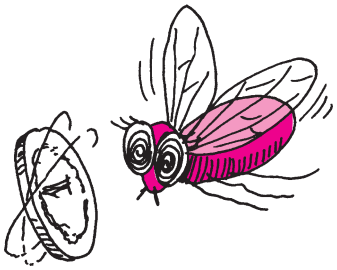
Jak rzucać monetą przez telefon

Wojciech GUZICKI

Dla każdego powinno być oczywiste, że można grać w szachy na odległość: przesyłając opisy kolejnych ruchów w listach, telefonując do przeciwnika, czy też wysyłając mu e-mail lub SMS. Nie ma w tym nic dziwnego, przecież przesyłamy mu informację o tym, co i tak widać na szachownicy. Inaczej jest z grami losowymi. Weźmy, na przykład, najprostszą grę losową: w orła i reszkę. Antek wybiera jedną z dwóch możliwości: orła lub reszkę, Bartek rzuca monetą. Jeśli wypadnie orzeł, to wygrywa Antek; jeśli wypadnie reszka, to wygrywa Bartek. Czy Antek i Bartek mogą zagrać w orła i reszkę na odległość? Chwila zastanowienia pozwala nam dostrzec trudność. Wyobraźmy sobie, że Antek wybiera orła i pisze lub telefonuje do Bartka, przekazując mu tę informację. Bartek teraz rzuca monetą i odpowiada Antkowi, że – niestety! – wypadła reszka. Czy Antek może mu wierzyć, nie widząc, czy Bartek naprawdę rzucił monetą i co naprawdę wypadło?



Wydaje się, że gra w gry losowe na odległość nie jest w takim razie możliwa. Okazuje się jednak, że jest możliwa. Zobaczymy, że Antek i Bartek mogą rozegrać grę w „orła i reszkę", nie spotykając się i tylko przesyłając informacje na odległość. Pomoże im w tym znajomość pewnych faktów z pogranicza teorii liczb i informatyki.

Umówimy się, że w dalszym ciągu zwrot „umiemy rozwiązać" jakieś zadanie oznacza to, że znany jest algorytm znajdujący w rozsądnie krótkim czasie rozwiązanie tego zadania. Zwrot „nie umiemy rozwiązać" oznacza natomiast, że żaden taki algorytm nie jest dotychczas znany. Słowo algorytm może tu oznaczać również tzw. algorytm probabilistyczny, dający rozwiązanie z bardzo dużym prawdopodobieństwem, graniczącym z pewnością.

Metoda gry w orła i reszkę na odległość jest skuteczna dlatego, że pewne zadania umiemy rozwiązywać, innych natomiast nie umiemy. Przyjrzyjmy się teraz paru zadaniom obu typów.

1. Umiemy znajdować największy wspólny dzielnik dwóch dużych (np. dwustucyfrowych) liczb naturalnych za pomocą tzw. algorytmu Euklidesa.

2. Umiemy sprawdzić, czy dana duża liczba (np. mająca około 200 cyfr w zapisie dziesiętnym) jest liczbą pierwszą. Czytelnik może znaleźć informacje na ten temat w kwietniowym numerze *Delty* z 1997 roku. Umiemy również znajdować tak duże liczby pierwsze.

3. Nie umiemy rozkładać na czynniki dużych liczb złożonych. Na przykład, jeśli liczba n jest iloczynem dwóch przypadkowo wybranych liczb pierwszych dwustucyfrowych p i q, to za pomocą żadnego znanego algorytmu nie znajdziemy czynników p i q w czasie krótszym niż miliardy lat.

4. Przypuśćmy, że mamy dane dwie różne liczby pierwsze p i q oraz dwie liczby a i b, takie że $0 \leqslant a < p$ oraz $0 \leqslant b < q$. Wtedy umiemy znaleźć liczbę x, taką że reszta z dzielenia x przez p wynosi a oraz reszta z dzielenia x przez q wynosi b. Jest to szczególny przypadek tzw. chińskiego twierdzenia o resztach.

5. Przypuśćmy teraz, że p jest liczbą pierwszą. Liczbę a, taką że $0 < a < p$, nazywamy **resztą kwadratową** modulo p, jeśli istnieje liczba x, taka że x^2 daje przy dzieleniu przez p resztę a. Umiemy stwierdzić, czy dana liczba a jest resztą kwadratową modulo p.

