WYKŁAD 14

20.1 Konstrukcja ciał (skończonych)

Naszym celem obecnie jest konstrukcja ciała skończonego. Takie ciało uzyskamy przez wydzielenie pierścienia $\mathbb{F}[x]$ przez odpowiednią kongruencję. Jest to analogiczna konstrukcja do konstrukcji $\mathbb{Z}_p$ jako wydzielenia $\mathbb{Z}$ przez kongruencję podzielności przez liczbę pierwszą. Naszym ciałem zwykle jest ciało skończone (np. $\mathbb{Z}_p$), ale wszystko działa też dla ciał o charakterystyce $+\infty$.

Definicja 20.5 (Kongruencja w pierścieniu)**.** Relacja $\equiv \subseteq R^2$ jest *kongruencją* w pierścieniu R, jeśli

- jest relacją równoważności
- jest kongruencją w grupie $(R, +)$ oraz kongruencją w półgrupie $(R, \cdot)$.

$f \equiv_h g$
$\Downarrow$
$h \mid f-g$
$h \mid g-f$

$h \mid f-f=0$

$h \mid f-g$
$h \mid g-\omega$
$h \mid (f-g)+(g-\omega) = f-\omega$

Definicja 20.6 (Kongruencja modulo wielomian)**.** Dla ciała $\mathbb{F}$ oraz pierścienia wielomianów $\mathbb{F}[x]$ o współczynnikach z tego ciała oraz wielomianu $h \in \mathbb{F}[x]$ definiujemy kongruencję $\equiv_h$ na $\mathbb{F}[x]$:

$$f \equiv_h g \iff h \mid (f - g).$$

Lemat 20.7. *Dla ciała $\mathbb{F}$ oraz pierścienia wielomianów $\mathbb{F}[x]$ o współczynnikach z tego ciała oraz wielomianu $h \in \mathbb{F}[x]$ relacja $\equiv_h$ jest kongruencją na pierścieniu.*

Łatwo sprawdzić, że jest to relacja równoważności oraz że operacje dodawania oraz mnożenia są dobrze zdefiniowane (tj. nie zależą od wyboru reprezentanta). Ponadto uzyskany pierścień jest pierścieniem przemiennym z jednością.

$f \equiv_h f'$
$g \equiv_h g'$

$f+g \equiv_h f'+g'$

$h \mid f-f'$
$h \mid g-g'$
$h \mid f-f'+g-g'$
$h \mid (f+g)-(f'+g')$

$f \cdot g = f' \cdot g'$
$fg - f'g' = fg - f'g + f'g - f'g' =$
$= (f-f')g + f'(g-g')$

Fakt 20.8. *Operacje $+, \cdot$ są dobrze zdefiniowane w $\mathbb{F}[x]/\equiv_h$.*
$\mathbb{F}[x]/\equiv_h$ jest pierścieniem przemiennym z jednością.

$\mathbb{F}[x]/\equiv_h$

$[f]_h + [g]_h = [f+g]_h$

$[1]_h \cdot [f]_h = [1 \cdot f]_h = [f]_h$

$[f]_h([g]_h + [g']) = [f]_h \cdot [g+g']_h = [f(g+g')]_h$
$= [fg + fg']_h = [fg]_h + [fg']_h$

Lemat 20.9. *Jeśli wielomian $h \in \mathbb{F}[x]$ jest nierozkładalny, to w $\mathbb{F}[x]/\equiv_h$ istnieje element odwrotny dla $f \not\equiv_h 0$.*

jeśli $h \nmid f$ $\quad nwd(f, h) = 1 = af + bh$

$[af] = [1 - bh]_h$
$= [1]_h - [bh]_h$
$= [1]_h$

Twierdzenie 20.10. *Jeśli wielomian h jest nierozkładalny, to ciało $\mathbb{F}[x]/\equiv_h$ (jako przestrzeń liniowa nad $\mathbb{F}$) ma wymiar $\deg(h)$. Jeśli $\mathbb{F}$ jest skończone, to takie rozszerzenie ma $|\mathbb{F}|^{\deg h}$ elementów.*

