MATEMATYKA DYSKRETNA 2010

A. PAWEŁ WOJDA

Spis treści

1. Wykład 1 - 3.III.2010

1.1. **Matematyka dyskretna.** Przez *matematykę dyskretną* rozumie się dział matematyki, w którym nie stosuje się aparatu topologicznego, a w każdym razie w której ten aparat ma znaczenie raczej drugorzędne[1]. Podczas wykładów nie zobaczymy więc ani pochodnych, ani całek. Będziemy za to wykorzystywać wiadomości z algebry, teorii mnogości, teorii liczb. Będziemy mówić o kombinatoryce i teorii grafów.
Na wykładzie porównywałem *matematykę ciągłą* z przemieszczającą się wskazówką zegarka, zaś *matematykę dyskretną* ze zmieniającemi się cyframi zegarka elektronicznego.

1.2. **Zasada indukcji matematycznej.** Zasada indukcji matematycznej jest studentom dobrze znana ze szkoły. Można ją sformułować następująco.
Niech będzie dany ciąg zdań $(T_n)_{n=k}^{\infty}$ (gdzie k jest pewną liczbą naturalną).

- Jeżeli zdanie T_k jest prawdziwe oraz
- dla każdego $n \geq k$ z faktu, że Tn jest prawdziwe wynika, że T_{n+1} jest prawdziwe,

wówczas dla wszystkich $n \geq k$ zdania T_n są prawdziwe.

Zasadę indukcji matematycznej można przyjąć jako pewnik. My jednak zauważyliśmy, że wynika ona z jeszcze łatwiejszej do zaakceptowania **zasady dobrego uporządkowania zbioru liczb naturalnych**. Zasada ta mówi, że każdy podzbiór zbioru liczb naturalnych $\mathbf{N}$ ma element najmniejszy. W bardzo prosty sposób udowodniliśmy, że z zasady dobrego uporządkowania zbioru liczb naturalnych wynika zasada indukcji matematycznej.

Przykład 1. Wieże Hanoi (Brahmy)
Zabawka polega na tym, że dane są 3 patyczki nazwane A, B i C na podstawkach oraz n kółeczek różnej średnicy z dziurkami w środku każdego. Kółka są nałożone na patyczek A tak, że nigdy żadne większe koło nie leży na kółku mniejszym (czyli są ułożone od największego na dole do najmniejszego na wierzchu). Kółka przekłada się po jednym tak, by korzystając z pośredniego patyczka B przełożyć wszystkie kółka na patyczek C cały czas trzymając się zasady, że nigdy kółko większe nie może być położone na mniejszym.
Problem jest następujący: w ilu ruchach da się rozwiązać nasze zadanie?

Oznaczmy przez a_n liczbę koniecznych ruchów przy n kółkach. Z łatwością stwierdzamy, że $a_0 = 0, a_1 = 1$ no i niezbyt trudno jest zauważyć, że $a_n = 2a_{n-1} + 1$ (dla $n > 0$). Stąd łatwo obliczyć, że $a_2 = 3, a_3 = 7, a_4 = 15$. Te liczby sugerują ogólny wzór. No i rzeczywiście, indukcyjnie udowodniliśmy, że

$$a_n = 2^n - 1$$

dla dowolnego n naturalnego.
Starałem się przekonać słuchaczy, że to bardzo dużo (przekładając 64 kółka z szybkością

[1]Od tej reguły są bardzo znaczące odstępstwa. Być może najczęściej cytowany artykuł matematyczny, to praca dotycząca teorii grafów Kazimierza Kuratowskiego charakteryzująca grafy planarna. Grafy to jeden z najważniejszych obiektów zainteresowań matematyki dyskretnej. Kazimierz Kuratowski zaś to jeden z najwybitniejszych topologów.

1 mikrosekundy jedno, można z łatwością oszacować czas potrzebny wsystkich kółek na grubo ponad 500 000 lat).

1.3. **Równania rekurencyjne.** Niech będzie zadany ciąg (a_n) w następujący sposób.

- Dane są wartości $a_0, a_1, ..., a_{k-1}$ (a więc k pierwszych wyrazów ciągu) oraz wzór
- $a_n = f(a_{n-1}, a_{n-2}, ...a_{n-k})$, gdzie f jest pewną funkcją.

Zdefiniowany w taki sposób ciąg (a_n) nazywamy **rekurencyjnym stopnia** k.

1.3.1. *Ciąg Fibonacciego.* Ciąg Fibonacciego[2] to z pewnością najsłynniejszy ciąg rekurencyjny (drugiego stopnia). Pomijając tu anegdotę o królikach, można go zdefiniować następująco:

- $f_0 = 1$
- $f_1 = 1$
- $f_{n+1} = f_n + f_{n-1}$ dla $n \geq 2$

Oczywiście i tym razem można z łatwością wypisać pierwszych kilka wyrazów ciągu:

$$f_2 = 2, f_3 = 3, f_4 = 5, f_5 = 8, f_6 = 13, f_7 = 21, f_8 = 34, f_9 = 55, f_{10} = 89$$

Tym razem jednak ciąg kolejnych wyrazów, nawet gdybyśmy wypisali ich znacznie więcej, nie sugeruje żadnego ogólnego wzoru. Na następnym wykładzie poznamy sposób jak sobie z niektórymi ciągami rekurencyjnymi radzić. Metoda którą poznamy obejmuje także ciąg Fibonacciego. Nie precyzując metody ogólnej ciąg Fibonacciego jednak rozwiązaliśmy. Okazało się, że

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right)$$

Tak skomplikowane rozwiązanie oczywiście wyjaśnia, dlaczego nie byliśmy w stanie odgadnąć ogólnego wzoru.

[2]Postaci i znaczeniu Fibonacciego (1175-1250) poświęciłem na wykładzie chwilkę. Warto poszperać w wyszukiwarce i poczytać o człowieku, który poruszył europejską matematykę, napisał pierwsze znaczące dzieła matematyczne w Europie po 1000 lat zacofania.

2. Wykład 2 - 10.III.2010

2.1. **Wyznacznik Vandermonde'a.** Z następującego twierdzenia dotyczącego wyznaczników, będziemy korzystać w najbliższej przyszłości.

Twierdzenie 1.

$$det \begin{vmatrix} 1 & 1 & ... & 1 \\ x_1 & x_2 & ... & x_n \\ & & ... & \\ x_1^{n-1} & x_2^{n-1} & ... & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i \le j \le n} (x_j - x_i)$$

2.2. **Równania rekurencyjne liniowe. Równaniem rekurencyjnym liniowym jednorodnym stopnia** k nazywamy równanie postaci

$$a_n = f(a_{n-1}, ..., a_{n-k}) \tag{1}$$

gdzie $f : \mathbf{R}^k \to \mathbf{R}$ jest pewną funkcją liniową, oraz zadane są wartości pierwszych k wyrazów ciągu (a_n), $a_0, a_1, ..., a_{k-1}$. Przy tych zamych założeniach równanie

$$a_n = f(a_{n-1}, ..., a_{n-k}) + g(n) \tag{2}$$

Nazywamy **równaniem liniowym niejednorodnym stopnia** k (o funkcji $g : \mathbf{N} \to \mathbf{R}$, poza tym, że jest to funkcja określona w zbiorze liczb naturalnych i o wartościach rzeczywistych, niczego szczególnego nie zakładamy). Dla tak ogólnie postawionego problemu nie będziemy w stanie tu przedstawić metody rozwiązania, niemniej ta postać ułatwi pewne zapisy.
Równaniem rekurencyjnym liniowym o stałych współczynnikach jednorodnym nazywamy równanie rekurencyjne postaci

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + ... + \alpha_k a_{n-k} \tag{3}$$

zaś równanie

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + ... + \alpha_k a_{n-k} + g(n) \tag{4}$$

nazywamy **równaniem rekurencyjnym liniowym o stałych współczynnikach niejednorodnym**.

Dla równania (3) równanie

$$r^k = \alpha_1 r^{k-1} + \alpha_2 r^{k-2} + ... + \alpha_{k-1} r + \alpha_k \tag{5}$$

nazywamy **równaniem charakterystycznym**.

Podczas wykładu zauważyliśmy następujące fakty.

- Jeśli dane są ciągi będące rozwiązaniami równania (1), to także dowolna kombinacja liniowa tych ciągów jest rozwiązaniem (1) (inaczej mówiąc, zbiór rozwiązań równania (1) jest podprzestrzenią przestrzeni wszystkich ciągów rzeczywistych).
- Warunki początkowe (czyli wartości ciągu dla pierwszych k indeksów) należą do k-wymiarowej podprzestrzeni przestrzeni wszystkich ciągów rzeczywistych.
- Dla każdego rozwiązania r równania charakterystycznego (5) ciąg (r^n) jest rozwiązaniem równania (3) (pomijamy w tym rozumowaniu, na razie, warunki początkowe).

- Z twierdzenia o wyznaczniku Vandermonde'a można wywnioskować, że jeśli równanie charakterystyczne (5) ma k **różnych** rozwiązań $r_1, r_2, ..., r_k$, wówczas rozwiązanie (1) ma (jedyne) rozwiązanie postaci

$$a'_n = c_1 r_1^n + c_2 r_2^n + ... + c_k r_k^n$$

To oczywiście oznacza, że w przypadku istnienia k różnych pierwiastków równania charakterystycznego problem równań liniowych jednorodnych o stałych współczynnikach jest teoretycznie rozwiązany[3].

Powiedzieliśmy także (już bez dowodu), że jeśli r_0 jest l-krotnym rozwiązaniem równania charakterystycznego, wówczas takie rozwiązanie dostarcza nam l niezależnych rozwiązań (1), mianowicie $r_0^n, nr_0^n, ..., n^{l-1}r_0^n$.

Równanie niejednorodne nauczyliśmy się rozwiązywać stosując **metodę przewidywań**. Metoda ta polega na zastosowaniu następującego algorytmu postępowania.

- Metodę stosujemy wyłącznie do przypadku gdy w równaniu (4) funkcja g jest postaci

$$g(n) = \beta q^n$$

- Przewidujemy rozwiązanie postaci

$$a''_n = An^{l-1}q^n$$

gdzie l jest krotnością pierwiastka charakterystycznego q (czyli przewidujemy rozwiązanie postaci $a''_n = Aq^n$ jeśli q nie jest pierwiastkiem charakterystycznym).
- Teraz nadszedł moment uwzględnienia faktu, że zadane mamy pierwsze k wyrazy ciągu: znajdujemy takie $c_1, c_2, ..., c_k$ by

$$a_n = a'_n + a''_n$$

spełniały warunki początkowe problemu, czyli tak, by

$$a'_i + a''_i = a_i \quad \text{dla } i = 0, 1, ..., k-1$$

Przykład 2. *Równania*

$$a_n - 3a_{n-1} = 5 \cdot 7^n$$

$$a_n - 3a_{n-1} = 5 \cdot 3^n$$

$a_0 = 4$.

