Liczby pierwsze i złożone, liczby względnie pierwsze

Tomasz Kossakowski

7 listopada 2025

Liczby pierwsze od wieków fascynują matematyków. Po dzisiejszym wykładzie zafascynują one również Ciebie.

Definicje

Definicja 1 (liczby pierwsze)

Liczbą pierwszą nazywamy taką liczbę całkowitą p większą od 1, której jedynymi dodatnimi dzielnikami są 1 i p.

Zbiór liczb pierwszych zwykle oznaczany jest symbolem $\mathbb{P}$. Wtedy możemy powiedzieć, że

$$\mathbb{P} := \{p \in \mathbb{N} : a \mid p \implies a \in \{1, p\}\}.$$

Początek ciągu liczb pierwszych to:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 \text{ itd.}$$

Definicja 2 (liczby złożone)

Liczbę całkowitą dodatnią n nazywamy złożoną, wtedy i tylko wtedy, gdy można ją przedstawić w postaci iloczynu $n = ab$, dla pewnych liczb całkowitych $a, b > 1$.

Początek ciągu liczb złożonych to:

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 39,$$
$$40, 42, 44, 45, 46, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 60, 62, 63, 64, 65, 66, 68, 69, 70, 72,$$
$$74, 75, 76, 77, 78, 80, 81, 82, 84, 85, 86, 87, 88, 90, 91, 92, 93, 94, 95, 96, 98, 99, 100 \text{ itd.}$$

Twierdzenie 1 (rozkład liczby)

Niech $(p_1, p_2, p_3, \ldots) = (2, 3, 5, \ldots)$ będą wszystkimi liczbami pierwszymi w kolejności rosnącej. Wówczas każdą liczbę naturalną n można zapisać, na dokładnie jeden sposób, w postaci

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots$$

gdzie $\alpha_1, \alpha_2, \alpha_3, \ldots$ są nieujemnymi liczbami całkowitymi. Ten zapis nazywamy *rozkładem liczby n na czynniki pierwsze*.
Uwaga: W rozkładzie powyżej pomijamy zapisywanie czynników postaci p_i^0 równych 1. W ten sposób rozkład ten ma zawsze skończenie wiele czynników.

Innymi słowy, jeśli dane jest s liczb pierwszych $p_1, \ldots, p_s$ oraz k liczb pierwszych $q_1, \ldots, q_k$ spełniających warunek

$$p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_k,$$

to $s = k$ oraz liczby p_i są po zmianie kolejności równe liczbom q_i.

Z rozkładem na czynniki pierwsze związane są następujące własności.

1. Iloczyn liczb całkowitych jest podzielny przez liczbę pierwszą p wtedy i tylko wtedy, gdy któraś z nich jest podzielna przez p.

2. Jeżeli dodatnia liczba całkowita jest podzielna przez różne liczby pierwsze $p_1, p_2, \ldots, p_m$, to jest także podzielna przez ich iloczyn.
3. Jeśli liczby a, b są krotnościami liczby pierwszej p w rozkładzie na czynniki pierwsze liczb n, m, to krotność liczby p w rozkładzie na czynniki pierwsze liczby $n \cdot m$ równa jest $a + b$.
4. Liczba całkowita dodatnia n jest a-tą potęgą liczby całkowitej wtedy i tylko wtedy, gdy każda liczba pierwsza występuje w rozkładzie n na czynniki pierwsze w krotności podzielnej przez a.

Ćwiczenie 1. Udowodnij, że liczb pierwszych jest nieskończenie wiele.

Ćwiczenie 2. Udowodnij, że liczba $\sqrt{2}$ jest niewymierna.

Definicja 3 (liczby względnie pierwsze)

Dwie liczby całkowite a i b nazywamy *względnie pierwszymi* wtedy i tylko wtedy, gdy ich największy wspólny dzielnik[a] jest równy 1, co zapisujemy jako $\mathrm{NWD}(a, b) = 1$.

[a] *Największym wspólnym dzielnikiem* dodatnich liczb całkowitych a i b nazywamy największą liczbę naturalną d taką, że $d \mid a$ i $d \mid b$. Oznaczamy go przez $\gcd(a, b)$ lub $\mathrm{NWD}(a, b)$.