6. Niech p będzie nadal liczbą pierwszą i niech a będzie resztą kwadratową modulo p. Umiemy wtedy znaleźć taką liczbę x, że $0 < x < p$ oraz liczba x^2 daje resztę a przy dzieleniu przez p. Są dwie takie liczby; jeśli jedną z nich jest x, to drugą jest $p - x$. Oczywiście, umiemy znaleźć je obie. Każdą z tych dwóch liczb (x oraz $p - x$) nazywamy pierwiastkiem kwadratowym z a modulo p.

7. Przypuśćmy teraz, że liczba n jest iloczynem dwóch dużych liczb pierwszych: $n = p \cdot q$ (liczby p i q mają po około 200 cyfr). Przypuśćmy następnie, że ktoś wybierze liczbę x względnie pierwszą z n (tzn. niepodzielną przez p i przez q)

Rozwiązanie zadania F 584.
Natężenie prądu płynącego przez amperomierz A_1 jest równe sumie prądów płynących przez woltomierz V_1 i amperomierz A_2

$$I_1 = I_{V_1} + I_2,$$

zatem natężenie prądu płynącego przez woltomierz V_1 jest równe

$$I_{V_1} = I_1 - I_2 = 0{,}3 \text{ mA},$$

a opór woltomierza

$$R = \frac{U_i}{I_{V_1}} = 32 \text{ k}\Omega.$$

Z warunków zadania mamy, że opory wszystkich woltomierzy są jednakowe i równe R. Suma wskazań wszystkich woltomierzy jest następującej postaci

$$\sum_{i=1}^{50} U_{V_i} = \sum_{i=1}^{50} I_{V_i} R = R \sum_{i=1}^{50} I_{V_i}.$$

Ale $\sum_{i=1}^{50} I_{V_i}$ to prąd płynący przez amperomierz A_1, tzn.

$$\sum_{i=1}^{50} I_{V_i} = I_1,$$

zatem

$$\sum_{i=1}^{50} U_{V_i} = RI_1 = 304 \text{ V}.$$

i obliczy resztę z dzielenia x^2 przez n; niech a będzie tą resztą. Nie umiemy wtedy, mając dane tylko liczby n i a, znaleźć ani jednej liczby y, takiej że y^2 daje resztę a przy dzieleniu przez n. Inaczej mówiąc, nie umiemy znaleźć pierwiastka kwadratowego z a modulo liczba złożona n.

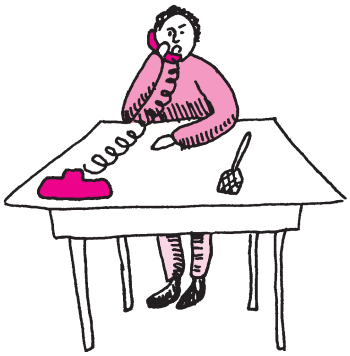
8. Umiemy natomiast rozwiązać poprzednie zadanie, jeśli znamy również liczby p i q. Okazuje się, że wtedy istnieją cztery rozwiązania. Niech b będzie resztą z dzielenia liczby a przez p i niech c będzie resztą z dzielenia liczby a przez q. Znajdujemy dwa pierwiastki kwadratowe z b modulo p: niech będą to r i s (oczywiście $s = p - r$). Następnie znajdujemy dwa pierwiastki kwadratowe z c modulo q: niech będą to t i u (wtedy $u = q - t$). Teraz za pomocą chińskiego twierdzenia o resztach możemy znaleźć cztery liczby: x_1, x_2, x_3 i x_4, których reszty z dzielenia przez p i q są odpowiednio równe:

	reszta z dzielenia przez p	reszta z dzielenia przez q
x_1	r	t
x_2	r	u
x_3	s	t
x_4	s	u

Wtedy liczby: x_1, x_2, x_3 i x_4 są wszystkimi pierwiastkami kwadratowymi z a modulo n. Można więc dowieść, że $x_4 = n - x_1$, $x_3 = n - x_2$ oraz:

a) liczby $x_1 - x_2$ oraz $x_3 - x_4$ dzielą się przez p i nie dzielą się przez q. Zatem
$$\mathrm{NWD}(x_1 - x_2, n) = \mathrm{NWD}(x_3 - x_4, n) = p.$$

b) liczby $x_1 - x_3$ oraz $x_2 - x_4$ dzielą się przez q i nie dzielą się przez p. Zatem
$$\mathrm{NWD}(x_1 - x_3, n) = \mathrm{NWD}(x_2 - x_4, n) = q.$$



c) liczby $x_1 - x_4$ oraz $x_2 - x_3$ nie dzielą się ani przez p, ani przez q. Zatem
$$\mathrm{NWD}(x_1 - x_4, n) = \mathrm{NWD}(x_2 - x_3, n) = 1.$$

