APROKSYMACJE p-ADYCZNE

FRANCISZEK HANSDORFER

1. Wstęp

W niniejszej pracy zajmuję się przede wszystkim obliczaniem pierwiastków kwadratowych w ciałach p-adycznych. W przeciwieństwie do standardowej rekurencji opartej na lemacie Hensela, metoda przedstawiona przeze mnie, oparta na pierwiastkach z jedynki, pozwala na uzyskanie wzorów **jawnych**. W konsekwencji odwołując się do struktury $\mathbb{Z}_p$ uzyskujemy ciekawe i nieoczywiste kongruencje modulo p^n. Na przykład dla każdego $n \in \mathbb{N}$, mamy $5 \equiv \left(3^{11^n} - 9^{11^n} - 5^{11^n} + 4^{11^n}\right)^2 \pmod{11^{n+1}}$.

Na koniec zajmuję się pewnymi ciągami w grupie $U(\mathbb{Z}/p^n\mathbb{Z})$, które przyjmują wszystkie wartości.

Chciałbym bardzo podziękować dr. hab. Mariuszowi Skałbie prof. UW za opiekę merytoryczną oraz pomysł tematu pracy.

2. Rozszerzenia ciał. Uzupełnienie ciała z normą

Definicja 1. Niech F będzie ciałem. Normą na F nazywamy funkcję $\| \ \| : F \to \mathbb{R}_{\geq 0}$ jeśli spełnia warunki:

(1) $\|a\| = 0 \iff a = 0$,
(2) $\|ab\| = \|a\| \, \|b\|$,
(3) $\|a + b\| \leq \|a\| + \|b\|$.

O metryce d zdefiniowanej jako $d(a, b) = \|a - b\|$ mówimy, że jest indukowana przez normę $\| \ \|$.

Definicja 2. W przestrzeni metrycznej (X, d) ciąg (x_n) nazywamy ciągiem Cauchy'ego, jeśli

$$\forall_{\varepsilon > 0} \exists_{N \in \mathbb{N}} \forall_{n,m \geq N} : d(x_n, x_m) < \varepsilon.$$

Definicja 3. Przestrzeń metryczną (X, d) nazywamy zupełną, jeśli każdy ciąg Cauchy'ego w X jest zbieżny w X.

Definicja 4. Niech F będzie ciałem, $\| \ \| : F \to \mathbb{R}_{\geq 0}$ normą na F, oraz $d : F^2 \to \mathbb{R}_{\geq 0}$ metryką indukowaną przez normę $\| \ \|$. Definiujemy relację na zbiorze ciągów Cauchy'ego w F następująco: $(x_n) \sim (y_n) \iff \lim_{n \to \infty} d(x_n, y_n) = 0$. $\sim$ jest relacją równoważności, więc możemy ustalić $\hat{F}$ jako zbiór klas abstrakcji ciągów Cauchy'ego w F względem relacji $\sim$. Przestrzeń $(\hat{F}, d)$ będziemy nazywać uzupełnieniem F względem normy $\| \ \|$.

Definicja 5. Niech $p \in \mathbb{P}$. Wykładnikiem p-adycznym liczby $m \in \mathbb{Z}$ nazywamy liczbę całkowitą $v_p(m)$ taką, że $p^{v_p(m)} \mid m$ oraz $p^{v_p(m)+1} \nmid m$. Niech teraz $a = \frac{m}{n}$, gdzie $m, n \in \mathbb{Z}$, wtedy $v_p(a) := v_p(m) - v_p(n)$.

Date: 30 kwietnia 2025.

Definiujemy odwzorowanie $\| \ \|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ jako

$$\|a\|_p = \begin{cases} 0 & \text{jeśli } a = 0, \\ p^{-v_p(a)} & \text{jeśli } a \neq 0. \end{cases}$$

Lemat 1. *Funkcja $\| \ \|_p$ jest normą na $\mathbb{Q}$.*

Dowód. $\|a\|_p = 0 \iff a = 0$ jest oczywiste. Niech teraz $x = p^k \frac{a}{b}, y = p^l \frac{c}{d}$, gdzie $a, b, c, d \in \mathbb{Z}$ nie są podzielne przez p. Wtedy

$$v_p(xy) = v_p\left(p^{k+l} \frac{ac}{bd}\right).$$

Ponieważ $p \nmid ac$, oraz $p \nmid bd$, to $v_p(xy) = k + l = v_p(x) + v_p(y)$.

$$v_p(x+y) = v_p\left(\frac{p^k ad + p^l bc}{bd}\right) = v_p(p^k ad + p^l bc) - v_p(b) - v_p(d).$$

Ponieważ $p^k \mid p^k ad + p^l bc$, lub $p^l \mid p^k ad + p^l bc$, to:

$$v_p(p^k ad + p^l bc) \geq \min\{k, l\} = \min\{v_p(x), v_p(y)\},$$

a ponieważ z założenia $p \nmid b$ oraz $p \nmid d$, to $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

Korzystając z powyższych zależności, otrzymujemy:

$$\|xy\|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)} p^{-v_p(y)} = \|a\|_p \|b\|_p .$$

$$\|x+y\|_p = p^{-v_p(x+y)} \leq \max\{p^{-v_p(x)}, p^{-v_p(y)}\} = \max\{\|x\|_p, \|y\|_p\} \leq \|x\|_p + \|y\|_p .$$

□

W myśl definicji 4 definiujemy $\mathbb{Q}_p$ jako uzupełnienie ciała $\mathbb{Q}$ z normą $\| \ \|_p$.

Definicja 6. $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \|x\|_p \leq 1\}$

Twierdzenie 1. *Każda klasa abstrakcji $a \in \mathbb{Q}_p$ zawiera dokładnie jeden ciąg Cauchy'ego $\{a_i\}$ taki, że*

(1) $\forall_{n \in \mathbb{N}} : 0 \leq a_n < p^n$
(2) $\forall_{n \in \mathbb{N}} : a_{n+1} \equiv a_n \pmod{p^n}$

Dowód. niech $\{b_n\} \neq \{a_n\}$, będzie ciągiem spełniający warunki (1) i (2). Wówczas dla pewnego k, jest $b_k \neq a_k$, a ponieważ $0 \leq a_k, b_k \leq p^k - 1$, to:

$$a_k \not\equiv b_k \pmod{p^k}.$$

Ale wtedy dla każdego $i > k$, mamy $a_i \equiv a_k \not\equiv b_k \equiv b_i \pmod{p^k}$, więc

$$\|a_i - b_i\|_p > \frac{1}{p^k}.$$

A zatem $[\{a_n\}]_\sim \neq [\{b_n\}]_\sim$.

Zauważmy, że jeśli istnieje ciąg spełniający warunki (1) i (2), dla każdego $a \in \mathbb{Z}_p$, czyli takiego, że $\|a\|_p \leq 1$, to istnieje również taki ciąg dla każdego $b \in \mathbb{Q}_p$. Istotnie dla każdego b istnieje $m \in \mathbb{Z}$, takie że $\|p^m b\|_p \leq 1$.

Możemy więc bez straty ogólności założyć, że $\|a\|_p \leq 1$.