Zauważmy, że dla każdego $p, r \in \mathbb{P}$, gdzie $p \neq r$ zachodzi $\mathrm{NWD}(p, r) = 1$.

Ćwiczenie 3. Niech a, b będą względnie pierwsze. Udowodnij, że jeżeli $a \mid c$ oraz $b \mid c$ to $ab \mid c$.

Lemat 1 (liczba dzielników iloczynu liczb względnie pierwszych)

Jeśli $\mathrm{NWD}(a, b) = 1$, to

$$\tau(a \cdot b) = \tau(a) \cdot \tau(b)$$

gdzie $\tau(n)$ oznacza liczbę dodatnich dzielników liczby n.

Lemat 2 (wzór na liczbę dzielników)

Niech $n > 1$ będzie liczbą naturalną o rozkładzie na czynniki pierwsze:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

gdzie $p_1, p_2, \ldots, p_k$ są różnymi liczbami pierwszymi, a $\alpha_1, \alpha_2, \ldots, \alpha_k$ są liczbami naturalnymi.
Wówczas liczba dodatnich dzielników liczby n wyraża się wzorem:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1),$$

gdzie $\tau(n)$ oznacza liczbę dodatnich dzielników liczby n.

Ćwiczenie 4. Udowodnij *lemat 2.*

Ćwiczenie 5. Czy istnieje liczba dodatnia o dokładnie 2025 dodatnich dzielnikach?

Ćwiczenie 6. Udowodnij, że jeżeli liczba dzielników liczby naturalnej n jest nieparzysta, to n jest kwadratem liczby naturalnej.

Lemat 3 (wzór na sumę dzielników)

Jeśli $n \in \mathbb{N}$ ma rozkład na czynniki pierwsze postaci $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, to

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1},$$

gdzie $\sigma(n)$ oznacza sumę dzielników liczby n.

Ćwiczenie 7. Udowodnij *lemat 3.*

Zadania

Zadanie 1. Wyznacz wszystkie liczby pierwsze p, dla których $p+4$ jest kwadratem liczby naturalnej.

Zadanie 2. Wyznacz wszystkie dodatnie liczby całkowite, które mają dokładnie trzy dodatnie dzielniki.

Zadanie 3. Wyznacz wszystkie liczby pierwsze p, dla których liczba

$$p^3 + p^2 + p - 3$$

również jest pierwsza.

Zadanie 4. Czy istnieje taka liczba całkowita $n > 2$, że liczba $n!$ ma dokładnie 101 dodatnich dzielników?

Zadanie 5 (10 OMJ-III-1)**.** Udowodnij, że każdą liczbę całkowitą większą od 5 można przedstawić w postaci sumy liczby pierwszej i liczby złożonej.

Zadanie 6. Udowodnij, że jeżeli $p \in \mathbb{P}$, $k \in \mathbb{N}$ oraz $0 < k < p$, to $\binom{p}{k}$ jest podzielne przez p.

Zadanie 7. Niech a, b, c i d będą dodatnimi liczbami całkowitymi takimi, że $ab = cd$. Pokaż, że istnieją dodatnie liczby całkowite p, q, r, s takie, że

$$a = pq, \quad b = rs, \quad c = pr, \quad d = qs.$$

Zadanie 8 (16OM-II-4)**.** Znaleźć wszystkie takie liczby pierwsze p, że $4p^2+1$ i $6p^2+1$ są również liczbami pierwszymi.

Zadanie 9 (15OMJ-II-5)**.** Dane są dodatnie liczby całkowite a, b o następującej własności: dla każdej liczby naturalnej $n \geqslant 1$ ułamek

$$\frac{a+n}{b+n}$$

jest skracalny. Wykaż, że $a = b$.

Zadanie 10 (76OM-I-3)**.** Dana jest dodatnia liczba całkowita n będąca iloczynem 2024 różnych liczb pierwszych. Wyznaczyć liczbę dodatnich liczb całkowitych k spełniających równość

$$n + \mathrm{NWD}(n, k) = k.$$

Zadanie 11. Wykaż, że nie istnieje taka trójka parami różnych liczb pierwszych (p, q, r), że liczba

$$\frac{(p+q)(q+r)(r+p)}{pqr}$$

jest całkowita.