Teraz możemy już opisać sposób gry w orła i reszkę na odległość. Zaczynamy od tego, że Bartek wybiera dwie duże liczby pierwsze p i q, mnoży je i iloczyn $n = p \cdot q$ wysyła Antkowi. Liczby p i q trzyma w tajemnicy. Antek wybiera następnie liczbę x, taką że $0 < x < n$, sprawdza, czy jest ona względnie pierwsza z n i podnosi do kwadratu. Następnie oblicza resztę z dzielenia x^2 przez n. Niech tą resztą będzie liczba a. Liczbę a Antek przesyła Bartkowi. Teraz Bartek rozwiązuje zadanie 8, tzn. znajduje cztery pierwiastki kwadratowe z a modulo n: x_1, x_2, x_3 i x_4. Oczywiście, liczba x wybrana przez Antka jest jedną z tych czterech liczb. Przypuśćmy, że $x = x_1$. Następuje najważniejsza część gry: rzut monetą. Dokładniej, następuje losowanie. Z czterech liczb: x_1, x_2, x_3 i x_4 Bartek wybiera jedną i odsyła ją Antkowi. Oznaczmy wybraną liczbę literą y. Antek oblicza $\mathrm{NWD}(x - y, n)$. Możliwe są teraz cztery przypadki:

a) $y = x_1$. Wtedy Antek dostaje tę samą liczbę, którą wybrał na początku. Zatem $x - y = 0$ i wtedy oczywiście
$$\mathrm{NWD}(x - y, n) = n.$$

b) $y = x_2$. Wtedy
$$\mathrm{NWD}(x - y, n) = \mathrm{NWD}(x_1 - x_2, n) = p.$$

c) $y = x_3$. Wtedy
$$\mathrm{NWD}(x - y, n) = \mathrm{NWD}(x_1 - x_3, n) = q.$$

d) $y = x_4$. Wtedy
$$\mathrm{NWD}(x - y, n) = \mathrm{NWD}(x_1 - x_4, n) = 1.$$

Okazuje się, że w dwóch przypadkach otrzymany największy wspólny dzielnik $x - y$ i n jest jedną z wybranych liczb pierwszych p i q. Zatem Antek umie

Rozwiązanie zadania M 1007.
Oznaczmy przez $x_0, x_1, \ldots, x_9$ kolejne liczby na okręgu.

$$x_0 = 100 - (x_1 + x_2 + x_3) - (x_4 + x_5 + x_6) - (x_7 + x_8 + x_9) \leqslant$$
$$\leqslant 100 - 3 \cdot 29 = 13.$$

Z drugiej strony układ liczb
$$13, 9\frac{2}{3}, 9\frac{2}{3}, \ldots, 9\frac{2}{3}$$
spełnia założenia zadania.
Odpowiedzią jest 13.

Rozwiązanie zadania F 583.
Woltomierze są jednakowe, zatem stosunki prądów płynących przez nie, są równe odpowiednio stosunkom wskazań woltomierzy. Oznaczając opór każdego woltomierza przez R mamy

$$U_3 = U_2 - RI_2,$$
$$U_2 = U_1 - R(I_2 + I_3).$$

Stąd

$$\frac{I_2 + I_3}{I_3} = \frac{U_2 + U_3}{U_3} = \frac{U_1 - U_2}{U_2 - U_3}.$$

Zatem

$$U_2^2 - U_3^2 = U_1U_3 - U_2U_3,$$

i ostatecznie

$$U_2 = -\frac{U_3}{2} + \sqrt{\frac{5}{4}U_3^2 + U_1U_2} \approx 8{,}6 \text{ V}.$$

rozłożyć liczbę n na czynniki. W pozostałych dwóch przypadkach Antek nie dostaje żadnej nowej informacji poza tą, którą miał na początku. Jeśli bowiem otrzymał od Bartka liczbę x_1, czyli x, to oczywiście nie dowiedział się niczego nowego. Jeśli natomiast otrzymał liczbę x_4, to zauważa, że dostał liczbę $n - x$, czyli też nie dowiaduje się niczego nowego.

