Zmodyfikowane wielomiany i twierdzenie Erdősa

Czesław BAGIŃSKI[*], *Edmund R. PUCZYŁOWSKI*[**]

[*]Wydział Informatyki, Politechnika Białostocka

[**]Instytut Matematyki, Uniwersytet Warszawski

Nierzadko zdarza się, że elementarnie brzmiące twierdzenie matematyczne ma skomplikowany dowód wymagający rozważenia pewnej liczby szczególnych przypadków. I chociaż samo twierdzenie może być piękne i mieć wiele walorów, uciążliwy nudny dowód to piękno może zamazywać. Na szczęście, czasami całą skomplikowaną kombinatorykę można wyeliminować zręcznie dobraną algebraiczną konstrukcją. W niniejszej notce chcielibyśmy to zademonstrować na przykładzie dowodu następującego twierdzenia Erdősa.

Jeżeli p jest liczbą pierwszą, to z dowolnego zbioru $2p-1$ liczb całkowitych można wybrać p liczb, których suma jest podzielna przez p.

W dowodzie wykorzystamy pewne zmodyfikowane wielomiany dwóch zmiennych, które teraz opiszemy. Na początek, przez $\mathbb{Z}_p$ oznaczmy zbiór liczb $0, 1, \ldots, p-1$ i wprowadźmy w nim operacje dodawania i mnożenia:

$$a \oplus b = \text{ reszta z dzielenia } a+b \text{ przez } p,$$

$$a \odot b = \text{ reszta z dzielenia } a \cdot b \text{ przez } p.$$

Własności tak określonych działań są podobne do własności zwykłych działań dodawania i mnożenia liczb (są one np. przemienne i łączne). W jakimś sensie są one nawet prostsze. Na przykład, niejednego ucznia może ucieszyć to, że dla dowolnych $a, b \in \mathbb{Z}_p$, $(a \oplus b)^p = a^p \oplus b^p$. Odnotujmy też, że w $\mathbb{Z}_p$ zachodzi $1 \oplus (p-1) = 0$. W efekcie $p-1$ oznaczamy przez -1.

Przez G oznaczymy zbiór wszystkich jednomianów dwóch zmiennych x i y, których stopień ze względu na każdą ze zmiennych nie przekracza $p-1$, tzn. $G = \{x^i y^j : \ 0 \leqslant i, j \leqslant p-1\}$. W zbiorze tym wprowadzamy zwykłą operację mnożenia jednomianów, ale w trosce o to, by iloczyn dwóch dowolnych elementów z G należał do G, wykładniki redukujemy modulo p. Innymi słowy przyjmujemy, że $x^p = 1 = y^p$. Oczywiście przyjmujemy także $x^0 = y^0 = 1$. Nietrudno zauważyć, że dla dowolnego $g \in G$, jeśli $g \neq 1$, to $g^n = 1$ wtedy i tylko wtedy, gdy p dzieli n.

Teraz przez $\mathbb{Z}_p[G]$ oznaczymy zbiór wszystkich wielomianów zmiennych x i y, o współczynnikach należących do $\mathbb{Z}_p$, których stopnie ze względu na każdą ze zmiennych nie przekraczają $p-1$:

$$\mathbb{Z}_p[G] = \{\sum_{i,j=0}^{p-1} a_{ij} x^i y^j : a_{ij} \in \mathbb{Z}_p\}.$$

Takie wielomiany możemy dodawać i mnożyć, tak jak dodaje się i mnoży zwykłe wielomiany liczbowe, tyle, że wprowadzamy dodatkową regułę, że jeśli w wyniku mnożenia pojawią się jednomiany $x^k y^l$, gdzie wykładniki k lub l są większe od $p-1$, to najpierw takie wykładniki redukujemy modulo p, a następnie w otrzymanym wielomianie redukujemy wyrazy podobne. Ponadto współczynniki wielomianów mnożymy i dodajemy według reguł działań w $\mathbb{Z}_p$.

Działania określone w $\mathbb{Z}_p[G]$ mają własności podobne do podstawowych własności działań na wielomianach o współczynnikach liczbowych. Tutaj jednak iloczyn dwóch niezerowych wielomianów może być równy zero.