$\mathbb{F}[x]/\equiv_h$

$1, x, x^2, \ldots, x^{\deg(h)-1}$ $\quad < \deg(h)$
$0 \quad 1 \qquad\qquad \deg(h)-1$

$f \in \mathbb{F}[x] \qquad f' \in \mathbb{F}[x] \qquad h \mid f - f' - \deg(f') < \deg(h)$
$x^i \qquad x^j$

Twierdzenie 20.11 (bez dowodu). *Dwa ciała skończone o p^k elementach są izomorficzne.*

Przykład 20.12. Wielomian nierozkładalny $x^2+1 \in \mathbb{R}[x]$; wychodzi izomorficzne z $\mathbb{C}$.

Przykład 20.13. Zbudujmy ciało 4-elementowe. $4 = 2^2$, więc bierzemy $\mathbb{F} = \mathbb{Z}_2$ i potrzebujemy wielomianu nierozkładalnego stopnia 2.

Lemat 20.14. *W $\mathbb{Z}_p[x]$ jest wielomian nierozkładalny dowolnego stopnia większego niż 0.*

Dowód polega na podaniu konkretnego wielomianu lub na zliczaniu wielomianów rozkładalnych i nierozkładalnych. Szczegółów nie podamy.

Przykład/Zastosowanie 20.15 (Kody Reeda-Solomona). Ustalamy ciało $\mathbb{F}$, zwykle jest to cialo $\mathbb{F} = \mathbb{F}_{2^m}$. Kodujemy wiadomość $(a_0, a_1, \ldots, a_{k-1})$, gdzie $a_i \in \mathbb{F}$ jako wielomian

$$\sum_{i=0}^{k-1} a_i x_i \in \mathbb{F}[x]$$

Przekazujemy tę wiadomość jako wartości $\bar{f}$ w n różnych niezerowych punktach $p_0, p_1, \ldots, p_{n-1} \in \mathbb{F}$, gdzie $n \geq k$. Punkty mogą być wybrane dowolnie, ale zwykle ten wybór jest ustalony, bo dla pewnych wartości (pierwiastki z 1) łatwiej się liczy.

Zbiór możliwych wiadomości oznaczamy przez RS a jej elementy nazywamy *słowami kodowymi*.

Jeśli $n = k$ to nic nie zyskujemy. Jeśli więcej, to jest pewna nadmiarowość.

Kody liniowe

Kody Reeda Salomona są szczególnym przypadkiem *kodów liniowych*, w których kodowane słowo traktowane jest element $\mathbb{F}^k$ a kodowanie to mnożenie przez ustaloną macierz K rozmiaru $n \times k$ (w naszym przypadku: macierz a'la Vandermonde), gdzie $n \geq k$; nie jest to jedyne możliwe kodowanie. W szczególności obraz (tj. słowo kodowe) jest z przestrzeni $\mathbb{F}^n$.

Odległość

Odległością (Hamminga) jest dla nas ilość pozycji, na których różnią się dwa komunikaty. Oznaczenie: $d(c, c')$. To jest odległość.

$d\left(\begin{smallmatrix}0\\1\\0\end{smallmatrix}, \begin{smallmatrix}1\\1\\0\end{smallmatrix}\right) = 1$ $\quad$ $d(\bar{v}, \bar{v}') = d(\bar{v}', \bar{v})$

$d\left(\begin{smallmatrix}0\\0\\0\end{smallmatrix}, \begin{smallmatrix}1\\1\\1\end{smallmatrix}\right) = 3$ $\quad$ $d(\bar{v}, \bar{v}) = 0$

$d(v, v') = 0 \Leftrightarrow v = v'$

$d(v, v') + d(v', v'') \geq d(v, v'')$

Odległość kodu C to

$$d(C) = \min_{u,v \in C, u \neq v} d(u, v) \ .$$

Lemat 20.16. *Odległość kodu Reeda-Solomona to* $n - k + 1$.

