w czasie), po zmodyfikowaną grawitację, w której w skrajnych przypadkach Λ nie ma w równaniach w ogóle, jest za to „piąta siła” – dodatkowe oddziaływanie, w wyniku którego grawitacja jest słabsza na bardzo dużych kosmicznych skalach, co skutkuje przyspieszającą ekspansją. Niektórzy natomiast twierdzą, że żadna modyfikacja grawitacji nie jest konieczna, należy natomiast zrewidować nasz opis Wszechświata jako jednorodnego i izotropowego. Według tego rodzaju modeli przyspieszanie ekspansji jest pozorne, a to, że je „widzimy”, wynika ze zbyt uproszczonego modelu, w którym obserwacje są interpretowane.

Większość modeli kosmologicznych, w tym ΛCDM, zakłada, że Wszechświat w odpowiednio dużych skalach jest jednorodny i izotropowy, dzięki czemu możemy przyjąć wiele symetrii i opisywać go prostą metryką Friedmana–Lemaître'a–Robertsona–Walkera. Niektórzy kosmologowie twierdzą jednak, że jest to nadmierne uproszczenie i właśnie to założenie prowadzi do „artefaktu”, jakim jest przyspieszająca ekspansja, pisaliśmy o tym w Δ^1_{16}. W niektórych z modeli „niejednorodnych” nie można globalnie zdefiniować średniej krzywizny czy gęstości, przez co inaczej interpretuje się w nich obserwacje np. supernowych (takie jak związek odległości z przesunięciami ku czerwieni).

Zarówno modele zmodyfikowanej grawitacji, jak i te zakładające znaczące niejednorodności, mają swoje wady, na pewno nie mniejsze niż standardowy model kosmologiczny, jakim jest ΛCDM. A ponieważ żadne obserwacje kosmologiczne nie wskazują obecnie na znaczne odstępstwa od modelu standardowego (a w każdym razie nie widać, aby jakiś inny model lepiej je wyjaśniał), brzytwa Ockhama odcina wszystko, co nie jest ΛCDM. Czy to się zmieni w najbliższych latach, gdy nowe, większe i głębsze przeglądy kosmosu staną się rzeczywistością? Czy ambitne programy, takie jak Euclid, LSST, JWST czy SKA, przybliżą nas do wyjaśnienia zagadki Λ, czy wręcz przeciwnie?

Jak wyciągnąć $\sqrt{2}$ modulo n?

*Mariusz SKAŁBA**

* Instytut Matematyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Niech n będzie liczbą nieparzystą. Pytamy, czy istnieje taka liczba całkowita x, że

$$x^2 \equiv 2 \pmod{n}\,? \tag{1}$$

Jeśli ta kongruencja ma rozwiązanie całkowite x, to na pewno istnieje rozwiązanie $x_1 \in \{0, 1, \ldots, n-1\}$. Wtedy liczba $x_2 = n - x_1$ też jest rozwiązaniem. Jak jednak rozstrzygnąć, czy kongruencja (1) w ogóle ma rozwiązania?

W przypadku, gdy $n = p$ jest liczbą pierwszą, dysponujemy praktycznym algorytmem, który rozstrzyga, czy kongruencja (1) ma rozwiązanie – oparty jest on na tzw. **kryterium Eulera**. Jest ono ściśle związane z **małym twierdzeniem Fermata**. To słynne twierdzenie mówi, że jeśli x nie dzieli się przez liczbę pierwszą p, to wówczas

$$x^{p-1} \equiv 1 \pmod{p}.$$

Jeśli kongruencja (1) ma rozwiązanie x, to możemy napisać

$$2^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p},$$

a zatem ostatecznie

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{2}$$

Kryterium Eulera stanowi, że powyższe rozumowanie można odwrócić: jeśli zachodzi kongruencja (2), to kongruencja (1) ma rozwiązanie. Warto w tym miejscu dodać, że potęgowanie a^k modulo n łatwo wykonać efektywnie nawet wtedy, gdy liczby n oraz k są ogromne! Oto zarys metody. Najpierw zapisujemy wykładnik k w układzie dwójkowym:

$$k = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_l}, \quad \text{gdzie } m_1 < m_2 < \cdots < m_l = \lfloor \log_2 k \rfloor .$$

Ponieważ

$$a^k = a^{2^{m_1}} \cdot a^{2^{m_2}} \cdot \ldots \cdot a^{2^{m_l}},$$

więc wystarczy wykonać m_l kolejnych podnoszeń do kwadratu, a na koniec $l-1$ mnożeń – wszystkie operacje wykonujemy modulo n, a więc na liczbach mniejszych od n.

