Czego dowiedzieliśmy się o rozważanej grze? Po pierwsze, przy odpowiedniej dysproporcji liczby dywizji, którymi dysponują gracze, istnieją równowagi Nasha w strategiach czystych, w których jeden z graczy ma zagwarantowaną wygraną. Po drugie, w sytuacji, gdy $A \leqslant D < A \cdot n$, nie istnieją równowagi Nasha w strategiach czystych, a żaden z graczy nie jest w stanie zagwarantować swojej wygranej z prawdopodobieństwem 1. W takich scenariuszach dla każdej przełęczy obrońca powinien z dodatnim prawdopodobieństwem przypisywać A dywizji, aby atakujący nie miał w odpowiedzi strategii, przy której na pewno wygra. Okazuje się zatem, że w każdej sytuacji, gdy atakujący nie może zagwarantować swojej wygranej, obrońcy opłaca się bronić na wszystkich frontach równocześnie.

Pseudopierwsze zoo

*Mikołaj ROTKIEWICZ**

* Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

O liczbach pseudopierwszych pisaliśmy w Δ^3_{22}. Przypomnijmy, że liczba pseudopierwsza (Fermata, przy podstawie a) to liczba złożona n, która „udaje" liczbę pierwszą w tym sensie, że spełnia podzielność $n|a^n - a$. O takim kamuflażu można mówić na wiele różnych sposobów.

Weźmy na warsztat (w miejsce ciągu geometrycznego (a^n)) ciąg $V_n = \alpha^n + \beta^n$, gdzie α, β są pierwiastkami, być może zespolonymi, trójmianu kwadratowego $f(X) = X^2 - aX + b$, natomiast a, b są liczbami całkowitymi. Początkowe wyrazy tego ciągu można szybko obliczyć, stosując rekurencję: $V_0 = 2$, $V_1 = a$, $V_{n+1} = aV_n - bV_{n-1}$ dla $n \geqslant 1$. Stąd widać również, że (V_n) jest ciągiem liczb całkowitych. Małe twierdzenie Fermata ma następujące uogólnienie:

Przedstawiony wzór rekurencyjny dla ciągu (V_n) wynika ze zsumowania następujących dwóch równości, prawdziwych na mocy definicji liczb α, β;
$$\alpha^{n+2} = a\alpha^{n+1} - b\alpha^n,$$
$$\beta^{n+2} = a\beta^{n+1} - b\beta^n.$$

Lemat 1. *Jeśli p jest liczbą pierwszą, to $V_p \equiv V_1 \pmod p$.*

Dowód. Niech $p > 2$. Zastosujemy wzory na pierwiastki równania kwadratowego. Mamy $V_p = \left(\frac{a+\sqrt{\Delta}}{2}\right)^p + \left(\frac{a-\sqrt{\Delta}}{2}\right)^p$, gdzie $\Delta = a^2 - 4b$. Po rozwinięciu część wyrazów sumy zredukuje się i otrzymamy

$$V_p = 2^{-p+1}\left(a^p + \sum_{j=1}^{(p-1)/2} \binom{p}{2j} a^{p-2j}\Delta^j\right).$$

W powyższej sumie $a^p \equiv a \pmod p$, a pozostałe składniki sumy są całkowite i podzielne przez p, gdyż $p \mid \binom{p}{2j}$. Ponadto $2^{p-1} \equiv 1 \pmod p$ i dlatego

$$V_p \equiv 2^{p-1}V_p \equiv a + 0 = V_1 \pmod p.$$

Przypadek $p = 2$ pozostawiamy Czytelnikowi. □

Lemat 1 prowadzi do pierwszego egzemplarza w naszym zoo. Liczbę złożoną n nazywa się *pseudopierwszą Dicksona*, jeśli

(D) $$V_n \equiv V_1 \pmod n$$

i $\mathrm{NWD}(n, 2b\Delta) = 1$. Warunek na NWD jest po to, by pominąć trywialne rozwiązania kongruencji (D). Okazuje się, że sprawdzenie warunku (D) można wykonać niemalże tak szybko jak sprawdzenie, czy $a^n \equiv a \pmod n$ (patrz ćwiczenie 1).