$t \geq$ wtedy $t \leq k-1$ kodujemy ciągi dł. $k-1$

ilości punktów

$p \neq p'$ $\quad \deg(p), \deg(p') \leq k-1$

$p \neq p'$ mogą mieć tę samą wartość w $\leq k-1$ punktach

$n - (k-1) = n - k + 1$ muszą mieć różne wartości

$d(p, p') \geq n - k + 1$

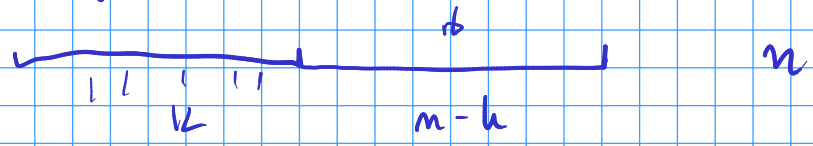
Optymalność odległości (ograniczenie Singletona)

Pokażemy teraz, że kody Reeda-Salomona są optymalne, tzn. jeśli kodujemy (dowolnym kodem) k-krotki elementów przy użyciu n-krotek, to któreś dwa mają odległość $\leq n - k + 1$.

Twierdzenie 20.17 (Ograniczenie Singletona). *Jeśli w zbiorze* $|\mathbb{F}|^n$ *wybierzemy* $|\mathbb{F}|^k$ *wektorów, to któreś dwa mają odległość najwyżej* $n - k + 1$.

$|F^k|$ elementów

„stoisk"

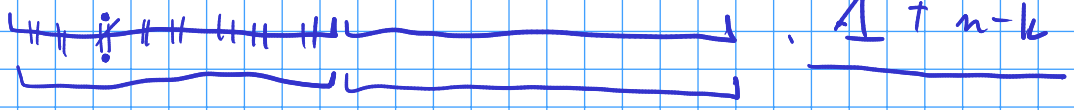


grupujemy po pierwszych k pozycjach

- v, v' są w tym samym st.

$$d(v, v') \leq n-k$$

w każdym stoisku jest jeden element.



$\cdot \underline{1 + n-k}$

Poprawianie błędów

Naturalne poprawianie: poprawiamy otrzymane słowo do najbliższego słowa kodowego.

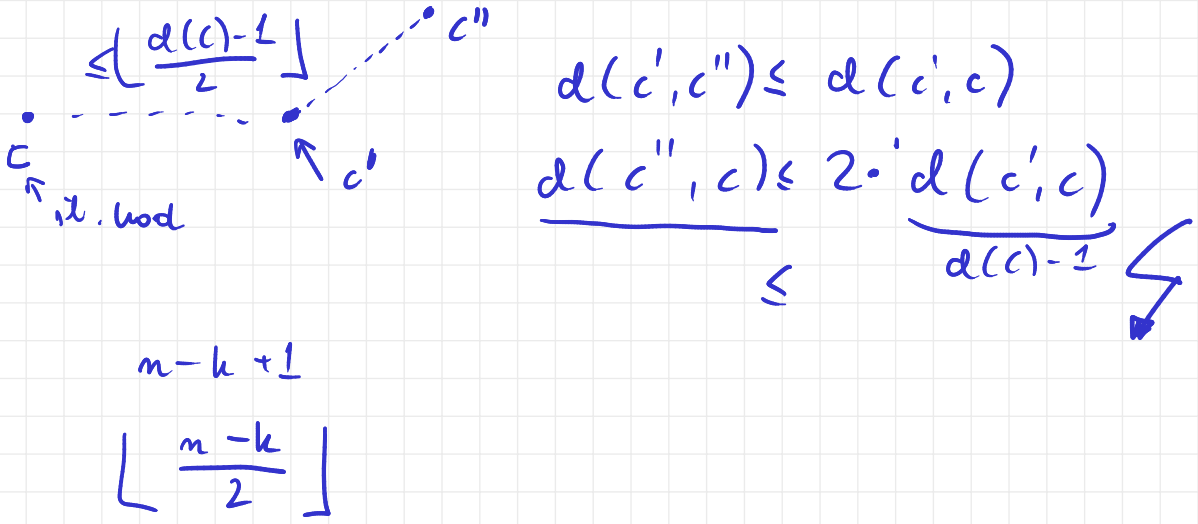
Twierdzenie 20.18. *Naturalne poprawianie poprawnie dekoduje słowo, jeśli ma ono mniej niż*

$$\frac{d(C)}{2}$$

błędów, czyli najwyżej

$$\left\lfloor \frac{d(C)-1}{2} \right\rfloor$$

błędów.