Zadanie 12. Rozwiąż równanie $p^p + q^q = r^r$ w liczbach pierwszych p, q, r.

Zadanie 13 (64OM-I-3)**.** Niech n będzie dodatnią liczbą całkowitą. Wykazać, że jeżeli suma wszystkich jej dodatnich dzielników jest nieparzysta, to liczba n jest kwadratem lub podwojonym kwadratem liczby całkowitej.

Zadanie 14 (Irańska OM 2005-II-1)**.** Niech $n, p > 1$ będą dodatnimi liczbami całkowitymi i niech p będzie liczbą pierwszą. Zakładając, że $n \mid p-1$ oraz $p \mid n^3 - 1$, udowodnij, że $4p-3$ jest kwadratem liczby całkowitej.

Zadanie 15 (55OM-II-4)**.** Wyznaczyć wszystkie dodatnie liczby całkowite n, mające dokładnie $\sqrt{n}$ dodatnich dzielników.

Zadanie 16 (73OM-II-3)**.** Dodatnie liczby całkowite a, b, c spełniają równość

$$a^3 + 4b + c = abc,$$

przy czym $a \geqslant c$ oraz liczba $p = a^2 + 2a + 2$ jest pierwsza. Wykazać, że p jest dzielnikiem liczby $a + 2b + 2$.

Zadanie 17 (IMO 1959, P1)**.** Udowodnij, że dla dowolnego $n \in \mathbb{N}$ ułamek

$$\frac{21n+4}{14n+3}$$

jest nieskracalny.

Rozwiązania ćwiczeń

Rozwiązanie 1. Przypuśćmy nie wprost, że liczb pierwszych jest skończenie wiele. Oznaczmy te liczby jako $p_1, p_2, \ldots, p_n$. Wiemy, że 2 jest liczbą pierwszą, więc $n \geqslant 1$. Rozpatrzmy liczbę

$$K = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Zauważmy, że jest ona większa od 1.
Liczba $p_1 \cdot p_2 \cdot \ldots \cdot p_n$ jest podzielna przez p_i dla $i \in \{1, \ldots, n\}$. Stąd K nie jest podzielna przez żadną z liczb pierwszych. Jednakże każda liczba całkowita większa od 1 jest podzielna przez jakąś liczbę pierwszą. Otrzymana sprzeczność kończy dowód.

Rozwiązanie 2. Załóżmy nie wprost, że istnieją takie liczby całkowite dodatnie p, q, że zachodzi równość

$$\sqrt{2} = \frac{p}{q}.$$

Przekształcając powyższą równość równoważnie, otrzymujemy

$$p^2 = 2q^2.$$

Niech

$$p = 2^\alpha a \quad \text{i} \quad q = 2^\beta b,$$

gdzie a, b są liczbami nieparzystymi. Innymi słowy, α i β będą wykładnikami przy dwójce w rozkładzie odpowiednio p i q na czynniki pierwsze. Zauważmy, że dana równość jest równoważna równości

$$2^{2\alpha} a^2 = 2^{2\beta+1} b^2.$$

Skoro a i b są nieparzyste, to wykładnik przy dwójce w rozkładzie na czynniki pierwsze wynosi odpowiednio 2α i $2\beta + 1$ dla odpowiednio lewej i prawej strony. Wiemy, że jeśli pewne dwie liczby są równe, to wykładniki przy tych samych liczbach pierwszych są sobie równe, czyli

$$2\alpha = 2\beta + 1.$$

Jednak lewa strona powyższej równości jest parzysta, a prawa nie. Otrzymana sprzeczność dowodzi, że $\sqrt{2}$ jest liczbą niewymierną.

Rozwiązanie 3. Ponieważ $\gcd(a, b) = 1$, rozkłady liczb a i b na czynniki pierwsze nie mają wspólnych liczb pierwszych.
Niech c będzie taką liczbą, że $a \mid c$ i $b \mid c$. W rozkładzie na czynniki pierwsze, c musi zawierać wszystkie czynniki pierwsze z a i wszystkie czynniki pierwsze z b z odpowiednimi wykładnikami.
Zatem c zawiera wszystkie czynniki pierwsze z ab, co oznacza że $ab \mid c$.