Niech $\{x_n\}$ będzie ciągiem Cauchy'ego zbieżnym do a. Możemy wówczas obrać $N(k) > k$, takie że dla każdego $i, j > N(k)$ zachodzi

$$\|x_i - x_j\|_p \leq \frac{1}{p^k}.$$

Zauważmy, że dla każdego $i, j > N(1)$ mamy

$$\|x_i\|_p \leq \max(\|x_j\|_p, \|x_j - x_i\|_p) \leq \max\left(\|x_j\|, \frac{1}{p}\right) \leq 1.$$

Lemat 2. *Niech $x \in \mathbb{Z}_p$. Wtedy dla każdego $k \in \mathbb{N}$ istnieje $g \in \mathbb{Z}$ takie, że*

$$\|g - x\|_p \leq \frac{1}{p^k}.$$

Dowód lematu. Niech $x = \frac{a}{b}$, gdzie $a, b \in \mathbb{Z}$ są względnie pierwsze. Ponieważ $\|x\|_p \leq 1$, to $p \nmid b$. Istnieją zatem $m, n \in \mathbb{Z}$, takie że $nb + mp^k = 1$. Niech $g = an$. Wówczas

$$\|g - x\|_p = \left\|an - \frac{a}{b}\right\|_p = \left\|\frac{a}{b}\right\|_p \|nb - 1\|_p \leq \|nb - 1\|_p = \left\|mp^k\right\|_p \leq \frac{1}{p^k}.$$

Po dodaniu do g dowolnej wielokrotności p^k nierówność dalej zachodzi, zatem możemy przyjąć $0 \leq g \leq p^k - 1$. □

Stosując powyższy lemat wielokrotnie dla ciągu $\{x_n\}$ otrzymujemy ciąg $\{a_n\}$, taki że

$$\left\|a_k - x_{N(k)}\right\|_p \leq \frac{1}{p^k}.$$

Zauważmy, że

$$\begin{aligned}\|a_{k+1} - a_k\|_p &= \left\|(a_{k+1} - x_{N(k+1)}) + (x_{N(k+1)} - x_{N(k)}) - (a_k - x_{N(k)})\right\|_p \\ &\leq \max\left(\frac{1}{p^{k+1}}, \frac{1}{p^k}, \frac{1}{p^k}\right) = \frac{1}{p^k}.\end{aligned}$$

Czyli $a_{k+1} \equiv a_k \pmod{p^k}$.

Analogicznie dowodzimy, że $|a_k - x_k| \leq \frac{1}{p^k}$. Zatem $\{a_n\} \sim \{x_n\}$. □

Warto zwrócić uwagę, na fakt, że jednoznaczna reprezentacja elementów $\mathbb{Q}_p$ jest czymś co nie występuje w przypadku norm archimedesowych (mamy przecież $1 = 0.(9)$). Natomiast w przypadku p-adycznym jeśli dwa rozwinięcia przedstawiają ten sam element z $\mathbb{Q}_p$, to wszystkie ich wyrazy są równe.

Twierdzenie 2. *α posiada okresowe rozwinięcie p-adyczne wtedy i tylko wtedy, gdy $\alpha \in \mathbb{Q}$.*

Dowód. Ponieważ odjęcie od α skończonego wyrażenia $\sum_{i=0}^{k} a_{-i}p^{-i}$ nie wpłynie na okresowość rozwinięcia, to możemy założyć, że $|\alpha|_p \leq 1$. Załóżmy, że rozwinięcie p-adyczne α ma okres n: $\alpha = \sum_{i=0}^{k-1} a_i p^i + p^k \left(\sum_{i=0}^{\infty}\sum_{j=0}^{n-1} b_j p^{in+j}\right)$, gdzie $0 \leq a_n, b_n < p$. Mamy wtedy:

$$\begin{aligned}\alpha &= \sum_{i=0}^{k-1} a_i p^i + p^k \left(\sum_{j=0}^{n-1} b_j \left(\sum_{i=0}^{\infty} p^{in+j}\right)\right) \\ &= \sum_{i=0}^{k-1} a_i p^i + p^k \left(\sum_{j=0}^{n-1} b_j \frac{p^j}{1-p^n}\right) \in \mathbb{Q}.\end{aligned}$$

Lemat 3. *Jeśli $\alpha = \frac{a}{b} \in (-1, 0) \cap \mathbb{Q}$, $b > 0$, $\mathrm{NWD}(a, b) = 1$, oraz $p \nmid b$, to rozwinięcie p-adyczne α jest okresowe.*

Dowód lematu 3. Z twierdzenia Eulera, dla $k = \varphi(b)$, mamy:

$$p^k \equiv 1 \pmod{b}.$$

Niech $p^k - 1 = bc$, gdzie $c \in \mathbb{N}$. Teraz:

$$\alpha = \frac{ac}{bc} = \frac{ac}{p^k - 1} = -ac\left(\frac{1}{1-p^k}\right).$$

Ponieważ $\frac{a}{b} \in (-1, 0)$, to $0 < -a < b$. Mnożąc obie strony nierówności przez c otrzymujemy $0 < -ac < bc$, czyli:

$$0 < -ac < p^k - 1.$$

Zatem możemy zapisać rozwinięcie p-adyczne $-ac$:

$$-ac = d_0 + d_1 p + \cdots + d_{k-1}p^{k-1}.$$

Zatem:

$$\alpha = (d_0 + d_1 p + \cdots + d_{k-1}p^{k-1})(1 + p^k + p^{2k} + \dots).$$

Zatem rozwinięcie α jest okresowe. □

Lemat 4. *Niech $\beta \in \mathbb{Z}_p \setminus \{-1\}$. Wówczas rozwinięcia p-adyczne β i $\beta + 1$ różnią się na co najwyżej skończenie wielu cyfrach.*

dowód lematu 4. Niech $\beta = \sum_{i=0}^{\infty} c_i p^i$.

Przypadek I: Dla każdego $i \in \mathbb{N} : c_i = p - 1$. Wówczas mamy $\beta = -1$, co jest sprzeczne z założeniem.

Przypadek II $c_0 < p - 1$. Wówczas rozwinięcie $\beta + 1$ różni się od β tylko na pierwszej cyfrze.

Przypadek III Istnieje takie $n \neq 0$, że $\forall_{i<n} : c_i = p - 1$ oraz $c_n < p - 1$. Wówczas rozwinięcie $\beta + 1$ różni się od β na dokładnie $n + 1$ pierwszych cyfrach. □

Bezpośrednio z lematu 4 wynika, że rozwinięcie $\beta \in \mathbb{Z}_p \setminus \{-1\}$ jest okresowe wtedy i tylko wtedy, gdy rozwinięcie $\beta + 1$ jest okresowe.

Możemy teraz dokończyć dowód twierdzenia:

Przypadek I $\alpha = -1$. Wówczas $\alpha = \sum_{i=0}^{\infty}(p-1)p^i$, więc rozwinięcie α jest okresowe.

Przypadek II $\alpha \in \mathbb{Z} \setminus \{-1\}$. Istnieje wówczas n takie, że $\alpha + n = -1$. Stosując wielokrotnie lemat 4 otrzymujemy, że rozwinięcie α jest okresowe.