$$\left\lfloor \frac{n-k}{2} \right\rfloor$$

Algorytm Berlekamp–Welch poprawiania błędów

Cel: dane $\vec{w} = [w_0, \ldots, w_{n-1}] \in \mathbb{F}^n$.
szukane: wielomian $f \in \mathbb{F}[x]$, t. że $\deg(f) < k$, $f(\alpha_i) \neq w_i$ dla najwyżej $e \leq \left\lfloor \frac{n-k}{2} \right\rfloor$ albo „?” jak nie ma takiego wielomianu.

Oznaczenie: $I = \{i \ : \ f(\alpha_i) \neq w_i\}$. Dobrze zdefiniowane, bo takie f jest jedyne. Jak nie ma wyniku, to trudno. Niech $e = |I|$.

Moglibyśmy po prostu wybrać te błędy, zinterpolować i rozwiązać...

Popatrzmy na wielomian

Definicja 20.19 (Error locator polynomial). Dla zbioru pozycji błędów I zdefiniujmy *error locator polynomial*:

$$E(x) = \prod_{i \in I} (x - \alpha_i) \ .$$

Dlaczego taki: głównie to wiedziano, że go należy użyć...

Idea chcemy:

$$Q = fE$$

Ten wielomian zeruje się tam, gdzie są błędy, i mówi coś o f tam, gdzie nie ma błędów.

A ściśle:

BW1 wielomian E, o wiodącym współczynniku 1, stopnia $e \leq \lfloor \frac{n-k}{2} \rfloor$

BW2 wielomian Q stopnia $\leq e + k - 1$

BW3 dla każdego i zachodzi $w_i E(\alpha_i) = Q(\alpha_i)$.

Słowem kodowym ma być Q/E (jako wielomian).

Uwaga. Jeśli Q/E nie jest zdefiniowane, bo się dzieli z resztą, albo ma za duży stopień, to zwracamy błąd.

Lemat 20.20. *Jeśli dla danego $\vec{w}$ istnieje $\vec{w'} \in RS$ takie że $d(w, w') \leq e \leq \lfloor \frac{n-k}{2} \rfloor$ to istnieją Q, E spełniające BW.*

$E = \prod_{i=I} (x - \alpha_i)$ $\quad I = \{ w_i \neq w_i' \}$

$|I| = n - h \quad \lfloor \frac{n-h}{2} \rfloor$

$Q = f \cdot E \quad f \leftrightarrow w'$

$\deg f \leq k-1 \quad \deg E = e$

Lemat 20.21. *Jeśli Q_1, E_1 oraz Q_2, E_2 spełniają BW, to $Q_1/E_1 = Q_2/E_2$.*

Uwaga. Zauważmy, że jest to równość ilorazów i reszt, tzn. może być, że oba dzielenia dają resztę. Ale jeśli jeden się dzieli bez reszty, to drugi też, tj. jeśli jest poprawny wynik algorytmu, to wszystkie zwracane dają to samo.

$Q_1, E_1, \quad Q_2, E_2$ spełniają war.