Obliczenia wartości $(a^n \mod n)$ można dokonać w czasie $O(\log n)$ – jak? Odpowiedź w dalszej części artykułu.

W poprzednim artykule wspominaliśmy o *liczbach Carmichaela*, które spełniają $a^n \equiv a \pmod n$ dla dowolnej liczby naturalnej a. Powstaje naturalne pytanie, czy istnieją liczby, które są liczbami pseudopierwszymi Dicksona dla dowolnych liczb całkowitych a, b? Odpowiedź jest twierdząca, najmniejszą z nich jest

$$n = 443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331.$$

W dalszej części artykułu przyjrzymy się własnościom ciągu (A_n), który zdefiniowany jest przez analogiczną rekurencję, lecz tym razem jest ona rzędu 3:

(1) $$A_0 = 3, \quad A_1 = 0, \quad A_2 = 2, \quad A_{n+1} = A_{n-1} + A_{n-2} \text{ dla } n \geqslant 2.$$

Lemat 2 ([L]). *Jeśli p jest liczbą pierwszą, to p dzieli A_p.*

Dowód. Z ogólnej teorii ciągów rekurencyjnych wnosimy, że $A_n = a\alpha^n + b\beta^n + c\gamma^n$, gdzie α, β, γ są rozwiązaniami (zespolonymi) równania $X^3 = X + 1$, natomiast a, b, c są pewnymi stałymi. Dociekliwy Czytelnik łatwo sprawdzi, że warunek początkowy podany w (1) wymusza $a = b = c = 1$, stąd $A_n = \alpha^n + \beta^n + \gamma^n$. Ze wzorów Viete'a mamy $\alpha + \beta + \gamma = 0$, więc

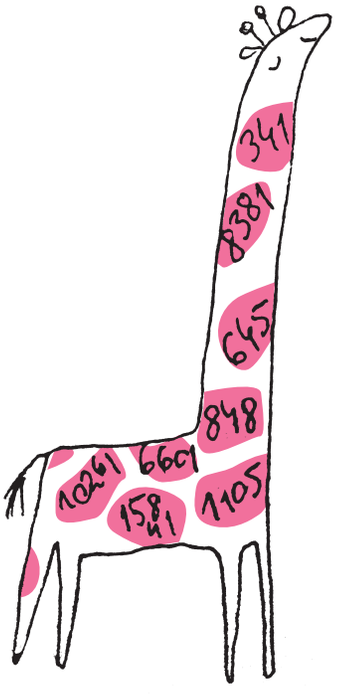
$$(2)\quad A_p = \alpha^p + \beta^p + \gamma^p - (\alpha+\beta+\gamma)^p = -\sum_{\substack{k_1+k_2+k_3=p \\ 0\leqslant k_1,k_2,k_3<p}} \frac{p!}{k_1!k_2!k_3!}\alpha^{k_1}\beta^{k_2}\gamma^{k_3} = p\cdot\Theta_p.$$

Zauważmy, że w powyższej sumie $\dfrac{p!}{k_1!k_2!k_3!}$ jest liczbą całkowitą podzielną przez p, więc Θ_p jest całkowitoliczbową kombinacją liczb postaci $\alpha^{k_1}\beta^{k_2}\gamma^{k_3}$. Dla dokończenia dowodu posłużymy się uogólnieniem pojęcia liczby całkowitej:

Definicja. Liczbę zespoloną θ nazywamy *algebraiczną*, jeśli θ jest pierwiastkiem pewnego wielomianu o współczynnikach całkowitych: $c_d\theta^d + c_{d-1}\theta^{d-1} + \ldots + c_1\theta + c_0 = 0$, gdzie $c_d \neq 0$. Jeśli dodatkowo założymy, że $c_d = 1$, to θ nazywamy liczbą *algebraiczną całkowitą*.

Dla przykładu: $\sqrt{2}$ oraz $\dfrac{1+\sqrt{5}}{2}$ są liczbami algebraicznymi całkowitymi, ale $\sqrt{2}/2$ już nie (ćwiczenie 2).