W zbiorze $\mathbb{Z}_p[G]$ rozważmy zbiór $\omega(G)$ wszystkich wielomianów postaci $\sum\limits_{i,j=0}^{p-1} a_{ij}(x^i y^j - 1)$. Zauważmy, że

$$\begin{aligned} &x^k y^l - 1 = (x^k - 1)y^l + y^l - 1 = \\ &= (x-1)(1 + x + x^2 + \ldots + x^{k-1})y^l + (y-1)(1 + y + y^2 + \ldots + y^{l-1}) = \\ &= (x-1)\alpha + (y-1)\beta \end{aligned}$$

dla odpowiednich $\alpha, \beta \in \mathbb{Z}_p[G]$. Wynika stąd, że jeśli $\alpha_1, \ldots, \alpha_n \in \omega(G)$, to $\alpha_1 \cdot \ldots \cdot \alpha_n$ jest sumą elementów postaci $(x-1)^m (y-1)^r c$, gdzie m, r są liczbami całkowitymi nieujemnymi takimi, że $m + r = n$ oraz $c \in \mathbb{Z}_p[G]$. Zauważmy także,

Rozwiązanie zadania F 724.
Pocisk wzniesie się na wysokość

$$H = \frac{u^2}{2g},$$

gdzie u to prędkość pocisku po przebiciu kuli. Z prawa zachowania pędu mamy, że

$$mu = mv - MV = mv - M\sqrt{2gh},$$

zatem

$$u = v - \frac{M}{m}\sqrt{2gh}.$$

Stąd otrzymujemy, że:

$$H = \frac{(v - \frac{M}{m}\sqrt{2gh})^2}{2g}.$$

Rozwiązanie zadania M 1218.
Odpowiedź: Takie ponumerowanie nie istnieje.

Załóżmy, że kolejne wierzchołki 20-kąta foremnego są ponumerowane liczbami $a_1, a_2, \ldots, a_{20}$. Wtedy

$$(*) \quad \begin{aligned} a_1 + a_2 + a_3 + a_4 &\leqslant 42 \\ a_2 + a_3 + a_4 + a_5 &\leqslant 42 \\ &\ldots \\ a_{20} + a_1 + a_2 + a_3 &\leqslant 42 \end{aligned}$$

Dodając nierówności $(*)$ stronami, uzyskujemy zależność

$$4 \cdot (a_1 + a_2 + \ldots + a_{20}) \leqslant 20 \cdot 42,$$

która z kolei jest równoważna nierówności

$$4 \cdot (1 + 2 + \ldots + 20) \leqslant 20 \cdot 42,$$

czyli $840 \leqslant 840$.

Wobec tego aby rozpatrywane ponumerowanie istniało, w nierównościach $(*)$ muszą zachodzić równości. Stąd w szczególności uzyskujemy

$$a_1 + a_2 + a_3 + a_4 = a_2 + a_3 + a_4 + a_5,$$

czyli $a_1 = a_5$. Otrzymaliśmy sprzeczność, gdyż wszystkie liczby $a_1, a_2, \ldots, a_{20}$ są różne.

że $(x-1)^p = x^p - 1^p = 0 = (y-1)^p$, a zatem jeśli $m \geqslant p$, to $(x-1)^m = (y-1)^m = 0$. Jeśli teraz $\alpha_1, \ldots, \alpha_{2p-1} \in \omega(G)$, to

$$\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{2p-1} = 0.$$

Rzeczywiście, po uwzględnieniu postaci czynników i ich wymnożeniu, iloczyn po lewej stronie tej równości stanie się sumą elementów postaci $(x-1)^m(y-1)^r c$, gdzie $m + r = 2p - 1$. Zatem albo $m \geqslant p$, albo $r \geqslant p$, co oznacza, że każdy składnik tej sumy jest równy zero.

Wyposażeni w tę wiedzę możemy przystąpić do dowodu twierdzenia Erdősa. Załóżmy więc, że $n_1, n_2, \ldots, n_{2p-1}$ są danymi liczbami całkowitymi. Możemy je zastąpić ich resztami modulo p i założyć, że są one nieujemne i nie przekraczają $p-1$. Niech

$$g_1 = x^{n_1}y,\ g_2 = x^{n_2}y,\ \ldots\ , g_{2p-1} = x^{n_{2p-1}}y.$$

Oczywiście $g_1 - 1, g_2 - 1, \ldots, g_{2p-1} - 1 \in \omega(G)$.