Przypadek III $\alpha \in \mathbb{Q} \setminus \mathbb{Z}$. Wówczas istnieje takie $m \in \mathbb{Z}$, że $\alpha + m \in (-1, 0)$. Na mocy lematu 3 rozwinięcie $\alpha + m$ jest okresowe. Natomiast stosując wielokrotnie lemat 4 otrzymujemy, że rozwinięcie α również jest okresowe. □

3. PODSTAWY TEORII LICZB

Definicja 7. Niech R będzie pierścieniem przemiennym z jedynką. Pochodną formalną wielomianu $R[x] \ni F(x) = c_0 + c_1 x + \cdots + c_k x^k$ określamy jako wielomian $F'(x) = c_1 + 2c_2 x + \cdots + k c_k x^{k-1}$. Jeśli $\deg F = 0$, to przyjmujemy $F'(x) \equiv 0$.

Twierdzenie 3. *(Lemat Hensela). Niech $F(x) \in \mathbb{Z}_p[x]$ i $a \in \mathbb{Z}_p$ takie, że $F(a) \equiv 0 \pmod{p}$ oraz $F'(a) \not\equiv 0 \pmod{p}$. Wówczas istnieje dokładnie jedno $b \in \mathbb{Z}_p$ takie, że $F(b) = 0$ oraz $b \equiv a \pmod{p}$.*

Dowód. Dowód przeprowadzimy przez indukcję.

Aby ciąg (a_n) określał liczbę z $\mathbb{Z}_p$, musi spełniać warunki:

(1) $a_n \equiv a_{n-1} \pmod{p^n}$,
(2) $0 \leq a_n < p^{n+1}$.

Gdy $n = 1$, to obieramy $a_0 \in \{0, 1, \ldots, p-1\}$, takie że $a_0 \equiv a \pmod{p}$. Każde a_1, spełniające warunek (1) i (2), musi być więc postaci

$$a_1 = a_0 + b_1 p, \quad b_1 \in \{0, 1, \ldots, p-1\}.$$

$$\begin{aligned} F(a_1) = F(a_0 + b_1 p) &= \sum_{i=0}^{k} c_i (a_0 + b_1 p)^i \equiv \sum_{i=0}^{k} c_i a_0^i + i c_i a_0^{i-1} b_1 p \pmod{p^2} \\ &= F(a_0) + F'(a_0) b_1 p. \end{aligned}$$

Ponieważ $F(a_0) \equiv 0 \pmod{p}$, to również $F(a_1) \equiv 0 \pmod{p}$. Możemy więc zapisać $F(a_1)$ jako $F(a_1) = \alpha p$, gdzie $\alpha \in \mathbb{Z}$. Wtedy, żeby $F(a_1) \equiv 0 \pmod{p^2}$, musi zachodzić:

$$\alpha p + F'(a_0) b_1 p \equiv 0 \pmod{p^2} \implies \alpha + F'(a_0) b_1 \equiv 0 \pmod{p}.$$

Ponieważ $F'(a_0) \not\equiv 0 \pmod{p}$, to istnieje dokładnie jedno takie $b_1 \in \{0, 1, \ldots, p-1\}$, że $b_1 \equiv -\frac{\alpha}{F'(a_0)} \pmod{p}$. Teraz krok indukcyjny. Załóżmy, że skonstruowaliśmy ciąg $(a_0, a_1, \ldots, a_{n-1})$. Z warunku (1) i (2) mamy $a_n = a_{n-1} + b_n p^n$, gdzie $b_n \in \{0, 1, \ldots, p-1\}$. Teraz rozkładamy $F(a_n)$ podobnie jak zrobiliśmy to dla $n = 1$, tym razem modulo p^n:

$$F(a_n) \equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^n \pmod{p^{n+1}}.$$

Ponieważ z założenia indukcyjnego $F(a_{n-1}) \equiv 0 \pmod{p^n}$, to możemy zapisać $F(a_n) = \alpha' p^n$. Wtedy, żeby $F(a_n) \equiv 0 \pmod{p^{n+1}}$, musi być

$$\alpha' p^n + F'(a_{n-1}) b_n p^n \equiv 0 \pmod{p^{n+1}},$$
$$\alpha' + F'(a_{n-1}) b_n \equiv 0 \pmod{p}.$$

Otrzymujemy więc, że $b_n \equiv -\frac{\alpha'}{F'(a_{n-1})} \pmod{p}$, a ponieważ $F'(a_{n-1}) \not\equiv 0 \pmod{p}$, to istnieje dokładnie jedno takie b_n. Teraz niech $b = a_0 + b_1 p + b_2 p^2 + \cdots$. Ponieważ dla każdego $n \geq 1$ zachodzi $F(b) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$, to $F(b) = 0$. □

Uwaga 1. Jak zostało pokazane w dowodzie lematu Hensela, $b_n \equiv -\frac{\alpha'}{F'(a_{n-1})} \pmod{p}$, czyli:

$$b_n p^n \equiv \frac{\alpha' p^n}{F'(a_{n-1})} \equiv \frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.$$

Możemy zapisać zatem rekurencję na a_n:

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

Lemat 5 (o podnoszeniu wykładnika p-adycznego)**.** *Niech $a, b \in \mathbb{Z}$, oraz $p \nmid a$ i $p \nmid b$. Wówczas jeśli $a \equiv b \pmod{p^n}$ dla $n \geq 1$, to:*

$$a^p \equiv b^p \pmod{p^{n+1}}.$$

Dowód. Niech $a = b + cp$, gdzie $c \in \mathbb{Z}$. Wówczas

$$a^p = (b + cp^n)^p = b^p + \binom{p}{1} b^{p-1} c p^n + \binom{p}{2} b^{p-2} c^2 p^{n+1} + \cdots + c^p p^{n+p}.$$

Ponieważ $p^{n+1} \mid \binom{p}{1} b^{p-1} c p^n$, to $a^p \equiv b^p \pmod{p^{n+1}}$. □

4. Pierwiastki z jedynki w $\mathbb{Q}_p$

Lemat 6. *Niech $r \in \{1, 2, \ldots, p-1\}$. Wówczas ciąg $x_n = r^{p^n}$ jest zbieżny w $\mathbb{Z}_p$.*

Dowód. Z małego twierdzenia Fermata mamy, że $r^p \equiv r \pmod p$, czyli $x_1 \equiv x_0 \pmod p$. Korzystając z lematu o podnoszeniu wykładnika p-adycznego n razy otrzymujemy:

$$\forall_{n\geq 0} : r^{p^{n+1}} \equiv r^{p^n} \pmod{p^{n+1}},$$

czyli

$$\forall_{n\geq 0} : x_{n+1} \equiv x_n \pmod{p^{n+1}}.$$

Z tego wynika, że $v_p(x_{n+1} - x_n) \geq n+1$, więc

$$d_p(x_{n+1}, x_n) \leq \left(\frac{1}{p}\right)^{n+1}.$$

Mamy więc $\lim_{n\to\infty} d_p(x_{n+1}, x_n) = 0$, gdyż d_p jest ultrametryką:

$$d_p(x_{n+k}, x_n) \leq \max\{d_p(x_n, x_{n+1}), \ldots, d_p(x_{n+k-1}, x_{n+k})\} \leq \left(\frac{1}{p}\right)^{n+1}.$$

x_n jest więc ciągiem Cauchy'ego. Ponieważ przestrzeń $\mathbb{Z}_p$ jest zupełna, to ciąg x_n jest zbieżny w $\mathbb{Z}_p$. □

Niech więc $\omega_r := \lim_{n\to\infty} r^{p^n}$.

