O wielomianach przyjmujących wartości będące liczbami pierwszymi

Prof. dr Jerzy BROWKIN

Rozwiązanie zadania F 265.
Masa rozgrzanego do temperatury T powietrza wynosi $m = pV\mu/RT$. Siła wyporu działająca na balonik jest równa:

$$m_0 g = \frac{pV\mu g}{RT_0},$$

gdzie V jest objętością balonika, T_0 – temperaturą otaczającego powietrza, μ jego masą molową. Jeśli przez M oznaczymy teraz masę powłoki balonika, to stąd otrzymamy warunek wznoszenia się balonika:

$$m_0 g > (M + m)g.$$

Stąd

$$T > \frac{T_0}{1 - MRT_0/(pV\mu)}.$$

Dla $M \approx 5$g, średnicy $\approx 0,35$ m, $T_0 \approx 300$ K i $p \approx 10^5$ Pa otrzymujemy temperaturę graniczną

$$T \approx 500 \text{ K} \approx 200°\text{C},$$

powyżej której gorące powietrze uniesie balonik.

1. Weźmy wielomian $f(x) = x^2 + x + 5$. Mamy $f(0) = 5$, $f(1) = 7$, $f(2) = 11$, $f(3) = 17$. Są to liczby pierwsze. Ponieważ $f(x) = x \cdot (x+1) + 5$, więc, oczywiście, $f(4)$ jest liczbą złożoną, podzielną przez 5.

Można sformułować pytanie ogólne: dla jakich liczb pierwszych p wielomian

$$f(x) = x^2 + x + p$$

dla $x = 0, 1, \ldots, p-2$ przyjmuje wartości będące liczbami pierwszymi (jasne jest, że dla $x = p - 1$ liczba $f(x)$ jest złożona, podzielna przez p)?

Już dla $p = 7$ tak nie jest: Liczba $f(1) = 1^2 + 1 + 7 = 9$ jest złożona.

L. Euler wiedział już w 1772 roku, że wielomiany

$$x^2 + x + 3,\ x^2 + x + 5,\ x^2 + x + 11,\ x^2 + x + 17 \text{ i } x^2 + x + 41$$

mają powyższą własność. Od tego czasu nie znaleziono żadnego innego. Od roku 1966 wiadomo, że innych takich wielomianów nie ma.

Omówię w dalszym ciągu, jak to udowodniono. Przecież badanie wszystkich liczb pierwszych p po kolei nie może prowadzić do celu!

2. Niech d będzie ustaloną liczbą naturalną, niepodzielną przez kwadrat żadnej liczby naturalnej większej od 1. Rozpatrzmy zbiór liczb A_d określony następująco:

$$A_d = \begin{cases} \{a + b\sqrt{-d} \,:\, a, b \in \mathbf{C}\}, & \text{jeżeli } 4 \nmid d+1, \\ \{a + b\frac{1+\sqrt{-d}}{2} \,:\, a, b \in \mathbf{C}\}, & \text{jeżeli } 4 \mid d+1, \end{cases}$$

$\mathbf{C}$ oznacza tu zbiór zwykłych liczb całkowitych.

Tak więc na przykład: $A_1 = \{a + b\sqrt{-1} \,:\, a, b \in \mathbf{C}\}$,
$A_2 = \{a + b\sqrt{-2} \,:\, a, b \in \mathbf{C}\}$,

ale
$$A_3 = \left\{a + b\frac{1+\sqrt{-3}}{2} \,:\, a, b \in \mathbf{C}\right\},$$

ponieważ $4 \mid 3 + 1$.

Można łatwo sprawdzić, że suma, różnica i iloczyn liczb należących do zbioru A_d też należy do tego zbioru. Zbiór ten ma wiele własności podobnych do odpowiednich własności zbioru liczb całkowitych $\mathbf{C}$. Na przykład każdą liczbę z $\mathbf{C}$ można przedstawić w postaci iloczynu liczb nierozkładalnych na czynniki. Podobnie jest z liczbami każdego ze zbiorów A_d.

3. Z każdym zbiorem A_d wiąże się pewną liczbę naturalną zwaną liczbą klas, którą oznaczamy przez h_d lub po prostu przez h. Z grubsza mówiąc, jeżeli $h_d = 1$, to własności zbioru A_d są bardzo podobne do własności zbioru liczb całkowitych $\mathbf{C}$, a im liczba h_d jest większa, tym zbiór A_d jest bardziej skomplikowany. Na przykład $h_d = 1$ wtedy i tylko wtedy, gdy w zbiorze A_d każda liczba daje się przedstawić jednoznacznie w postaci iloczynu czynników nierozkładalnych.

