

Świat jest pozytywny i kwadratowy

Jacek PYTLAK, Mariusz SKAŁBA*

Gdy ktoś zaczepi Was na ulicy i zapyta: *Co daje minus razy minus?*, to w zależności od nastroju odpowiecie bardzo krótko: *To nic nie daje* albo też krótko: *To daje bardzo dodatni plus*. Dlatego najpierw przypomnimy fragmenty teorii ogólnej, niezależnej od koniunktury.

Niech p będzie nieparzystą liczbą pierwszą i niech $\mathbb{F}_p = \{0, \dots, p-1\}$ będzie zbiorem reszt z dzielenia przez p . Wówczas dla niektórych reszt $r \neq 0$ istnieją dwie reszty x spełniające równanie

$$x^2 \equiv r \pmod{p},$$

a dla pozostałych niezerowych r nie ma w ogóle takich reszt x . W pierwszym przypadku mówimy, że r jest *resztą kwadratową modulo p* , a w drugim, że r jest *nieresztą kwadratową modulo p* . I tak na przykład z poniższej tabelki dla $p = 11$

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1

wynika, że 1, 3, 4, 5, 9 to reszty kwadratowe modulo 11, a 2, 6, 7, 8, 10 to niereszty kwadratowe modulo 11. To, że wiersz x^2 powyższej tabelki jest środkowo symetryczny, ma charakter ogólny, gdyż zawsze $(p-x)^2 \equiv x^2 \pmod{p}$. Zatem reszty z dzielenia przez p liczb

$$(*) \quad 1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$$

to reszty kwadratowe modulo p , a pozostałe liczby z ciągu $1, 2, 3, \dots, p-1$ to niereszty.

Jak stwierdzić, czy dana reszta a z dzielenia przez p jest resztą, czy też nieresztą kwadratową, nie przeszukując ciągu $(*)$? Mówi o tym znane kryterium Eulera:

$$a \text{ jest resztą kwadratową modulo } p \iff a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Od tej chwili będziemy zakładać, że liczba pierwsza p jest postaci $p = 4k + 3$. Można łatwo udowodnić, że takich liczb pierwszych jest nieskończenie wiele. Trudny jest natomiast dowód asymptotyki dla funkcji $\pi_{4,3}(x)$, która (z definicji) podaje liczbę liczb pierwszych p mniejszych równych x , spełniających kongruencję $p \equiv 3 \pmod{4}$:

$$\lim_{x \rightarrow \infty} \frac{\pi_{4,3}(x)}{x/\log x} = \frac{1}{2}.$$

Przypomnijmy, że analogiczna równość zachodzi dla samej funkcji $\pi(x)$, zliczającej liczbę wszystkich liczb pierwszych nie większych od x , przy czym w granicy po prawej stronie dostajemy 1. Statystycznie więc co druga liczba pierwsza jest interesującej nas postaci. Zauważmy, że na mocy kryterium Eulera dla $p = 4k + 3$ reszta $p-1$ jest nieresztą kwadratową, gdyż

$$(p-1)^{(p-1)/2} \equiv (-1)^{2k+1} \equiv -1 \not\equiv 1 \pmod{p}.$$

Ogólniej: z dwóch reszt a oraz $p-a$ jedna jest resztą, natomiast druga nieresztą kwadratową.

Przedstawione obserwacje pozwalają nam określić *pierwiastek arytmetyczny* z dowolnej reszty kwadratowej a . Niech mianowicie

$$b = a^{(p+1)/4} \pmod{p}.$$

Mamy teraz

$$b^2 \equiv a^{(p+1)/2} = a^{(p-1)/2} \cdot a \equiv a \pmod{p},$$

czyli rzeczywiście powyżej określone b jest jednym z pierwiastków kwadratowych z elementu a . A my dodatkowo uważamy, że b jest tym *lepszym* pierwiastkiem i chcemy go nazywać *pierwiastkiem arytmetycznym*! Przypomnijmy, że w zakresie liczb rzeczywistych pierwiastkiem kwadratowym arytmetycznym z dodatniej liczby a nazywamy taką (jedyną) dodatnią liczbę b , że $b^2 = a$.



W zbiorze liczb rzeczywistych $a \in \mathbb{R}$ jest dodatnie wtedy i tylko wtedy, gdy $a = b^2$ dla pewnego $b \in \mathbb{R}$. Od tej chwili niech „bycie kwadratem” będzie namiastką „dodatniości”. U nas b jako potęga reszty kwadratowej a jest też resztą kwadratową! Uzasadnia to traktowanie b jako pierwiastka arytmetycznego z a .

