więcej, pokażemy, że wielomian o współczynnikach całkowitych ma pierwiastek w $\mathbb{Z}_p$ wtedy i tylko wtedy, gdy ma całkowity pierwiastek modulo p^k, dla każdego $k \geq 1$. W szczególności: jeśli wielomian nie ma pierwiastka w $\mathbb{F}_p$, to nie ma pierwiastka w $\mathbb{Z}_p$, co upraszcza korzystanie z tw. H-M.

Idea Lematu Hensela a metoda Newtona szukania pierwiastków w $\mathbb{R}$.

- Niech $f \in \mathbb{R}[x]$. Zaczynamy od pewnej liczby x_0 i próbujemy zbliżyć się do pierwiastka za pomocą kolejnych przybliżeń:



- Może się niestety zdarzyć, że się nie zbliżymy, np. dla $f(x) = x^3 - x$ oraz startując od $x_0 = 1/\sqrt{5}$ mamy $a_1 = -1/\sqrt{5}$, $a_2 = 1/\sqrt{5}$ i zbieżności nie ma.

- Idea Lematu Hensela: startując od a_1 takiego, że $f(a_1) \equiv 0 \bmod p$ oraz $f'(a_1) \not\equiv 0 \bmod p$ konstruuje się przybliżenia a_n (pierwsze n cyfr się zgadza) pierwiastka α wielomianu f takie, że $f(a_n) \equiv 0 \bmod p^n$ i pokazuje się, że:

$$a_{n+1} = a_n - f(a_n)/f'(a_n).$$

Przykład. Od pierwiastka mod $\mathbb{F}_p$ do pierwiastka w $\mathbb{Q}_p$.

- Wiemy, że $7 \equiv 1^2 \bmod 3$, czyli dla $f(x) = x^2 - 7$ mamy $f(1) \equiv 0 \bmod 3$.

Przykład. Od pierwiastka mod $\mathbb{F}_p$ do pierwiastka w $\mathbb{Q}_p$.

- Wiemy, że $7 \equiv 1^2 \bmod 3$, czyli dla $f(x) = x^2 - 7$ mamy $f(1) \equiv 0 \bmod 3$.
- Choć $7 \not\equiv 1^2 \bmod 9$, to $7 \equiv (1+3)^2 \mod 9$, czyli 1 można **podnieść** do pierwiastka modulo 3^2, który daje taką samą resztę przy dzieleniu przez 3.

Przykład. Od pierwiastka mod $\mathbb{F}_p$ do pierwiastka w $\mathbb{Q}_p$.

- Wiemy, że $7 \equiv 1^2 \bmod 3$, czyli dla $f(x) = x^2 - 7$ mamy $f(1) \equiv 0 \bmod 3$.
- Choć $7 \not\equiv 1^2 \bmod 9$, to $7 \equiv (1+3)^2 \mod 9$, czyli 1 można **podnieść** do pierwiastka modulo 3^2, który daje taką samą resztę przy dzieleniu przez 3.
- Mamy też:

$$7 \equiv (1 + 3 + 3^2)^2 \bmod 3^3$$
$$7 \equiv (1 + 3 + 3^2)^2 \bmod 3^4$$
$$7 \equiv (1 + 3 + 3^2 + 2 \cdot 3^4) \bmod 3^5$$
$$\vdots$$
$$7 \equiv (1 + 3 + 3^2 + 2 \cdot 3^4 + 2 \cdot 3^7 + 3^8 + 3^9 + 2 \cdot 3^{10})^2 \bmod 3^{11}$$

Przykład. Od pierwiastka mod $\mathbb{F}_p$ do pierwiastka w $\mathbb{Q}_p$.

- Wiemy, że $7 \equiv 1^2 \bmod 3$, czyli dla $f(x) = x^2 - 7$ mamy $f(1) \equiv 0 \bmod 3$.
- Choć $7 \not\equiv 1^2 \bmod 9$, to $7 \equiv (1+3)^2 \mod 9$, czyli 1 można **podnieść** do pierwiastka modulo 3^2, który daje taką samą resztę przy dzieleniu przez 3.
- Mamy też:

$$
\begin{aligned}
7 &\equiv (1+3+3^2)^2 \bmod 3^3 \\
7 &\equiv (1+3+3^2)^2 \bmod 3^4 \\
7 &\equiv (1+3+3^2+2\cdot 3^4) \bmod 3^5 \\
&\vdots \\
7 &\equiv (1+3+3^2+2\cdot 3^4+2\cdot 3^7+3^8+3^9+2\cdot 3^{10})^2 \bmod 3^{11}
\end{aligned}
$$

- Narzuca się więc podejrzenie, że 7 jest kwadratem w $\mathbb{Q}_3$, o pierwiastku:

$$1+3+3^2+2\cdot 3^4+2\cdot 3^7+3^8+3^9+2\cdot 3^{10}+\ldots$$

będącym **podniesieniem** pierwiastka mod 3 do pierwiastka mod 3^n, $n \geq 1$.