2.3. **Metody zliczania.**

[3]Właściwie byłby rozwiązany, nie tylko *teoretycznie*, gdybyśmy umieli rozwiązywać równania algebraiczne. Tymczasem nie tylko tego nie umiemy, ale wiemy, że metoda rozwiązywania takich równań nie istnieje.

2.3.1. *Zasada włączania-wyłączania (metoda sita).*

Twierdzenie 2. (Formuła Sita[4] lub Zasada Włączania i Wyłączania) *Niech $A_1, A_2, ..., A_n$ będą zbiorami skończonymi. Wówczas zachodzi wzór*

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} (-1)^{k+1} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}|.$$

Formułę sita wykazaliśmy metodą indukcji matematycznej.

2.3.2. *Miasta Parzyste i Nieparzyste.* W mieście P o 32 mieszkańcach kluby są tworzone według następujących zasad.

(i) Każdy klub ma parzystą liczbę członków.
(ii) Przecięcie dowolnych dwóch klubów ma parzystą liczbę elementów.

Natomiast w mieście N (także o 32 mieszkańcach) kluby są tworzone według tak, by

(a) Każdy klub miał nieparzystą liczbę członków.
(b) Przecięcie dowolnych dwóch klubów miało parzystą liczbę elementów.

Problem. Jaka jest maksymalna liczba klubów w P, a jaka w N?
Wykazaliśmy, że w P można utworzyć co najmniej $2^{16} \geq 65536$ klubów, podczas gdy w N co najwyżej 32.
Bardzo się zdziwiliśmy!
Oszacowanie liczby klubów w P znaleźliśmy stosując metody czysto kombinatoryczne. Dla oszacowania liczby klubów w N stosowaliśmy podstawowe wiadomości dotyczące wymiaru pewnej przestrzeni liniowej. Przydała się więc algebra liniowa.

[4]Dokładniej: "sita Eratostenesa". Eratostenes, (276-194 p.n.e) był kustoszem Biblioteki Aleksandryjskiej i jednym z największych umysłów starożytności. Sito Eratostenesa służyło do "odsiewania" liczb pierwszych od "plew" innych liczb. Jego innym, wielkim osiągnięciem była próba zmierzenia promienia Ziemi przez zmierzenie długości cieni rzucanych w południe przez dwie tyczki: jednej ustawionej w Aleksandrii, drugiej zaś w Syene (dzisiejszy Asuan). Wynik jaki otrzymał różnił sie tylko o 1% od nam znanego, a było to w czasach kiedy w kulistość Ziemi wierzył mało kto!

3. Wykład 3 - 17.III.2010

3.1. **Metody zliczania c.d.** Poza twierdzeniem Cantora (twierdzenie 9), o wszystkich zbiorach występujących poniżej zakładamy, że są skończone.

3.1.1. *Liczność zbioru par.*

$$|A \times B| = |A| \cdot |B|$$

3.1.2. *Wariacje z powtórzeniami.* Niech $B^A = \{f : A \to B\}$. Wwczas

$$|B^A| = |B|^{|A|}$$

(dow. indukcyjny ze względu na $|A|$).

3.1.3. —*Wariacje bez powtórzeń.*

$$|\{f : A \to B | f - bijekcja\}| = |B|(|B| - 1) \cdot ... \cdot (|B| - |A| + 1)$$

Wniosek 3. *Liczba permutacji zbioru n elementowego:* $n!$

3.1.4. *Liczba k elementowych podzbiorów zbioru n elementowego.* Niech $\binom{A}{k} = \{B \subset A : |B| = k\}$.

$$\left|\binom{A}{k}\right| = \binom{|A|}{k} = \frac{n!}{k!(n-k)!}$$

Wniosek 4. (1) $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$
(2) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

3.1.5. *Wzór Cauchy'ego.*

Twierdzenie 5.

$$\binom{p+q}{m} = \sum_{k=0}^{m} \binom{p}{k}\binom{q}{m-k}$$

3.1.6. *Wybory z powtórzeniami.* Wykorzystując model Lovásza-Pélikana-Vesztera wykazaliśmy następujące.

Twierdzenie 6. *Istnieje dokładnie* $\binom{n+r-1}{r}$ *rozwiązań całkowitych nieujemnych równania*

$$x_1 + x_2 + ... + x_n = r$$

3.1.7. *Zasada Gołębnika (szufladkowa Dirichleta).*

Twierdzenie 7. *Niech A i B będą zbiorami skończonymi,* $f : A \to B$.
(1) *Jeśli* $A| > |B|$ *wówczas f nie jest różnowartościowa.*
(2) *Jeśli* $|A| < |B|$ *wówczas f nie jest suriekją.*

Wniosek 8 (Twierdzenia Erdősa-Szekéresza)**.** *Niech* $n \in \mathbf{N}$. *Każdy ciąg różnych* $n^2 + 1$ *liczb rzeczywistych zawiera* $n + 1$ *wyrazowy podciąg monotoniczny.*

Twierdzenie 9 (Cantor)**.** *Niech A będzie dowolnym (niekoniecznie skończonym!) zbiorem. Nie istnieje suriekcja zbioru A na zbiór wszystkich podzbiorów zbioru A.*

4. Wykład 4 - 24.III.2010

4.1. **Metody zliczania c.dc.d.**

4.1.1. *Liczby Stirlinga pierwszego rodzaju.* Przypomnieliśmy co to jest permutacja, jak zapisujemy permutacje w przypadku zbioru skończonego (wyglądało na to, że nie wszyscy wiedzieli!), co to jest cykl permutacji (permutacja cykliczna) i jak rozkładamy permutację na iloczyn (złożenie) cykli.

$c(n,k)$ - liczba permutacji zbioru n-elementowego, które mają k cykli.

Twierdzenie 10. *Niech* $k, n \in \mathbf{N}, 0 < k \leq n$.

(1) $c(n,k) = c(n-1,k-1) + (n-1)c(n-1,k)$.
(2) $c(n,n) = 1$
(3) $c(n,0) = c(0,k) = 0$.

Dow. ...

Oznaczmy

$$[x]_n = x(x-1)\cdot ... \cdot (x-n+2)(x-n+1)$$

$$[x]_n = \sum_{k=0}^{n} s(n,k)x^k$$

Współczynniki $s(n,k)$ nazwyamy **liczbami Stirlinga I-go rodzaju**.

Twierdzenie 11. *Niech* $k, n \in \mathbf{N}, 0 < k < n$. *Wówczas*

(1) $s(n,k) = s(n-1,k-1) - (n-1)s(n-1,k)$.
(2) $s(n,n) = 1$.
(3) $s(n,0) = s(0,k) = 0$

Dow. ...

Twierdzenie 12. *Niech* $n, k \in \mathbf{N}, k \leq n$.

$$c(n,k) = (-1)^{n+k}s(n,k)$$

Dow. ...

4.1.2. *Liczba permutacji danego typu.*

Definicja 1. *Permutację* $\sigma \in S_n$ *nazywamy typu* $1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}$ *jeżeli ma* λ_i *cykli długości* i *(w rozkładzie kanonicznym na cykle rozłączne), dla* $i = 1, \dots, n$.

Uwaga. Oczywiście, jeśli permutacja σ jest typu $1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}$, wówczas zachodzi:

$$1\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = n$$

Twierdzenie 13 (Cauchy'ego)**.** *Jeśli* $1\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = n$, *wówczas liczba permutacji typu* $1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}$ *jest równa*

$$h(\lambda_1, ..., \lambda_n) = \frac{n!}{1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}\lambda_1!\lambda_2!...\lambda_n!}$$

Dow. ...

4.1.3. *Liczba podziałów zbioru.*

Definicja 2. *Rodzina*[5] $\{A_i\}_{i=1,...,n}$ *jest* **podziałem zbioru** X *jeżeli:*

(1) $X = \bigcup_{i=1,...,n} A_i$,
(2) $A_i \cap A_j$ *dla* $i \neq j$.

Definicja 3. *Podział zbioru n-elementowego jest typu* $1^{\lambda_1}2^{\lambda_2}...n^{\lambda_n}$ *jeśli zawiera* λ_i *zbiorów liczności i (dla* $i = 1, ..., n$*).*

Uwaga: Jeśli istnieje podział n-elementowego zbioru typu $1^{\lambda_1}2^{\lambda_2}...n^{\lambda_n}$, wówczas $1\lambda_1 + 2\lambda_2 + ... + n\lambda_n = n$.

Twierdzenie 14. *Jeśli* $1\lambda_1 + 2\lambda_2 + ... + n\lambda_n = n$ *wówczas liczba podziałów typu* $1^{\lambda_1}2^{\lambda_2}...n^{\lambda_n}$ *dana jest wzorem*

$$P(\lambda_1, ..., \lambda_n) = \frac{n!}{\lambda_1!\lambda_2!...\lambda_n!(1!)^{\lambda_1}(2!)^{\lambda_2}\dots(n!)^{\lambda_n}}$$

Dow. ...

4.1.4. *Liczby Stirlinga II rodzaju.*

Definicja 4. *Liczbą Stirlinga II rodzaju nazywamy* $S(n, k)$ *– liczbę podziałów zbioru n-elementowego na k podzbiorów niepustych.*

Twierdzenie 15.

$$S(n,k) = \sum_{\lambda_1+...+\lambda_n=k;\ \lambda_1+...+n\lambda_n=n} \frac{n!}{\lambda_1!\lambda_2!...\lambda_n!(1!)^{\lambda_1}(2!)^{\lambda_2}\dots(n!)^{\lambda_n}}$$

Twierdzenie 16. *(Zależność rekurencyjna dla liczb Stirlinga II rodzaju)*

(1) $S(n, n) = 1$ *(dla* $n \geq 0$*),*
(2) $S(n, 0) = 0$ *dla* $n > 0$,
(3) $S(n, k) = S(n-1, k-1) + kS(n-1, k)$ *dla* $0 < k < n$

Dow. ...