Wniosek 1. Dla każdego $n, k \in \mathbb{N}$, mamy:

$$d_p(x_{n+k}, x_n) \leq \left(\frac{1}{p}\right)^{n+1}.$$

Ponieważ $\lim_{k\to\infty} x_{n+k} = \omega_r$, to

$$d_p(\omega_r, x_n) \leq \left(\frac{1}{p}\right)^{n+1}.$$

Lemat 7. *ω_r jest pierwiastkiem z jedynki w $\mathbb{Q}_p$. Ponadto jeśli $r_1 \neq r_2$, to również $\omega_{r_1} \neq \omega_{r_2}$.*

Dowód. Niech ponownie $x_n = r^{p^n}$. Mamy wtedy $x_n^p = x_{n+1}$. Zatem:

$$\lim_{n\to\infty} x_n^p = \lim_{n\to\infty} x_{n+1}$$

$$\omega_r^p = \omega_r$$

A ponieważ $\forall_{n\in\mathbb{N}} p \nmid x_n$, to $\omega_r \neq 0$. Mamy więc:

$$\omega_r^{p-1} = 1.$$

Zatem ω_r jest pierwiastkiem z jedynki.

Teraz druga część lematu. Mamy $r_1 \neq r_2$, czyli $\omega_{r_1} \equiv r_1 \not\equiv r_2 \equiv \omega_{r_2} \pmod p$. Zatem $\omega_{r_1} \neq \omega_{r_2}$. □

Zwróćmy uwagę na przypadek, gdy $r = g$, gdzie g jest pierwiastkiem pierwotnym modulo p. Wówczas z definicji $g^{p-1} \equiv 1 \pmod p$, oraz $\forall_{0<n<p-1} : g^n \not\equiv 1 \pmod p$. Mamy

$$\omega_g^n \equiv g^n \not\equiv 1 \pmod p,$$

więc $\omega_g^n \neq 1$. Ponieważ $g^{p-1} \equiv 1 \pmod{p}$, to z lematu o podnoszeniu wykładnika p-adycznego mamy, że dla każdego $k \in \mathbb{N}$ zachodzi

$$g^{(p-1)p^k} \equiv 1 \pmod{p^{k+1}},$$

więc

$$\omega^{p-1} = 1.$$

Zatem ω_g jest pierwiastkiem z jedynki stopnia $p-1$.

Mając pierwiastki pierwotne z jedynki stopnia $p-1$ w $\mathbb{Q}_p$ możemy też skonstruować pierwiastki stopnia $k|p-1$. Istotnie dla $\omega = \omega_g^{\frac{p-1}{k}}$, otrzymujemy:

$$\forall_{n<k} \omega^n \neq 1,$$

oraz

$$\omega^k = \omega_g^{p-1} = 1.$$

Definicja 8. Niech $\omega \in \mathbb{Q}_p$ będzie pierwiastkiem z jedynki stopnia q, gdzie $q|p-1$, oraz niech $a \in \{0, 1, \ldots, q-1\}$. sumę $g_a = \sum_{t=1}^{q-1} \left(\frac{t}{q}\right) \omega^{at}$ nazywamy kwadratową sumą Gaussa. (gdzie $\left(\frac{t}{q}\right)$ oznacza symbol Legendre'a).

Lemat 8. $g_a = \left(\frac{a}{q}\right) g_1$

Dowód. Gdy $a = 0$, to $\omega^{at} = 1$, więc $g_0 = \sum_{t=0}^{q-1} \left(\frac{a}{q}\right) = 0$, ponieważ jest tyle samo reszt i niereszt kwadratowych. Gdy $a \neq 0$, to $f(t) = at \pmod{q}$ jest bijekcją na zbiorze $\{1, \ldots, q-1\}$, więc

$$\left(\frac{a}{q}\right) g_a = \sum_{t=1}^{q-1} \left(\frac{at}{q}\right) \omega^{at} = \sum_{x=1}^{q-1} \left(\frac{x}{q}\right) \omega^x = g_1.$$

Mnożąc obie strony równości przez $\left(\frac{a}{q}\right)$ otrzymujemy:

$$\left(\frac{a^2}{q}\right) g_a = \left(\frac{a}{q}\right) g_1,$$

$$g_a = \left(\frac{a}{q}\right) g_1.$$

□

Twierdzenie 4. $g_a^2 = (-1)^{\frac{p-1}{2}} q$ *dla* $a \neq 0$.

Dowód. Rozważmy sumę $\sum_{a=1}^{q-1} g_a g_{q-a}$. Ponieważ $a \neq 0$, mamy $g_a g_{q-a} = \left(\frac{a}{q}\right)\left(\frac{q-a}{p}\right) g_1^2 = \left(\frac{a}{q}\right)\left(\frac{-a}{q}\right) g_1^2 = \left(\frac{-1}{q}\right) g_1^2$. Zatem

$$\sum_a g_a g_{q-a} = \left(\frac{-1}{q}\right) g_1^2 (q-1).$$

Natomiast z definicji kwadratowych sum Gaussa mamy:

$$g_a g_{q-a} = \sum_x \left(\frac{x}{q}\right) \omega^{ax} \sum_y \left(\frac{y}{q}\right) \omega^{a(q-y)},$$

a ponieważ $\omega^q = 1$, to:

$$g_a g_{q-a} = \sum_x \sum_y \left(\frac{x}{q}\right)\left(\frac{y}{q}\right)\omega^{a(x-y)}.$$

Rozważmy sumą $\sum_a \omega^{a(x-y)}$. Gdy $x - y = 0$, to $\sum_a \omega^{a(x-y)} = q$. W przeciwnym przypadku mamy:

$$\sum_a \omega^{a(x-y)} = \frac{\omega^{p(x-y)} - 1}{\omega^{(x-y)} - 1} = 0.$$

Zatem

$$\sum_a g_a g_{q-a} = \sum_x \sum_y \left(\frac{x}{q}\right)\left(\frac{y}{q}\right)\delta(x,y)q = (q-1)q.$$

Przyrównując wyniki wyznaczonych na dwa sposoby wartości wyrażenia $\sum_a g_a g_{q-a}$, otrzymujemy:

$$\left(\frac{-1}{q}\right) g_1^2 (q-1) = (q-1)q,$$

$$g_1^2 = \left(\frac{-1}{q}\right) q.$$

□

Lemat 8 oraz twierdzenie 4 w wersji zespolonej można znaleźć w książce [2]. My potrzebujemy wersji p-adycznej.

5. Pierwiastki kwadratowe w $\mathbb{Q}_p$

Twierdzenie 5. *Dla każdego $r \not\equiv 0 \pmod p$, oraz $p > 2$, mamy $\sqrt{r} \in \mathbb{Q}_p$ wtedy i tylko wtedy, gdy r jest resztą kwadratową modulo p.*

Dowód. Istnienie pierwiastka kwadratowego z a w $\mathbb{Q}_p$ jest równoważne z rozwiązywalnością równania $f(x) = x^2 - r = 0$ w $\mathbb{Q}_p$.

Zauważmy, że kongruencja $f'(a) = 2a \equiv 0 \pmod p$ ma jedno rozwiązanie $a \equiv 0 \pmod p$. Natomiast $x^2 - r \equiv 0 \pmod p$ ma rozwiązanie wtedy i tylko wtedy, gdy r jest resztą kwadratową modulo p. Jeżeli takie a istnieje, to w szczególności $a \not\equiv 0 \pmod p$, ponieważ zgodnie z założeniem $r \not\equiv 0 \pmod p$. Istnienie takiego a, że $f(a) \equiv 0 \pmod p$ oraz $f'(a) \not\equiv 0 \pmod p$, na mocy lematu Hensela implikuje, że $f(x) = 0$ ma rozwiązanie w $\mathbb{Q}_p$.