Załóżmy teraz, że liczba 2 przeszła test Eulera. Nasuwa się teraz pytanie: jak znaleźć x spełniające kongruencję (1)?

Jeśli $p \equiv 3 \pmod 4$, to wystarczy przyjąć

$$x \equiv 2^{\frac{p+1}{4}} \pmod{p}.$$

Pokazuje to poniższy rachunek

$$x^2 \equiv 2^{\frac{p+1}{2}} \equiv 2^{\frac{p-1}{2}} \cdot 2^1 \equiv 2 \pmod{p}$$

(na mocy (2)).

Jeżeli natomiast $p \equiv 1 \pmod 4$, to nieco komplikując powyższą metodę (szczegóły pominiemy), można obliczyć x spełniające (1), **o ile** mamy do dyspozycji taką liczbę s, że kongruencja

$$x^2 \equiv s \pmod p \tag{3}$$

nie ma rozwiązań. Taką liczbę s nazywamy *niereszą kwadratową modulo p*. Łatwo udowodnić, że w ciągu liczb $1, 2, \ldots, p-1$ jest dokładnie $(p-1)/2$ niereszt. Dla pozostałych liczb s z powyższego ciągu kongruencja (3) ma rozwiązanie – nazywamy je *resztami kwadratowymi modulo p*. I tak np. dla $p = 7$ liczby $1, 2, 4$ są resztami kwadratowymi, a liczby $3, 5, 6$ niereszami kwadratowymi. Natomiast dla $p = 11$ nieresty kwadratowe to $2, 6, 7, 8, 10$, a reszty kwadratowe to $1, 3, 4, 5, 9$. Niereszę kwadratową s, której używamy we wzmiankowanym powyżej algorytmie pierwiastkowania modulo p, łatwo znaleźć praktycznie nawet dla bardzo dużych liczb pierwszych p. Wystarczy mianowicie wylosować liczbę $s \in \{1, 2, \ldots, p-1\}$ i sprawdzić, czy jest niereszą kwadratową, stosując, na przykład, kryterium Eulera. W przypadku niepowodzenia losujemy i testujemy inną liczbę s. Prawdopodobieństwo wylosowania niereszty w każdej próbie wynosi $1/2$, a zatem przeciętnie bardzo szybko znajdziemy niereszę. Jest to przykład **algorytmu zrandomizowanego**. Rzucając 20 razy symetryczną monetą, możemy, oczywiście, wyrzucić same *reszty* (niektórzy mówią *reszki*), ale prawdopodobieństwo tego jest małe.

A może lepiej testować po kolei liczby $s = 1, 2, 3 \ldots$, aż do skutku, czyli do napotkania niereszty? Niech więc $N(p)$ oznacza najmniejszą niereszę kwadratową modulo p. Najlepszy wynik bezwarunkowy pochodzi od D.A. Burgessa

$$N(p) < p^{\frac{1}{4\sqrt{e}}+\varepsilon}$$

dla każdego $\varepsilon > 0$ i $p > p_0(\varepsilon)$. Natomiast przy założeniu **uogólnionej hipotezy Riemanna** N.C. Ankeny pokazał oszacowanie znacznie lepsze

$$N(p) < C(\log p)^2 \text{ dla pewnej stałej } C > 0.$$

Tak więc prymitywny algorytm testowania kolejnych liczb s jest (warunkowo) bardzo efektywny.