Lemat Hensela

Niech $f \in \mathbb{Z}_p[x]$. Załóżmy, że istnieje $a_1 \in \mathbb{Z}_p$ taka, że:

$$f(a_1) \equiv 0 \bmod p \cdot \mathbb{Z}_p$$

gdzie $p \cdot \mathbb{Z}_p = \{p \cdot q | q \in \mathbb{Z}_p\}$ oraz

$$f'(a_1) \not\equiv 0 \bmod p \cdot \mathbb{Z}_p.$$

Wówczas istnieje dokładnie jedna $\alpha \in \mathbb{Z}_p$ taka, że

$$\alpha \equiv a_1 \bmod p \cdot \mathbb{Z}_p \quad \text{oraz } f(\alpha) = 0.$$

Uwaga. Oczywiście $\mathbb{Z} \subseteq \mathbb{Z}_p$ oraz każde rozwinięcie p-adyczne liczby całkowitej dodatniej jest skończone (to po prostu rozwinięcie w bazie p), więc jeśli $f \in \mathbb{Z}[x]$ oraz $\alpha \in \mathbb{Z}$, to warunek $f(a_1) \equiv 0 \bmod p \cdot \mathbb{Z}_p$ jest podzielnością $f(a_1)$ przez p. Natomiast ogólnie dla $a, b \in \mathbb{Z}_p$ mamy: $a - b \in p^n \cdot \mathbb{Z}_p \Leftrightarrow |a - b|_p \leq 1/p^n$.

Lemat Hensela

Niech $f \in \mathbb{Z}_p[x]$. Załóżmy, że istnieje $a_1 \in \mathbb{Z}_p$ taka, że: $f(a_1) \equiv 0 \bmod p \cdot \mathbb{Z}_p$ oraz $f'(a_1) \not\equiv 0 \bmod p \cdot \mathbb{Z}_p$. Wówczas istnieje dokładnie jedna $\alpha \in \mathbb{Z}_p$ taka, że $\alpha \equiv a_1 \bmod p \cdot \mathbb{Z}_p$ oraz $f(\alpha) = 0$.

Przykład. Niech $f(x) = x^3 - 2$. Mamy

$$f(3) = 25 \equiv 0 \bmod 5, \quad \text{oraz} \quad f'(3) = 27 \not\equiv 0 \bmod 5.$$

A zatem lemat Hensela mówi, że istnieje dokładnie jeden pierwiastek sześcienny liczby 2 w $\mathbb{Z}_5$, który przystaje 3 modulo 5. jest to *w przybliżeniu*:

$$3 + 2 \cdot 5^2 + 2 \cdot 5^3 + 3 \cdot 5^4 + \ldots \qquad (\diamondsuit)$$

Nie poruszamy tu tego wątku, ale ten pierwiastek sześcienny z liczby 2 jest *liczbą niewymierną* także w sensie p-adycznym (jego rozwinięcie nie jest periodyczne od pewnego miejsca lub równoważnie: jest to iloraz elementów z $\mathbb{Z}_p$), co oznacza, że możemy za pomocą układów kongruencji wyznaczać kolejne przybliżenia α postaci $(\diamondsuit)$, ale zapis p-adyczny α pozostanie dla nas nieznany (tak, jak i „w $\mathbb{R}$”).

Lemat Hensela

Niech $f \in \mathbb{Z}_p[x]$. Załóżmy, że istnieje $a_1 \in \mathbb{Z}_p$ taka, że: $f(a_1) \equiv 0 \bmod p \cdot \mathbb{Z}_p$ oraz $f'(a_1) \not\equiv 0 \bmod p \cdot \mathbb{Z}_p$. Wówczas istnieje dokładnie jedna $\alpha \in \mathbb{Z}_p$ taka, że $\alpha \equiv a_1 \bmod p \cdot \mathbb{Z}_p$ oraz $f(\alpha) = 0$.

Przykład. Weźmy $f(x) = x^3 - x - 2$. Mamy

$$f(0) \equiv 0 \bmod 2, \quad \text{oraz} \quad f'(0) \not\equiv 0 \bmod 2,$$
$$f(1) \equiv 0 \bmod 2, \quad \text{oraz} \quad f'(1) \equiv 0 \bmod 2.$$

Czyli istnieje dokładnie jedno $\alpha \in \mathbb{Z}_2$ takie, że $f(\alpha) = 0$ oraz $\alpha \equiv 0 \bmod 2$.

Natomiast 1 **nie podnosi** się do pierwiastka w $\mathbb{Z}_2$, bo nie podnosi się nawet modulo 4: jeśli $\beta \in \mathbb{Z}_2$ oraz $\beta \equiv 1 \bmod 2$, to mamy $\beta \equiv 1 \bmod 4$ lub $\beta \equiv 3 \bmod 4$. Ale

$$f(1) \equiv 2 \bmod 4 \quad \text{oraz} \quad f(3) \equiv 2 \bmod 4,$$

więc stąd $f(\beta) \equiv 2 \not\equiv 0 \bmod 4$.

Dowód Lematu Hensela

- Indukcja ze względu na n. Pokażemy, że istnieje ciąg $a_n \in \mathbb{Z}_p$ taki, że $f(a_n) \equiv 0 \bmod p^n$ oraz $a_n \equiv a_1 \bmod p$. Następnie dokonamy przejścia do granicy uzyskując $f(\alpha) = 0$.