Aby udowodnić twierdzenie w drugą stronę, należy jedynie zauważyć, że jeśli $a \in \mathbb{Q}_p$ jest pierwiastkiem f, to $a^2 \equiv r \pmod{p^n}$. Dla $n = 1$ mamy $a^2 \equiv r \pmod p$, czyli r jest resztą kwadratową modulo p. □

6. Aproksymacje p-adyczne pewnych liczb niewymiernych

6.1. **Metoda oparta na pierwiastkach z jedynki.** Jak zostało wykazane w rozdziale 4., w $\mathbb{Q}_p$, mamy pierwiastki z jedynki stopnia $n|p-1$. Oznaczymy je w tym rozdziale jako ω_n.

Rozważmy $\omega_q \in \mathbb{Q}_p$, gdzie $q \in \mathbb{P}$. Wówczas za pomocą kwadratowych sum Gaussa możemy przedstawić w $\mathbb{Q}_p$ liczbę „$\sqrt{q}$" albo „$\sqrt{-q}$" (w zależności od wartości q mod 4). Istotnie na mocy twierdzenia 4 mamy:

(1) Jeśli $q \equiv 1 \pmod 4$, to:

$$g_1^2 = q$$

$$\left(\sum_{t=1}^{q-1} \left(\frac{t}{q}\right) \omega_q^t\right)^2 = q$$

(2) Jeśli $q \equiv 3 \pmod 4$, to:

$$g_1^2 = -q$$

$$\left(\sum_{t=1}^{q-1} \left(\frac{t}{q}\right) \omega_q^t\right)^2 = -q.$$

Przykład 1. Niech $p = 11$, wówczas $q = 5$ spełnia warunek $q|p-1$. 6 jest generatorem $\mathbb{F}_{11}^*$, więc $6^{\frac{10}{5}} \equiv 3$ jest elementem rzędu 5 w $\mathbb{F}_{11}^*$. Możemy więc przyjąć $\omega_5 = \lim_{n\to\infty} 3^{p^n}$. Ponieważ $5 \equiv 1 \pmod 4$, to mamy:

$$5 = \left(\sum_{t=1}^{4} \left(\frac{t}{5}\right) \omega_5^t\right)^2 = \left(\omega_5 - \omega_5^2 - \omega_5^3 + \omega_5^4\right)^2 = \left(\lim_{n\to\infty} 3^{11^n} - 9^{p^n} - 5^{11^n} + 4^{11^n}\right)^2,$$

Z wniosku 1 mamy również:

$$5 \equiv \left(3^{11^n} - 9^{11^n} - 5^{11^n} + 4^{11^n}\right)^2 \pmod{11^{n+1}}.$$

Przykład 2. Niech $p = 29$. 8 generuje grupę multiplikatywną $\mathbb{F}_{29}^*$. Zatem $8^{\frac{28}{7}} \equiv 7$ jest elementem rzędu 7. Niech więc $\omega_7 = \lim_{n\to\infty} 7^{29^n}$. Tym razem mamy $7 \equiv 3 \pmod 4$, więc:

$$g_1^2 = -7$$

$$\left(\sum_{t=1}^{6} \left(\frac{t}{7}\right) \omega_7^t\right)^2 = -7.$$

$$\left(\omega_7 + \omega_7^2 - \omega_7^3 + \omega_7^4 - \omega_7^5 - \omega_7^6\right)^2 = -7,$$

$$\lim_{n\to\infty} \left(7^{29^n} + 20^{29^n} - 24^{29^n} + 23^{29^n} - 16^{29^n} - 25^{29^n}\right)^2 = -7.$$

Mamy również:

$$\left(7^{29^n} + 20^{29^n} - 24^{29^n} + 23^{29^n} - 16^{29^n} - 25^{29^n}\right)^2 \equiv -7 \pmod{29^{n+1}}.$$

Niech $q_1, q_2, \ldots q_n$ będą dzielnikami pierwszymi $p-1$. Wtedy w $\mathbb{Q}_p$ znajdują się pierwiastki z jedynki: $\omega_{q_1}, \omega_{q_2}, \ldots \omega_{q_n}$. Możemy więc za ich pomocą przedstawić $\sqrt{\left(\frac{-1}{q_1 q_2 \ldots q_n}\right) q_1 q_2 \ldots q_n}$. Jako iloczyn sum Gaussa:

(1) Jeżeli $q_1 q_2 \ldots q_n \equiv 1 \pmod 4$, to:

$$g_{q_1}^2 g_{q_2}^2 \ldots g_{q_n}^2 = q_1 q_2 \ldots q_n$$

(2) Natomiast jeżeli $q_1 q_2 \ldots q_n \equiv 3 \pmod 4$, to:

$$g_{q_1}^2 g_{q_2}^2 \ldots g_{q_n}^2 = -q_1 q_2 \ldots q_n.$$

Przykład 3. Niech $p = 61$. 2 generuje $\mathbb{F}_{61}^*$, więc $2^{\frac{60}{3}} \equiv 47$ jest rzędu 3. Możemy przyjąć $\omega_3 = \lim_{n\to\infty} 47^{61^n}$.

Z kolei $2^{\frac{60}{5}} \equiv 9$, więc $\omega_5 = \lim_{n\to\infty} 9^{61^n}$. Mamy wtedy:

$$-3 = \left(\left(\frac{1}{3}\right)\omega_3 + \left(\frac{2}{3}\right)\omega_3^2\right)^2 = \left(\omega_3 - \omega_3^2\right)^2,$$

$$5 = \left(\sum_{t=1}^{4}\left(\frac{t}{5}\right)\omega_5^t\right)^2 = \left(\omega_5 - \omega_5^2 - \omega_5^3 + \omega_5^4\right)^2.$$

Więc

$$\begin{aligned} -15 &= \left(\omega_3 - \omega_3^2\right)^2\left(\omega_5 - \omega_5^2 - \omega_5^3 + \omega_5^4\right)^2 \\ &= \lim_{n\to\infty}\left(47^{61^n} - 13^{61^n}\right)^2\left(9^{61^n} - 20^{61^n} - 58^{61^n} + 34^{61^n}\right)^2. \end{aligned}$$

Rozważając pierwiastki w $\mathbb{Z}_p$ możemy uzyskać też inną klasę tożsamości modulo p^n.

Niech $\omega_q \in \mathbb{Z}_p$ będzie pierwiastkiem pierwotnym stopnia $q|p-1$. Wtedy mamy:

$$1 = \frac{1-\omega_q}{1-\omega_q} = \frac{1-\omega_q^{q+1}}{1-\omega_q} = \sum_{n=0}^{q}\omega_q^n.$$

$$\sum_{n=1}^{q-1}\omega_q^n = -1.$$

Przykład 4. Niech $p = 43$. 18 jest generatorem $\mathbb{F}_{43}^*$, więc $18^{\frac{42}{6}} \equiv 7$ jest elementem rzędu 6. Niech więc $\omega_6 = \lim_{n\to\infty} 7^{43^n}$. Mamy:

$$\omega_6 + \omega_6^2 + \omega_6^3 + \omega_6^4 + \omega_6^5 = -1,$$

więc:

$$7^{43^n} + 6^{43^n} + 42^{43^n} + 36^{43^n} + 37^{43^n} \equiv -1 \pmod{43^{n+1}}.$$

Lemat 9. *Niech $p \in \mathbb{P}$. Rozważmy generator g grupy multiplikatywnej $U(\mathbb{Z}/p^2\mathbb{Z})$. Wówczas g jest generatorem grupy $U(\mathbb{Z}/p^n\mathbb{Z})$ dla każdego $n \geq 2$.*

Ten lemat udowodniony został w dowodzie twierdzenia 2. na stronie 43 w [2]. □

Definicja 9. Punktem skupienia ciągu (x_n) nazywamy dowolną granicę zbieżnego podciągu (x_n).