$P = Q_1 E_2 - Q_2 E_1$

$\forall_i \quad P(\alpha_i) = \underbrace{Q_1(\alpha_i) E_2(\alpha_i)}_{w_i E_1(\alpha_i)} - \underbrace{Q_2(\alpha_i) E_1(\alpha_i)}_{w_i E_2(\alpha_i)}$

$n \leftarrow$ wartości $= 0 \qquad e \leq \frac{n-h}{2}$

$\deg(Q_1 E_2) \leq e + h - 1 + e = 2e + h - 1 \leq 2 \cdot \frac{n-h}{2} + h - 1 \leq n - 1$

$\deg(P) \leq n-1$

$P \equiv 0$

$\Leftarrow Q_1 E_2 - Q_2 E_1 = 0$

$\frac{Q_1}{E_1} = \frac{Q_2}{E_2}$

To jak to odtworzyć? Będziemy interpolować wielomiany. Zauważmy, że nie interesuje nas, czy ten układ jest jednoznacznie określony, może być nadokreślony lub niedookreślony — dowolne rozwiązanie jest OK i wiemy, że jakieś jest.

Czas działania: Trzeba rozwiązać układ równań $\mathcal{O}(n^3)$ (da się może ciut szybciej w zależność od danych) oraz podzielić dwa wielomiany — $\mathcal{O}(n^3)$. Ponownie dla specyficznych wartości może być ciut lepiej.

20.2 Rozszerzenia ciał

Alternatywne podejście konstrukcji ciała skończonego (w pewnym sensie bardziej naturalne): dodawanie elementu do ciała. Najmniejsze ciało zawierające dany element: tak myślimy o $\mathbb{C}$: to jest najmniejsze ciało zawierające $\mathbb{R}$ oraz i.

Przykład 20.22. Liczby postaci $\{a+b\sqrt{3} : a,b \in \mathbb{R}$ są ciałem. Jedyna nietrywialna operacja to odwrotność, ale łatwo sprawdzić, że $(a+b\sqrt{3})(a-b\sqrt{3}) = a^2-3b^2 \neq 0$ i tym samym łatwo podać element odwrotny do $a+b\sqrt{3}$.

Definicja 20.23 (Rozszerzenie ciała)**.** Dla ciała $\mathbb{F}$ przez $\mathbb{F}\langle S\rangle$ oznaczamy najmniejsze ciało zawierające $\mathbb{F}, S$.

Rozszerzenie $\mathbb{F}\langle a\rangle$ jest *przestępne*, jeśli a nie jest pierwiastkiem żadnego wielomianu z $\mathbb{F}[x]$ takie a również nazywamy przestępnym. Jest *algebraiczne*, jeśli a jest pierwiastkiem jakiegoś wielomianu z $\mathbb{F}[x]$.

Żeby ta definicja miała sens, to elementy S powinny być albo zupełnie „spoza" albo z jakiegoś ciała $\mathbb{F}' \supseteq \mathbb{F}$.

20.2.1 Rozszerzenie przestępne

Jak wygląda rozszerzenie przestępne? Możemy sobie wyobrazić, że dodajemy do $\mathbb{F}$ jakiś „świeży" element α. W nowym ciele muszą być też wszystkie wielomiany z $\mathbb{F}[\alpha]$ oraz ich odwrotności. Są więc też wszystkie ilorazy wielomian przez wielomian.

Definicja 20.24 (Ciało ułamków prostych)**.** Rozważmy ciało $\mathbb{F}$ oraz wielomiany nad nim $\mathbb{F}[x]$. Na zbiorze $\{\frac{f}{g} : f,g \in \mathbb{F}[x], g \neq 0\}$ wprowadzamy relację równoważności $\frac{f}{g} \sim \frac{f'}{g'} \iff fg' = f'g$. Tak określony zbiór jest ciałem z naturalnie zadanym dodawaniem oraz mnożeniem:

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg'+f'g}{gg'} \qquad \frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'}$$

Twierdzenie 20.25. *Ciało ułamków prostych dla $\mathbb{F}$ jest izomorficzne z $\mathbb{F}\langle a\rangle$ dla przestępnego α.*

20.2.2 Rozszerzenia algebraiczne

Rozważamy teraz przypadek $\mathbb{F}\langle a\rangle$ gdy a jest pierwiastkiem jakiegoś wielomianu w $\mathbb{F}[x]$. Chcielibyśmy powiedzieć, że w takim razie to rozszerzenie zawiera $a, a^2, \ldots, a^{k-1}$, gdzie wielomian nierozkładalny, którego a jest pierwiastkiem, ma stopień k. (Tak jak w konstrukcji ciał skończonych). Ale czy tak jest, w szczególności, czy takie wielomian istnieje?