Niestety przedstawiona analogia jest ułomna, gdyż w doskonałym (czyli rzeczywistym) świecie suma elementów dodatnich jest dodatnia, a w świecie reszt nie musi tak być. Dla przykładu

$$3 \equiv 5^2 \pmod{11} \text{ oraz } 5 \equiv 4^2 \pmod{11}, \text{ ale } 8 \not\equiv b^2 \pmod{11} \text{ dla } b \in \mathbb{F}_{11}.$$

Takie ciała jak $\mathbb{R}$ czy też $\mathbb{Q}$ wyróżniają się tym, że można w nich wprowadzić relację porządku, która jest zgodna z oboma działaniami, tzn. zarówno iloczyn, jak i suma elementów dodatnich jest dodatnia. Natomiast ciało liczb zespolonych oraz ciała skończone nie są tak porządnie uporządkowane. Tak więc nasz świat rzeczywisty, chociaż tak niedoskonały, nie jest najgorszym z możliwych do pomyślenia światów.

Jest też w użyciu matematycznym bardziej naturalne i praktyczne pojęcie „dodatniości” w zbiorze reszt niż powyższe „bycie resztą kwadratową”. Jeśli mianowicie p jest dowolną liczbą pierwszą nieparzystą, to zbiór liczb całkowitych w przedziale $(-p/2, p/2)$ jest zbiorem reprezentantów ciała $\mathbb{F}_p$ reszt z dzielenia przez p . Od teraz klasę reszt mod p będziemy nazywać *dodatnią*, gdy ma swojego przedstawiciela w przedziale $(0, p/2)$, a *ujemną*, gdy ma przedstawiciela w $(-p/2, 0)$.

Ważnym zastosowaniem tej dychotomii jest lemat Gaussa: najwygodniejszy portal do Prawa Wzajemności dla Reszt Kwadratowych (PWdRK) – Gauss użył go w swoim piątym dowodzie PWdRK. Pozwoliły tu sobie na dygresję historyczną: przed Gaussem nikt nie potrafił udowodnić PWdRK. Z czwórki gigantów arytmetyki wyższej wymienionych przez Gaussa w przedmowie do *Disquisitiones Arithmeticae*: Fermata, Eulera, Lagrange’a i Legendre’a, tylko ten ostatni był bliski poprawnego dowodu. Sam Gauss podał sześć dowodów; po Gaussie opublikowano ponad 250 dowodów! Ta ogromna liczba różnych dowodów słynnego twierdzenia świadczy pośrednio o jego wielorakich powiązaniach z resztą matematyki.

To wszystko jest bardzo piękne, ale my teraz nie o tym... Przy powyższej definicji „dodatniości” nie jest prawdą, że nasza metoda pierwiastkowania w $\mathbb{F}_p^*$ dla $p \equiv 3 \pmod{4}$ zawsze daje pierwiastek „dodatni” (tzn. resztę z przedziału $(0, p/2)$), ale okazuje się, że jednak trochę częściej niż „ujemny”: *w przedziale $(0, p/2)$ jest mianowicie więcej reszt niż niereszt!* Nie ma prostego uzasadnienia tej prawidłowości, warto jednak wspomnieć, z jakiego ogólniejszego i ważnego twierdzenia to wynika. Dla $p = 3$ teza jest oczywista. Załóżmy w dalszym ciągu, że $p \geq 7$. Niech $\mathcal{R}$ oznacza liczbę reszt kwadratowych modulo p w przedziale $(0, p/2)$, a $\mathcal{N}$ liczbę niereszt w tym przedziale. Ponadto przez h oznaczmy

rząd grupy klas ideałów pierścienia liczb całkowitych ciała $\mathbb{Q}(\sqrt{-p})$.

Zapewne nawet wśród Czytelników *Delt*y jest wielu takich, dla których powyższa definicja jest niezrozumiała. Nie szkodzi – dla nas istotne jest tylko to, że liczba h jako rząd (czyli liczba elementów) grupy jest dodatnia. Okazuje się bowiem, że liczba $\mathcal{R} - \mathcal{N}$ wynosi h albo $3h$ w zależności od tego, czy $q \equiv 7 \pmod{8}$, czy też $q \equiv 3 \pmod{8}$, a stąd oczywiście $\mathcal{R} > \mathcal{N}$! Pierwsze dowody wspomnianej równości dotyczącej $\mathcal{R} - \mathcal{N}$ podał Dirichlet w połowie XIX wieku, tworząc w ten sposób zręby analitycznej teorii liczb. Natomiast pierwszy całkowicie elementarny (to nie znaczy, że prosty!) dowód podał matematyk amator H.L.S. Orde w 1978 roku w artykule *On Dirichlet’s class number formula* (Journal of London Mathematical Society 18). Ten dowód można znaleźć w 5. rozdziale książki profesora Władysława Narkiewicza *Classical Problems in Number Theory* (PWN, Warszawa 1986).

Prawo wzajemności reszt kwadratowych orzeka, że jeśli p i q są liczbami pierwszymi i choć jedna z nich daje resztę 1 z dzielenia przez 4, to p jest resztą kwadratową modulo q wtedy i tylko wtedy, gdy q jest resztą kwadratową modulo p . Jeśli obie liczby dają resztę 3 z dzielenia przez 4, to p jest resztą kwadratową modulo q wtedy i tylko wtedy, gdy q nie jest resztą kwadratową modulo p .