Podzielność

Rozkład na czynniki pierwsze

1. Udowodnij, że jeśli $a^n | b^{n+1}$ dla pewnych liczb całkowitych a, b i wszystkich liczb całkowitych dodatnich n, to $a|b$.

   Rozwiązanie: W rozkładzie na czynniki pierwsze otrzymujemy $nk_i \leq (n+1)l_i$ dla wszystkich n, skąd $k_i \leq l_i$.

2. Przez jaką najwyższą potęgę liczby pierwszej p dzieli się $n!$, gdzie n jest liczbą całkowitą nieujemną?

   Rozwiązanie: $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ...$

3. Udowodnij, że $\frac{(k+l)!}{k!l!}$ jest liczbą całkowitą dla dowolnych całkowitych nieujemnych k, l.

   Rozwiązanie: Ponieważ $\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$, dla dowolnej liczby pierwszej p i $j \geq 1$, w liczniku jest co najmniej tyle samo czynników podzielnych przez p^j co w mianowniku.

4. [14MOM] Niech m, n będą dowolnymi nieujemnymi liczbami całkowitymi. Udowodnij, że $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ jest liczbą całkowitą.

   Rozwiązanie: Ponieważ $\lfloor 2x+2y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x+y \rfloor$, dla dowolnej liczby pierwszej p i $j \geq 1$, w liczniku jest co najmniej tyle samo czynników podzielnych przez p^j co w mianowniku.

5. Uzasadnij, że najmniejsza wspólna wielokrotność liczb $1, 2, ..., 2n$ jest podzielna przez $\binom{2n}{n}$.

   Rozwiązanie: $\left(\left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor\right) + \left(\left\lfloor \frac{2n}{p^2} \right\rfloor - 2\left\lfloor \frac{n}{p^2} \right\rfloor\right) + ... \leq \#\left\{j : \frac{2n}{p^j} \geq 1\right\} = \max\left\{j : \frac{2n}{p^j \geq 1}\right\}$.

6. [55OM] Wyznaczyć wszystkie liczby całkowite dodatnie n, mające dokładnie $\sqrt{n}$ dzielników dodatnich.

   Rozwiązanie: Musi być $n = p_1^{2k_1}...p_m^{2k_m}$ i $p_1^{k_1}...p_m^{k_m} = (1+2k_1)...(1+2k_n)$. Stąd wszystkie p_i są nieparzyste. Skoro $p_i^{k_i} > 1+(p_i-1)k_i$ gdy $p_i > 3$ lub $k_i > 1$, musi być $p_i = 3$ i $k_i = 1$, a więc $n = 3$. Osobno trzeba rozważyć $n = 1$.

7. [56OM] Wyznaczyć wszystkie dodatnie liczby całkowite n, dla których n^n+1 oraz $(2n)^{2n}+1$ są liczbami pierwszymi.

   Rozwiązanie: Gdy n ma nieparzysty czynnik pierwszy, to n^n+1 jest złożona; zatem $n = 2^k$. Wobec tego $k2^k$ oraz $(k+1)2^{k+1}$ nie mogą mieć nieparzystego czynnika pierwszego, skąd $k \in \{0, 1\}$, czyli $n \in \{1, 2\}$. Obie te liczby spełniają warunki zadania.

8. [57OM] Niech c będzie ustaloną liczbą całkowitą dodatnią. Ciąg (a_n) jest określony przez warunki $a_1 = 1$, $a_{n+1} = d(a_n)+c$ dla $n = 1, 2, ...$, gdzie $d(m)$ oznacza liczbę dodatnich dzielników liczby m. Wykazać, że istnieje taka liczba całkowita dodatnia k, że ciąg $a_k, a_{k+1}, a_{k+2}, ...$ jest okresowy.

   Rozwiązanie: Wystarczy dowieść, że ciąg (a_n) jest ograniczony. Łatwo sprawdzić, że $2^k \geq \frac{4}{3}(k+1)$ dla $k \geq 2$ oraz $a^k \geq 3^k \geq \frac{4}{3}(k+1)$ dla $k \geq 1$ i $a \geq 3$. Zatem dla liczb większych od 2 zachodzi $d(p_1^{k_1}...p_n^{k_n}) = (k_1+1)...(k_n+1) \leq \frac{3}{4}p_1^{k_1}...p_n^{k_n}$, a więc $a_{n+1} \leq \frac{3}{4}a_n + c$, skąd $a_n \leq 4c$.

9. [58OM] Niech $F(k)$ będzie iloczynem wszystkich dodatnich dzielników liczby całkowitej dodatniej k. Rozstrzygnąć, czy istnieją różne liczby całkowite dodatnie m, n, dla których $F(m) = F(n)$.

   Rozwiązanie: Jeśli $p_1, p_2, ..., p_n$ są liczbami pierwszymi, to w rozkładzie $F(p_1^{k_1}...p_n^{k_n})$ na czynniki pierwsze czynnik p_i występuje dokładnie $\frac{k_i}{2}(k_1+1)(k_2+1)...(k_n+1)$ razy. Jeśli $F(p_1^{k_1}...p_n^{k_n}) = F(p_1^{l_1}...p_n^{l_n})$, to $\frac{k_i}{2}(k_1+1)(k_2+1)...(k_n+1) = \frac{l_i}{2}(l_1+1)(l_2+1)...(l_n+1)$, skąd w szczególności $k_il_j = k_jl_i$. Stąd łatwo $k_i = cl_i$ dla pewnego (wymiernego) c; pozostaje zauważyć, że $c = 1$. Zatem jeśli $F(a) = F(b)$, to $a = b$.