Dowód Lematu Hensela

- Indukcja ze względu na n. Pokażemy, że istnieje ciąg $a_n \in \mathbb{Z}_p$ taki, że $f(a_n) \equiv 0 \mod p^n$ oraz $a_n \equiv a_1 \mod p$. Następnie dokonamy przejścia do granicy uzyskując $f(\alpha) = 0$.
- Gdy $n = 1$ sprawa jest jasna: bierzemy $a_1 = \alpha$. Zakładamy, że teza działa dla n i szukamy $a_{n+1} \in \mathbb{Z}_p$, że $f(a_{n+1}) \equiv 0 \mod p^{n+1}$ oraz $a_{n+1} \equiv a_1 \mod p$.

Dowód Lematu Hensela

- Indukcja ze względu na n. Pokażemy, że istnieje ciąg $a_n \in \mathbb{Z}_p$ taki, że $f(a_n) \equiv 0 \bmod p^n$ oraz $a_n \equiv a_1 \bmod p$. Następnie dokonamy przejścia do granicy uzyskując $f(\alpha) = 0$.
- Gdy $n = 1$ sprawa jest jasna: bierzemy $a_1 = \alpha$. Zakładamy, że teza działa dla n i szukamy $a_{n+1} \in \mathbb{Z}_p$, że $f(a_{n+1}) \equiv 0 \bmod p^{n+1}$ oraz $a_{n+1} \equiv a_1 \bmod p$.
- Warunek $f(a_{n+1}) \equiv 0 \bmod p^{n+1}$ implikuje $f(a_{n+1}) \equiv 0 \bmod p^n$. Z założenia indukcyjnego istnieje a_n takie, że $f(a_n) \equiv 0 \bmod p^n$, więc szukamy w istocie takiego $t_n \in \mathbb{Z}_p$, że:

$$a_{n+1} = a_n + p^n t_n.$$

Dowód Lematu Hensela

- Indukcja ze względu na n. Pokażemy, że istnieje ciąg $a_n \in \mathbb{Z}_p$ taki, że $f(a_n) \equiv 0 \bmod p^n$ oraz $a_n \equiv a_1 \bmod p$. Następnie dokonamy przejścia do granicy uzyskując $f(\alpha) = 0$.
- Gdy $n = 1$ sprawa jest jasna: bierzemy $a_1 = \alpha$. Zakładamy, że teza działa dla n i szukamy $a_{n+1} \in \mathbb{Z}_p$, że $f(a_{n+1}) \equiv 0 \bmod p^{n+1}$ oraz $a_{n+1} \equiv a_1 \bmod p$.
- Warunek $f(a_{n+1}) \equiv 0 \bmod p^{n+1}$ implikuje $f(a_{n+1}) \equiv 0 \bmod p^n$. Z założenia indukcyjnego istnieje a_n takie, że $f(a_n) \equiv 0 \bmod p^n$, więc szukamy w istocie takiego $t_n \in \mathbb{Z}_p$, że:
$$a_{n+1} = a_n + p^n t_n.$$
- Aby wyznaczyć $f(a_n + p^n t_n) \bmod p^{n+1}$ uzasadnimy najpierw następującą tożsamość:
$$f(X + Y) = f(X) + f'(X)Y + g(X, Y)Y^2 \qquad (*),$$
gdzie $g(X, Y)$ to wielomian zmiennych X, Y o współczynnikach w $\mathbb{Z}_p$. Swoją drogą, czy $(*)$ nie przypomina Państwu nieco wzoru Taylora?

Dowód Lematu Hensela

- Dowód wzoru $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$.

Dowód Lematu Hensela

- Dowód wzoru $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$.
- Zapisując $f(X) = c_0 + c_1X + \ldots + c_dX^d$ mamy:

$$f(X+Y) = \sum_{i=0}^{d} c_i(X+Y)^i = c_0 + \sum_{i=1}^{d} c_i(X^i + iX^{i-1}Y + g_i(X,Y)Y^2),$$

gdzie $g_i \in \mathbb{Z}_p[X,Y]$

Dowód Lematu Hensela

- Dowód wzoru $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$.
- Zapisując $f(X) = c_0 + c_1X + \ldots + c_dX^d$ mamy:

$$f(X+Y) = \sum_{i=0}^{d} c_i(X+Y)^i = c_0 + \sum_{i=1}^{d} c_i(X^i + iX^{i-1}Y + g_i(X,Y)Y^2),$$

  gdzie $g_i \in \mathbb{Z}_p[X,Y]$
- Zatem:

$$\begin{aligned} f(X+Y) &= \sum_{i=0}^{d}(c_iX^i + ic_iX^{i-1}Y + c_ig_i(X,Y)Y^2) = \\ &= f(X) + f'(X)Y + g(X,Y)Y^2, \end{aligned}$$

  gdzie $g(X,Y) = \sum_{i=1}^{d} c_ig_i(X,Y) \in \mathbb{Z}_p[X,Y]$.
- A zatem udowodniliśmy $(*)$.