W 1935 r. C.L. Siegel udowodnił, że $\lim\limits_{d\to\infty} h_d = \infty$. To znaczy, istnieje tylko skończona liczba takich liczb d, że $h_d = 1$, tylko skończona liczba takich liczb d, że $h_d = 2$, itd.

Już C.F. Gauss w 1801 r. udowodnił, że $h_d = 1$ dla $d = 1, 2, 3, 7, 11, 19, 43, 67$ i 163. Przypuszczano, że innych d o tej własności nie ma.

H. Heilbronn i E. Linfoot w 1934 r. udowodnili, że może być jeszcze co najwyżej jedna taka liczba d, że $h_d = 1$, tzw. hipotetyczna dziesiąta wartość d. Dopiero w 1967 r. H.M. Stark wykazał, że tej dziesiątej liczby nie ma, tzn. mamy $h_d = 1$ tylko dla dziewięciu liczb d znanych już Gaussowi.

4. Jaki jest związek między tymi własnościami liczb h_d a zagadnieniem rozpatrywanym na początku dotyczącym wielomianów przyjmujących wartości będące liczbami pierwszymi?

Otóż, F.G. Frobenius w 1912 r. i C. Rabinowitsch w 1913 r. udowodnili następujące twierdzenie: Wielomian $f(x) = x^2 + x + p$ przyjmuje dla $x = 0, 1, 2, \ldots, p-2$ wartości będące liczbami pierwszymi wtedy i tylko wtedy, gdy dla $d = 4p - 1$ mamy $h_d = 1$.

Stąd na mocy twierdzenia Starka o liczbach d, dla których $h_d = 1$, od razu wynika, że wielomiany znane Eulerowi wyczerpują wszystkie wielomiany o interesującej nas własności.

5. Wydawałoby się, że na tym problematyka ta została wyczerpana. A jednak nie! Można bowiem oczekiwać, iż z takimi liczbami d, że $h_d = 2$ lub $h_d = 3$ itd. można również związać pewne wielomiany kwadratowe, które dla $x = 0, 1, 2, \ldots, ?$ przyjmują tylko wartości będące liczbami pierwszymi.

d	przypadek	$f(x)$
5	II	$2x^2 + 2x + 3$
$6 = 2 \cdot 3$	I	$2x^2 + 3$
$10 = 2 \cdot 5$	I	$2x^2 + 5$
13	II	$2x^2 + 2x + 7$
$15 = 3 \cdot 5$	III	$3x^2 + 3x + 2$
$22 = 2 \cdot 11$	I	$2x^2 + 11$
$35 = 5 \cdot 7$	III	$5x^2 + 5x + 3$
37	II	$2x^2 + 2x + 19$
$51 = 3 \cdot 17$	III	$3x^2 + 3x + 5$
$58 = 2 \cdot 29$	I	$2x^2 + 29$
$91 = 7 \cdot 13$	III	$7x^2 + 7x + 5$
$115 = 5 \cdot 23$	III	$5x^2 + 5x + 7$
$123 = 3 \cdot 41$	III	$3x^2 + 3x + 11$
$187 = 11 \cdot 17$	III	$11x^2 + 11x + 7$
$235 = 5 \cdot 47$	III	$5x^2 + 5x + 13$
$267 = 3 \cdot 89$	III	$3x^2 + 3x + 23$
$403 = 13 \cdot 31$	III	$13x^2 + 13x + 11$
$427 = 7 \cdot 61$	III	$7x^2 + 7x + 17$

Istotnie, w 1974 r. M.D. Hendy uogólnił twierdzenie Frobeniusa–Rabinowitscha na przypadek $h = 2$. Wiadomo, że jeżeli $h_d = 2$, to liczba d musi być jednej z następujących postaci:

I. $d = 2p$, gdzie p jest liczbą pierwszą nieparzystą,
II. $d = q$ jest liczbą pierwszą spełniającą $4 \mid q - 1$,
III. $d = rs$, gdzie r i s są liczbami pierwszymi spełniającymi $r < s$ oraz $4 \mid r + s$.

W tych przypadkach Hendy rozpatruje, odpowiednio, następujące wielomiany:

I. $f(x) = 2x^2 + p, \quad x = 0, 1, 2, \ldots, p - 1,$
II. $f(x) = 2x^2 + 2x + p, \ p = \frac{q+1}{2}, \quad x = 0, 1, 2, \ldots, p - 2,$
III. $f(x) = rx^2 + rx + p, \ p = \frac{r+s}{4}, \quad x = 0, 1, 2, \ldots, p - 2.$

Hendy udowodnił, że $h_d = 2$ wtedy i tylko wtedy, gdy odpowiedni wielomian $f(x)$ dla wskazanych wartości x przyjmuje wartości będące liczbami pierwszymi.