Niech $\mathbb{A}$ oznacza zbiór liczb algebraicznych całkowitych. Okazuje się, że działania dodawania i mnożenia liczb z $\mathbb{A}$ nie wyprowadzają poza $\mathbb{A}$. (Dowód tego ważnego twierdzenia Czytelnik łatwo znajdzie w [BB-S, M]). Ponieważ (A_n) jest z definicji ciągiem liczb całkowitych, więc liczba $\Theta_p = A_p/p$ jest wymierna. Z drugiej strony, $\alpha, \beta, \gamma \in \mathbb{A}$, więc również $\Theta_p \in \mathbb{A}$. Twierdzenie o pierwiastkach wymiernych wielomianów o współczynnikach całkowitych można zapisać krótko: $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$, tj. każda wymierna liczba algebraiczna całkowita jest całkowita. To oznacza, że $\Theta_p \in \mathbb{Z}$, więc $p \mid A_p$. □



W krótkiej notce [P] Raoul Perrin postawił pytanie o istnienie liczby złożonej n takiej, że $n|A_n$. Takie liczby nazywamy współcześnie *liczbami pseudopierwszymi Perrina* (lub po prostu *liczbami Perrina*).

Przez ponad 80 lat od postawienia problemu w [P] i kilku prób jego rozwiązania, nie była znana żadna liczba Perrina. Odkryto ją w sposób bardzo naturalny, niemalże na kartce papieru z ołówkiem w ręku [A-S]. Jak? Otóż zamieniając α, β, γ w (2) na $\alpha^m, \beta^m, \gamma^m \in \mathbb{A}$, dostajemy szybko

$$(3)\qquad A_{mp} \equiv A_m \pmod{p}$$

dla każdej liczby naturalnej m. Zatem $A_{p^2} \equiv A_p \equiv 0 \pmod{p}$. Podzielność A_{p^2} przez p to tylko „połowa sukcesu" – ale sugeruje, że może warto ograniczyć poszukiwania liczb pseudopierwszych Perrina do kwadratów liczb pierwszych. Ta heurystyka okazała się słuszna – liczbą pseudopierwszą Perrina (jak się okazuje, najmniejszą!) jest $n = 521^2 = 271441$.

Jak trudne jest sprawdzenie warunku $n \mid A_n$? Obliczenie reszt z dzielenia kolejnych wyrazów ciągu A_k przez n dla $1 \leqslant k \leqslant n$ byłoby bardzo kosztowne, bo wymaga aż $O(n)$ kroków. Lepiej posłużyć się rachunkiem macierzowym: dla macierzy

$$M = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \text{ mamy } M\begin{bmatrix} A_n \\ A_{n+1} \\ A_{n+2} \end{bmatrix} = \begin{bmatrix} A_{n+1} \\ A_{n+2} \\ A_{n+3} \end{bmatrix}, \text{ skąd } M^{n-2}\begin{bmatrix} A_0 \\ A_1 \\ A_2 \end{bmatrix} = \begin{bmatrix} A_{n-2} \\ A_{n-1} \\ A_n \end{bmatrix}.$$

Obliczenie $M^n \bmod n$ można wykonać w $O(\log_2 n)$ krokach, stosując rekurencyjnie równości $M^k = (M^{k/2})^2$ dla parzystych $k \leqslant n$ i $M^k = M \cdot (M^{\frac{k-1}{2}})^2$ w przypadku, gdy k jest liczbą nieparzystą. Każdy z kroków polega na obliczeniu iloczynu macierzy 3×3 modulo N, więc całkowity koszt obliczenia M^n wynosi $O((\log_2 N)^2 \log_2 n)$ operacji bitowych. Inny sprytny algorytm wyznaczenia A_n podajemy w ćwiczeniu 5.

Można dowieść, że $A_{p^2} \equiv A_p \pmod{p^2}$, więc dla dowodu, że 271441 jest liczbą Perrina, wystarczy sprawdzić, że $521^2 \mid A_{521}$, co przy zastosowaniu podanego algorytmu zrobimy, wykonując 10 operacji mnożenia modulo 521^2 macierzy 3×3.

Ciąg (A_n) ma kilka innych ciekawych własności teorioliczbowych, z pomocą których możemy zbudować silniejszy test pierwszości. Rekurencję (1) można

odwrócić: $A_{n-1} = -A_n + A_{n+2}$, skąd

$$(A_0, A_{-1}, A_{-2}, \ldots) = (3, -1, 1, 2, -3, 4, -2, -1, \ldots).$$

Dowód następującego lematu jest analogiczny do dowodu lematu 2 i pozostawiamy go jako ćwiczenie.