Definicja 20.26. Dla ciała $\mathbb{F}$ oraz elementu a z jego rozszerzenia przez $I(a)$ (ideał a) oznaczamy

$$\{f \in \mathbb{F}[x] \,:\, \bar{f}(a) = 0\}$$

Lemat 20.27. *Dla ciała $\mathbb{F}$ oraz elementu a z jego rozszerzenia $I(a)$ jest zamknięty na dodawanie i mnożenie przez wielomiany z $\mathbb{F}[x]$.*

$f(a)=0 \quad g(a)=0 \quad (f+g)(a)=0 \qquad f(a)=0 \quad gf(a)=0$

Lemat 20.28. *Dla ciała $\mathbb{F}$ oraz elementu a z jego rozszerzenia $I(a)$ jest postaci*

$I(a)=$ (f) $\qquad \{f \cdot g \,:\, g \in \mathbb{F}[x]\}$

dla pewnego wielomianu nierozkładalnego $f \in \mathbb{F}[x]$. W szczególności $\bar{f}(a) = 0$.

$I(a)$ suma i wiel.

$nwd(f,g) = fg + f'h$

$I(a) \quad I(a) \quad I(a)$

$nwd(I(a)) \qquad f_1, f_2, f_3, \ldots$

$nwd(f_1, f_2) \quad nwd(f_1, f_2, f_3)\ldots$

$f(a)=0$

$f \leftarrow$ wielk. $\quad I(a) = \{g \cdot f : g \in \mathbb{F}[x]\}$

$f = f_1 \cdot f_2 \qquad f_1(a) \cdot f_2(a) = 0$

Stopień rozszerzenia to stopień tego wielomianu.

Wniosek 20.29. Rozszerzenie algebraiczne $\mathbb{F}\langle a\rangle$ jest izomorficzne z $\mathbb{F}[x]/_{\sim_h}$, gdzie h generuje $I(a)$.

$\mathbb{C} \quad x^2+1 \quad i \quad x^2+1$

20.3 Ciała algebraicznie domknięte

Definicja 20.30 (Ciało algebraicznie domknięte)**.** Ciało $\mathbb{F}$ jest *algebraicznie domknięte*, jeśli każdy wielomian nierozkładalny jest stopnia 1.

Fakt 20.31. *Ciało $\mathbb{F}$ jest algebraicznie domknięte wtedy i tylko wtedy gdy każdy wielomian ma pierwiastek.*

Fakt 20.32. *Ciało algebraicznie domknięte jest nieskończone.*

Przykład 20.33. $\mathbb{C}$ jest ciałem algebraicznie domkniętym. Nie jest nim $\mathbb{R}$ ani żadne $\mathbb{Z}_p$.

Twierdzenie 20.34. *Dla ciała $\mathbb{F}$ istnieje $\mathbb{F}' \supseteq \mathbb{F}$, które jest algebraicznie domknięte oraz działania $\mathbb{F}'$ obcięte do $\mathbb{F}$ to działania $\mathbb{F}$.*

Rozdział 21

Skończone $\mathbb{F}^*$ jest cykliczne

Chcemy pokazać, że jeśli $\mathbb{F}$ jest skończone, to $\mathbb{F}^*$ jest cykliczna. Dowód opiera się na wykazaniu, że istnieje w niej element rzędu $n = |\mathbb{F}| - 1$, co daje, że jest on generatorem. Aby to pokazać, będziemy dla każdego $k \leq n$ zliczać w grupie cyklicznej n elementowej oraz w grupie $\mathbb{F}^*$ elementy, które są rzędu k. Zauważmy, że wystarczy pokazać, że w grupie $\mathbb{F}^*$ jest nie więcej, niż w C_n (grupa cykliczna o n elementach).