W 1975 r. H.M. Stark wyznaczył wszystkie takie liczby d, że $h_d = 2$. Jest ich 18. W tabelce obok podane są te liczby i odpowiadające im wielomiany.

Tak więc z wyników Hendy'ego i Starka otrzymujemy na przykład, że tylko dla liczb pierwszych $p = 3, 5, 11$ i 29 wielomian $f(x) = 2x^2 + p$ ma tę własność, że dla $x = 0, 1, 2, \ldots, p - 1$ każda z liczb $f(x)$ jest pierwsza. Tę własność wielomianu $2x^2 + 29$ znał już L. Euler w 1772 r.

6. Ostatnio O. Radić znalazł kilka wielomianów postaci $kx^2 + kx + p$ oraz $2kx^2 + p$, które dla $x = 0, 1, 2, \ldots, p - 2$ i odpowiednio dla $x = 0, 1, 2, \ldots, p - 1$ przyjmują wartości będące liczbami pierwszymi. Są wśród nich pewne z wielomianów wymienionych wyżej, a także pewne inne, na przykład $6x^2 + 7$.

Wydaje się więc, że trzeba szukać jakichś uogólnień twierdzeń Frobeniusa, Rabinowitscha i Hendy'ego dla $h \geq 3$. Rozpatrzmy przypadek $h = 4$.

Wiadomo, że jeżeli $h_d = 4$, to liczba d musi być jednej z następujących postaci:

I. $d = 2pq$, gdzie p i q są różnymi liczbami pierwszymi,
II. $d = 2p$, gdzie p jest liczbą pierwszą nieparzystą,
III. $d = pq$, gdzie p i q są różnymi liczbami pierwszymi,
IV. $d = p$, gdzie p jest liczbą pierwszą nieparzystą,
V. $d = pqr$, gdzie p, q i r są różnymi liczbami pierwszymi.

Ograniczmy się do przypadku I. Z istniejących tablic liczb h_d dla $d \leq 500$ można wypisać wszystkie takie liczby d postaci I, że $h_d = 4$. Liczb takich jest 7. Zapewne innych takich liczb d nie ma, ale dotąd nikt tego nie udowodnił, tak jak to zrobił Stark dla $h = 1$ i $h = 2$.

Dla każdego takiego $d = 2pq$, gdzie $q < p$, rozpatrzmy wielomian $f(x) = 2qx^2 + p$. Okazuje się, że każdy z tych wielomianów $f(x)$ dla $x = 0, 1, 2, \ldots, p - 1$ przyjmuje wartości będące liczbami pierwszymi. Liczby d i odpowiadające im wielomiany podajemy w tabelce obok.

d	$f(x)$
$30 = 2 \cdot 3 \cdot 5$	$6x^2 + 5$
$42 = 2 \cdot 3 \cdot 7$	$6x^2 + 7$
$70 = 2 \cdot 5 \cdot 7$	$10x^2 + 7$
$78 = 2 \cdot 3 \cdot 13$	$6x^2 + 13$
$102 = 2 \cdot 3 \cdot 17$	$6x^2 + 17$
$130 = 2 \cdot 5 \cdot 13$	$10x^2 + 13$
$190 = 2 \cdot 5 \cdot 19$	$10x^2 + 19$

Dla $d = 42$ otrzymujemy wielomian podany przez Radicia. Równie dobrze można by tu rozpatrywać wielomiany $2px^2 + q$. Mają one analogiczną własność.

7. Co dalej? Oczywiście, można próbować zbadać analogicznie inne małe wartości h, choć dotąd nie zostały wyznaczone wszystkie takie liczby d, które odpowiadają danej wartości $h \geq 3$. Nie jest jednak jasne, jaki wielomian należy przyporządkować danej liczbie d. Jak widzieliśmy wyżej, budowa takiego wielomianu była różna w różnych przypadkach.

Interesujące, czy można pobić rekord Eulera, tzn. znaleźć wielomian postaci $kx^2 + kx + p$ lub $2kx^2 + p$, gdzie p jest liczbą pierwszą większą od 41, który dla $x = 0, 1, 2, \ldots, p - 2$ lub odpowiednio $x = 0, 1, 2, \ldots, p - 1$ przyjmowałby tylko wartości będące liczbami pierwszymi. Z pewnej ogólnej hipotezy A. Schinzla o wielomianach, tzw. hipotezy H, wynika, że taki wielomian istnieje.

8. Czytelnik pragnący uzyskać dokładniejsze informacje na tematy omawiane wyżej może sięgnąć do książek:

W. Narkiewicz, *Classical problems in number theory*, Warszawa 1986.
W. Sierpiński, *Elementary theory of numbers*, Warszawa 1987.