Rozwiązanie 4. Każdy dodatni dzielnik d liczby n ma postać:

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

gdzie wykładniki β_i spełniają nierówności:

$$0 \leqslant \beta_1 \leqslant \alpha_1, \quad 0 \leqslant \beta_2 \leqslant \alpha_2, \quad \ldots, \quad 0 \leqslant \beta_k \leqslant \alpha_k$$

Dla każdej liczby pierwszej p_i wykładnik β_i może przyjmować $\alpha_i + 1$ różnych wartości: $0, 1, 2, \ldots, \alpha_i$.
Ponieważ wybory wykładników dla różnych liczb pierwszych są niezależne, na mocy reguły mnożenia, łączna liczba możliwych kombinacji wykładników wynosi:

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

Każda taka kombinacja wyznacza dokładnie jeden dzielnik liczby n, zatem:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

co kończy dowód.

Rozwiązanie 5. Tak, np. $\tau\left(2^{2024}\right) = 2025$.

Rozwiązanie 6. Niech $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ będzie rozkładem liczby n na czynniki pierwsze.
Wówczas liczba dzielników wynosi:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

Jeśli $\tau(n)$ jest nieparzysta, to każdy czynnik $(\alpha_i + 1)$ musi być nieparzysty. Zatem każdy α_i musi być parzysty.
Niech $\alpha_i = 2\beta_i$ dla $i = 1, 2, \ldots, k$. Wtedy:

$$n = p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k} = \left(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}\right)^2$$

czyli n jest kwadratem liczby naturalnej.

Rozwiązanie 7. Każdy dzielnik naturalny liczby n można przedstawić w postaci:

$$d = p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k},$$

gdzie:

$$\lambda_i \in \mathbb{Z},\ 0 \leqslant \lambda_i \leqslant \alpha_i. \tag{1}$$

Ponieważ różnym układom liczb $\lambda_1 \ldots \lambda_k$ spełniającym (1) odpowiadają różne dzielniki n, więc:

$$\sigma(n) = \sum p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k}, \tag{2}$$

gdzie sumowanie rozciąga się na wszystkie układy liczb całkowitych spełniające (1).
Każdy składnik sumy (2) występuje dokładnie raz, dlatego tę sumę można „zwinąć" do postaci iloczynowej:

$$\sigma(n) = \left(1 + p_1^1 + \ldots + p_1^{\alpha_1}\right)\left(1 + p_2^1 + \ldots + p_2^{\alpha_2}\right) \ldots \left(1 + p_k^1 + \ldots + p_k^{\alpha_k}\right).$$

Z kolei i-ty czynnik powyższego iloczynu jest skończoną sumą szeregu geometrycznego o ilorazie p_i, więc

$$1 + p_i^1 + \ldots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}.$$

Stąd teza.

Rozwiązania zadań

Rozwiązanie 1. Szukamy liczb pierwszych p spełniających równanie $p + 4 = n^2$ dla pewnej liczby naturalnej n. Po przekształceniu tego równania i skorzystaniu ze wzoru skróconego mnożenia, uzyskujemy rozkład liczby p na czynniki:

$$p = n^2 - 4 = (n - 2)(n + 2).$$

Przypomnijmy, że p jako liczba pierwsza ma dokładnie dwa dzielniki naturalne: 1 i p. Czynnik $n + 2$ jest liczbą naturalną większą od 1, dlatego $n + 2 = p$. Drugi czynnik jest więc równy 1. Otrzymujemy układ równań

$$\begin{cases} n + 2 = p \\ n - 2 = 1, \end{cases}$$

którego rozwiązaniem jest para liczb $n = 3$ i $p = 5$. Zatem jedyną liczbą spełniającą warunki zadania jest $p = 5$.

Rozwiązanie 2. Z ćwiczenia 5 wiemy, że każda liczba dodatnia n o nieparzystej liczbie dodatnich dzielników jest kwadratem liczby całkowitej. Zatem jeśli n ma dokładnie trzy dzielniki, to $n = k^2$ dla pewnej liczby całkowitej k. Jeżeli liczba k jest pierwsza, to n ma dokładnie trzy dzielniki: 1, k, n. W przeciwnym przypadku dowolny dzielnik pierwszy liczby k jest kolejnym dzielnikiem liczby n. Wobec tego dokładnie trzy dodatnie dzielniki mają te i tylko te dodatnie liczby całkowite, które są kwadratami liczb pierwszych.

