III Uniwersytecki Obóz Olimpiady Matematycznej
Bardo Śląskie, 11.2018

Równania diofantyczne i pierścień Gaussa $\mathbb{Z}[\mathrm{i}]$

Równania diofantyczne są postaci

$$f(x_1, \ldots, x_n) = 0,$$

gdzie f jest wielomianem. Dla przykładu:

$$x^k + y^k - z^k = 0, \qquad k \geq 2.$$

Celem jest odpowiedź na pytanie czy istnieją rozwiązania całkowite równania i jeżeli istnieją, to ich wyznaczenie. Jednym ze sposobów ich rozwiązywania jest metoda faktoryzacji.

1. Znajdź wszystkie rozwiązania całkowite równania

$$(x^2+1)(y^2+1) + 2(x-y)(1-xy) = 4(1+xy).$$

2. Niech p i q będą dwoma liczbami pierwszymi. Znajdź wszystkie dodatnie liczby całkowite x, y spełniające równanie

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{pq}.$$

3. (Indie) Wyznacz wszystkie nieujemne całkowite rozwiązania równania

$$(xy-7)^2 = x^2 + y^2$$

4. (OM) Rozwiąż równanie w liczbach całkowitych

$$x^2(y-1) + y^2(x-1) = 1.$$

5. Rozwiąż w liczbach całkowitych

$$x^2 + 6xy + 8y^2 + 3x + 6y = 2.$$

6. (Indie) Wyznacz wszystkie wartości n dla których równanie

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$$

ma dokładnie 5 rozwiązań w zbiorze liczb naturalnych.

7. (Rosja) Wyznacz wszystkie nieujemne całkowite rozwiązania równania

$$x^3 - y^3 = xy + 61.$$

8. Rozwiąż równanie diofantyczne

$$x - y^4 = 4$$

wiedząc, że x jest liczbą pierwszą.

9. (Rumunia) Rozwiąż w liczbach całkowitych

$$x^6 + 3x^3 + 1 = y^4.$$

10. (USA) Wyznacz wszystkie nieujemne całkowite rozwiązania równania

$$(x^2+y)(x+y^2) = (x-y)^3.$$

Liczby zespolone $\mathbb{C}$ są postaci $x + \mathrm{i}y$, gdzie $x, y \in \mathbb{R}$ oraz $\mathrm{i}^2 = -1$. **Liczby całkowite Gaussa** $\mathbb{Z}[\mathrm{i}]$ są postaci $a + \mathrm{i}b$, gdzie $a, b \in \mathbb{Z}$. Dla $a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ definiujemy **normę**:

$$N(a+b\mathrm{i}) = (a+b\mathrm{i})(a-b\mathrm{i}) = a^2 + b^2.$$

Element $\alpha \in \mathbb{Z}[\mathrm{i}]$ nazywamy **jednostką**, jeżeli istnieje $\beta \in \mathbb{Z}[\mathrm{i}]$ takie, że $\alpha\beta = 1$ (wówczas $\beta = \alpha^{-1}$).

11. Właściwości normy:

- $N(\alpha) = 0$ wtedy i tylko wtedy gdy $\alpha = 0$;
- $N(\alpha\beta) = N(\alpha)N(\beta)$.

12. W $\mathbb{Z}[\mathrm{i}]$ istnieją dokladnie 4 jednostki: $\{1, \mathrm{i}, -1, -\mathrm{i}\}$.

$\alpha \in \mathbb{Z}[\mathrm{i}]$ jest liczbą **pierwszą Gaussa** jeżeli $N(\alpha) > 1$ oraz z faktu, że $\alpha = \beta\gamma$ wynika, że β lub γ jest jednostką. Liczby pierwsze Gaussa: $1 + i$, 3, $2 + \mathrm{i}$, $2 - \mathrm{i}$, 7, 11, $2 + 3\mathrm{i}$, $2 - 3\mathrm{i}$. Liczby, które nie są liczbami pierwszymi Gaussa: $2 = (1 + \mathrm{i})(1 - \mathrm{i})$, $5 = (1 + 2\mathrm{i})(1 - 2\mathrm{i})$.

13. (Dzielenie z resztą w $\mathbb{Z}[\mathrm{i}]$) Dla każdych $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ i $\beta \neq 0$ istnieją $\gamma, \rho \in \mathbb{Z}[\mathrm{i}]$ takie, że

$$\alpha = \gamma \cdot \beta + \rho \qquad \text{oraz} \qquad N(\rho) < N(\beta).$$

Mówimy, że β **dzieli** α jeżeli istnieje $\gamma \in \mathbb{Z}[\mathrm{i}]$ tż. $\alpha = \beta\gamma$. Element $\delta \in \mathbb{Z}[\mathrm{i}]$ jest **największym wspólnym dzielnikiem (NWD)** liczb α i β, jeżeli δ jest elementem o największej normie takim, że $\delta|\alpha$ i $\delta|\beta$. NWD jest wyznaczone z dokładnością do mnożenia przez jednostkę i nie jest jedyne. NWD może zostać wyznaczony algorytmem Euklidesa.

14. Oblicz $\mathrm{NWD}(1 - 8\mathrm{i}, 5 + 5\mathrm{i})$.

15. $\alpha \in \mathbb{Z}[i]$ jest liczbą pierwszą Gaussa wtedy i tylko wtedy, gdy dla dowolnych $\beta, \gamma \in \mathbb{Z}[\mathrm{i}]$ jeżeli $\alpha|\beta\gamma$, to $\alpha|\beta$ lub $\alpha|\gamma$.