4.2. **Arytmetyka modularna.**

4.2.1. *Twierdzenie o dzieleniu liczb całkowitych i jego konsekwencje.*

Twierdzenie 17. *Dla dowolnych liczb całkowitych* a *i* b, $b > 0$ *istnieją jednoznacznie wyznaczone liczby* $q, r \in \mathbf{Z}$ *takie, że* $a = bq + r$*, przy czym* $0 \leq r < b$.

Liczby q oraz r nazywamy, odpowiednio, **ilorazem** i **resztą** dzielenia a przez b.

Warto podkreślić, że twierdzenie 17 nie jest tym, które większość studentów pamięta ze szkoły[6].

Mówimy, że d jest **największym wspólnym dzielnikiem** liczb całowitych a i b jeżeli

- $d|a$ i $d|b$ oraz
- dla każdego $c \in \mathbf{Z}$: $c|a\ \wedge c|b \Rightarrow c|d$

[5]Inaczej: zbiór zbiorów.

[6]Sprawdź, jaki jest wynik dzielenia liczby -9 przez 7?

Algorytm Euklidesa
Niech $a, b \in \mathbf{Z}$, $a, b \neq 0$.
Tworzymy rekurencyjnie ciąg (r_n):
$r_0 = a, \quad r_1 = b$
$r_{n-1} = q_n r_n + r_{n+1}$, gdzie $0 \leq r_{n+1} < r_n$.

Twierdzenie 18. *Niech $a, b \in \mathbf{Z}$, $a, b \neq 0$. Istnieje takie k całkowite, że $r_k \neq 0$, $r_{k+1} = 0$ (gdzie ciąg (r_n) jest wyznaczony przy pomocy algorytmu Euklidesa). Co więcej, mamy wówczas $r_k = \mathrm{NWD}(a, b)$.*

5. Wykład 5 - 31.III.2010

5.1. **Arytmetyka modularna c.d.**

Twierdzenie 19 (O postaci NWD)**.** *Niech $a, b \in \mathbf{Z}$ nie równe równocześnie zero. Wówczas*

$$NWD(a,b) = \min\{c > 0 : c = \alpha a + \beta b, \alpha, \beta \in \mathbf{Z}\}$$

Dow. ...

Uwaga. Zauważmy, że dzięki twierdzeniu 19 oraz algorytmowi Euklidesa, dla dowolnych liczb całkowitych a i b umiemy nie tylko efektywnie policzyć ich NWD, ale także przedstawić w postaci

$$d = \alpha a + \beta b$$

W najbliższej przeszłości ta umiejętność bardzo nam się przyda.

Definicja 5. *Mówimy, że dwie liczby całkowite a i b są* **względnie pierwsze***, jeśli $NWD(a,b) = 1$.*
Piszemy wówczas $a \perp b$.

5.2. **Grupy.**

5.2.1. *Przypomnienie pojęcia grupy.* Zbiór G z działanem $*$ nazywamy **grupą** jeżeli $*$ jest w G działaniem

- łącznym,
- posiadającym element neutralny e, oraz
- takim, że dla dowolnego $g \in G$ istnieje $g' \in G$ spełniający

$$g * g' = g' * g = e$$

(element odwrotny elementu g).

Jeśli działanie $*$ jest w G przemienne, wówczas G nazywamy **przemienną** lub **abelową**.

Przykłady: grupa Kleina, $\mathbf{Z}_n$ (dla różnych n).

5.2.2. *Grupy $\mathbf{Z}_n^*$.* Dłuższą chwilę poświęciliśmy zbiorowi $\mathbf{Z}_n$ (n naturalne i większe od 1) z działaniem mnożenia. Dość oczywistym jest, że elementem neutralnym dla mnożenia w $\mathbf{Z}_n$ jest 1. Łatwo się okazało, że dla niektórych n do niektórych elementów $\mathbf{Z}_n$ nie ma elementów odwrotnych. Tak więc, choć dla dodawania $\mathbf{Z}_n$ zawsze jest grupą przemienną, dla mnożenia nigdy grupą nie jest (bo 0 nie ma elementu odwrotnego). Postanowiliśmy tak zmodyfikować $\mathbf{Z}_n$, by jednak grupę multyplikatywną (t.j. z działaniem mnożenia) otrzymać. Rychło okazało się, że z $\mathbf{Z}_n$ nie wystarczy usunąć zera. Na szczęście udało się udowodnić następujące twierdzenie.

Twierdzenie 20. *Element $a \in \mathbf{Z}_n$ ma w $\mathbf{Z}_n$ element odwrotny ze względu na mnożenie wtedy i tylko wtedy gdy $a \perp n$*

Dow. ...

Stąd już tylko krok do następnego, ważnego twierdzenia.

Twierdzenie 21. *Niech $\mathbf{Z}^*$ będzie zbiorem elementów Z_n względnie pierwszych z n. Wówczas $\mathbf{Z}_n^*$ jest grupą przemienną z mnożeniem.*

Uwaga. Znowu, dzięki algorytmowi Euklidesa, umiemy do dowolnego elementu $a \in \mathbf{Z}_n^*$ efektywnie znaleźć element odwrotny.

5.2.3. *Chińskie Twierdzenie o Resztach.*

Twierdzenie 22 (Sun Ze ok. 450 r.)**.** *Niech a, b, n, k będą liczbami całkowitymi, $n, k > 0$, $n \perp k$. Wówczas istnieje dokładnie jedno rozwiązanie $x_0 \in \mathbf{Z}$, $0 \leq x_0 < nk$ układu równań:*

$$\begin{cases} x & \equiv & a & (\ mod\ n) \\ x & \equiv & b & (\ mod\ k) \end{cases}$$

Co więcej, każde rozwiązanie tego układu różni się od x_0 o wielokrotność nk.

Dow. ... (Warto znać, bo zawiera algorytm roawiązywania układów modularnych, o których mówi twierdzenie!)

Na koniec wykładu była anegdota o cesarzu (chińskim), a *de facto* pewne zastosowanie twierdzenia do policzenia liczności zbioru, bez liczenia wszystkich jego elementów.

6. Wykład 6 - 21.IV.2010

Uwaga: Napis DOM! na marginesie oznacza, że zdanie podane w tekście pozostawione zostało do udowodnienia (całkowicie lub częściowo) w domu lub na ćwiczeniach.

6.1. **Grupy c.d.**

6.1.1. *Homomorfizmy grup.* Niech $(G;*)$ i $(H,\circ)$ będą grupami. Odwzorowanie $\phi : G \to H$ nazywamy **homomorfizmem grup** jeśli dla wowolnych $a, b \in G$ spełniony jest warunek

$$\phi(a * b) = \phi(a) \circ \phi(b)$$

Jeśli, dodatkowo, ϕ jest bijekcją, wówczas homomorfizm ten nazywamy **izomorfizmem**. Wówczas grupy nazywamy **izomorficznymi**.

Przykład. Sprawdziliśmy, że

$$\phi : \mathbf{Z}_5 \ni k \to k \in \mathbf{Z}$$

nie jest homomorfizmem, zaś

$$\psi\mathbf{Z} \ni k \to k_{[5]} \in \mathbf{Z}_5$$

homomorfizmem jest[7].
Inne przykłady też były.

6.1.2. *Podgrupy.* Niech $(G;*)$ będzie grupą. $H \subset G$ jest **podgrupą** grupy G jeśli H z działaniem $*_{|_H}$ (czyli z działanie $*$ zacieśnionym do zbioru H) jest grupą.
Przykład. $\{0, 2, 4, 6\}$ jest podgrupą grupy $\mathbf{Z}_8$ (addytywnej).
$\mathbf{Q}$, $\mathbf{Z}$ są podgrupami addytywnej grupy $\mathbf{R}$.

Przykład. Sprawdziliśmy, że grupa Kleina jest izomorficzna z pewną podgrupą
DOM! grupy permutacji czterech elementów a także, że grupa izometrii sześcianu wykonalnych bez zniszczenia tego sześcianu, jest podgrupą grupy permutaci zbioru ośmioelementowego (wierzchołków sześcianu).

Twierdzenie 23. *Niech G będzie grupą multyplikatywną, $H \subset G$, $H \neq \emptyset$. H jest podgrupą grupy G wtedy i tylko wtedy, gdy dla dowolnych elementów $a, b \in H$*

$$ab^{-1} \in H$$

DOM! Dow... coś chyba mówiłem, ale bardzo szybko, a więc $\longrightarrow$...

Krotność i potęga elementu w grupie.
Niech G będzie grupą addytywną. Krotność elementu $a \in G$ definiujemy następująco.

(1) $0a = 0$
Należy zwrócić uwagę na fakt, że 0 z lewej strony równości oznacza liczbę całkowitą 0, zaś 0 z prawej strony równości jest elementem neutralnym grupy G. Mogą to być (i na ogół są) zupełnie różne elementy, które oznaczamy tym samym symbolem.
(2) Dla $n \in \mathbf{N}$:
$(n + 1)a = na + a$

[7]Przez $k_{[n]}$ oznaczamy resztę z dzielenia k przez n (inaczej mówiąc, *obcinamy* k modulo n).

(3) Dla $n \in \mathbf{Z}, n < 0$:
$na = (-n)(-a)$

Jeśli H jest grupą multyplikatywną, wówczas definiujemy potęgi całkowite elementu $a \in H$.

(1) $a^0 = 1$
1 oznacza tu oczywiście element neutralny grupy H.
(2) Dla $n \in \mathbf{N}$:
$a^{n+1} = a \cdot a^n$
(3) Dla $n \in \mathbf{Z}$ i $n < 0$:
$a^n = (a^{-1})^{-n}$

Uwaga 1. *Zbiór wszystkich całkowitych krotności pewnego elementu a dowolnej grupy addytywnej jest podgrupą tej grupy.*
Podobnie:
Zbiór wszystkich całkowitych potęg elementu a grupy multyplikatywnej jest podgrupą. DOM!

Podgrupę potęg elementu a (w grupie multyplikatywnej) nazywamy podgrupą **generowaną** przez ten element. Oczywiście rząd elementu i rząd podgrupy generowanej przez ten element są identyczne.

Rząd elementu w grupie. Niech G będzie grupą multyplikatywną, $a \in G$. Mówimy, że a jest rzędu k jeżeli

$$k = \min\{n \in \mathbf{N} - \{0\} : a^n = 1\}$$

Zauważyliśmy, że w $\mathbf{Z}_8$ rząd elementu 2 jest równy 4 (przenosząc przy okazji pojęcie rzędu na grupy addytywne).
W grupie $\mathbf{Z}$ żaden, poza 0, element nie ma rzędu (w takiej sytuacji mówimy także, że rzędem elementu jest ∞).