Lemat 3. *Jeśli p jest liczbą pierwszą, to $A_{-p} \equiv -1 \pmod p$.*

Liczbę złożoną n nazywamy *silną liczbą Perrina*, jeśli $n \mid A_n$ oraz $n \mid 1 + A_{-n}$. Liczba 521^2 nie spełnia ostatniej podzielności, więc nie jest silną liczbą Perrina. Z kolei $A_{-p^2} \equiv -1 \pmod{p^2}$ już dla $p = 7$, 11 i 29 (por. ćwiczenie 3). Czy silne liczby Perrina w ogóle istnieją? Tak, a ich poszukiwania ułatwia następująca klasyfikacja liczb pierwszych.

Popatrzmy na możliwe rozkłady wielomianu $H(X) = X^3 - X - 1$, czyli wielomianu charakterystycznego rekurencji (1), nad ciałem $\mathbb{F}_p$ – ciałem reszt z dzielenia przez liczbę pierwszą p (informacje w pigułce o ciałach $\mathbb{F}_p$ znajdują się na marginesie). Na przykład $X^3 - X - 1 \equiv (X-2)(X^2+2X+3) \pmod 5$, gdzie zapis $P_1(X) \equiv P_2(X) \pmod m$ oznacza, że wielomian $P_1(X) - P_2(X)$ ma wszystkie współczynniki podzielne przez liczbę naturalną m. Ponieważ wielomian stopnia 3 ma co najwyżej trzy pierwiastki, możliwe są 4 przypadki:

(i) $H(X) \equiv (X-a)(X-b)(X-c) \pmod p$ dla pewnych trzech różnych reszt $a, b, c \in \mathbb{Z}$.
(ii) Wielomian H nie ma pierwiastków w ciele $\mathbb{F}_p$, tj. $p \nmid H(a)$ dla wszystkich $a \in \mathbb{Z}$. Wówczas H jest wielomianem nierozkładalnym nad ciałem $\mathbb{F}_p$.
(iii) $H(X) \equiv (X-a)Q(X) \pmod p$ dla pewnego $a \in \mathbb{Z}$ i wielomianu Q nierozkładalnego nad ciałem $\mathbb{F}_p$.
(iv) $H(X) \equiv (X-a)^2(X-b) \pmod p$ dla pewnych $a, b \in \mathbb{Z}$.

W przypadkach (i), (ii) i (iii) mówimy, że liczba pierwsza p jest typu **S**, **I** i **Q**, odpowiednio. Przypadek (iv) ma miejsce tylko dla $p = 23$ (co ma związek z tym, że -23 jest *wyróżnikiem* wielomianu $H(X)$). Przykłady liczb pierwszych zadanych typów podajemy w ćwiczeniu 7.

O zbiorze F mówimy, że jest ciałem, jeśli jego elementy można dodawać, odejmować, mnożyć i dzielić (z wyjątkiem dzielenia przez 0, które jest jedynym elementem o własności $0 + x = x$ dla każdego $x \in F$). Więcej o ciałach można przeczytać w Δ^{10}_{17}. Zbiór $\mathbb{F}_p$ powstaje na drodze redukcji (abstrakcji) modulo p, tzn. liczby całkowite x, x' uznajemy za *równoważne*, jeśli $x \equiv x' \pmod p$. Redukcja ta jest możliwa, gdyż jeśli $x \equiv x' \pmod p$ oraz $y \equiv y' \pmod p$, to $x + x' \equiv y + y' \pmod p$ oraz $xx' \equiv yy' \pmod p$. Elementy zbioru $\mathbb{F}_p$ można dzielić, więc $\mathbb{F}_p$ jest ciałem: chcąc podzielić $x \bmod p$ przez $y \bmod p$, gdzie $p \nmid y$, szukamy takiego z, że $x \equiv yz \pmod p$.