Podsumujmy: jeśli Bartek wylosuje x_1 lub x_4, to Antek nie dowiaduje się niczego nowego poza tym, co wiedział na początku gry: zna liczbę n i wybraną przez siebie liczbę x. Jeśli natomiast Bartek wylosuje x_2 lub x_3, to umożliwi Antkowi rozłożenie liczby n na czynniki. Teraz można już umówić się, kto wygrywa w tej grze. Jeśli na końcu Antek umie rozłożyć n na czynniki, to wygrywa, jeśli nie umie, to przegrywa. Widzimy, że zasadnicze rozstrzygnięcie gry nastąpiło w momencie losowania jednej z czterech liczb przez Bartka. W dwóch przypadkach wygrywa Antek, w dwóch Bartek. To tak, jakby Bartek rzucił monetą, która ma dwa orły i dwie reszki. Jeśli wypadnie którykolwiek z orłów, to wygrywa Bartek; jeśli którakolwiek z reszek, to wygrywa Antek. Zatem każdy z nich ma prawdopodobieństwo wygranej równe $\frac{1}{2}$, tak jak przy rzucie zwykłą monetą.

Dokładniejsza analiza pokazuje, że Antek ma nieco większą szansę na wygranie. Może on bowiem po prostu zgadnąć jeden z czynników pierwszych liczby n. Może także, wybierając liczbę x, trafić na liczbę podzielną przez p lub przez q i rozłożyć w ten sposób n na czynniki. Prawdopodobieństwa tych zdarzeń są jednak tak bardzo małe, że w praktyce możemy je zaniedbać.

Innymi grami losowymi, w które trudno grać na odległość, są gry w karty. Wynaleziono inne metody, za pomocą których można rozdać karty graczom tak, by mogli zagrać np. w pokera. Inaczej jest jednak z grą w brydża: to jest gra par, a nie indywidualnych graczy i trudno byłoby zapobiec nielegalnej wymianie informacji między graczami w jednej parze.

Skojarzenia

Witold BEDNAREK

W teorii liczb rozważane są, między innymi, następujące liczby (do tej pory nie wiadomo, czy jest ich nieskończenie wiele):

A. Liczby pierwsze bliźniacze: para liczb pierwszych różniących się o 2, a więc postaci p i $p+2$.

B. Liczby pierwsze Mersenne'a: liczby pierwsze postaci $2^p - 1$.

C. Liczby pierwsze Sophie Germain: takie liczby pierwsze p, że $2p+1$ jest również liczbą pierwszą.

A z C

Czy istnieje para liczb bliźniaczych będących liczbami Sophie Germain?

Liczby:

$$p, \quad p+2, \quad 2p+1, \quad 2(p+2)+1$$

muszą być pierwsze. Nie może być $p = 2$, bo wtedy $p + 2 = 4$ jest liczbą złożoną. Jeżeli $p = 3$, to pozostałe liczby: 5, 7, 11 są pierwsze. Załóżmy dalej, że $p > 3$. Wówczas p jest postaci $3k + 1$ lub $3k + 2$. W pierwszym przypadku liczba

$$p + 2 = (3k + 1) + 2 = 3(k + 1)$$

jest złożona. W drugim przypadku liczba

$$2(p + 2) + 1 = 2(3k + 2 + 2) + 1 = 3(2k + 3)$$

też jest złożona. Ostatecznie stwierdzamy, że jedyną taką parą są liczby 3 i 5.

A z B

Czy istnieje para liczb bliźniaczych będących liczbami Mersenne'a?

Mamy równanie

$$(2^{p_1} - 1) - (2^{p_2} - 1) = 2,$$

czyli $2^{p_4} - 2^{p_2} = 2$. Jedyną parą potęg dwójki różniącą się o 2 jest para 4 i 2, a więc $2^{p_1} = 4$ i $2^{p_2} = 2$. Stąd $p_1 = 2$ i $p_2 = 1$, ale 1 nie jest liczbą pierwszą. Zatem odpowiedź jest negatywna.

B z C

Czy istnieje liczba Mersenne'a będąca liczbą Sophie Germain?

Liczby

$$2^p - 1 \quad \text{i} \quad 2(2^p - 1) + 1$$

muszą być pierwsze. Mamy

$$2(2^p - 1) + 1 = 2^{p+1} - 1.$$

Jeżeli $p = 2$, to liczby

$$2^p - 1 = 2^2 - 1 = 3 \quad \text{i} \quad 2^{p+1} - 1 = 2^3 - 1 = 7$$

są pierwsze. Jeżeli $p > 2$, to p jest nieparzyste, czyli $p = 2k + 1$. Zatem

$$2^{p+1} - 1 = 2^{2k+2} - 1 = (2^{k+1} - 1)(2^{k+1} + 1)$$

jest liczbą złożoną. Wobec tego tylko liczba 3 jest zarówno liczbą Mersenne'a, jak i liczbą Sophie Germain.