Dowód Lematu Hensela

- Przypomnijmy, że szukamy w takiego $t_n \in \mathbb{Z}_p$, że $a_{n+1} = a_n + p^n t_n$ i mamy do dyspozycji formułę $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$, gdzie $g(X,Y)$ to wielomian zmiennych X, Y o współczynnikach w $\mathbb{Z}_p$.

Dowód Lematu Hensela

- Przypomnijmy, że szukamy w takiego $t_n \in \mathbb{Z}_p$, że $a_{n+1} = a_n + p^n t_n$ i mamy do dyspozycji formułę $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$, gdzie $g(X,Y)$ to wielomian zmiennych X, Y o współczynnikach w $\mathbb{Z}_p$.
- Niech $x = a_n, y = p^n t_n$ oraz $z = g(x,y)$, dla pewnego $z \in \mathbb{Z}_p$. Mamy zatem:

  $f(a_n + p^n t_n) = f(a_n) + f'(a_n)p^n t_n + zp^{2n}t_n^2 \equiv f(a_n) + f'(a_n)p^n t_n \bmod p^{n+1} \quad (\dagger).$

Dowód Lematu Hensela

- Przypomnijmy, że szukamy w takiego $t_n \in \mathbb{Z}_p$, że $a_{n+1} = a_n + p^n t_n$ i mamy do dyspozycji formułę $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$, gdzie $g(X,Y)$ to wielomian zmiennych X, Y o współczynnikach w $\mathbb{Z}_p$.
- Niech $x = a_n, y = p^n t_n$ oraz $z = g(x,y)$, dla pewnego $z \in \mathbb{Z}_p$. Mamy zatem:

  $$f(a_n + p^n t_n) = f(a_n) + f'(a_n)p^n t_n + z p^{2n} t_n^2 \equiv f(a_n) + f'(a_n)p^n t_n \bmod p^{n+1} \quad (\dagger).$$

- Pamiętajmy, że z założenia indukcyjnego $a_n \equiv a_1 \bmod p$, czyli $f'(a_n)p^n t_n \equiv f'(a_1)p^n t_n \bmod p^{n+1}$. Zatem z $(\dagger)$:

  $$\begin{aligned} f(a_n + p^n t_n) \equiv 0 \bmod p^{n+1} &\iff f(a_n) + f'(a_1)p^n t_n \equiv 0 \bmod p^{n+1} \\ &\iff f'(a_1)t_n \equiv -f(a_n)/p^n \bmod p, \end{aligned}$$

  gdzie $f(a_n)/p^n \in \mathbb{Z}_p$, bo z zał. ind. mamy $f(a_n) \equiv 0 \bmod p^n$.

Dowód Lematu Hensela

- Przypomnijmy, że szukamy w takiego $t_n \in \mathbb{Z}_p$, że $a_{n+1} = a_n + p^n t_n$ i mamy do dyspozycji formułę $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$, gdzie $g(X,Y)$ to wielomian zmiennych X, Y o współczynnikach w $\mathbb{Z}_p$.
- Niech $x = a_n, y = p^n t_n$ oraz $z = g(x,y)$, dla pewnego $z \in \mathbb{Z}_p$. Mamy zatem:

  $$f(a_n + p^n t_n) = f(a_n) + f'(a_n)p^n t_n + z p^{2n} t_n^2 \equiv f(a_n) + f'(a_n)p^n t_n \bmod p^{n+1} \quad (\dagger).$$

- Pamiętajmy, że z założenia indukcyjnego $a_n \equiv a_1 \bmod p$, czyli $f'(a_n)p^n t_n \equiv f'(a_1)p^n t_n \bmod p^{n+1}$. Zatem z $(\dagger)$:

  $$\begin{aligned} f(a_n + p^n t_n) \equiv 0 \bmod p^{n+1} &\iff f(a_n) + f'(a_1)p^n t_n \equiv 0 \bmod p^{n+1} \\ &\iff f'(a_1)t_n \equiv -f(a_n)/p^n \bmod p, \end{aligned}$$

  gdzie $f(a_n)/p^n \in \mathbb{Z}_p$, bo z zał. ind. mamy $f(a_n) \equiv 0 \bmod p^n$.
- A zatem t_n wyznaczamy z ostatniej kongruencji modulo p (czyli w ciele $\mathbb{Z}_p$), bo przecież w założeniach lematu mamy $f'(a_1) \not\equiv 0 \bmod p$. Zakończyliśmy krok indukcyjny: mamy a_{n+1} taki, że $f(a_{n+1}) \equiv 0 \bmod p^{n+1}$ oraz $a_{n+1} \equiv a_n \bmod p^n$.

Dowód Lematu Hensela

- Znaleźliśmy ciąg $a_n \in \mathbb{Z}_p$ taki, że $f(a_n) \equiv 0 \bmod p^n$ oraz $a_n \equiv a_1 \bmod p$. Wiemy też, że $a_{n+1} \equiv a_n \bmod p^n$, dla każdego n. Zatem ciąg (a_n) jest Cauchy'ego. Niech $\alpha = \lim_{n\to\infty} a_n$. Pokażemy, że $f(\alpha) = 0$ oraz $\alpha \equiv a_1 \bmod p$.