Ciąg $(A_n \bmod m)_{n=-\infty}^{\infty}$ jest okresowy, ponieważ jest tylko skończenie wiele możliwości na $(A_{n-1}, A_n, A_{n+1}) \bmod m$ dla każdej ustalonej liczby naturalnej m, a każda taka trójka wyznacza ten ciąg jednoznacznie, w przód i tył. Oznaczmy przez ω_m okres podstawowy ciągu $(A_n \bmod m)$. Poniższy lemat pozostawiamy bez dowodu.

Lemat 4 ([A-S]). *Jeśli liczba pierwsza p jest typu* **S**, *to $\omega_p | p-1$, jeśli jest typu* **Q**, *to $\omega_p | p^2 - 1$, jeśli zaś typu* **I**, *to $\omega_p | p^2 + p + 1$.*

Przypomnijmy, liczba złożona n jest liczbą Carmichaela, jeśli dla każdej liczby całkowitej a zachodzi podzielność $n \mid a^n - a$. Zdarza się, że liczba jest jednocześnie liczbą Carmichaela i silną liczbą Perrina, i nie jest to takie dziwne. Przypuśćmy, że liczba Carmichaela $C = \prod_{i=1}^{k} p_i$ jest iloczynem różnych liczb pierwszych typu **S**. Na mocy Lematu 4, $\omega_{p_i} \mid p_i - 1$, zaś z kryterium Korselta (patrz np. Δ^3_{22}), $p_i - 1 \mid C - 1$. Zatem $C \equiv 1 \pmod{\omega_{p_i}}$, więc $A_C \equiv A_1 = 0 \pmod{p_i}$ i podobnie $A_{-C} \equiv A_{-1} = -1 \pmod{p_i}$, więc C jest silną liczbą Perrina. Najmniejszą z takich liczb jest

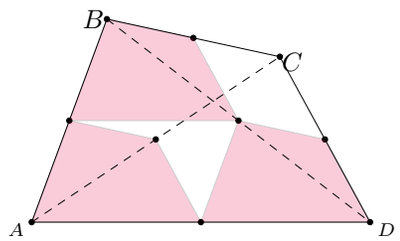
$$7045248121 = 821 \cdot 1231 \cdot 6971.$$

Szczególna postać dzielników pierwszych tej liczby pozwala szybko uzasadnić, że jest ona liczbą Carmichaela. Przyjrzyjmy się teraz liczbie

$$n = 24306384961 = 19 \cdot 53 \cdot 79 \cdot 89 \cdot 3433.$$

To również jest liczba Carmichaela, dość osobliwa, bowiem nie wszystkie dzielniki pierwsze liczby n są typu **S**. Liczby pierwsze $q_1 = 19$, $q_2 = 53$, $q_3 = 79$ i $q_4 = 89$ są typu **Q**, zaś $q_5 = 3433$ jest typu **S**. Liczby te są tak dobrane, że $n \equiv 1 \pmod{q_i^2 - 1}$ dla każdego $1 \leqslant i \leqslant 4$ (a nie tylko $n \equiv 1 \pmod{q_i - 1}$) oraz $n \equiv 1 \pmod{q_5 - 1}$. Z lematu 4 natychmiast dostajemy $A_n \equiv A_{n \bmod \omega_{q_i}} = A_1 = 0 \pmod{q_i}$ dla $1 \leqslant i \leqslant 5$. Zatem $n \mid A_n$. Zupełnie analogicznie sprawdzamy warunek $A_{-n} \equiv A_{-1} = -1 \pmod n$. Zatem n jest silną liczbą Perrina.

Rozwiązanie zadania M 1763.
Rozważmy dowolny czworokąt $ABCD$. Suma kątów przy wierzchołkach jest równa 360°, więc wśród sum $\sphericalangle A + \sphericalangle B$ i $\sphericalangle C + \sphericalangle D$ jedna nie przekracza 180°. To samo dotyczy $\sphericalangle B + \sphericalangle C$ i $\sphericalangle D + \sphericalangle A$. Bez straty ogólności załóżmy, że są to sumy $\sphericalangle A + \sphericalangle B$ i $\sphericalangle D + \sphericalangle A$.
W kątach wewnętrznych o wierzchołkach A, B i D umieśćmy kopie wyjściowego czworokąta w skali $\frac{1}{2}$, jak pokazano na rysunku.