Twierdzenie 24. *W dowolnej grupie skończonej G każdy element ma rząd skończony.*

Dow. ...

6.1.3. *Grupy transformacji i Twierdzenie Cayleya.* Niech X będzie dowolnym zbiorem niepustym. Każdą podgrupę grupy $S(X)$ permutacji zbioru X nazywamy **grupą transformacji**.

Przykłady ...

Twierdzenie 25 (Cayley)**.** *Każda grupa jest izomorficzna z pewną grupą transformacji.*

Dow. ...

7. Wykład 7 - 28.IV.2010

Uwaga: Egzamin I termin: 22 czerwca 2010 w U2
Godz. 9.00

7.1. **Grupy c.d.c.d.**

7.1.1. *Twierdzenie Lagrange'a.*

Twierdzenie 26 (Lagrange'a)**.** *Niech H będzie podgrupą grupy skończonej G, $a = |H|, b = |G|$. Wówczas $a|b$.*

Definicja 6 (Przystawanie modulo półgrupa)**.** *Niech H będzie podgrupą grupy G, $a, b \in G$. Mówimy, że a* **przystaje do** *b* **modulo** *H (piszemy $a \equiv b \ (mod\ H)$ lub aR_Hb) jeżeli $ab^{-1} \in H$.*

Lemat 27. *Jeżeli H jest podgrupą G wówczas relacja przystawania modulo H jest w G relacją równoważności.*

Lemat 28. *Niech G będzie dowolną grupą, zaś H jej podgrupą. Wówczas klasą elementu neutralnego grupy G modulo H jest zbiór H.*

Lemat 29. *Niech G będzie dowolną grupą, zaś H jej podgrupą. Wówczas dowolne dwie klasy równoważności modulo H są równoliczne (bijektywne)*[8]*.*

Oczywiście twierdzenie Lagrange'a wynika natychmiast z lematu 29.

7.1.2. *Wnioski z twierdzenia Lagrange'a.*

Wniosek 30. *Każdy element grupy skończonej G ma rząd będący dzielnikiem rzędu grupy G.*

Twierdzenie 31 (Eulera)**.** *Jeśli liczby naturalne a, n są względnie pierwsze, wówczas*

$$a^{\varphi(n)} \equiv 1 \ (mod \ \ n)$$

Twierdzenie 32 (Małe Twierdzenie Fermata)**.** *Jeśli p jest liczbą pierwszą, $a \in \mathbf{Z}$, to*

$$a^p \equiv a(\ mod\ p)$$

7.2. **Kwadratowe residua modulo.**

Twierdzenie 33. *Niech p będzie liczbą pierwszą i niech $a \in \mathbf{Z}_p$. Wówczas a ma co najwyżej dwa pierwiastki kwadratowe w $\mathbf{Z}_p$.*

Niech $n \in \mathbf{N}, a \in \mathbf{Z}_n$. Mówimy, że a jest **kwadratowym residuum modulo** n, jeżeli istnieje $b \in \mathbf{Z}_n$ takie, że $a = b^2 \pmod n$.

Twierdzenie 34. *Niech $p \in \mathbf{N}$ będzie liczbą pierwszą, $p \equiv 3 \ (mod\ 4)$ i niech a będzie residuum kwadratowym w $\mathbf{Z}_p$. Wówczas pierwiastkami kwadratowymi a z $\mathbf{Z}_p$ są $a^{\frac{p+1}{4}} \ (mod\ p)$ oraz $-a^{\frac{p+1}{4}} \ (mod\ p)$.*

[8] W przypadku gdy G jest grupą skończoną oznacza to, że dowolne dwie klasy równoważności modulo H mają taką samą liczbę elementów.

7.3. **Zasady kryptografii z kluczem publicznym.** Wyobraźmy sobie, że mamy trzy osoby: Alicję, Boba i Ewę. Alicja chce przeslać Bobowi pewne informacje tak, by Ewa (ani nikt inny poza Bobem) nie mógł odgadnąć ich treści mimo, że informacje te przekazywane są w sposób jawny[9]. Warto w tym miejscu zdać sobie sprawę, że każdą informację można traktować jako liczbę. Standardowym zapisem jest powszechnie znany kod ASCII który można z łatwością zdobyć, na przykład za pomocą internetu (w kodzie tym każdemu znakowi odpowiada 3-cyfrowa liczba, *a* to 097, spacja to 032, *o* to 111 itd). Kod ASCII ma jednak oczywistą wadę: wszyscy go znają, a w każdym razie wiedzą jak sie w niego zaopatrzyć. Tak więc Alicja i Bob będą musieli przesyłane dane zaszyfrować (funkcję szyfrującą oznaczać będziemy przez E[10], na dodatek wychodząc z założenia, że wszystkie przesyłane wiadomości są podsłuchiwane (przez Ewę).

By osiągnąć swój cel, Alicja i Bob będą postępowali według następującego schematu:

1	Bob znajduje funkcję kodującą (szyfrującą) E oraz dekodującą D, a więc takie by $D(E(l)) = l$
2	Bob przesyła tekstem otwartym (Ewa widzi przekaz) funkcję E Alicji
3	Alicja koduje informację którą chce przesłać Bobowi według otrzymanej przez niego instrukcji (tę instrukcje zna także Ewa). Inaczej mówiąc Alicja oblicza wartość $m = E(l)$
4	Alicja wysyła Bobowi m (Ewa oczywiście także widzi przesyłaną informację)
5	Bob liczy $D(m)$ i poznaje treść przesyłki Alicji

Wydaje się, że znalezienie w tej sytuacji skutecznej metody szyfrowania chroniącej przesyłane informacje przed niezdrową[11] ciekawością Ewy będzie bardzo trudne. Okazuje się, że taka metoda istnieje, choć opiera się na bardzo, na pozór, kruchej podstawie. Tą podstawą jest przekonanie (hipoteza), że nie istnieje skuteczna metoda faktoryzacji liczb naturalnych. Rzeczywiście, choć pomnożenie *ręcznie*, a więc bez użycia komputera dwóch dużych, powiedzmy o 500 pozycjach dziesiętnych liczb, wydaje się czynnością kłopotliwą, wymagającą dużej ilości czasu i papieru, dla komputera jest proste i odbywa się w mgnieniu oka, dając w rezultacie liczbę o 1000 miejscach dziesiętnych. Nawet naszemu domowemu komputerowi taka czynność zajmie mniej niż sekundę. Jeśli jednak odwrócimy zagadnienie, czyli jeśli otrzymamy 1000-pozycyjną liczbę $n = pq$, gdzie p i q są nieznanymi nam liczbami pierwszymi, i zadanie nasze będzie polegało na znalezieniu p i q, to będziemy musieli wykonać liczbę dzieleń (prób) rzędu 10^{500}, co nawet najszybszemu komputerowi zajmie niewyobrażalną ilość czasu[12]. Na dodatek, gdyby wynaleziono komputery o wiele szybsze niż znane do tej pory, wystarczy zwiększyć liczbę cyfr znaczących n

[9] *Rozszyfrujmy* kilka spraw. Dlaczego Alicja, Bob i Ewa? To proste. Alicja, bo na literę A, Bob bo na literę B, E bo po angielsku *podsłuchiwacz* to *eavesdropper* (a więc na literę E, jak Ewa (*Eve*)). Rozsądnie jest także założyć, że wszystkie przesyłane informacje mogą być śledzone. Czyż nie tak jest gdy wyjmujemy pieniądze z bankomatu lub, w jeszcze większym stopniu, gdy płacimy za zakupy dokonywane za pośrednictwem internetu?

[10] E od angielskiego *encoding*

[11] A przede wszystkiem niebezpieczną dla Alicji i Boba!

[12] Sam sprawdź. Przyjmij, że jedno dzielenie wymaga 1 mikrosekundy, a dla ułatwienia obliczeń, że minuta ma 100 sekund, doba 100 godzin, rok 1000 dni.

z 1000 do 2000 by liczba operacji potrzebnych do znalezienia faktoryzacji wzrosła 10^{1000} krotnie.

Poniżej pokażemy w jaki sposób rozważania na temat złożoności obliczeniowej mnożenia i znajdowania rozkładu liczb na czynniki pierwsze mogą być przydatne w kryptografii.

7.4. **Metoda Rabina.** Metodę kodowania Rabina[13] można opisać następująco. Niech n będzie ustaloną, wystarczająco dużą (powiedzmy 300-cyfrową) liczbą. Funkcją kodującą jest

$$E(l) = l^2 (\mod n)$$

Oznacza to tyle, że Bob prześle Alicji liczbę n i funkcję kodującą. Alicja obliczy $l^2 \pmod n$, prześle tę informacje Bobowi. Ewa, podsłuchiwaczka, będzie znała zarówno l^2 jak i n, a jednak, z powodów opisanych wyżej, nie będzie w stanie obliczyć l. Zauważmy. że tak świetnie liczące pierwiastki kalkulatory (czy komputery) są w tej sytuacji zupełnie bezużyteczne. Na przykład gdybyśmy obliczyli przy pomocy kalkulatora $\sqrt{10}$ to otrzymalibyśmy 3.1621..., co nijak ma się do pierwiastka z 10 (mod 13) (dwie liczby dają w kwadracie 10 (mod 13), mianowicie 6 i 7). Jak to jednak możliwe, że Bob będzie w stanie zrobić to, czego nie jest w stanie uczynić Ewa, to znaczy obliczyć l?

Oto opis metody.

