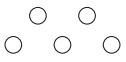
Jak złamałem system RSA

Juliusz Szczęsny BATURA

Jakiś czas temu usłyszałem w radiu ogólnikową wiadomość o systemie szyfrującym RSA. Jego niezawodność, jak wtedy zrozumiałem, polega na tym, że jeśli znamy iloczyn $e = p \cdot q$ dwóch liczb pierwszych p i q, bardzo trudno jest odnaleźć czynniki p i q, oczywiście przy założeniu, że są to bardzo duże liczby. To mnie zaintrygowało, bo w tym akurat czasie bawiłem się *mnożeniem trapezowym* liczb naturalnych: jeśli k i n są liczbami naturalnymi, to przez ich *iloczyn trapezowy* rozumiem liczbę $k \# n$ równą sumie k kolejnych liczb naturalnych, wśród których największą jest n. Nazwę uzasadniają przykładowe diagramy 1 i 2. Ulegając tej konwencji, tradycyjne mnożenie liczb naturalnych nazwalibyśmy *prostokątnym*, a odpowiednikiem tradycyjnego kwadratu liczby naturalnej n jest tu n-ta liczba trójkątna



$2 \# 3 = 5$

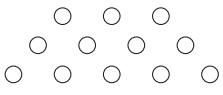
Diagram 1

$$n \# n = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Mniejsza o powody, dla których takie iloczyny mnie zaciekawiły. Łatwo zauważyć, że każda liczba nieparzysta w sensie tradycyjnym jest w „sensie trapezowym" parzysta, bo

$$2k + 1 = k + (k + 1) = 2 \# (k + 1).$$

W szczególności więc nieparzyste liczby pierwsze w sensie tradycyjnym nie są *pierwszymi* ze względu na mnożenie trapezowe.



$3 \# 5 = 12$

Diagram 2

Zauważmy dalej, że każdy iloczyn dwóch liczb naturalnych można w specyficzny sposób przedstawić za pomocą trzech liczb trójkątnych. Mamy mianowicie, dla $p < q$,

$$p \cdot q = \frac{p(p+1)}{2} + \frac{(q-1)q}{2} - \frac{(q-p-1)(q-p)}{2} =$$
$$= (1 + 2 + \ldots + p) + (1 + 2 + \ldots + (q-1)) - (1 + 2 + \ldots + (q-p-1)).$$

Sprawdzenie tej równości pozostawiam Czytelnikom, ale przypuszczam, że zrezygnują z tego sprawdzenia, jeśli tylko uważnie przyjrzą się diagramom 3 i 4. Otóż dla $n = 24 = 4 \cdot 6 = 3 \cdot 8$ mamy

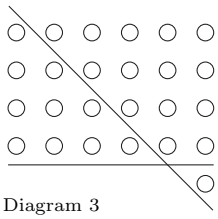


Diagram 3

$$4 \cdot 6 = (1 + 2 + 3 + 4) + (1 + 2 + 3 + 4 + 5) - 1 =$$
$$= \frac{4(4+1)}{2} + \frac{5(5+1)}{2} - \frac{(6-4-1)(6-4)}{2}.$$

W tym przypadku iloczyn ma więcej niż jeden rozkład na odpowiednią sumę trzech liczb trójkątnych. Liczba takich rozkładów zależy od ilości dzielników. Jeżeli zatem mamy do czynienia z iloczynem dwóch liczb pierwszych $e = p \cdot q$, analogiczny rozkład na sumę trzech liczb trójkątnych będzie jeden i tylko jeden, na przykład, gdy $e = 3 \cdot 7$, otrzymujemy diagram 5, co ilustruje rozkład

$$21 = 3 \cdot 7 = (1 + 2 + 3) + (1 + 2 + 3 + 4 + 5 + 6) - (1 + 2 + 3).$$

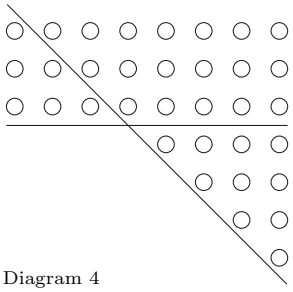


Diagram 4

Ogólnie, dla iloczynu dwóch różnych liczb pierwszych p i q $(p < q)$ prawdziwy i jednoznaczny jest wzór:

$$p \cdot q = t_1 + t_2 - t =$$
$$= (1 + 2 + \ldots + p) + (1 + 2 + \ldots + (q-1)) - (1 + 2 + \ldots + (q-p-1)) =$$
$$= \frac{p(p+1)}{2} + \frac{(q-1)q}{2} - \frac{(q-p-1)(q-p)}{2}.$$

Ten rozkład na sumę trzech liczb trójkątnych w moich rozważaniach stał się podstawą ataku na system RSA. Rozkład na iloczyn czynników jest równoważny ze znalezieniem odpowiednich liczb trójkątnych.