Podsumujmy nasze dotychczasowe rozważania: jeśli moduł n jest liczbą pierwszą, to w zasadzie potrafimy poradzić sobie zarówno z rozstrzygnięciem, czy 2 jest resztą kwadratową modulo n, jak i ze znalezieniem wszystkich rozwiązań kongruencji (1) w zbiorze $\{1, 2, \ldots, n-1\}$ (są dwa takie rozwiązania).

A jak jest dla liczb złożonych n? Rozpatrzymy najprostszy przypadek, gdy $n = pq$ jest iloczynem dwóch różnych liczb pierwszych. Do dzisiaj nie jest znana żadna efektywna uniwersalna metoda rozstrzygania, czy kongruencja (1) ma rozwiązanie. Załóżmy jednak, że dobra wróżka rzekła: *Tak, kongruencja* (1) *jest rozwiązalna, a Twoje zadanie to znaleźć jej wszystkie rozwiązania x w zbiorze* $\{1, 2, \ldots, n-1\}$. Załóżmy dalej, że jakimś *cudem* wypisaliśmy wszystkie (cztery – wynika to z chińskiego twierdzenia o resztach) rozwiązania kongruencji (1):

$$1 \leqslant x_1 < x_2 < x_3 < x_4 \leqslant pq - 1.$$

Ponieważ kongruencja $y^2 \equiv 2 \pmod p$ ma dokładnie dwa rozwiązania y_1, y_2 w zbiorze $\{1, 2, \ldots, p-1\}$, więc dla pewnych $1 \leqslant i < j \leqslant 3$ mamy $x_i \equiv x_j \pmod p$, a zatem liczba $x_j - x_i$ dzieli się przez p. Oczywiście, $x_j - x_i$ nie dzieli się przez $n = pq$, gdyż $1 \leqslant x_j - x_i < pq - 2$. A zatem

$$\mathrm{NWD}(x_j - x_i, n) = p.$$

Liczby $\mathrm{NWD}(x_2 - x_1, n)$, $\mathrm{NWD}(x_3 - x_2, n)$, $\mathrm{NWD}(x_3 - x_1, n)$ potrafimy obliczyć, bardzo efektywnie stosując najsłynniejszy algorytm na świecie – algorytm Euklidesa. W ten sposób znaleźliśmy nietrywialny dzielnik p liczby $n = pq$. Najbardziej pomógł nam *cud* (a nie wróżka). Tym samym naszkicowaliśmy główną myśl dowodu twierdzenia, że kompletne rozwiązanie kongruencji (1) dla modułu złożonego n jest co najmniej tak trudne, jak rozkład n na czynniki pierwsze. Natomiast samo tylko rozstrzygnięcie, czy (1) ma rozwiązanie, wydaje się istotnie łatwiejsze niż rozkład na czynniki, ale jak już wspomnieliśmy wcześniej, nikt nie umie zrobić efektywnie nawet tego.

Rozwiązanie zadania F 966.
Zatrzymanie pojazdu następuje, gdy praca wykonana przez siły tarcia równa jest początkowej energii kinetycznej pojazdu:

$$\frac{mv_0^2}{2} = mgfs,$$

gdzie m oznacza masę pojazdu, g – przyspieszenie ziemskie, a s drogę przebytą do zatrzymania.

a) Gdy prędkość początkowa v_1 jest większa od v_0, to podczas hamowania na drodze s energia kinetyczna zmaleje o wartość odpowiadającą prędkości v_0 i po przebyciu drogi s pojazd będzie poruszał się z prędkością

$$v = \sqrt{v_1^2 - v_0^2}.$$

Dla $v_1 = 60\,\mathrm{km/godz.}$ i $v_0 = 50\,\mathrm{km/godz.}$, $v = 33{,}17\,\mathrm{km/godz.}$

b) W przypadku mokrej nawierzchni pojazd podczas hamowania na drodze s straci tylko f_1/f_0 część swojej energii kinetycznej. Jego prędkość po przybyciu drogi s wyniesie więc:

$$v = v_0\sqrt{1 - \frac{f_1}{f_0}}.$$

Dla $v_0 = 50\,\mathrm{km/godz.}$, $f_1 = 0{,}4$ i $f_0 = 0{,}6$, $v = 28{,}87\,\mathrm{km/godz.}$