Rozwiązanie 3. Rozważmy najpierw przypadek, w którym p jest liczbą parzystą, czyli $p = 2$. Wówczas

$$p^3 + p^2 + p - 3 = 8 + 4 + 2 - 3 = 11,$$

więc $p = 2$ spełnia warunki zadania.
W sytuacji, gdy p jest liczbą nieparzystą, liczba

$$p^3 + p^2 + p - 3$$

jest parzysta, czyli

$$p^3 + p^2 + p - 3 = 2.$$

Po przekształceniach otrzymujemy równanie

$$p(p^2 + p + 1) = 5.$$

Ponieważ 5 jest liczbą pierwszą oraz liczby p i $p^2 + p + 1$ są większe od 1, to powyższe równanie nie ma rozwiązań. Jedyną liczbą spełniającą warunki zadania jest zatem liczba $p = 2$.

Rozwiązanie 4. Nie. Dla $n > 2$ liczba $n!$ ma przynajmniej dwa różne czynniki pierwsze w rozkładzie: 2 i 3. Wówczas liczba dzielników $n!$ jest złożona, zatem nie może być równa 101.

Rozwiązanie 5. Zauważmy, że jeżeli $n \geqslant 6$ jest liczbą parzystą, to $n - 2$ jest liczbą parzystą większą od 2, a więc liczbą złożoną. Stąd otrzymujemy przedstawienie $n = 2 + (n-2)$ liczby n jako sumy liczby pierwszej i liczby złożonej. Podobnie, jeśli $n \geqslant 6$ jest liczbą nieparzystą, to $n - 3$ jest liczbą parzystą większą od 2, a więc liczbą złożoną. Wobec tego $n = 3 + (n - 3)$ to szukane przedstawienie liczby n w postaci sumy liczby pierwszej i liczby złożonej.

Rozwiązanie 6. W tym celu zapiszmy

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p \cdot \frac{(p-1)(p-2)\dots(p-k+1)}{k(k-1)\dots 1} = pS.$$

Teraz p dzieli to wyrażenie, jeśli S jest liczbą całkowitą. Oto sedno sprawy: wiemy, że pS jest liczbą całkowitą. Ponieważ p jest względnie pierwsze ze wszystkimi liczbami $k, k-1, \dots, 1$, zatem p nie wnosi żadnego wkładu w to, aby pS było liczbą całkowitą. Stąd S musi być liczbą całkowitą, co kończy dowód.

Rozwiązanie 7. Skoro

$$\frac{a}{c} = \frac{d}{b},$$

zatem oba ułamki są równe pewnemu wspólnemu ułamkowi nieskracalnemu, powiedzmy $\frac{q}{s}$, gdzie $\gcd(q, s) = 1$. Wtedy $(a, c) = (pq, ps)$ dla pewnego p oraz $(b, d) = (rs, rq)$ dla pewnego r. To kończy dowód.

Rozwiązanie 8. Do rozwiązania zadania dojdziemy badając podzielność liczb $u = 4p^2 + 1$ i $v = 6p^2 + 1$ przez 5. Wiadomo, że reszta z dzielenia przez liczbę naturalną iloczynu dwóch liczb całkowitych równa się reszcie z dzielenia przez ową liczbę iloczynu ich reszt. Na tej podstawie znajdziemy łatwo, co następuje:

$$\begin{array}{llll}
\text{Gdy } p \equiv 0 \pmod 5, & \text{wtedy } u \equiv 1 \pmod 5, & v \equiv 1 \pmod 5;\\
\text{Gdy } p \equiv 1 \pmod 5, & \text{wtedy } u \equiv 0 \pmod 5, & v \equiv 2 \pmod 5;\\
\text{Gdy } p \equiv 2 \pmod 5, & \text{wtedy } u \equiv 2 \pmod 5, & v \equiv 0 \pmod 5;\\
\text{Gdy } p \equiv 3 \pmod 5, & \text{wtedy } u \equiv 2 \pmod 5, & v \equiv 0 \pmod 5;\\
\text{Gdy } p \equiv 4 \pmod 5, & \text{wtedy } u \equiv 0 \pmod 5, & v \equiv 2 \pmod 5.
\end{array}$$