Dowód Lematu Hensela

- Znaleźliśmy ciąg $a_n \in \mathbb{Z}_p$ taki, że $f(a_n) \equiv 0 \bmod p^n$ oraz $a_n \equiv a_1 \bmod p$. Wiemy też, że $a_{n+1} \equiv a_n \bmod p^n$, dla każdego n. Zatem ciąg (a_n) jest Cauchy'ego. Niech $\alpha = \lim_{n\to\infty} a_n$. Pokażemy, że $f(\alpha) = 0$ oraz $\alpha \equiv a_1 \bmod p$.
- Z równości $a_{n+1} \equiv a_n \bmod p^n$ dla wszystkich n mamy $a_m \equiv a_n \bmod p^n$, dla wszystkich $m > n$, czyli innymi słowy

$$|a_m - a_n|_p \leq p^{-n}$$

więc po przejściu $m \to \infty$ mamy

$$\alpha \equiv a_n \bmod p^n.$$

Dla $n = 1$ dostajemy zatem $\alpha \equiv a_1 \bmod p$.

Dowód Lematu Hensela

- Znaleźliśmy ciąg $a_n \in \mathbb{Z}_p$ taki, że $f(a_n) \equiv 0 \bmod p^n$ oraz $a_n \equiv a_1 \bmod p$. Wiemy też, że $a_{n+1} \equiv a_n \bmod p^n$, dla każdego n. Zatem ciąg (a_n) jest Cauchy'ego. Niech $\alpha = \lim_{n\to\infty} a_n$. Pokażemy, że $f(\alpha) = 0$ oraz $\alpha \equiv a_1 \bmod p$.
- Z równości $a_{n+1} \equiv a_n \bmod p^n$ dla wszystkich n mamy $a_m \equiv a_n \bmod p^n$, dla wszystkich $m > n$, czyli innymi słowy

  $$|a_m - a_n|_p \leq p^{-n}$$

  więc po przejściu $m \to \infty$ mamy

  $$\alpha \equiv a_n \bmod p^n.$$

  Dla $n = 1$ dostajemy zatem $\alpha \equiv a_1 \bmod p$.
- Dalej korzystamy z założenia, że $f(a_n) \equiv 0 \bmod p^n$ i mamy:

  $$\alpha \equiv a_n \bmod p^n \Rightarrow f(\alpha) \equiv f(a_n) \equiv 0 \bmod p^n \Rightarrow |f(\alpha)|_p \leq \frac{1}{p^n}.$$

  Skoro szacowanie to zachodzi dla wszystkich n, to mamy $f(\alpha) = 0$.

Dowód Lematu Hensela

- Pozostał dowód jednoznaczności α jako jedynego pierwiastka f w $\mathbb{Z}_p$, który przystaje do a_1 modulo p. Niech $f(\beta) = 0$ oraz $\beta \equiv a_1 \bmod p$. Aby pokazać, że $\beta = \alpha$, wystarczy pokazać, że $\beta \equiv \alpha \bmod p^n$, dla wszystkich n.

Dowód Lematu Hensela

- Pozostał dowód jednoznaczności α jako jedynego pierwiastka f w $\mathbb{Z}_p$, który przystaje do a_1 modulo p. Niech $f(\beta) = 0$ oraz $\beta \equiv a_1 \bmod p$. Aby pokazać, że $\beta = \alpha$, wystarczy pokazać, że $\beta \equiv \alpha \bmod p^n$, dla wszystkich n.
- Dowód jest indukcyjny. Dla $n = 1$ jest jasne, bo α i β przystają do a_1 mod p. Niech $n \geq 1$ i załóżmy, że $\beta \equiv \alpha \bmod p^n$. Mamy więc

$$\beta = \alpha + p^n \gamma_n, \text{ gdzie } \gamma_n \in \mathbb{Z}_p.$$

Dowód Lematu Hensela

- Pozostał dowód jednoznaczności α jako jedynego pierwiastka f w $\mathbb{Z}_p$, który przystaje do a_1 modulo p. Niech $f(\beta) = 0$ oraz $\beta \equiv a_1 \bmod p$. Aby pokazać, że $\beta = \alpha$, wystarczy pokazać, że $\beta \equiv \alpha \bmod p^n$, dla wszystkich n.
- Dowód jest indukcyjny. Dla $n = 1$ jest jasne, bo α i β przystają do a_1 mod p. Niech $n \geq 1$ i załóżmy, że $\beta \equiv \alpha \bmod p^n$. Mamy więc

$$\beta = \alpha + p^n \gamma_n, \text{ gdzie } \gamma_n \in \mathbb{Z}_p.$$

- Rachunek podobny do (†) daje nam:

$$f(\beta) \equiv f(\alpha + p^n \gamma_n) \equiv f(\alpha) + f'(\alpha) p^n \gamma_n \bmod p^{n+1}.$$