(1) Bob wybiera dwie duże liczby pierwsze p i q takie, by $p \equiv q \equiv 3 \pmod 4$. Następnie oblicza $n = pq$ i przesyła Alicji (a wszystko to podgląda Ewa).
(2) Alicja konwertuje swoją wiadomość w kodzie ASCII otrzymując liczbę l i oblicza $m = l^2 \pmod n$. Następnie przesyła Bobowi m. Ewa widzi m, zna już n, nie umie jednak obliczyć p i q, bo to jest właśnie trudny problem faktoryzacji.
(3) Bob znajduje pierwiastki z m obliczając wpierw $a = m^{\frac{p+1}{4}} \pmod p$, $b = -m^{\frac{p+1}{4}} \pmod p$, $c = m^{\frac{q+1}{4}} \pmod q$ oraz $d = -m^{\frac{q+1}{4}} \pmod q$, a następnie rozwiązując cztery układy równań modularnych:

$$\begin{cases} x \equiv a \pmod p \\ x \equiv c \pmod q \end{cases} \quad \begin{cases} x \equiv a \pmod p \\ x \equiv d \pmod q \end{cases}$$

$$\begin{cases} x \equiv b \pmod p \\ x \equiv c \pmod q \end{cases} \quad \begin{cases} x \equiv b \pmod p \\ x \equiv d \pmod q \end{cases}$$

Układy równań modularnych mają jednoznaczne rozwiązania modulo $n = pq$ dzięki lematowi chińskiemu. Otrzymamy więc aż cztery rozwiazania, choć wiemy, że dobre jest tylko jedno z nich. To jednak, by wśród rozwiązań odróżnić właściwe będzie dla Boba bardzo proste. Po przejściu z kodu ASCII na litery otrzyma jedną wiadomość sensowną i trzy ciągi znaków nie mających sensu.

Przykład. Alicja ma wiadomość $w = 15$. Bob wybiera $n = 209 = 11 \cdot 19$ (zauważmy, że $11, 19 \equiv 3 \pmod 4$).
Alicja liczy: $15^2 = 225 \equiv 16 \pmod{209}$
i przesyą Bobowi, który oblicza:
$16^{\frac{11+1}{4}} = 16^3 \equiv 5^3 \equiv 25 \cdot 5 \equiv 3 \cdot 5 = 15 \equiv 4 \pmod{11}$
$16^{\frac{19+1}{4}} = 16^5 = 16^2 \cdot 16^2 \cdot 16 = 256 \cdot 256 \cdot 16 \equiv 9 \cdot 9 \cdot 16 = 81 \cdot 16 \equiv 5 \cdot 16 \equiv 5 \cdot 16 = 80 \equiv 4 \pmod{19}$

[13]Nazwa od twórcy metody: Michaela Rabina

Bob rozwiązuje teraz (oczywiście korzystając z chińskiego twierdzenia o resztach) cztery układy równań modularnych:

$$\begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 4 \pmod{19} \end{cases} \quad \begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 15 \pmod{19} \end{cases}$$

$$\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 4 \pmod{19} \end{cases} \quad \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 15 \pmod{19} \end{cases}$$

Rzeczywiście, łatwo sprawdzić, że jeden z tych układów ma rozwiązanie, równe 15.

8. Wykład 8 - 5.V.2010

8.1. **Metoda RSA.** O ile metoda Rabina wykorzystuje Małe Twierdzenie Fermata, to metoda RSA[14] opiera się na twierdzeniu Eulera.

Opis metody RSA.

(1) Bob:
   (a) Znajduje 2 duże liczby pierwsze p, q, liczy $n = pq$ oraz $\varphi(n) = (p-1)(q-1)$.
   (b) Wybiera (dowolne) $e \in \mathbf{Z}^*_{\varphi(n)}$ (a więc e jest względnie pierwsze z $\varphi(n)$).
   (c) Oblicza $d = e^{-1}$ w $\mathbf{Z}^*_{\varphi(n)}$.

(2) Ewa: Widzi! Widzi zarówno n jak i e. Wie także jaka jest funkcja szyfrująca.

(3) Alicja:
   (a) Liczy $l = m^e \pmod n$
   (b) Wysyła l Bobowi.

Bob: Liczy

$$l^d = (m^e)^d \equiv m \tag{6}$$

Prawdziwość wzoru 6 wymaga uzasadnienia. Oto one.

(a) Przypadek: $m \perp n$. Skoro $ed \equiv 1 \pmod{\varphi(n)}$ mamy: $ed = 1 + k\varphi(n)$ (gdzie n jest pewną liczbą całkowitą. Wówczas

$$m^{ed} = m^{1+k\varphi(n)} = m(m^{\varphi(n)})^k \equiv m(\text{ mod } n)$$

(b) Przypadek: m i n nie są względnie pierwsze. Wtedy albo $p|m$ albo $q|m$ (gdyby $p|m$ i $q|m$ to mielibyśmy sprzeczność z założeniem, że $m < n$[15]). Załóżmy, że $p|m$ oraz $q \not| m$.
Mamy teraz: $m^{ed} = m^{1+k(p-1)(q-1)} = m(m^{q-1})^{k(p-1)}$. Ale $q \perp m$ (bo q jest liczbą pierwszą i q nie dzieli m). Wiemy że, $\varphi(q) = q - 1$. A więc $m^{ed} \equiv m \cdot 1^{k(p-1)} = m \pmod q$.
Ostatecznie otrzymaliśmy

$$m^{ed} \equiv m \ (mod\ q)$$

Mamy także

$$m^{ed} \equiv m \ (mod\ p)$$

(bo $m \equiv 0 \pmod p$). Z chińskiego twierdzenia o resztach m jest jedynym rozwiązaniem układu równań

$$m \equiv l^d \ (mod\ q)$$

$$m \equiv 0 \ (mod\ p)$$

(tak czy inaczej mamy $m \equiv l^d \pmod n$, niezależnie od tego, czy $m \perp n$, czy też nie).

---

[14] Nazwa metody od pierwszych liter nazwisk jej twórców: Rivest, Shamir i Adleman.

[15] Zakładamy, że liczby szyfrowane są mniejsze od n, w przeciwnym przypadku ulegałyby obcięciu modulo n, a więc zniekształceniu. Takie szyfrowanie byłoby bez sensu!

8.2. **Grupy c.d.**

8.2.1. *Lemat Burnside'a.* **Definicja.** Niech G będzie grupą multyplikatywną. Mówimy, że G **działa na zbiorze** X jeśli jest określone odwzorowanie $\varphi : G \times X \to X$ spełniające następujące dwa warunki (piszemy $g(x)$ zamiast $\varphi(g, x)$):

(1) dla dowolnych $g_1, g_2 \in G$ oraz dla każdego $x \in X$ $(g_1 \cdot g_2)(x) = g_1(g_2(x))$
(2) dla dowolnego $x \in X$ $e(x) = x$ (gdzie e jest elementem neutralnym grupy G).

Przykłady: grupa Kleina jako podgrupa permutacji na zbiorze $\{1, 2, 3, 4\}$.

Twierdzenie 35. *Jeśli grupa G działa na zbiorze X, $g \in G$, to g jest bijekcją.*

Dla grupy G działającej na zbiorze X oraz el. $x \in X$ **stabilizatorem** x nazywamy

$$Stab\ x = \{g \in G : g(x) = x\}$$

Przykład ..

Twierdzenie 36. *Stabilizator dowolnego elementu $x \in X$ jest podgrupą grupy G.*

Przykład. Grupa obrotów sześcianu (foremnego).

Orbitą elementu $x \in X$ nazywamy zbiór

$$Orb\ x = \{g(x) : g \in G\}$$

Relacja R określona przez

$$xRy \iff \exists g \in G :\ g(x) = y$$

jest w X równoważnościowa.

Twierdzenie 37. *Jeśli skończona grupa G działa na zbiorze X, wówczas dla każdego $x \in X$*

$$|G| = |Stab\ x| \cdot |Orb\ x|$$

Dowód. Niech $x \in X$. Oznaczmy przez H stabilizator elementu x (czyli: $H = Stab\ x$). Na mocy twierdzenia 36 wiemy, że H jest podgrupą grupy G. Możemy wic, podobnie jak w dowodzie twierdzenia Lagrange'a (tw. 26), rozważać warstwy grupy G modulo podgrupa H (czyli zbiór klas abstrakcji relacji R zdefiniowanej przez $gRh \Leftrightarrow gh^{-1} \in H$). Przypomnijmy, że w dowodzie twierdzenia Lagrange'a zbiór warstw G modulo H oznaczyliśmy przez G/H i wykazaliśmy, że

- Warstwa dowolnego elementu $a \in G$ jest postaci Ha,
- Wszystkie warstwy są równoliczne (a ponieważ warstwą elementu neutralnego jest H, w przypadku skończonym każda warstwa ma tyle samo elementów co podgrupa H).

Tym razem wykażemy, że każda warstwa jest równoliczna ze orbitą elementu x. Zdefiniujmy funkcję

$$\varphi : G/H \ni Hg \to g^{-1}(x) \in Orb\ x$$

Nim wykażemy, że φ jest bijekcją, musimy udowodnić, że

- $g^{-1}(x) \in Orb\ x$
- φ jest dobrze określona czyli, że jeżeli $Hg = Hh$, to

Rzeczywiście, w orbicie elementu x są wszystkie wartości funkcji z G na elemencie x, no a przecież g^{-1} jest elementem G.
Przypuśćmy teraz, że $Hg = Hh$. Ponieważ $e \in H$, musi w H istnieć taki element f, że $g = fh$ A wobec tego

$$g^{-1}(x) = (fh)^{-1}(x) \Rightarrow g^{-1}(x) = (h^{-1}f^{-1})(x) = h^{-1}(f^{-1}(x))$$

Ale $f \in H$, zaś H jest stabilizatorem x, czyli $f^{-1}(x) = x$ i otrzymujemy ostatecznie $g^{-1}(x) = h^{-1}(x)$, czyli $\varphi(hg) = \varphi(Hh)$.

- φ **jest iniektywna:** $\varphi(Hg) = \varphi(Hh) \Rightarrow g^{-1}(x) = h^{-1}(x) \Rightarrow h \circ g^{-1}(x) = x \Rightarrow hg^{-1} \in H \Rightarrow Hg = Hh$
- φ **jest suriektywna:** Niech $y \in Orb\ x$. Wówczas istnieje $g \in G$ takie, że $y = g(x)$, a wtedy $y = h^{-1}(x)$ dla $h = g^{-1}$, czyli $y = \varphi(Hh)$. ■

Przykład – ilustracja funkcjonowania twierdzenia 37.
Grupa izometrii pięciokąta.
Przykład. Grupa izometrii wykonalnych sześciościanu: 24-elementowa

9. Wykład 9 - 12.V.2010

9.1. **Lemat Burnside'a.** Dla danej grupy G działającej na zbiorze X oraz $ginG$ zbiór punktów stałych g oznaczamy przez $Fix\ g$:

$$Fix\ g = \{x \in X : g(x) = x\}$$

Twierdzenie 38 (Lemat Burnside'a)**.** *Niech G będzie grupą skończoną działającą na zbiorze skończonym X. Wówczas liczba N orbit zbioru X ze względu na G wynosi*

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix\ g|$$

Przykłady ...
Dowód (metodą podwójnego zliczania)...