Z powyższego wynika, że liczby u i v mogą być obie liczbami pierwszymi tylko wtedy, gdy $p \equiv 0 \pmod 5$, tzn. gdy $p = 5$, ponieważ p ma być liczbą pierwszą. W tym przypadku $u = 4 \cdot 5^2 + 1 = 101$, $v = 6 \cdot 5^2 + 1 = 151$, więc są to istotnie liczby pierwsze.
Zatem jedynym rozwiązaniem zadania jest liczba $p = 5$.

Rozwiązanie 9. Przypuśćmy, że $a \neq b$. Przyjmijmy, bez straty ogólności, że $a > b$. Ponieważ liczb pierwszych jest nieskończenie wiele, więc istnieje taka dodatnia liczba naturalna n, że liczba $p = a + n$ jest pierwsza. Wtedy ułamek

$$\frac{a+n}{b+n}$$

można skrócić jedynie przez p. Jednak liczba $b+n$ nie może być podzielna przez p, gdyż $b+n < a+n = p$. Uzyskaliśmy sprzeczność, z której wynika, że $a = b$.

Rozwiązanie 10. Udowodnimy, że liczba k spełnia równość $n + \mathrm{NWD}(n, k) = k$ wtedy i tylko wtedy, gdy $k = n + d$ dla pewnego dzielnika d liczby n.
Z jednej strony, jeśli $k = n + \mathrm{NWD}(n, k)$, to k jest postulowanej postaci, bowiem $\mathrm{NWD}(n, k)$ dzieli n.
Z drugiej strony, dla dowolnej liczby k postaci $n + d$, gdzie d dzieli n, mamy

$$n + \mathrm{NWD}(n, k) = n + \mathrm{NWD}(n, n + d) = n + \mathrm{NWD}(n, d) = n + d = k.$$

To oznacza, że liczb k spełniających równość z zadania jest tyle samo ile jest dzielników liczby n. Ponieważ n jest iloczynem 2024 różnych liczb pierwszych, więc ma 2^{2024} dzielników.

Rozwiązanie 11. Załóżmy, że istnieją takie parami różne liczby pierwsze p, q i r, dla których liczba

$$\frac{(p+q)(q+r)(r+p)}{pqr}$$

jest całkowita.
Gdyby $p \mid p+q$, to wówczas $p \mid q$, co rzecz jasna przeczy temu, że p i q są różnymi liczbami pierwszymi. Stąd liczba p nie dzieli liczby $p+q$. Analogicznie dowodzimy, że p nie dzieli liczby $p+r$. Wiemy, że zachodzi podzielność

$$p \mid (p+q)(q+r)(r+p).$$

Skoro p dzieli jeden z czynników, to $p \mid q+r$, skąd

$$p \mid p+q+r.$$

Analogicznie dowodzimy, że

$$q \mid p+q+r$$

oraz

$$r \mid p+q+r.$$

Skoro liczby p, q i r są różnymi liczbami pierwszymi, to na mocy powyższych podzielności możemy stwierdzić, że

$$pqr \mid p+q+r.$$

Załóżmy, bez straty ogólności, że p jest największą z liczb p, q i r. Otrzymujemy ciąg nierówności

$$pqr > p \cdot 2 \cdot 2 = 4p > 3p > p+q+r,$$

co jest sprzeczne z wcześniej otrzymaną podzielnością.

Rozwiązanie 12. Gdyby liczby p, q, r były większe od 2, to skoro są pierwsze, musiałyby być nieparzyste. Wtedy jednak $2 \mid p^p + q^q$, co jest niemożliwe, gdy $2 \nmid r^r$. Oznacza to, że co najmniej jedna z liczb p, q, r jest równa 2. Skoro p, q, r są pierwsze, to $p, q \geqslant 2$, więc $r^r = p^p + q^q \geqslant 8$. Nie może zajść więc $r = 2$. W takim razie $p = 2$ lub $q = 2$. Bez straty ogólności załóżmy, że $p = 2$. Pozostaje rozwiązać równanie