Ze względu na założone nierówności kopia $ABCD$ umieszczona w wierzchołku A ma po jednym punkcie wspólnym z dwoma pozostałymi kopiami, które z kolei mają tylko jeden wspólny punkt – środek przekątnej BD.

Rozwiązanie zadania M 1764.
Ponieważ $(a_k - a_{k+1})^2 \geqslant 0$, to

$$\frac{a_k^2}{a_{k+1}} \geqslant 2a_k - a_{k+1}$$

dla $k = 1, 2, \ldots, n$ ($a_{n+1} := a_1$). Liczba $2a_k - a_{k+1}$ jest całkowita, więc

$$\left\lfloor \frac{a_k^2}{a_{k+1}} \right\rfloor \geqslant 2a_k - a_{k+1},$$

zatem

$$\sum_{k=1}^{n} \left\lfloor \frac{a_k^2}{a_{k+1}} \right\rfloor \geqslant \sum_{k=1}^{n} (2a_k - a_{k+1}) = \sum_{k=1}^{n} a_k.$$

Wiadomo, że liczb Carmichaela jest nieskończenie wiele. Co więcej, udowodniono, że liczb Carmichaela, których każdy dzielnik pierwszy ma typ **S**, również jest nieskończenie wiele. Każda taka liczba jest silną liczbą Perrina, więc tych ostatnich też jest nieskończenie wiele. Z drugiej strony nie wiadomo, czy liczb Perrina z co najmniej jednym dzielnikiem typu **Q** lub **I** jest nieskończenie wiele.

Liczby Perrina to bardzo rzadkie okazy. Przedstawmy trochę statystyk – jest 1700 liczb Perrina mniejszych niż 10^{14}, wśród nich 942 są silnymi liczbami Perrina, a tylko 30 z nich jest liczbami Carmichaela.

Wspomnieliśmy o liczbach pseudopierwszych Fermata, Carmichaela, Dicksona i Perrina. Oprócz tego są jeszcze liczby pseudopierwsze Eulera, Lucasa, Lehmera, Szekeresa i ich różne warianty – a lista ta jest niepełna. Czy to matematyczne zoo liczb pseudopierwszych ma jakiś wspólny mianownik? Jon Grantham [G] podjął próbę (udaną) usystematyzowania występujących definicji liczb pseudopierwszych. Dla ustalonego wielomianu $P \in \mathbb{Z}[X]$ wprowadził pojęcie liczby P-pseudopierwszej Frobeniusa, której definicja wykracza niestety poza ramy tekstu popularnonaukowego. Wspomnijmy jednak, że liczby $(X - a)$-pseudopierwsze Frobeniusa to dokładnie liczby pseudopierwsze Fermata przy podstawie a, każda liczba $(X^3 - X - 1)$-pseudopierwsza Frobeniusa jest silną liczbą Perrina, a każda liczba $(X^2 - aX + b)$-pseudopierwsza Frobeniusa to taka, która jest jednocześnie liczbą pseudopierwszą Dicksona i Lucasa.

Definicja liczby pseudopierwszej Lucasa jest bardzo podobna do definicji liczby pseudopierwszej Dicksona. Przytaczamy ją dla Czytelników Zainteresowanych: rozważamy ciąg (U_n) określony rekurencją $U_0 = 0, U_1 = 1$ oraz $U_{n+1} = aU_n - bU_{n-1}$. Niech $\Delta = b^2 - 4ac$. Liczba złożona n jest *liczbą pseudopierwszą Lucasa*, jeśli jest względnie pierwsza z $2b\Delta$ oraz spełnia podzielność $n \mid U_{n-\varepsilon(n)}$, gdzie $\varepsilon(n)$ jest pewną funkcją o wartościach ± 1 (konkretnie: symbolem Jacobiego $\left(\frac{\Delta}{n}\right)$).