9.2. **Teoria grafów.** Definicja grafu prostego. Rząd (ozn. $|G|$) i rozmiar (ozn. $\| G \|$) grafu G. Wierzchołki **połączone**, wierzchołki i krawdzie **incydentne**. **Stopień** wierzchołka v (ozn. $d_G(v)$) w grafie G.

Twierdzenie 39. *Jeśli $G = (V; E)$ jest grafem zwykłym skończonym, wówczas*

$$\| G \| = \frac{1}{2} \sum_{v \in V} d_G(v)$$

Wniosek 40. *W dowolnym grafie skończonym liczba wierzchołków stopni stopni nieparzystych jest parzysta.*

Twierdzenie 41 (O podawaniu rąk[16])**.** *W dowolnym grafie zwykłym (prostym) istnieją co najmniej dwa wierzchołki tego samego stopnia.*

Dow. ...
Definicje **trasy, ścieżki, drogi, cyklu** w grafie. Graf **spójny**.

Twierdzenie 42. *Jeśli graf G ma dokładnie dwa wierzchołki stopnia nieparzystego, to wierzchołki te połączone są ścieżką (a co za tym idzie, są we wspólnej składowej).*

Dow. ...

9.2.1. *Grafy eulerowskie.* Definicja **multigrafu (grafu)**
Definicja **cyklu Eulera**, **grafów eulerowskich**. Anegdota o mostach królewieckich.

Twierdzenie 43 (Eulera)**.** *Multigraf bez wierzchołków izolowanych jest eulerowski wtedy i tylko wtedy gdy*

(1) *jest spójny,*
(2) *stopień dowolnego wierzchołka jest parzysty.*

Dow. ...

[16] *Handshaking Theorem*

10. Wykład 10 - 19.V.2010

10.1. **Grafy eulerowskie c.d.**

Wniosek 44. *W multigrafie G bez wierzchołków izolowanych istnieje (otwarta) droga eulerowska wtedy i tylko wtedy, gdy*

(1) *G jest spójny,*
(2) *dokładnie dwa wierzchołki G są stopnia nieparzystego.*

Dow. ...

Algorytm Fleury'ego znajdowania cyklu Eulera.
Algorytm ten znajduje cykl Eulera w grafie[17] spełniającym warunki twierdzenia Eulera (graf spójny, stopnie wszystkich wierzchołków parzyste).
Algorytm działa według następujących reguł.

(1) Algorytm rozpoczyna swoje działanie od dowolnego wierzchołka u (od tego jednak momentu już ustalonego).
(2) Tworzymy ciąg ES, do którego w każdej kolejnej iteracji dopisujemy następną krawędź e tworzonego cyklu eulerowskiego, którą z kolei *wyrzucamy* ze zbioru krawędzi grafu, tworząc w ten sposób *bieżący* graf G'. Jeśli w wyniku tej operacji w grafie pojawia się wierzchołek izolowany (stopnia zero), wówczas usuwamy go także.

Powiedzmy, że ostatnim wierzchołkiem, do którego dotarliśmy jest wierzchołek v nie izolowany w bieżącym grafie G'. Niech e będzie krawędzią G' taką, że

- jednym z jej końców jest v a drugim, powiedzmy, w.
- $G' - \{e\}$ jest dalej spójny chyba, że stopień v w G' jest równy 1).
  Uwaga: To, że e można tak właśnie wybrać, udowodnimy później.
- Do ciągu ES dopisujemy e, G' (graf *bieżący*) zastępujemy przez $G' - \{e\}$ (jeśli v stał się po tej operacji izolowany, to usuwamy go z grafu również). Jeśli w jest w nowym grafie G' izolowany, algorytm się kończy. Skonstruowaliśmy cykl Eulera. Jeśli nie, kontynuujemy od wierzchołka w.

Jest oczywistym, że algorytm się kończy, gdy graf G' nie ma już krawędzi, a więc gdy ES jest ciągiem krawędzi tworzącym cykl Eulera.
Pozostaje jednak wykazać, że algorytm jest wykonalny, to znaczy, że w każdym etapie można w G' wybrać taką krawędź e o końcu w v, że $G' - \{e\}$ jest spójny chyba, że v w $G' - \{e\}$ jest izolowany (wtedy v także z G' usuwamy i w dalszym ciągu mamy, rzecz jasna, graf spójny)[18].
W tym celu zauważmy, że graf G' jest spójny (z konstrukcji) oraz, że w G' albo

(i) są dokładnie 2 wierzchołki stopnia nieparzystego (jednym z nich jest wtedy u a drugim v),
albo
(ii) wszystkie wierzchołki są stopnia parzystego (tak będzie jesli $v = u$).

W przypadku (i) dołączamy do G' nową krawędź łączącą u i v (wierzchołki stopni nieparzystych).
W dugim przypadku nie robimy nic[19].
W obu przypadkach w efekcie otrzymujemy graf, który jest spójny (bo G' taki

[17] Zamiast mówić (pisać) *multigraf* najczęściej mówimy i piszemy *graf*

[18] Proszę zauważyć, że ten dowód jest, niewiele ale jednak, różny od tego, który był podany ma wykładzie. Oba są dobre.

[19] Czyli to, co lubimy najbardziej!

był) i ma wszystkie wierzchołki stopnia parzystego. Jest więc eulerowski (na mocy twierdzenia Eulera). Łatwo stwierdzić teraz, że można tak wybrać e, krawędź o jednym końcu w v, by $G' - \{e\}$ był spójny (chyba, że $d_{G'}(v) = 1$, lecz ten przypadek, to najmniejszy problem, opisany został już powyżej).

10.2. **Grafy płaskie i planarne.** Definicja grafów płaskich i planarnych. Regiony. Stopień regionu (podczas wykładu stopień oznaczałe inaczej, lepiej jest jednak oznaczać tak jak poniżej, czyli przez *deg* R).

Twierdzenie 45 (Euler)**.** *Jeśli G jest grafem płaskim rzędu n o rozmiarze m i o f regionach, wówczas*

$$n = m - f + 2$$

Dow. ...

Definicja stopnia regionu: **stopniem regionu** deg R nazywamy długość (liczbę krawędzi) najkrótszej drogi stanowiącej jego brzeg.

Twierdzenie 46. *Jeśli G jest grafem płaskim o regionach $R_1, \ldots, R_f$ oraz rozmiarze m, wówczas*

$$\sum_{i=1}^{f} deg\ R_i = 2m$$

11. Wykład 11 - 26.V.2010

11.1. **Garfy planarne c.d.** Udowodniliśmy następujący wniosek z twierdzenia 45 (Eulera).

Wniosek 47. *Jeśli G jest grafem planarnym spójnym bez pętli i krawędzi wielokrotnych rzędu n, rozmiaru m i o f regionach, wówczas*

(1) $3f \leq 2m$
(2) $m \leq 3n - 6$

Wniosek 48. *Grafy K_5 i $K_{3,3}$ nie są planarne.*

Def. bryły regularnej.
Siatki wielościanów.

Twierdzenie 49 (O bryłach platońskich)**.** *Jedynymi bryłami regularnymi są czworościan, sześcian, ośmiościan, dwunastościan i dwudziestościan.*

Dowód....

Twierdzenie 50 (K. Kuratowski)**.** *Graf prosty G jest planarny wtedy i tylko wtedy gdy nie zawiera podgrafów homeomorficznych z K_5 ani z $K_{3,3}$.*

11.2. **Drzewa i lasy. Drzewem** nazywamy dowolny graf prosty (tzn. bez pętli i krawędzi wielokrotnych) spójny i bez cykli. **Las** to graf, którego każda składowa jest drzewem.

Twierdzenie 51. *Graf prosty jest drzewem wtedy i tylo wtedy, gdy dowolne dwa jego wierzchołki połączone są dokładnie jedną ścieżką.*

Dowód. ...

Twierdzenie 52. *Jeśli graf T jest drzewem, wówczas $\| T \| = |T| - 1$.*

Dowód. ...

Twierdzenie 53 (O własnościach drzew)**.** *Niech $T = (V; E)$ będzie grafem zwykłym. Następujące warunki są równoważne.*

(1) *T jest drzewem.*
(2) *T jest spójny i dla dowolnego $e \in E$ graf $T - e$ nie jest spójny.*
(3) *T nie zawiera cykli i $|T| = \| T \| + 1$*
(4) *T jest spójny i $|T| = \| T \| + 1$*
(5) *T nie zaweiera cykli i dla dowolnych niepołączonych wierzchołków a, b grafu T graf $T \cup \{ab\}$ zawiera dokładnie jeden cykl.*

Uwaga: $T \cup \{ab\}$ to graf otrzymany z T przez dodanie krawędzi ab (inaczej: przez połaczenie wierzchołków a i b krawędzią).
Dow. ...

Twierdzenie 54. *Niech T będzie dowolnym drzewem zaś v jego dowolnym wierzchołkiem. Wówczas istnieje taka numeracja wierzchołków T: $v = v_1, v_2, \ldots, v_n$ oraz krawędzi $e_1, e_2, \ldots, e_{n-1}$, że wierzchołek v_{i+1} jest połączony z dokładnie jednym spośród wierzchołków $v_1, ..., v_{i-1}$ krawędzią e_i.*

Przykład...

Macierz incydencji grafu G. $M = (a_{ij})$ nazywamy macierzą incydencji grafu G o zbiorach wierzchołków $\{v_1, \ldots, v_n\}$ i krawędzi $\{e_1, \ldots, e_m\}$ jeżeli

$$a_{ij} = \begin{cases} 1 & \text{jeśli wierzchołek } v_i \text{ jest jednym z końców krawędzi } e_j, \\ 0 & \text{w przeciwnym przypadku} \end{cases}$$

Przykład...

12. Wykład 12 - 2.VI.2010

Uwaga egzamin!
Przypominam:
Egzamin pisemny 22-go czerwca w U2, 9-12
Egzamin ustny dla sób zwolnionych z pisemnego na podstawie wysokich ocen z zaliczeń:
22-go czerwca w B.7, na I piętrze w moim pokoju od godz. 8.00
(numeru pokoju nie pamiętam, jestem w nim zaledwie 12 ostatich lat, ale każde dziecko wskaże)
lista szczegółowa, z orientacyjnym terminem rozpoczęcia egzaminu ukaże się w terminie późniejszym.
II termin: 20 września, 9-12, w s. 1.8 paw. B7 (Czarnowiejska 70, za budynkiem Metalurgii)
III termin: 27 września w s. 2.1 B7

12.1. **Drzewa c.d.**

Wniosek 55. *Macierz incydencji drzewa rzędu n jest rzędu $n-1$.*

Dow. ...