$$4 + q^q = r^r.$$

Zauważmy, że skoro $r^r > q^q$, to $r > q$, więc też $r \geqslant q+1$. Zatem

$$r^r \geqslant r^{q+1} > q^{q+1}.$$

Łącząc otrzymane zależności, otrzymujemy

$$q^q + 4 > q^{q+1},$$

i w konsekwencji

$$q^q(q-1) < 4.$$

Jednakże $q - 1 \geqslant 1$ oraz

$$q^q \geqslant 2^2 = 4,$$

więc

$$(q-1)q^q \geqslant 4,$$

co jest sprzeczne z otrzymaną wcześniej nierównością.
Otrzymana sprzeczność dowodzi, że nie istnieje trójka liczb pierwszych (p, q, r) spełniająca daną równość.

Rozwiązanie 13. *Sposób 1:* Oznaczmy przez k wykładnik przy 2 w rozkładzie na czynniki pierwsze liczby n. Wówczas

$$n = 2^k \cdot l,$$

gdzie k jest nieujemną liczbą całkowitą, l zaś — dodatnią liczbą nieparzystą.
Suma parzystych dzielników liczby n jest parzysta, jeśli więc suma wszystkich dodatnich dzielników liczby n jest nieparzysta, to nieparzystych dzielników jest nieparzyście wiele.
Liczba l, jako nieparzysta, ma wyłącznie nieparzyste dzielniki oraz każdy z nich jest też dzielnikiem liczby n. Również na odwrót, każdy nieparzysty dzielnik liczby n musi być także dzielnikiem liczby l. Wobec tego nieparzyste dzielniki

liczby n to wszystkie dzielniki liczby l. Skoro jest ich nieparzyście wiele, to wnioskujemy, iż liczba l jest kwadratem pewnej liczby całkowitej m.
Oznacza to, że

$$n = 2^k \cdot l = 2^k \cdot m^2.$$

Jeśli liczba k jest parzysta, to liczba $\frac{k}{2}$ jest całkowita nieujemna i wówczas n jest kwadratem:

$$n = \left(2^{\frac{k}{2}} \cdot m\right)^2.$$

Jeśli zaś liczba k jest nieparzysta, to liczba $\frac{k-1}{2}$ jest całkowita nieujemna i wtedy n jest podwojonym kwadratem:

$$n = 2 \cdot \left(2^{\frac{k-1}{2}} \cdot m\right)^2.$$

To kończy dowód.
Sposób 2: Jeśli $n = 1$, to n jest kwadratem. Niech teraz $n > 1$. Przedstawmy liczbę n w postaci rozłożonej na czynniki pierwsze, wtedy na mocy twierdzenia 5 suma jej dodatnich dzielników równa jest

$$(1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \ldots + p_2^{\alpha_2}) \cdot \ldots \cdot (1 + p_j + p_j^2 + \ldots + p_j^{\alpha_j}).$$

Skoro iloczyn ten jest nieparzysty, to każdy jego czynnik jest nieparzysty.
Jeśli $p_1 = 2$, to czynnik $1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1}$ jest liczbą nieparzystą niezależnie od wartości α_1. Z kolei dla każdej nieparzystej liczby pierwszej p_i jej kwadrat, sześcian itd. również są nieparzyste, więc suma $1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i}$ jest nieparzysta wtedy i tylko wtedy, gdy ma nieparzystą liczbę składników, czyli gdy wykładnik α_i jest parzysty.
Oznacza to, że w rozkładzie na czynniki pierwsze liczby n wszystkie czynniki nieparzyste występują w parzystych potęgach. Otrzymujemy stąd wniosek, że

$$n = 2^k \cdot m^2,$$

gdzie k jest liczbą całkowitą nieujemną, m zaś — dodatnią liczbą całkowitą. Wobec tego $n = \left(2^{\frac{k}{2}} \cdot m\right)^2$, jeśli liczba k jest parzysta, oraz $n = 2 \cdot \left(2^{\frac{k-1}{2}} \cdot m\right)^2$, jeśli liczba k jest nieparzysta.
To kończy dowód.