16. Liczba Gaussa ma parzystą normę wtedy i tylko wtedy, gdy dzieli się przez $1+\mathrm{i}$. Wniosek: Jeżeli $a+b\mathrm{i}$ jest liczbą pierwszą Gaussa o parzystej normie, to $a^2+b^2 = 2$ i z dokładnością do jednostki liczba ta wynosi $1+\mathrm{i}$.

17. Znajdź wszystkie liczby pierwsze Gaussa o normie co najwyżej 20.

18. Jeżeli $\alpha \in \mathbb{Z}[\mathrm{i}]$ jest liczbą pierwszą Gaussa, to istnieje liczba pierwsza $p \in \mathbb{Z}^+$ taka, że $\alpha|p$.

19. Jeżeli norma liczby $\alpha \in \mathbb{Z}[i]$ jest liczbą pierszą, to α jest liczbą pierwszą Gaussa.

20. Jeżeli p jest liczbą pierwszą taką, że $p = 3 \bmod 4$, to p jest liczbą pierwszą Gaussa (np. 3 i 7).

21. Liczba pierwsza p nie jest liczbą pierwszą Gaussa wtedy i tylko wtedy, gdy jest sumą dwóch kwadratów.
22. Jeżeli liczba pierwsza p nie jest liczbą pierwszą Gaussa oraz $p \neq 0$, to z dokładnością do mnożenia przez jednostkę, p jest iloczynem dwóch liczb pierwszych Gaussa, które są sprzeżone i mają normę p.
23. Niech p będzie liczbą pierwszą. Wówczas następujące warunki są równoważne

a) $p = 2$ lub $p = 1 \bmod 4$;

b) równanie $x^2 = -1 \bmod p$ ma rozwiązanie;

c) (Twierdzenie Fermata o sumie kwadratów) $p = a^2 + b^2$ jest sumą dwóch kwadratów.

24. Z dokładnością do mnożenia przez jednostki liczby pierwsze Gaussa są następującej postaci:

- $1 + i$ jest liczbą pierwszą Gaussa o normie 2;
- każda liczba pierwsza p taka, że $p = 3 \bmod 4$, jest liczbą pierwszą Gaussa o normie p^2;
- dla każdej liczby pierwszej takiej, że $p = 1 \bmod 4$ istnieje dokładnie jedna para liczb pierwszych Gaussa α i $\overline{\alpha}$ o normie p i takich, że $p = \alpha\overline{\alpha}$.

25. (**Zasadnicze twierdzenie arytmetyki dla** $\mathbb{Z}[\mathrm{i}]$). Niech P_0 oznacza zbiór wszystkich niestowarzyszonych liczb pierwszych Gaussa, tzn takich, że dla dowolnej liczby pierwszej Gaussa α w zbiorze P_0 jest tylko jedna liczba postaci $\delta\alpha$ dla pewnej jednostki δ. Wówczas każda liczba $\beta \in \mathbb{Z}[\mathrm{i}]$ może być jednoznacznie przedstawiona w postaci

$$\beta = \mathrm{i}^k \prod_{\pi \in P_0} \pi^{k_\pi}$$

dla pewnych $k \in \{0, 1, 2, 3\}$, $\pi_k \geq 0$. Tylko skończenie wiele współczynników k_π jest niezerowych.

26. (Fermat) Znajdź wszystkie całkowite rozwiązania równania

$$x^2 + 4 = y^3.$$

27. Znajdź wszystkie całkowite rozwiązania równania

$$x^5 - 1 = y^2.$$

28. Znajdź wszystkie trójki pitagorejskie, tzn. względnie pierwsze dodatnie całkowite rozwiązania równania

$$x^2 + y^2 = z^2$$

29. Załóżmy, że x, y, z są liczbami naturalnymi spełniającymi

$$xy = z^2 + 1.$$

Pokaż, że istnieją liczby całkowite a, b, c, d takie, że $x = a^2 + b^2$, $y = c^2 + d^2$ i $z = ac + bd$.

30. Rozwiąż równanie

$$x^2 + y^2 = z^n,$$

gdzie x, y są względnie pierwsze i $n \geq 3$.

31. Znajdź wszystkie czwórki (u, v, w, s) spełniające uogólnione równanie Pitagorasa

$$u^2 + v^2 + w^2 = s^2$$

32. Rozwiąż równanie w liczbach naturalnych

$$x^2 + 4 = y^n,$$

gdzie $n > 1$.

33. Wskaż nieskończenie wiele rozwiązań równania

$$x^2 + y^2 = z^3.$$

34. Niech $n = a \cdot b^2$ będzie liczbą całkowitą i a będzie liczbą bezkwadratową. Pokaż, że n jest sumą dwóch kwadratów wtedy i tylko wtedy, gdy żadna liczba pierwsza $q = 3 \bmod 4$ nie dzieli a.

35. (Bałkańska Olimpiada Matematyczna, 2018) Niech q będzie dodatnią liczbą wymierną. Dwie mrówki początkowo znajdują się w tym samym punkcie na płaszczyźnie. W n-tej minucie ($n \geq 1$) każda z nich decyduje, który z kierunków wybrać: północ, południe, wschód, czy zachód i przemieszcza się w tym kierunku o q^n metrów. Po pewnym (skończonym czasie) mrówki ponownie się spotkały mimo iż szły innymi ścieżkami. Wyznacz wszystkie możliwe wartości q.

(db)