Lemat 21.1. *Niech $R(G,k)$ oznacza liczbę elementów rzędu k w grupie abelowej G. Jeśli dla grupy skończonej G o n elementach zachodzi dla każdego k*

$$R(G,k) \leq R(C_n,k)$$

to G jest izomorficzne z C_n.

$$n = \sum_{k=0}^{n} R(G,k) \leq \sum_{k=0}^{n} R(C_n,k) = n$$

$$R(G,k) < R(C_n,k) \quad \lightning$$

Niestety, zliczanie elementów rzędu k jest dość kłopotliwe. Łatwiej jest zliczyć elementy, których rząd *dzieli* k.

21.1 Rzędy elementów w grupie cyklicznej

Lemat 21.2. *Niech g będzie generatorem grupy cyklicznej G o n elementach. Wtedy g^m jest jej generatorem $\iff \operatorname{nwd}(m,n) = 1$. W szczególności G ma $\varphi(n)$ generatorów.*

$\Rightarrow$ $\quad nwd(m,n) = 1 = am + bn$

$am = 1 - bn$ $\quad$ n - rzęd g

$(g^m)^a = g^{am} = g^{1-bn} = g^1 \cdot g^{-bn}$

$g^n = e$

$= g^1 \cdot e = g^1 \in \langle g^m \rangle$

$\langle G \rangle = \langle g \rangle \subseteq \langle g^m \rangle \subseteq \langle G \rangle$

$\Leftarrow$ $\quad g^m \leftarrow$ generator $\langle G \rangle$

$g = g^{am} = g \cdot g^{am-1} = g$

$g^{am-1} = e \iff n \mid am-1$

$am - 1 = bn$

$nwd(m,n) = 1 \Leftarrow am - bn = 1$

- $\varphi(n)$ generatorów $\quad 1, \dots, n-1$

$\varphi(n)$ liczb wzgl. pier. z n.

$|G|$ jest el. rzędu d

$g_1, g_1, \dots, g_n \leftarrow$ wszystkie el. rzędu d

$\langle g_1, \dots, g_n \rangle \leftarrow$ ujemna

$\langle h \rangle$

$h^d = e$

$(g_1^{dm_1} g_2^{dm_2} \dots g_n^{dm_n}) = e$

$h^d = e$

$h^{d'} = e \quad d' < d$

$g_1 = h^{n_1} \quad g_1^{d'} = (h_1^{d'})^{n_1} = e \quad d > d' \lightning$

rzęd $h = d$ $\quad h \in \dots$

$\varphi(d)$

Na ćwiczeniach pokazaliśmy lemat:

Lemat 21.3. *Jeśli G jest cykliczna, to każda jej podgrupa jest cykliczna.*

Lemat 21.4. *Niech G będzie grupą cykliczną rzędu n. W G istnieje element rzędu d wtedy i tylko wtedy, gdy $d|n$.*

Dla ustalonego rzędu d tych elementów jest $\varphi(d)$ i są one wszystkie elementami podgrupy rzędu d.

21.2 Rzędy elementów w $\mathbb{F}^*$

Pokazaliśmy wcześniej, że:

Lemat 21.5 (Przypomnienie). *Równanie $x^k = 1$ ma w ciele skończonym $\mathbb{F}$ najwyżej k różnych pierwiastków.*

Lemat 21.6. *Niech G będzie grupą skończoną rzędu n. Jeśli dla dowolnego $k \in \mathbb{N}$ zbiór $\{g \in G : g^k = e\}$ ma najwyżej k ~~elementów~~, to G jest cykliczna.*

Wszystkie el. sp. $\underbrace{g^k = e}$ w G tq w G_k.
el. rzędu k w G tq w G_k

G_k – cykliczna $\varphi(k)$

$\varphi(k)$ w C_n

$R(G,k) = R(G_k,k) = \varphi(k) = R(C_n,k)$

założenie tw. gęst sp.

G jest izomorficzna z C_n.

Twierdzenie 21.7. *Grupa $\mathbb{F}^*$ jest cykliczna.*

$\mathbb{F}^*$

$x^h = 1$ $\leq h$ rozw.