Rozwiązanie 14. W tego typu problemach staramy się wydobyć jak najwięcej informacji poprzez ograniczanie i upraszczanie wielokrotności. Zatem: $n \mid p - 1$ implikuje $p \geqslant n + 1$ oraz $p = nk + 1$ dla pewnego $k \in \mathbb{Z}_+$. Ponadto $p \mid (n-1)(n^2 + n + 1)$ implikuje $p \mid n - 1$ lub $p \mid n^2 + n + 1$. Jednakże $p \mid n - 1$ jest niemożliwe. Zatem $p \mid n^2 + n + 1$. To daje $p \leqslant n^2 + n + 1$. Dalej,

$$nk + 1 \mid n^2 + n + 1 \mid kn^2 + kn + k \implies nk + 1 \mid kn^2 + kn + k - n(nk + 1) = nk + k - n.$$

Zatem $nk + 1 \leqslant nk + k - n \implies n + 1 \leqslant k$. W zależności od p oznacza to $n(n + 1) + 1 \leqslant nk + 1 = p$. Czy to coś przypomina? Wcześniej mieliśmy $p \leqslant n^2 + n + 1$. Zatem zachodzi $p = n^2 + n + 1$. To bezpośrednio daje $4p - 3 = (2n + 1)^2$.

Rozwiązanie 15. Oczywiście n jest nieparzystym kwadratem. Niech $n = p_1^{2a_1} p_2^{2a_2} \ldots p_k^{2a_k}$, wtedy

$$\sqrt{n} = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} = (2a_1 + 1)(2a_2 + 1) \ldots (2a_k + 1).$$

Teraz $p_i \geqslant 3$ dla wszystkich i, co oznacza że $p_i^{a_i} \geqslant 3^{a_i} \geqslant 2a_i + 1$ gdy $a_i \geqslant 1$. Zatem równość musi zachodzić wszędzie, tzn. $p_i = 3$ oraz $3^{a_i} = (2a_i + 1)$, co prowadzi do jedynego rozwiązania $n = 9$.
Należy również sprawdzić przypadek $n = 1$, który jest rozwiązaniem, gdyż $\sqrt{1} = 1$ i liczba 1 ma dokładnie 1 dodatni dzielnik.
Odpowiedź: Jedynymi rozwiązaniami są $n = 1$ i $n = 9$.

Rozwiązanie 16. Ponieważ $b(ac - 4) = a^3 + c$, więc $ac - 4 > 0$. Zatem

$$b = \frac{a^3 + c}{ac - 4}.$$

Należy więc wykazać, że liczba

$$a + 2 \cdot \frac{a^3 + c}{ac - 4} + 2 = \frac{a^2c - 4a + 2a^3 + 2c + 2ac - 8}{ac - 4}$$

dzieli się przez p. Ponieważ $c \leqslant a$, więc $ac - 4 < a^2 < a^2 + 2a + 2 = p$. W szczególności $\mathrm{NWD}(p, ac-4) = 1$, więc wystarczy dowieść, że liczba $a^2c - 4a + 2a^3 + 2c + 2ac - 8$ dzieli się przez p. Wynika to z następującego rachunku:

$$\begin{aligned} a^2c - 4a + 2a^3 + 2c + 2ac - 8 &= c(a^2 + 2a + 2) + 2a^3 - 4a - 8 \\ &= cp + 2(a^2 + 2a + 2)(a - 2) \\ &= p(c + 2a - 4). \end{aligned}$$

Rozwiązanie 17. Zauważmy, że:

$$\frac{21n+4}{14n+3} = \frac{(14n+3)+(7n+1)}{14n+3} = 1 + \frac{7n+1}{14n+3}$$

Zatem wynika z tego, że $7n+1$ i $14n+3$ muszą być względnie pierwsze dla każdej liczby naturalnej n, aby ułamek był nieskracalny. Teraz problem sprowadza się do udowodnienia, że $\frac{7n+1}{14n+3}$ jest nieskracalny. Przekształcamy ten ułamek jako:

$$\frac{7n+1}{(7n+1)+(7n+1)+1} = \frac{7n+1}{2(7n+1)+1}$$

Ponieważ mianownik $2(7n+1)+1$ różni się od wielokrotności licznika $7n+1$ o 1, licznik i mianownik muszą być względnie pierwszymi liczbami naturalnymi. Stąd wynika, że $\frac{21n+4}{14n+3}$ jest nieskracalny.