12.2. **Drzewa jako przestrzenie metryczne.** Niech G będzie grafem prostym. **Odległością wierzchołków** a i b nazywamy liczbę $\mathrm{dist}_G(a,b)$ równą długości najkrótszej ścieżki z a do b.
dist_G spełnia warunki metryki.
Ekscentrycznością wierzchołka a grafu $G=(V;E)$ nazywamy

$$Ec_G = \max\{dist_G(a,b) : b \in V\}$$

Wierzchołek centralny to wierzchołek o ekscentryczności najmniejszej w grafie, **peryferyjny** to taki, który ma ekscentryczność maksysmalną. **Centrum** grafu to zbiór wierzchołków centralnych.

Twierdzenie 56 (Dőnes Kőnig)**.** *Każde drzewo ma centrum złożone z jednego lub dwóch połączonych wierzchołków.*

Dowód - ładny i łatwy. Podczas wykładu nie powiedziałem, że twierdzenie to jako pierwszy udowodnił Dőnes Kőnig[20].

12.3. **Drzewa z korzeniem i drzewa binarne. Korzeń drzewa** T - dowolny, wyróżniony wierzchołek.
Drzewo binarne - drzewo, w którym korzeń jest wierzchołkiem stopnia 2, pozostałe wierzchołki są stopnia 3 lub 1 (liście)
Poziom wierzchołka w drzewie (z korzeniem) - odległość od korzenia.
Wysokość drzewa - maksymalna odległość wierchołka od korzenia.

[20]Węgierski matematyk, który w 1935 roku opublikował właściwie pierwszą monografię z teorii grafów. Ta książka jest bardzo szczególna także dlatego, że zawiera wiele nowych twierdzeń. Stąd większość wyników Kőniga ma datę 1935. Opublikowanie jego monografii spowodowało ogromne zwiększenie zainteresowania teorią grafów. Pewno Kőnig jest w znacznie większym stopniu ojcem teorii grafów niż Euler. Ale po co te rozważania? Czy można być bardziej ojcem czegoś niż kto inny? :)

Przykład 3. *Model funkcjonowania automatu rozpoznającego monety - drzewo binarne o 9 wierzchołkach.*

Twierdzenie 57. *Każde drzewo binarne ma rząd nieparzysty.*

Dow. ...

Twierdzenie 58. *W dowolnym drzewie binarnym T rzędu n jest $p = \frac{n+1}{2}$ liści i $k = \frac{n-3}{2}$ wierzchołków stopnia 3.*

Twierdzenie 59. *Niech T będzie drzewem binarnym o p liściach i wysokości h. Wówczas $h \geq \lceil \log p \rceil$.*

12.4. **Dendryty. Dendrytem** grafu G nazywamy podgraf T tego grafu, który jest drzewem i $|T| = |G|$.

Twierdzenie 60. *Graf G jest spójny wtedy i tylko wtedy gdy ma dendryt.*

ALGORYTM DRZEWO

Grafy z wagami. Problem minimalnego dendrytu. **Algorytmy Kruskala i Prima**[21] znajdowania dendrytu minimalnego.

Podczas wykładu obiecałem, że w tych notatkach podam te algorytmy (jeszcze raz, bo podczas wykładu (chyba?) podałem) i na dodatek napiszę dowody. Przepraszam, ale nie zdąże. Mam inną propozycję. Tę część wykładu realizuję według książki Rossa i Wrighta [6]. Jeśli jesteście ciekawi **(mam nadzieję**, że jesteście, **wiem**, że nie wszyscy), zarówno algorytmy jak i dowody ich funkcjonowania na stronach 382-291 tej książki. Tam też algorytm DRZEWO.

[21]Zaniepokoiło mnie, że nie wiedziałem podczas wykładu kim był Prim i w związku z tym, jak należy czytać jego nazwisko. Już wiem! To amerykański matematyk (Princeton), Robert Clay Prim (1921 -) - chyba żyjący, bo Wikipedia podaje tylko datę urodzenia. A więc czytamy to nazwisko po angielsku. Dowiedziałem się także innych, ciekawych rzeczy (w [3] - to naprawdę świetna książka!). Otóż znacznie przed Kruskalem i Primem blisko podania algorytmów znajdowanie dendrytów optymalnych byli czeski matematyk Otakar Borůvka (1899-1995, nad u jest kółko, nie kropka, ale nie umiem) oraz Jan Czekanowski (1882-1965). W tym drugim przypadku najciekawsze jest nie to, że Czekanowski byl Polakiem (innym też to się zdaża), lecz fakt, że to antropolog (choć matematykę też studiował - ciekawe informacje o nim w Wikipedii).

13. Wykład 13 - 9.VI.2010

13.1. **Kolorowanie wierzchołków grafu**
Liczba chromatyczna. Kolorowaniem wierzchołków grafu (prostego[22]) $G = (V; E)$ nazywamy dowolną funkcję

$$c : E \to C$$

gdzie C jest skończonym zbiorem, nazywanym **zbiorem kolorów**.
Kolorowanie jest **właściwe** jeśli spełnia warunek $xy \in E \Rightarrow c(x) \neq c(y)$.
Liczba chromatyczna grafu G:

$$\chi(G) = \min\{k : \exists c : E \to [1, k], c \text{ - kolorowanie właściwe grafu } G\}$$

Przykład 4. $\chi(C_{2k}) = 2, \quad \chi(C_{2k+1}) = 3, \quad \chi(K_n) = n$

Problem i twierdzenie o 4-kolorowalności grafów planarnych (historia **problemu czterech kolorów**).

Przykłady...

Definicja 7. $\kappa(G) = \max\{k : G \textit{ jest } k- \textit{ spójny}\}$
$\Delta(G) = \max\{d_G(v) : v \in V\}$

Twierdzenie 61 (???[23])**.** *Dla dowolnego grafu prostego G prawdziwa jest nierówność $\chi(G) \leq \Delta(G)$.*

Dow. ...

Twierdzenie 62 (Brooks)**.** *Jeśli G jest grafem spójnym i nie jest ani cyklem nieparzystym ani grafem pełnym, to $\chi(G) \leq \Delta(G)$*

Dowód twierdzenia Brooksa nie podałem podczas wykładu.

13.2. **Wielomiany chromatyczne.** Oznaczmy przez d_i liczbę pokolorowań właściwych wierzchołków grafu (prostego) G rzędu n. Wówcza wierzchołki G można pokolorować (w sposób właściwy) $d_i\binom{\lambda}{i}$ kolorami. Stąd oczywiście istnieje

$$P_G(\lambda) = \sum_{i=1}^{n} d_i \binom{\lambda}{i} \tag{7}$$

różnych pokolorowań właściwych wierzchołków grafu G. Zauważmy, że nie istnieje pokolowanie 0 kolorami ani więcej niż n kolorami, stąd rzeczywiście we wzorze (7) sumowanie można rozpocząć od $i = 0$ i zakończyć na $i - n$. $P_G(\lambda)$ zdefiniowane wzorem (7) nazywamy **wielomianem charakterystycznym grafu** G[24]

Przykład.

---

[22]Można mówić o kolorowaniu wierzchołków, a także krawędzi, grafów niekoniecznie prostych, szczególnie ma to sens w przypadku kolorowania krawędzi multigrafów, krawędzi i/lub wierzchołków grafów skierowanych. O tego typu kolorowaniach nie będę jednak mówił w trakcie wykładów.

[23]To twierdzenie jest powszechnie znane, nie wiadomo kto je jako pierwszy udowodnił. W literaturze angielskojęzycznej pisze się w takich przypadkach *folclore*. Może mi ktoś podpowie, jak to można określić po polsku?

[24]We wzorze (7) λ oznacza równocześnie liczbę kolorów i zmienną nieokreśloną wielomianu (zazwyczaj oznaczaną przez x). Ta podwójna rola, którą odgrywa tu λ formalnie jest niezupełnoie poprawna, nie prowadzi jednak do nieporozumień.

Twierdzenie 63. $P_{K_n}(\lambda) = \lambda(\lambda-1)\cdot ...\cdot(\lambda-n+1)$

Dow. ...

Twierdzenie 64. $P_{P_n}(\lambda) = \lambda(\lambda-1)^{n-1}$

Niech a i b będą dwoma wierzchołkami nie połączonymi w grafie G. Przez G' oznaczmy graf powstały z G przez połączenie wierzchołków a i b krawędzią, zaś przez G'' graf powstały przez zastąpienie w G wierzchołków a i b jednym wierzchołkiem c połączonym z wszystkimi wierzchołkami połączonymi w G z a lub z b.

Twierdzenie 65 (Whitney)**.**

$$P_G(\lambda) = P_{G'}(\lambda) + P_{G''}(\lambda)$$

Dow. ...
Przykład...
Zauważyliśmy, że twierdzenie Whitneya daje metodę (co prawda kompletnie algorytmicznie nieefektywną) znajdowania wielomianu chromatycznego grafu.

13.3. **Kolorowanie krawędzi. Kolorowaniem krwędzi** grafu prostego $G = (V; E)$ nazywamy dowolną funkcję

$$c : E \to C$$

Kolorowanie krawędzi jest właściwe jeśli krawędzie incydentne są różnych kolorów. Minimalną liczbę kolorów konieczną do pokolorowania właściwego krawędzi grafu G nazywamy **indeksem chromatycznym** i oznaczamy przez $\chi'(G)$.

Twierdzenie 66 (Twierdzenie Vizinga)**.** *Dla dowolnego grafu prostego*

$$\Delta(G) \le \chi'(G) \le \Delta(G) + 1$$

Dowód twierdzenia Vizinga nie był podany podczas wykładu.

13.4. **Grafy skierowne i turnieje.**

Definicja 8. Grafem prostym skierowanym *nazywamy* $G = (V; E)$*, gdzie* $E \subset V \times V - \{(x, x) : x \in V\}$.
Elementy zbioru V *nazywamy* **wierzchołkami** *zaś elementy zbioru* E **łukami** *grafu* G.
Turniejem *nazywamy graf skierowany w którym dowolne dwa wierzchołki połączone są dokładnie jednym łukiem.*

Przykłady.