Zatem $(g_1 - 1)(g_2 - 1) \cdot \ldots \cdot (g_{2p-1} - 1) = 0$. Rozwijając lewą stronę tej równości, otrzymamy wielomian, który jest sumą -1 oraz jednomianów postaci $\pm g_{i_1} \ldots g_{i_k}$, gdzie k nie przekracza $2p-1$. Zauważmy, że w skład wyrazu wolnego tego wielomianu wchodzą oprócz -1 jednomiany, dla których $g_{i_1} g_{i_2} \cdot \ldots \cdot g_{i_k} = 1$. Ponieważ jest on równy 0, więc dla pewnego k oraz $i_1, i_2, \ldots, i_k$ takich, że $1 \leqslant k, i_1, i_2, \ldots, i_k \leqslant 2p-1$, mamy $g_{i_1} g_{i_2} \cdot \ldots \cdot g_{i_k} = 1$. To zaś oznacza, że $x^{n_{i_1} + n_{i_2} + \ldots + n_{i_k}} y^k = 1$. W efekcie $x^{n_{i_1} + n_{i_2} + \ldots + n_{i_k}} = 1$ oraz $y^k = 1$. Z tych równości wynika, że k oraz $n_{i_1} + n_{i_2} + \ldots + n_{i_k}$ są podzielne przez p. Ponieważ jednak $1 \leqslant k \leqslant 2p-1$, więc $k = p$. Zatem suma, $n_{i_1} + n_{i_2} + \ldots + n_{i_p}$, p spośród liczb $n_1, n_2, \ldots, n_{2p-1}$ jest podzielna przez p i dowód został zakończony.

Rozwiązania zadań lingwistycznych

1. umi-kumama-hiku, lua iako me ka iwa, hiku iako me ka ono, mano me ka lua lau me ka iako me ka lima.

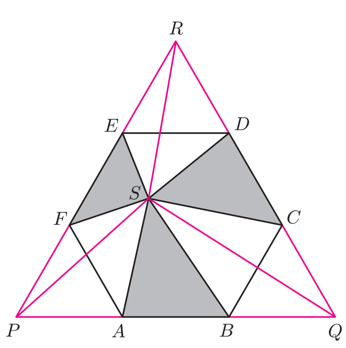
2. Z analizy przykładów można dojść do tego, że język ten posługuje się systemem dwudziestkowym (inne możliwe bazy – widać, że w grę wchodzą tylko dzielniki sześćdziesiątki – łatwo wykluczyć). Liczebniki „n-naście" z zadania są tworzone jako 10(„la")$+n$. Dwudziestki („kal") z rzędem jedności łączy wyraz *yete*. Zatem: 43=ka kal yete oš, 72=oš kal yete la ka, 100=ho kal, 139=uak kal yete la bolon, 355=la uuk kal yete la ho, 360=la uašak kal.

3. Mansyjskie nazwy liczebników tworzone są w następujący sposób:

5	at	50	atlow
6	xõt	60	xõtlow
8	ńollow	80	ńolsāt
9	ontəllow	90	ontəlsāt
$10+\alpha$	α-xujplow	100α	α-sāt
$10(\beta-1)+\alpha$	(10β) nopəl α	$100(\beta-1)+\alpha$	(100β)-n α
$90+\alpha$	90α	$900+\alpha$	900α

a) 405, 76, 819; b) xõtlow nopəl ńollow, ńolsāt, ńollowsātn xõtxujplow.

4. Nazewnictwo liczebników bazuje na systemie dwudziestkowym (ogun $X = 20 \cdot X$). Rzędy wymieniane są w kolejności rosnącej (jedności, dziesiątki/dwudziestki). Liczby postaci $10(2n+1)$ wyraża się jako ẹwa din ogun $(n+1)$. Do/od pełnych dziesiątek dodaje się (*l-*) jedności do 4 lub odejmuje (*din*) od 1 do 5. Zatem: a) 144, 45; b) ọkan, eje, eji l-ẹwa din ogun ẹta, ọkan din ogun arun.



Rozwiązanie zadania M 1217.

Niech a będzie długością boku sześciokąta $ABCDEF$. Wówczas $[ABCDEF] = \frac{3}{2}a^2\sqrt{3}$, gdzie $[\mathcal{F}]$ oznacza pole figury $\mathcal{F}$.

Niech P będzie punktem przecięcia prostych EF i AB, Q punktem przecięcia prostych AB i CD, a R punktem przecięcia prostych CD i EF. Każdy z trójkątów PFA, QBC, RDE jest równoboczny o boku długości a. Wobec tego trójkąty SAB, SPA i SBQ mają równe pola – każdy z nich ma podstawę długości a i jednakową wysokość opuszczoną na tę podstawę. Zatem $[ABS] = \frac{1}{3}[PQS]$. Analogicznie uzyskujemy równości

$$[CDS] = \frac{1}{3}[QRS] \quad \text{oraz} \quad [EFS] = \frac{1}{3}[RPS].$$

Ponieważ trójkąt PQR jest równoboczny o boku $3a$, więc na mocy otrzymanych zależności uzyskujemy

$$[ABS] + [CDS] + [EFS] = \frac{1}{3}([PQS] + [QRS] + [RPS]) = \frac{1}{3}[PQR] = \frac{1}{3} \cdot \frac{(3a)^2\sqrt{3}}{4} = \frac{1}{2}[ABCDEF].$$