Dowód Lematu Hensela

- Pozostał dowód jednoznaczności α jako jedynego pierwiastka f w $\mathbb{Z}_p$, który przystaje do a_1 modulo p. Niech $f(\beta) = 0$ oraz $\beta \equiv a_1 \bmod p$. Aby pokazać, że $\beta = \alpha$, wystarczy pokazać, że $\beta \equiv \alpha \bmod p^n$, dla wszystkich n.
- Dowód jest indukcyjny. Dla $n = 1$ jest jasne, bo α i β przystają do a_1 mod p. Niech $n \geq 1$ i załóżmy, że $\beta \equiv \alpha \bmod p^n$. Mamy więc
$$\beta = \alpha + p^n \gamma_n, \text{ gdzie } \gamma_n \in \mathbb{Z}_p.$$
- Rachunek podobny do (†) daje nam:
$$f(\beta) \equiv f(\alpha + p^n \gamma_n) \equiv f(\alpha) + f'(\alpha) p^n \gamma_n \bmod p^{n+1}.$$
- Skoro α, β są pierwiastkami f, to dostajemy
$$0 \equiv f'(\alpha) p^n \gamma_n \bmod p^{n+1} \quad \Longrightarrow \quad f'(\alpha)\gamma_n \equiv 0 \bmod p.$$
Skoro zaś $f'(\alpha) \equiv f'(a_1) \not\equiv 0 \bmod p$, to $\gamma_n \equiv 0 \bmod p$, czyli $\beta \equiv \alpha \bmod p^{n+1}$, co kończy dowód Lematu Hensela.

Wniosek

Niech $f \in \mathbb{Z}_p[x]$. Załóżmy, że istnieje liczba p-adyczna $a_1 \in \mathbb{Z}_p$ taka, że $|f(a_1)|_p < 1$ oraz $|f'(a_1)|_p = 1$. Wówczas kładąc, dla każdego $n \geq 1$

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

określamy ciąg zbieżny, którego granica $\alpha \in \mathbb{Z}_p$ jest jedyną liczbą p-adyczną całkowitą taką, że $|\alpha - a_1|_p < 1$ oraz $f(\alpha) = 0$.

Uwaga. Tym razem zapisałem warunki podzielności w języku nierówności na normach. Czy widzą Państwo, że $|f(a_1)|_p < 1$ to jest to samo, co stwierdzenie $f(a_1) \equiv 0 \bmod p\mathbb{Z}_p$, czyli $f(a_1)$ jest podzielne przez p?

Dla pewności: a_1 nie musi mieć jednej cyfry! Może mieć ich nieskończenie wiele, ale pierwsza od prawej ma być taka, jak w docelowej liczbie α. Potem poprawiamy kolejne cyfry (w prawo), a więc a_n ma już n takich samych cyfr jak liczba α.

Wniosek

Niech $f \in \mathbb{Z}_p[x]$. Załóżmy, że istnieje liczba p-adyczna $a_1 \in \mathbb{Z}_p$ taka, że $|f(a_1)|_p < 1$ oraz $|f'(a_1)|_p = 1$. Wówczas kładąc, dla każdego $n \geq 1$

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

określamy ciąg zbieżny, którego granica $\alpha \in \mathbb{Z}_p$ jest jedyną liczbą p-adyczną całkowitą taką, że $|\alpha - a_1|_p < 1$ oraz $f(\alpha) = 0$.

Fakt

Wielomian o współczynnikach w $\mathbb{Z}$ ma pierwiastek w $\mathbb{Z}_p$ wtedy i tylko wtedy, gdy ma całkowity pierwiastek modulo p^k, dla każdego $k \geq 1$.

Dowód.

- Jeśli $f(\alpha) = 0$, dla pewnego $\alpha \in \mathbb{Z}_p$, to zgodnie z twierdzeniem z Wykładu 16 istnieje ciąg liczb całkowitych $(a_1, a_2, a_2, \ldots)$ taki, że $a_k = b_0 + \ldots + b_{k-1}p^{k-1}$ taki, że:

$$\alpha \equiv a_k \bmod p^k. \qquad (*)$$

Dowód.

- Jeśli $f(\alpha) = 0$, dla pewnego $\alpha \in \mathbb{Z}_p$, to zgodnie z twierdzeniem z Wykładu 16 istnieje ciąg liczb całkowitych $(a_1, a_2, a_2, \ldots)$ taki, że $a_k = b_0 + \ldots + b_{k-1}p^{k-1}$ taki, że:

$$\alpha \equiv a_k \bmod p^k. \qquad (*)$$

- Czyli $f(a_k) = f(\alpha) \bmod p^k$ oraz $f(\alpha) = 0$ implikuje $f(a_k) \equiv 0 \bmod p^k$.

Dowód.

- Jeśli $f(\alpha) = 0$, dla pewnego $\alpha \in \mathbb{Z}_p$, to zgodnie z twierdzeniem z Wykładu 16 istnieje ciąg liczb całkowitych $(a_1, a_2, a_2, \ldots)$ taki, że $a_k = b_0 + \ldots + b_{k-1}p^{k-1}$ taki, że:

$$\alpha \equiv a_k \bmod p^k. \qquad (*)$$

- Czyli $f(a_k) = f(\alpha) \bmod p^k$ oraz $f(\alpha) = 0$ implikuje $f(a_k) \equiv 0 \bmod p^k$.