Nie wypada nie wspomnieć tutaj o przełomie, jaki dokonał się w 2002 roku za sprawą znalezienia prostego, wielomianowego (względem liczby cyfr w zapisie danej liczby) i deterministycznego testu pierwszości, zwanego algorytmem AKS, od pierwszych liter jego odkrywców: Agrawala, Kayala i Saxena (patrz Δ_{12}^6). Słowo *deterministyczny* oznacza tu tyle, że dla dowolnej liczby n udziela on poprawnej odpowiedzi na pytanie, czy jest to liczba pierwsza. Jednak w praktyce powszechnie stosowanym testem pierwszości (Mathematica, Pari/GP, Maxima, Sage, ...) jest algorytm Baillie-PSW (od jego autorów: Pomerance, Selfridge, Wagstaff), który choć nie jest deterministyczny (stwierdza jedynie, że dana liczba n jest „prawdopodobnie" pierwsza lub że n jest na pewno złożona), jest znacznie szybszy. Jest on połączeniem testów pierwszości Fermata (przy bazie 2) i Lucasa (dla odpowiednio dobranych parametrów a, b – patrz margines).

Nieznane są przykłady liczb złożonych, które algorytm Baillie-PSW uznałby za pierwsze. Wiadomo, że nie ma takich poniżej 10^{19}, jednak przypuszcza się, że jest ich nieskończenie wiele.

Ćwiczenia (wskazówki dostępne na `deltami.edu.pl`)

1. Niech $a, b \in \mathbb{Z}$ i niech (V_n) będzie ciągiem zadanym przez warunki: $V_0 = 2$, $V_1 = a$, $V_{n+1} = aV_n - bV_{n-1}$. Uzasadnić wzory
$$V_{2n} = V_n^2 - 2b^n, \quad V_{2n+1} = V_n V_{n+1} - ab^n.$$
2. Uzasadnić, że $\frac{\sqrt{2}}{2}$ nie jest liczbą algebraiczną całkowitą.
3. Pierwiastkami wielomianu $X^3 - X - 1$ są $\alpha \approx 1{,}32 \in \mathbb{R}$, $\beta \approx -0{,}66 + 0{,}56i = \frac{1}{\sqrt{\alpha}}(\cos\phi + i\sin\phi)$ oraz $\gamma = \bar{\beta}$, gdzie $\phi \approx 1{,}55\frac{\pi}{2}$, a dokładniej rozwinięcie w ułamek łańcuchowy $2\phi/\pi$ daje oszacowanie $1\frac{16}{29} < \frac{\phi}{\pi/2} < 1\frac{101}{183}$. Uzasadnić wzór
$$A_{-n} = 2(\sqrt{\alpha})^n \cos(n\phi) + \alpha^{-n}$$
dla $n > 0$, a następnie na podstawie podanych przybliżeń i lematu 3 wywnioskować, że $A_{-29} = -1$.
4. Udowodnić, że dla każdej liczby pierwszej $p \neq 5$ iloczyn $F_{p+1}F_{p-1}$ jest podzielny przez p, gdzie $(F_n)_{n\geqslant 1} = (1, 1, 2, 3, 5, \ldots)$ jest ciągiem Fibonacciego.
5. Uzasadnić, że ślad macierzy M^n (suma liczb na przekątnej NW—SE), gdzie $M = \left[\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right]$, wynosi A_n, dla każdego $n \in \mathbb{Z}$.
Wniosek. Dostajemy krótki algorytm dla sprawdzenia, czy n jest liczbą Perrina.
6. Udowodnić lemat 3.
7. Uzasadnić, że 2 jest typu **I**, 5 typu **Q**, natomiast $59 = 4^3 - 4 - 1$ typu **S**. (59 jest najmniejszą liczbą pierwszą typu **S**.)
8. Uzasadnić, że liczba $904631 = 7 \cdot 13 \cdot 9941$ jest liczbą Perrina, natomiast $16043638781521 = 13 \cdot 223 \cdot 691 \cdot 829 \cdot 9661$ jest silną liczbą Perrina.

Literatura

[A-S] W. Adams, D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. 39 (1982).

[L] E. Lucas, *Sur la recherche de grands nombres premiers*, A. F. Congrès du Clermont-Ferrand (1876).

[P] R. Perrin, *Item 1484*, L'Intermédiaire des Math. 6 (1899).

[G] J. Grantham (2001), *Frobenius pseudoprimes*, Math. Comp. 70 (234): 873–891.

[BB-S] A. Białynicki-Birula, M. Skałba, *Lectures on Number Theory.*

[M] D. A. Marcus, *Number fields.*