Twierdzenie 6. *Niech g będzie generatorem $U(\mathbb{Z}/p^n\mathbb{Z})$. Wówczas dla każdego p, dowolna liczba $\alpha \in \mathbb{Z}_p^*$ jest pewnym punktem skupienia ciągu $x_n = g^n$.*

Dowód. Niech $\alpha = \sum_{n=0}^{\infty} c_n p^n \in \mathbb{Z}_p^*$. Wtedy mamy $\|\alpha\|_p = 1$, czyli $c_0 \not\equiv 0 \pmod{p}$. niech $k \in \mathbb{N}$, oraz $\alpha_k = \sum_{n=0}^{k-1} c_n p^n < p^k$. Ponieważ $p \nmid c_0$, to $\alpha_k \in U(\mathbb{Z}/p^n\mathbb{Z})$. Z lematu 9 mamy, że istnieje g, takie że dla każdego $n \in \mathbb{N}$ g jest generatorem $U(\mathbb{Z}/p^n\mathbb{Z})$. Istnieje zatem takie $w_k \in \mathbb{N}$, że

$$g^{w_k} \equiv \alpha_k \pmod{p^k}.$$

Zatem $\|\alpha_k - g^{w_k}\|_p \leq \left(\frac{1}{p}\right)^k$. A ponieważ $\|\alpha - \alpha_k\|_p \leq \left(\frac{1}{p}\right)^k$, to

$$\|\alpha - g^{w_k}\|_p \leq \max\left(\|\alpha_k - g^{w_k}\|_p, \|\alpha - \alpha_k\|_p\right) = \left(\frac{1}{p}\right)^k.$$

Zatem

$$\lim_{k\to\infty} g^{w_k} = \alpha.$$

□

Rozważmy teraz ciąg $x_n = g^n + k^n$, gdzie g jest generatorem $U(\mathbb{Z}/p^n\mathbb{Z})$, a $k \in \mathbb{Z}$. W pierwszym przybliżeniu p-adycznym, czyli dla $n = 1$, mamy następujące twierdzenie:

Twierdzenie 7. *Niech g będzie generatorem grupy multiplikatywnej $U(\mathbb{Z}/p\mathbb{Z})$. Wówczas jeżeli $p \equiv 1 \pmod 3$ oraz jeżeli 2 jest resztą sześcienną modulo p, to istnieje takie $k \in U(\mathbb{Z}/p\mathbb{Z}) \setminus \{1, g\}$, że każdy element $U(\mathbb{Z}/p\mathbb{Z})$ jest pewnym wyrazem ciągu*

$$x_n = g^n + k^n.$$

Dowód. Ponieważ $3 \mid p-1$, to w $U(\mathbb{Z}/p\mathbb{Z})$ jest pierwiastek trzeciego stopnia z jedynki. Jeżeli g jest generatorem tej grupy, to możemy przyjąć pierwiastek trzeciego stopnia, jako:

$$\omega = g^{\frac{p-1}{3}}.$$

Niech $k_i = g\omega^i$, dla $i \in \{1, 2\}$. Wtedy

$$g^n + k^n = g^n(1 + \omega^{ni}).$$

Ponieważ $\omega^3 = 1$, to dla $l \in \mathbb{Z}$ możemy zapisać ciąg x_n w postaci:

$$x_n = \begin{cases} 2g^{3l} & \text{dla } n \equiv 0 \pmod 3 \\ g^{3l+1}(1+\omega^i) & \text{dla } n \equiv 1 \pmod 3 \\ g^{3l+2}(1+\omega^{2i}) & \text{dla } n \equiv 2 \pmod 3 \end{cases}$$

Dla każdego $c \in \mathbb{Z}$ ciąg cg^n jest różnowartościowy. Każdy z trzech podciągów (dla $n \equiv 0, 1$ lub $2 \pmod 3$) zawiera więc $\frac{p-1}{3}$ różnych elementów z grupy. Wystarczy teraz pokazać, że te podciągi nie mają elementów wspólnych. Ponieważ zgodnie z założeniem 2 jest resztą sześcienną modulo p, to każdy wyraz ciągu x_n dla $n = 3l$ jest resztą sześcienną modulo p.

Zauważmy teraz, że

$$g^{3l+1}(1+\omega^i) = g^{3l+1}(-\omega^{2i}) = (-g^l)^3 g\omega^{2i},$$

oraz

$$g^{3l+2}(1+\omega^{2i}) = g^{3l+2}(-\omega^i) = (-g^l)^3 g^2\omega^i.$$

Jeżeli $(-g^l)^3 g\omega^{2i}$ miałoby być resztą sześcienną, to $g\omega^{2i} = gg^{2i(p-1)/3}$ też, ale gdyby tak było, to $1 + 2i\frac{p-1}{3} \equiv 0 \pmod 3$, czyli $\frac{p-1}{3} \not\equiv 0 \pmod p$, co jest sprzeczne z założeniem. Zatem $g\omega^{2i}$ a więc też każdy wyraz ciągu x_n dla $n = 3l+1$ jest niereszą sześcienną modulo p.

Ponieważ $g\omega^{2i}$ jest niereszą sześcienną, to $(g\omega^{2i})^2 = g^2\omega^i$ też. Zatem każdy wyraz x_n dla $n = 3l+2$ też posiada tą własność.

Gdyby podciągi x_n dla $n = 3l+1$ i $n = 3l+2$ miały elementy wspólne, to istniałyby takie $a, b \in \mathbb{Z}$, że:

$$-g^{3a+1}\omega^{2i} \equiv -g^{3b+2}\omega^i \pmod p,$$

czyli

$$g^{3a+1}\omega^i \equiv g^{3b+2} \pmod p,$$
$$g\omega^{2i} \equiv \left(g^{a-b}\right)^3 \pmod p,$$

to $g\omega^{2i}$ byłoby resztą sześcienną. Sprzeczność.

Zatem żaden podciąg nie ma z innym elementów wspólnych, więc ciąg x_n ma $p-1$ różnych wyrazów. □

Uwaga 2. Istnieją liczby pierwsze p postaci innej niż w powyższym twierdzeniu, dla których istnieje $k \in \mathbb{Z}/p\mathbb{Z}\setminus\{0,1,g\}$, takie że ciąg x_n zawiera wszystkie elementy z $U(\mathbb{Z}/p\mathbb{Z})$. Na przykład $p = 3389$, $g = 6$ i $k = 190$ spełniają powyższy warunek, ale jednocześnie $3389 \equiv 2 \pmod 3$.