- Na odwrót, załóżmy, że kongruencja $(*)$ ma rozwiązanie całkowite a_k, dla każdego $k \geq 1$. Skorzystamy z ćwiczenia, którego rozwiązanie polecam:

Dowód.

- Jeśli $f(\alpha) = 0$, dla pewnego $\alpha \in \mathbb{Z}_p$, to zgodnie z twierdzeniem z Wykładu 16 istnieje ciąg liczb całkowitych $(a_1, a_2, a_2, \ldots)$ taki, że $a_k = b_0 + \ldots + b_{k-1}p^{k-1}$ taki, że:
$$\alpha \equiv a_k \bmod p^k. \qquad (*)$$
- Czyli $f(a_k) = f(\alpha) \bmod p^k$ oraz $f(\alpha) = 0$ implikuje $f(a_k) \equiv 0 \bmod p^k$.
- Na odwrót, załóżmy, że kongruencja $(*)$ ma rozwiązanie całkowite a_k, dla każdego $k \geq 1$. Skorzystamy z ćwiczenia, którego rozwiązanie polecam:

Ćwiczenie

Każdy nieskończony ciąg całkowitych liczb p-adycznych ma podciąg zbieżny.[a]

[a] W języku topologicznym: przestrzeń $(\mathbb{Z}_p, |.|_p)$ jest zwarta, a $\mathbb{Q}_p$ jest lokalnie zwarta! Oczywiście ani $\mathbb{R}$, ani $\mathbb{Z}$ nie są zwarte, ale każdy przedział $[x, y] \subseteq \mathbb{R}$ już jest zwarty, prawda?

Dowód.

- Jeśli $f(\alpha) = 0$, dla pewnego $\alpha \in \mathbb{Z}_p$, to zgodnie z twierdzeniem z Wykładu 16 istnieje ciąg liczb całkowitych $(a_1, a_2, a_2, \ldots)$ taki, że $a_k = b_0 + \ldots + b_{k-1}p^{k-1}$ taki, że:

$$\alpha \equiv a_k \bmod p^k. \qquad (*)$$

- Czyli $f(a_k) = f(\alpha) \bmod p^k$ oraz $f(\alpha) = 0$ implikuje $f(a_k) \equiv 0 \bmod p^k$.

- Na odwrót, załóżmy, że kongruencja $(*)$ ma rozwiązanie całkowite a_k, dla każdego $k \geq 1$. Weźmy podciąg zbieżny (a_{k_i}) ciągu (a_k) o granicy α. Pokażemy, że jest to rozwiązanie równania $f(\alpha) = 0$.

Dowód.

- Jeśli $f(\alpha) = 0$, dla pewnego $\alpha \in \mathbb{Z}_p$, to zgodnie z twierdzeniem z Wykładu 16 istnieje ciąg liczb całkowitych $(a_1, a_2, a_2, \ldots)$ taki, że $a_k = b_0 + \ldots + b_{k-1}p^{k-1}$ taki, że:
$$\alpha \equiv a_k \bmod p^k. \qquad (*)$$
- Czyli $f(a_k) = f(\alpha) \bmod p^k$ oraz $f(\alpha) = 0$ implikuje $f(a_k) \equiv 0 \bmod p^k$.
- Na odwrót, załóżmy, że kongruencja $(*)$ ma rozwiązanie całkowite a_k, dla każdego $k \geq 1$. Weźmy podciąg zbieżny (a_{k_i}) ciągu (a_k) o granicy α. Pokażemy, że jest to rozwiązanie równania $f(\alpha) = 0$.
- Łatwo pokazać, że wielomiany to funkcje ciągłe w normie $|.|_p$, więc
$$f(\alpha) = \lim_{i \to \infty} f(a_{k_i}).$$
Z drugiej strony $f(a_{k_i}) \equiv 0 \bmod p^{k_i}$. Czyli $f(a_{k_i}) \to 0$, więc $f(\alpha) = 0$.

Zastosowania lematu Hensela

- Weźmy formę wymierną $x^2 + 11y^2 = 3$. Nie ma ona rozwiązań całkowitych, ale ma nietrywialne rozwiązania nad $\mathbb{R}$ oraz nad wszystkimi $\mathbb{Z}_p$. Nad $\mathbb{R}$ sprawa jest jasna, zaś dla $\mathbb{Z}_p$ pokazuje się, że:
  - dla $p \neq 2, 11$ kongruencja $x^2 \equiv 3 - 11y^2 \bmod p$ ma niezerowe rozwiązanie (argument z zasadą szufladkową), co pozwala użyć lematu Hensela,
  - dla $p = 2$ okazuje się, że $3/11 \equiv 1 \bmod 8$, więc $3/11$ to kwadrat w $\mathbb{Z}_2$, skąd wiemy, że $0^2 + 11y^2 = 3$ ma rozwiązanie w $\mathbb{Z}_2$,
  - dla $p = 11$ mamy $3 \equiv 5^2 \bmod 11$, więc $x^2 + 11 \cdot 0^2 = 3$ ma rozwiązanie w $\mathbb{Z}_{11}$.