Definicja 9. Ścieżka o początku w x **i końcu w** y*, to ciąg*

$$(x = a_1, e_1, a_2, e_2, ..., a_{k-1}e_{k-1}, a_k = y)$$

wierzchołków $a_1, ..., a_k$ *i łuków* $e_1, ..., e_{k-1}$ *takich, że* $e_i = (a_i, a_{i+1})$ *dla* $i = 1, ..., k$ *oraz* $a_i \neq a_j$ *dla* $i \neq j$.
Ścieżkę nazywamy **hamiltonowską** *(albo* **Hamiltona***) jeśli zawiera wszystkie wierzchołki grafu.*

Twierdzenie 67 (Rédei)**.** *Każdy turniej zawiera ścieżkę (skierowaną) Hamiltona.*

Dow. ...

14. Wykład 14 - 16.VI.2010

Terminy egzaminów:
I (i oby ostatni): 22 czerwca godz. 9.00 w U2 - pisemny
Dla tych, którzy z pisemnej części egzaminu będą zwolnieni, część ustna w B7, także 22-go od (zapewne) 9.00
szczegóły ogłoszę, gdy będę wiedział dokładnie kto jest zwolniony
II i III termin: 20 o 9.00 i 27 września o 13.30 w B7

Szczerze, trochę egoistycznie, życzę powodzenia!!!

14.1. Turnieje -ciąg dalszy.

Definicja 10. *W dowolnym grafie skierowanym G oznaczamy $d_G^+(v) = |\{u \in V : (v,u) \in E\}|$. i nazywamy* **półstopniem** *wierzchołka v. Jeśli G jest turniejem, wówczas wektor $(a_1 \leq a_2 \leq ... \leq a_n)$ półstopni wierzchołków G nazywamy* **wektorem wyników** *turnieju G..*

Twierdzenie 68 (Landau)**.** *Ciąg niemalejący $(a_1 \leq a_2 \leq ... \leq a_n)$ jest wektorem wyników pewnego turnieju wtedy i tylko wtedy gdy*

$$\sum_{i=1}^{k} a_i \leq \binom{n}{k}$$

dla każdego $k, 1 \leq k \leq n$, przy czym dla $k = n$ zachodzi równość.

Dowodu nie będę podaswał, choć ładny. Jako ciekawostkę mogę jednak podać, że autor twierdzenia, Landau, nie był matematykiem. Nie jest to także znany fizyk o tym nazwisku. Chodzi o biologa. Twierdzenie Landaua bywa cytowane w pracach biologicznych. Sam czytałem kiedyś pracę naukową o zachowaniu makaków (to takie małpy). *Turniejami* w pracy o makakach były walki pomiędzy makakami. Uczony badał, czy jest jakaś relacja pomiędzy wynikami (niegroźnych) walk makaków a częstością wzajemnych pieszczot (polegającymi na wzajemnym pozbawianiu się dokuczliwych insektów).

14.2. Liczba nieizomorficznych turniejów rzędu n.

Twierdzenie 69. *Niech $\sigma \in S_n$ będzie permutacją typu $d = 1^{d_1}2^{d_2}...n^{d_n}$ działającą na zbiorze turniejów rzędu n. Jeśli σ ma cykl*[25] *długości parzystej (czyli jeśli $d_{2k} > 0$ dla pewnego k) $|Fix\ \sigma| = 0$. W przeciwnym przypadku $|Fix\ \sigma| = 2^{t(d)}$, gdzie*

$$t(d) = \frac{1}{2}\left(\sum_{i,j=1}^{n}(i,j)d_i d_j - \sum_{i=1}^{n} d_i\right)$$

Uwaga. (i,j) to, jak pamiętamy, NWD(i,j). W dowodzie są wykorzystywane lemat Burnside'a oraz twierdzenie Cauchyego. Warto więc sobie te twierdzenia przypomnieć.

Dow.
Najpierw wykażemy, że gdy jeden z cykli jest parzysty, wówczas $|Fix\ \sigma| = 0$. Rzeczywiście, przypuśćmy, że istnieje cykl $(a_1, a_2, ..., a_{2i})$. Bez straty ogólności możemy

[25]Oczywiście mowa tu o cyklach permutacji σ w rozkładzie na cykle (permutacje cykliczne) rozłączne. Pamiętamy, że taki rozkład istnieje i jest jednoznaczny.

założyć, że $(a_1, a_{1+\frac{i}{2}}) \in E(T)$. Gdyby $\sigma(T) = T$ wówczas $\sigma(a_1, a_{1+\frac{i}{2}}) \in E(T)$, $\sigma^2(a_1, a_{1+\frac{i}{2}}) \in E(T)$, etc. W szczególności $\sigma^{\frac{i}{2}}(a_1, a_{1+\frac{i}{2}}) \in E(T)$. Tymczasem $\sigma^{\frac{i}{2}}(a_1, a_{1+\frac{i}{2}}) = (a_{1+\frac{i}{2}}, a_1)$, a to jest sprzeczne z założeniem, że T jest turniejem (w turnieju dwa wierzchołki są połączone dokładnie jednym łukiem, a nie dwoma, przeciwnie skierowanymi łukami.

Od tego momentu będziemy zakładali, że wszystkie cykle permutacji σ są nieparzyste (inaczej: $d_2 = d_4 = ... = 0$).
Niech więc będzie cykl (nieparzysty) $(a_1, ..., a_i)$ permutacji σ. Na wierzchołkach tego cyklu można zbudować $2^{\frac{i-1}{2}}$ różnych turniejów T_i (rzędu i) takich, że $\sigma(T_i) = T_i$. Bierze się to stąd, że każdą cięciwę tego cyklu[26] a_1, a_α można nadać jedną z dwóch orientacji (które zostają zachowane po wzięciu na nich wartości permutacji σ i jej kolejnych potęg).
Dla wszystkich cykli długości (nieparzystej!) i otrzymamy $2^{d_i \frac{i-1}{2}}$ turniejów T_i takich, że $\sigma(T_i) = T_i$. A dla wszystkich cykli permutacji łacznie $2^{\sum_{i=1}^{n} d_i \frac{i-1}{2}}$ turniejów na których permutacja σ jest stała.

Teraz zajmijmy się możliwą orientacją łuków pomiędzy cyklami tej samej długości i (liczbę tych cykli w turnieju oznaczyliśmy przez d_i. Możliwości wybnoru łuków pomiędzy cyklami długości jest i, zaś wszystkich par $\binom{d_i}{2}$. Mamy więc $2^{\binom{d_j}{2} i}$ możliwości.

Rozpatrzmy teraz przypadek cykli o różnych długościach i oraz j, powiedzmy $(a_1, ..., a_i)$ i $(b_1, ..., b_j)$. Orbita dowolnego łuku, powiedzmy, dla ustalenia uwagi, (a_1, b_1) ma NWW(i, j) elementów. Ponieważ zaś tych łuków pomiędzy $\{a_1, ..., a_i\}$ a $\{b_1, ..., b_j\}$ jest $i \cdot j$, to łuków o których orientacji możemy rozstrzygać dowolnie jest $\frac{i \cdot j}{\text{NWW}(i,j)}$ =NWD$(i, j) = (i, j)$ (przypominam, że (i, j) to tylko inne oznaczenie dla NWD). Mamy więc $2^{(i,j)}$ możliwości.
Ostatecznie turniejów T spełniających $\sigma(T) = T$ jest $2^{t(d)}$, gdzie

$$t(d) = \sum_{i=1}^{n} \frac{d_i(i-1)}{2} + \sum_{i=1}^{n} \binom{d_i}{2} i + \sum_{1 \le i < j \le n} d_i d_j (i, j)$$

a po przeliczeniach (łatwych) otrzymamy, dla dowolnej permutacji σ typu $2^{d_1} ... n^{d_n}$, $(d = (d_1, ..., d_n)$ i $d_2 = ... = 0)$:

$$t(d) = \frac{1}{2} \left(\sum_{i,j} d_i d_j (i, j) - \sum_{i=1}^{n} d_i \right)$$

Twierdzenie 70 (Davis)**.** *Liczba nieizomorficznych turniejów $T(n)$ rzędu n dana jest wzorem*

$$T(n) = \sum_{d}^{*} \frac{2^{t(d)}}{\prod i^{d_i} d_i!}$$

(gdzie $t(d)$ jest określone w twierdzeniu poprzednim, zaś $\sum_d^*$ oznacza sumę po wszystkich d spełniających $d_1 + 3d_3 + 3d_+ ... + nd_n = n$ oraz $d_{2l} = 0$ dla każdego l).

[26] Tu dalej mamy do czynienia z cyklem permutacji $(a_1, ..., a_i)$, co nie przeszkadza nam jednak traktować $\{a_1, ..., a_i\}$ jako wierzchołków turniejów i budować na nich cyklu z cięciwami!

Dowód. W dowodzie wykorzystamy

- lemat Burnside'a
- twierdzenie Cauchy'ego o tym, że wszystkich permutacji typu $d = 1^{d_1}2^{d_2}...n^{d_n}$ jest

$$\frac{n!}{1^{d_1}d_1!2^{d_2}d_2!...n^{d_n}d_n!}$$

Rzeczywiście, wykorzystując twierdzenie 69, lemat Burnside'a i twierdzenie Cauchy'ego (twierdzenie 13) otrzymujemy:

$$T(n) = \frac{1}{n!}\sum_{\sigma\in S_n}|\text{Fix }\sigma| = \sum_{d}^{*}\frac{n!}{1^{d_1}d_1!...n^{d_n}d_n!}2^{t(d)} = \sum_{d}^{*}\frac{2^{t(d)}}{\prod_i i^{d_i}d_i!}$$

Literatura

[1] M. Aigner i G.M. Ziegler, Dowody z Księgi, PWN, Warszawa 2002.
[2] W.J Gilbert, W.K. Nicholson, Algebra współczesna z zastosowaniami, WNT, Warszawa 2008.
[3] R.P. Grimaldi, Discrete and Combinatorial Mathematics - An Appiled Introduction, Addison-Wesley 1994.
[4] N. Koblitz, Algebraiczne aspekty kryptografii, WNT, Warszawa 2000
[5] Zb. Palka i A. Ruciński, Wykłady z kombinatoryki, WNT 2004.
[6] K.A Ross i Ch.R.B. Wright, Matematyka dyskretna, PWN 2000.
[7] E.R. Scheinerman, Mathematics - Discrete Introduction, Brooks/Cole 2000.
[8] R.J. Wilson, Wprowadzenie do teorii grafów, PWN 1998.