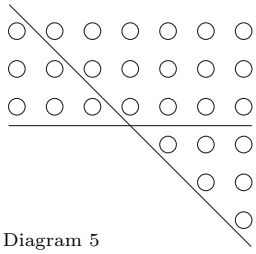


Diagram 5

Ponieważ p i q, jako liczby pierwsze większe od 2, są liczbami nieparzystymi, więc odpowiednio $q - 1$ jest liczbą parzystą, a $q - p - 1$ nieparzystą. Zapiszmy więc $q - p - 1 = 2y - 1$, skąd otrzymujemy

$$t = \frac{(q-p-1)(q-p)}{2} = \frac{(2y-1) \cdot 2y}{2} = 2y^2 - y.$$

Zatem t należy do zbioru $T = \{1, 6, 15, 28, 45, \ldots\} = \{2r^2 - r : r \in \mathbb{N}\}$, czyli do podzbioru zbioru wszystkich liczb trójkątnych zawierającego co drugą liczbę.

Dalsze moje „skomplikowane” rozważania dotyczące znalezienia rozkładu liczby $e = pq$ w postaci $t_1 + t_2 - t$, gdzie t_1, t_2, t są liczbami trójkątnymi, „zniszczył” profesor Andrzej Schinzel, którego poprosiłem o uwagi. Podpowiedział, że przecież

$$e = \frac{p(p+1)}{2} + \frac{q(q-1)}{2} - \frac{(q-p-1)(q-p)}{2} = \left(\frac{q+p}{2}\right)^2 - \left(\frac{q-p}{2}\right)^2.$$

Jeśli teraz przyjmiemy

$$q + p = 2x, \qquad q - p = 2y,$$

to otrzymamy układ

$$\begin{cases} 2y^2 - y = t, \\ x^2 - y^2 = e. \end{cases}$$

Pierwsze z równań nieznacznie ogranicza obszar poszukiwań, drugie zaś prowadzi do algorytmu rozkładu znanego od dawna jako algorytm Fermata. Algorytm polega na podstawianiu kolejnych wartości w miejsce y i badaniu, czy $e + y^2$ jest kwadratem. Jest jasne, że jeśli liczby p i q różnią się niewiele, to stosując ten algorytm, szybko znajdziemy rozkład liczby e (zauważmy, że drugie z równań nie odgrywa praktycznie żadnej istotnej roli). Od dawna jednak wiadomo, że takich par liczb p i q nie należy brać jako podstawę systemu RSA. A trzeba wiedzieć, że liczby pierwsze brane jako p i q w bezpiecznych systemach są ogromne. Do ich zapisu w systemie dziesiętnym trzeba użyć setek cyfr.

Można zażartować, że jeszcze tym razem system RSA oparł się mojemu atakowi. Mówiąc poważnie, jeśli weźmiemy pod uwagę to, że NSA (National Security Agency – Narodowa Agencja Bezpieczeństwa Stanów Zjednoczonych), zwana też No Such Agency („Nie Ma Takiej Agencji”), systematycznie zatrudnia tysiące matematyków, to można przypuszczać, że wszystkie nieskomplikowane ataki na ten system zostały już wyczerpująco przebadane i mnie, skromnemu grafikowi i nauczycielowi wychowania plastycznego, choć po studiach matematycznych sprzed 30 lat, nic już do znalezienia nie zostało.

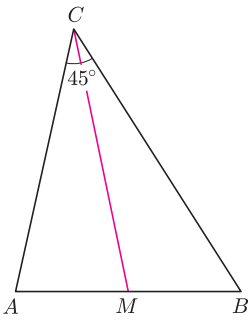
Zadania

Redaguje Ewa CZUCHRY

F 765. W cylindrycznym naczyniu przykrytym tłokiem znajduje się na początku $\nu = 1$ mol pary wodnej o temperaturze T i ciśnieniu p. Ciśnienie nasyconej pary wodnej przy takiej samej temperaturze wynosi $2p$. Następnie tłok przesuwa się tak, że objętość pod nim zmniejsza się czterokrotnie. Znaleźć masę skondensowanej wody, jeśli temperatura nie zmieniła się. Masa molowa wody $\mu = 0{,}018$ kg/mol.
Rozwiązanie na str. 23

F 766. W połowie długości poziomej rurki, zatkanej z dwóch stron, znajduje się tłok o powierzchni S. Po jego obu stronach znajduje się para wodna o ciśnieniu p. W takiej samej temperaturze para ta kondensuje się przy ciśnieniu $2p$. Rurkę postawiono pionowo i tłok opadł na wysokość czterokrotnie mniejszą od wyjściowej. Znaleźć masę tłoka. Tarcie tłoka o ścianki zaniedbać, temperatura po obu jego stronach jest taka sama.
Rozwiązanie na str. 7

Redaguje Waldemar POMPE



M 1279. Dany jest trójkąt ABC, w którym $\sphericalangle ACB = 45^\circ$ (rysunek). Punkt M jest środkiem boku AB. Wykazać, że

$$\frac{CM}{AB} \leqslant \frac{1+\sqrt{2}}{2}.$$

Rozwiązanie na str. 24

M 1280. Wykazać, że dla każdej liczby całkowitej $n > 1$ liczba $n^n - n^2 + n - 1$ jest podzielna przez $(n-1)^2$.
Rozwiązanie na str. 7

M 1281. Na szachownicy 9×9 ustawiono 9 wież w taki sposób, że żadne dwie nie biją się. Następnie każdą wieżę przestawiono na inne pole ruchem konika szachowego. Wykazać, że po tym przestawieniu pewne dwie wieże biją się.
Rozwiązanie na str. 6