  Dokładne omówienie powyższego i inne przykłady w:
  `kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf`.
- Na stronie K. Conrada można też poczytać o wielu ogólniejszych wersjach Lematu Hensela i ich zastosowaniach:
  `https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`.
- W ogóle polecam stronę K. Conrada:
  `https://kconrad.math.uconn.edu/blurbs/`

Uwagi odnośnie dowodu twierdzenia Hasse-Minkowskiego

- Dla $n = 3$ dowód wymaga drobiazgowego uzasadnienia, że jeśli forma $ax^2 + by^2 + cz^2$ ma pierwiastki modulo p, gdzie a, b, c są względnie pierwszymi liczbami całkowitymi, to jest izotropowa.

  Dokładna ekspozycja tego wątku jest przeprowadzona w świetnej książce: *p-adic Numbers: An Introduction* autorstwa F. Gouvêa (BUW, IMPAN...).
- Bardzo swobodną i skrótową, ale jednak przystępną opowieść o dowodzie twierdzenia H-M dla dowolnego n można znaleźć w tekście popularnym: `http://www.math.union.edu/~hatleyj/Capstone.pdf`. Porządne opracowanie pozostające również na poziomie elementarnym to na przykład praca magisterska: A. Gamzon: *The Hasse-Minkowski Theorem*, która będzie kolejną lekturą nieobowiązkową.
- Pełen dowód można przeczytać w klasycznej (ale trudnej i wprost legendarnej) książce wielkiego matematyka francuskiego Jean-Pierre Serre'a (medalista Fieldsa 1954, dziś ma 94 lata): *A course in Arithmetic* (1973).

Równania stopnia 3

- Słynny przykład Selmera z 1954 roku mówi, że równanie $3x^3 + 4y^3 + 5z^3 = 0$ ma jedyne rozwiązanie $(0, 0, 0)$ nad $\mathbb{Q}$, ale ma niezerowe rozwiązanie zarówno nad $\mathbb{R}$, jak i nad każdym $\mathbb{Q}_p$. Więcej kontrprzykładów i opowieści skąd je brać (i jakie mają znaczenie geometryczne): Aitken, Lemmermeyer: *Counterexamples to the Hasse principle* (arXiV).

- Stwierdzenie, czy dane równanie diofantyczne ma skończenie wiele rozwiązań w $\mathbb{Z}$ może być (znacznie!) łatwiejsze niż zrobienie tego nad $\mathbb{Q}$. Przykład: słynny wynik Mordella z 1920 roku mówi, że dla każdego $k \in \mathbb{Z}$ równanie $y^2 = x^3 + k$ ma skończenie wiele całkowitych rozwiązań. Ale jak opisać wymierne? To już bardzo trudne zadanie. Problemy tego typu są bardzo głębokie i wiążą się z wielkimi wynikami końca XX wieku, w tym z dowodem WTF. W zasadzie można powiedzieć, że jeden z problemów milenijnych (za 10^6\$), czyli hipoteza Bircha i Swinenrtona-Dyera mówi o związku pomiędzy zachowaniem rozwiązań wymiernych oraz rozwiązań rzeczywistych i p-adycznych w równaniach stopnia 3 (krzywe eliptyczne).

Epilog...

- A gdyby nie wybierać między $\mathbb{R}$, $\mathbb{Q}_p$, tylko rozszerzać $\mathbb{Q}$ o wszystko naraz?
- Bardzo proszę: rozważamy zbiór $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \prod_{p \in \mathbb{P}} \mathbb{Q}_p$, złożony z ciągów:

$$(x_\infty, x_2, x_3, x_5, \ldots, x_p, \ldots) \qquad (\heartsuit)$$

  i rozważamy podzbiór takich ($\heartsuit$), że $|x_p|_p \leq 1$, dla prawie wszystkich $p \in \mathbb{P}$ (skończenie wiele może tego nie spełniać). Na zbiorze tym wprowadzamy dodawanie i mnożenie, i powstaje tzw. **pierścień adelowy** (ale nie ciało 😐)! Oczywiście $\mathbb{Q}$ wkłada się diagonalnie w $\mathbb{A}_{\mathbb{Q}}$, czyli $\mathbb{Q} \ni x \mapsto (x, x, x, \ldots) \in \mathbb{A}_{\mathbb{Q}}$.
- Ciekawostka: badając $\mathbb{A}_{\mathbb{Q}}$ można zrozumieć, że równość $|x|_\infty \cdot \prod_{p \in \mathbb{P}} |x|_p = 1$ ma coś wspólnego (coś: całka wzgl. miary dyskretnej na $SL_2(\mathbb{A}_{\mathbb{Q}})/SL_2(\mathbb{Q})$ 😎) ze wzorem:

$$1 = \frac{\pi^2}{6} \cdot \prod_{p \in \mathbb{P}} (1 - p^{-2}).$$

  Ale to już inna historia.
  (https://cds.cern.ch/record/1101062/files/978-3-540-71175-9_BookBackMatter.pdf)