Uwaga 3. Ponieważ g jest generatorem, to istnieje $l \neq p-1$, takie że $k = g^l$. Wówczas

$$x_n = g^n + (g^n)^l.$$

Ciąg x_n zawiera więc wszystkie elementy z $U(\mathbb{Z}/p\mathbb{Z})$ wtedy i tylko wtedy, gdy istnieje takie $l \neq p-1$, że $x \to x + x^l$ jest bijekcją na $U(\mathbb{Z}/p\mathbb{Z})$. Ciąg liczb p, dla których takie l istnieje można znaleźć w [4, A306787].

Twierdzenie 8. *Dla dowolnych $p \in \mathbb{P}$ i $g, k \in U(\mathbb{Z}/p^m\mathbb{Z})$, gdzie $m \in \mathbb{N}$ ciąg*

$$x_n = g^n - k^n$$

nie zawiera wszystkich elementów z $U(\mathbb{Z}/p^m\mathbb{Z})$.

Dowód. Z twierdzenia Eulera mamy, że $x_{n+p^{m-1}(p-1)} \equiv x_n \pmod{p^m}$, więc x_n ma okres co najwyżej $p^{m-1}(p-1)$. Ale $x_0 \equiv x_{p^{m-1}(p-1)} \equiv 0 \pmod p$, więc $\{x_n\}_{n\in\mathbb{N}} = \{0, x_1, x_2, \ldots, x_{p^{m-1}(p-1)-1}\}$. Zatem ciąg (x_n) nie zawiera wszystkich elementów z $U(\mathbb{Z}/p^m\mathbb{Z})$. □

Twierdzenie 9. *Niech $p > 2$ będzie liczbą pierwszą. Ponadto niech g będzie wybranym generatorem $U(\mathbb{Z}/p^2\mathbb{Z})$. Wówczas istnieje $k \in \mathbb{N}\setminus 1, g$ takie, że każdy element $\alpha \in \mathbb{Z}_p^*$ jest pewnym punktem skupienia ciągu*

$$x_n = g^n + k^n.$$

Dowód. Niech $k = g^{3p-2}$. Rozważmy funkcję $f(x) = x + x^{3p-2}$. Mamy, że $x + x^{3p-2} \equiv 2x \pmod{x^p - x}$. Dla każdego $\alpha \in \mathbb{Z}_p^*$ przyjmijmy więc funkcję pomocniczą $F_\alpha(x) = x + x^{3p-2} - 2\alpha$. Wtedy $F_\alpha(\alpha) = 0$. Mamy również $F'_\alpha(\alpha) = 1 + (3p-2)\alpha^{3p-3} \equiv -1 \not\equiv 0 \pmod p$. Zatem na mocy lematu Hensela, Istnieje dokładnie jedno $\beta \in \mathbb{Z}_p^*$, takie że $F_\alpha(\beta) = 0$, czyli $f(\beta) = 2\alpha$.

Z twierdzenia 6 mamy, że każde $\beta \in \mathbb{Z}_p^*$ jest pewnym punktem skupienia ciągu g^n. Istnieje więc ściśle rosnący ciąg n_i, taki że $\lim_{i\to\infty} g^{n_i} = \beta$. Ponieważ f jest funkcją wielomianową, to jest ciągła w metryce p-adycznej, więc:

$$\lim_{n\to\infty} x_n = \lim_{i\to\infty} f(g^{n_i}) = f(\lim_{k\to\infty} g^{n_k}) = f(\beta) = 2\alpha.$$

Zatem każdy element $\mathbb{Z}_p^*$ jest pewnym punktem skupienia ciągu x_n. □

Rozpatrzmy teraz konstrukcję trójmianów permutacyjnych.

Niech $\mathbb{P} \ni p \equiv 1 \pmod 3$, $\langle g\rangle = \mathbb{F}_p^*$, oraz niech $\omega = g^{\frac{p-1}{3}}$. Rozważamy ciąg:

$$x_n = g^n(a + b\omega^n + c\omega^{2n}).$$

Jeśli dobierzemy wartości parametrów $a, b, c \in \mathbb{F}_p$ tak, że $x_n \mod p = \mathbb{F}_p^*$, to otrzymujemy trójmian permutacyjny:

$$f(x) = x(a + bx^{\frac{p-1}{3}} + cx^{\frac{2(p-1)}{3}}).$$

Każdy wyraz ciągu x_n możemy przedstawić jako element jednego z trzech podciągów:

$$\begin{aligned} x_{3k} &= g^{3k}(a+b+c) \\ x_{3k+1} &= g^{3k+1}(a+b\omega+c\omega^2) \\ x_{3k+2} &= g^{3k+2}(a+b\omega^2+c\omega). \end{aligned}$$

Oznaczmy teraz $c_1 = a+b+c$, $c_2 = a+b\omega+c\omega^2$, oraz $c_3 = a+b\omega^2+c\omega$.

Niech $\mathbb{H} = \{x^3 : x \in \mathbb{F}_p^*\}$. Definiujemy wówczas charakter:

$$\chi(r) = \begin{cases} 1 & \text{gdy } r \in \mathbb{H} \\ \omega & \text{gdy } r \in g\mathbb{H} \\ \omega^2 & \text{gdy } r \in g^2\mathbb{H}. \end{cases}$$

Ponieważ dla ustalonego i wartość $\chi(x_{3k+i})$ jest stała, to żeby $x_n \mod p = \mathbb{F}_p^*$, podciągi $x_{3k}, x_{3k+1}, x_{3k+2}$ modulo p muszą zawierać się w parami różnych warstwach: $\mathbb{H}, g\mathbb{H}$ oraz $g^2\mathbb{H}$. Zatem $(\chi(c_1), \chi(c_2)\omega, \chi(c_3)\omega^2)$ muszą realizować permutację zbioru $\{1, \omega, \omega^2\}$. Ponieważ $|\mathbb{H}| = \frac{p-1}{3}$, to liczba trójek (c_1, c_2, c_3) dla których taka permutacja rest realizowana, to $3!\left(\frac{p-1}{3}\right)^3 = \frac{2}{9}(p-1)^3$.

Aby odzyskać współczynniki a, b, c rozwiązujemy układ równań:

$$\begin{cases} a+b+c = c_1 \\ a+b\omega+c\omega^2 = c_2 \\ a+b\omega^2+c\omega = c_3, \end{cases}$$

czyli

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}.$$

Zauważmy, że pierwsza macierz jest macierzą Vandermonde'a, zatem:

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{vmatrix} = (\omega-1)(\omega^2-1)(\omega^2-\omega) \neq 0.$$

Istnieje więc również macierz odwrotna. Wobec tego dla każdej trójki (c_1, c_2, c_3) otrzymujemy dokładnie jedną trójkę (a, b, c). Istnieje więc dokładnie $\frac{2}{9}(p-1)^3$ wielomianów permutacyjnych postaci:

$$f(x) = ax + bx^{\frac{p-1}{3}+1} + cx^{\frac{2(p-1)}{3}+1}.$$

6.2. **Metoda uniwersalna oparta na lemacie Hensela.** Pokazane zostało w uwadze do lematu Hensela, że pierwiastek wielomianu $F(x)$ w $\mathbb{Z}_p$ określony przez ciąg a_n jest zadany przez rekurencję:

$$a_n = a_{n-1} - \frac{F(a_{n-1})}{F'(a_{n-1})}.$$

Przy czym $F(a_0) \equiv 0 \pmod p$ oraz $F'(a_0) \not\equiv 0 \pmod p$.

Lemat 10. *Niech $F(x) = x^2 - r$, gdzie $r \in \mathbb{Z}_p$, $r \not\equiv 0 \pmod p$ i $\sqrt{r} \in \mathbb{Z}_p$. Wówczas ciąg a_n zdefiniowany przez rekurencję:*

$$a_n = \frac{a_{n-1} + \frac{r}{a_{n-1}}}{2},$$

jest zbieżny do $\sqrt{r}$.

Dowód. Ponieważ $\sqrt{r} \in \mathbb{Z}_p$, to z twierdzenia 5 mamy, że r jest resztą kwadratową modulo p. Zatem istnieje $a_0 \in \mathbb{Z}_p$ takie, że:

$$F(a_0) = a_0^2 - r \equiv 0 \pmod p.$$

Mamy $F'(x) = 2x$, więc $F'(a_0) = 2a_0 \not\equiv 0 \pmod p$. Zatem ciąg a_n zdefiniowany rekurencją:

$$a_n = a_{n-1} - \frac{F(a_{n-1})}{F'(a_{n-1})} = a_{n-1} - \frac{a_{n-1}^2 - r}{2a_{n-1}} = \frac{a_{n-1} + \frac{r}{a_{n-1}}}{2}.$$

na mocy lematu Hensela jest zbieżny do $\sqrt{r}$. □

Przykład 5. Niech $p = 11$. Wówczas $r = 5$ jest resztą kwadratową modulo 11. Jednym z rozwiązań kongruencji $x^2 \equiv 5 \pmod{11}$ jest $x = 4$. Zatem ciąg a_n reprezentujący $\sqrt{5}$ zdefiniowany jest przez rekurencję:

$$a_n = \frac{a_{n-1} + \frac{5}{a_{n-1}}}{2},$$

gdzie $a_0 = 4$.

6.3. **Porównanie metod.** Z własności sum Gaussa mamy:

$$y_n = \sum_{t=1}^{q-1} \left(\frac{t}{q}\right) x_n^t$$

oraz

$$\lim_{n\to\infty} y_n^2 = \left(\frac{-1}{q}\right) q.$$

Zatem:

$$\|y_{n+1} - y_n\|_p = \left\| \sum_{t=1}^{q-1} \left(\frac{t}{q}\right) x_{n+1}^t - \sum_{t=1}^{q-1} \left(\frac{t}{q}\right) x_n^t \right\|_p \leq$$

$$\leq \max_{1\leq k\leq q-1} \left(\left\| \left(\frac{k}{q}\right) (x_{n+1}^k - x_n^k) \right\|_p \right).$$

Ponieważ $x_{n+1}^n - x_n^n = (x_{n+1} - x_n)(x_{n+1}^{n-1} + x_{n+1}^{n-2} x_n + \cdots + x_n^{n-1})$, oraz dla $p \nmid n$, mamy:

$$x_{n+1}^{n-1} + x_{n+1}^{n-2} x_n + \cdots + x_n^{n-1} \equiv n x_n \not\equiv 0 \pmod p,$$

to

$$\left\|x_{n+1}^n - x_n^n\right\|_p = \|x_{n+1} - x_n\|_p .$$

Wobec tego

$$\max_{1\leq k\leq q-1} \left(\left\| \left(\frac{k}{q}\right) (x_{n+1}^k - x_n^k) \right\|_p \right) \leq \|x_{n+1} - x_n\|_p .$$

A ponieważ z wniosku 1 mamy $\|x_{n+1} - x_n\|_p \leq \left(\frac{1}{p}\right)^{n+1}$, to

$$\|y_{n+1} - y_n\|_p \leq \left(\frac{1}{p}\right)^{n+1}.$$

Czyli

$$\left\|\left(\frac{-1}{q}\right) q - y_n^2\right\| \leq \left(\frac{1}{p}\right)^{n+1}.$$

Innymi słowy, dla n otrzymujemy przybliżenie $\sqrt{\left(\frac{-1}{q}\right) q}$ z dokładnością do $\mathbf{n+1}$ **cyfr p-adycznych**.

Teraz rozważmy metodę Hensela:

Twierdzenie 10. *Niech $F(x) \in \mathbb{Z}_p[x]$, oraz $x_0 \in \mathbb{Z}_p$ takie, że $F(x_0) \equiv 0 \pmod{p}$ i $F'(x_0) \not\equiv 0 \pmod{p}$. Wówczas ciąg x_n zdefiniowany rekurencją:*

$$x_n = x_{n-1} - \frac{F(x_{n-1})}{F'(x_{n-1})},$$

spełnia

$$\|F(x_n)\|_p \leq \left(\frac{1}{p}\right)^{2^n}.$$

Dowód. Dowód przeprowadzimy przez indukcję. Dla $n = 0$ mamy $\|F(x_0)\|_p = \frac{1}{p} = \left(\frac{1}{p}\right)^{2^0}$. Załóżmy, że dla n zachodzi $\|F(x_n)\|_p \leq \left(\frac{1}{p}\right)^{2^n}$. Wówczas rozwijając $F(x_{n+1})$ w szereg Taylora wokół x_n mamy:

$$F(x_{n+1}) = F(x_n - \frac{F(x_n)}{F'(x_n)}) = \sum_{k=1}^{\deg F} \frac{F^{(k)}(x_n)F(x_n)^k}{k!F'(x_n)^k} = \sum_{k=2}^{\deg F} \frac{F^{(k)}(x_n)F(x_n)^k}{k!F'(x_n)^k}.$$

A ponieważ $\|F(x_n)\|_p \leq \left(\frac{1}{p}\right)^{2^n}$, oraz $\|F'(x_n)\|_p \geq 1$, to

$$\|F(x_{n+1})\| = \max_{2 \leq k \leq \deg F} \left(\frac{F^{(k)}(x_n)F(x_n)^k}{k!F'(x_n)^k}\right) \leq \left(\frac{1}{p}\right)^{2^{n+1}}.$$

□

Zatem po n iteracjach, otrzymujemy przybliżenie $F(x)$ z dokładnością do $\mathbf{2^n}$ **cyfr p-adycznych**.

7. Kontynuacja badań

Dla dowolnej liczby pierwszej nieparzystej p istnieje $g \in \mathbb{Z}$ takie, że reszty liczb g^n wyczerpują wszystkie reszty mod p różne od 0. W twierdzeniu 7 wszystkie reszty modulo p powstają jako reszty liczb ciągu $g^n + k^n$ mod p. Narzuca się pomysł scharakteryzowania wszystkich takich liczb g, k oraz p. Nie wydaje się to zbyt łatwe.

Metoda aproksymacji niektórych pierwiastków kwadratowych oparta na pierwiastkach z jedynki nie ma charakteru uniwersalnego. Na przykład wydaje się wątpliwe, aby można było w ten sposób aproksymować liczbę $\sqrt{2} \in \mathbb{Z}_7$. Nie jest jednak jasne jak dowodzić takich negatywnych rezultatów - to również będzie przedmiotem moich dalszych badań.

Bibliografia

[1] Z I Borevich i I R Shafarevich. *Number Theory*. Pure & Applied Mathematics S. San Diego, CA: Academic Press, 1966.

[2] Kenneth Ireland i Michael Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer New York, 1990.

[3] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. 2 wyd. Graduate texts in mathematics. New York, NY: Springer, 1996.

[4] OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequences*. Published electronically at `http://oeis.org`. 2024.