10. [58OM] Liczbę całkowitą dodatnią nazwiemy *białą*, jeżeli jest równa 1 lub jest iloczynem parzystej liczby liczb pierwszych (niekoniecznie różnych). Pozostałe liczby całkowite dodatnie nazwiemy *czarnymi*. Zbadać, czy istnieje taka liczba całkowita dodatnia, że suma jej białych dzielników jest równa sumie jej czarnych dzielników.

    Rozwiązanie: Załóżmy, że n jest najmniejszą liczbą o tej własności i załóżmy, że $n = p^{2k-1}m$ dla pewnej liczby pierwszej p i dla m niepodzielnego przez p. Niech b, c oznacza odpowiednio sumę białych i czarnych dzielników m. Porównując sumę białych dzielników n z sumą czarnych dzielników, otrzymujemy $\frac{p^{2k}-1}{p^2-1}(b+pc) = \frac{p^{2k}-1}{p^2-1}(pb+c)$, skąd $b = c$, sprzeczność. Gdy $n = p^{2k}m$, to analogicznie $\frac{p^{2k+2}-1}{p^2-1}b + p\frac{p^{2k}-1}{p^2-1}c = p\frac{p^{2k}-1}{p^2-1}b + \frac{p^{2k+2}-1}{p^2-1}c$ i znów $b = c$. Zatem takie liczby nie istnieją.

Permutacje

1. Udowodnij małe twierdzenie Fermata: jeśli p jest liczbą pierwszą, to $n^p \equiv n \pmod{p}$ dla wszystkich liczb całkowitych n.

2. [58OM] Niech p będzie liczbą pierwszą. Dowieść, że istnieje taka permutacja $(x_1, x_2, ..., x_{p-1})$ zboru $\{1, 2, ..., p-1\}$, że liczby x_1, x_1x_2, $x_1x_2x_3$, ..., $x_1x_2...x_{p-1}$ dają różne reszty przy dzieleniu przez p.

   Rozwiązanie: Niech $x_1 = 1$, $(k-1)x_k \equiv k \pmod{p}$. Oczywiście $x_k \neq x_1$ dla $k > 1$. Gdyby $x_k = x_l = a$ dla $k > l > 1$, to mielibyśmy $a(k-1) - a(l-1) \equiv k - l \pmod{p}$, skąd $a \equiv 1 \pmod{p}$.

3. [60OM] Dana jest liczba całkowita $n \geq 2$. Niech $r_1, r_2, ..., r_{n-1}$ będą odpowiednio resztami z dzielenia liczb 1, $1+2$, $1+2+3$, ..., $1+2+...+(n-1)$ przez n. Znaleźć wszystkie takie wartości n, że ciąg $(r_1, r_2, r_3, ..., r_{n-1})$ jest permutacją ciągu $(1, 2, 3, ..., n-1)$.

   Rozwiązanie: Zachodzi $1+2+...+k = \frac{k(k+1)}{2}$ oraz $\frac{k(k+1)}{2} - \frac{l(l+1)}{2} = \frac{(k-l)(k+l+1)}{2}$. Aby te liczby nie były podzielne przez n gdy $0 < l < k < n$, n musi być postaci $2p$ dla pewnej liczby pierwszej p.

4. [60OM] Dana jest liczba pierwsza p. Po lewej stronie tablicy napisano liczby $1, 2, 3, ..., p-1$, zaś po prawej stronie liczbę 0. Wykonujemy ciąg $p-1$ ruchów, z których każdy przebiega następująco. Wybieramy jedną z liczb napisanych po lewej stronie tablicy, dodajemy ją do wszystkich pozostałych liczb na dablicy, po czym wymazujemy wybraną liczbę. Rozstrzygnąć, dla jakich wartości p można w kolejnych ruchach wybierać liczby w taki sposób, by liczba pozostała na tablicy po wykonaniu wszystkich ruchów była podzielna przez p.

   Rozwiązanie: Jeśli $p - j_k$ oznacza numer ruchu, w którym wybrano liczbę równą początkowo k, to po prawej stronie zostanie liczba $2^{j_1} + 2 \cdot 2^{j_2} + 3 \cdot 2^{j_3} + ... + (p-1) \cdot 2^{j_{p-1}}$. Ciąg $(j_1, j_2, ..., j_{p-1})$ jest dowolną permutacją ciągu $(1, 2, ..., p-1)$, a ponadto ciąg reszt z dzielenia liczb $2^1, 2^2, ..., 2^{p-1}$ przez p jest pewną ustaloną permutacją ciągu $(1, 2, ..., p-1)$. Wybierzmy $j_1, j_2, ..., j_n$ tak, aby 2^{j_k} dzielone przez p dawało resztę k. Wtedy na tablicy pozostanie liczba, której reszta z dzielenia przez p wynosi $1^2 + 2^2 + ... + (p-1)^2 = \frac{p(p-1)(2p-1)}{6}$. Jeśli $p > 3$, to ta liczba jest podzielna przez p. Dla $p \in \{2, 3\}$ odpowiedź jest przecząca.

Reszty modulo

1. [550M] Rozstrzygnąć, czy istnieje liczba pierwsza p oraz liczby całkowite nieujemne x, y, z spełniające równanie $(12x+5)(12y+7) = p^z$.

   Rozwiązanie: Gdyby tak było, $p^k \equiv 5 \pmod{12}$ i $p^l \equiv 7 \pmod{12}$ dla pewnych k, l, skąd $p \equiv 5 \pmod{12}$ i $p \equiv 7 \pmod{12}$, sprzeczność.

2. [57OM] Wyznaczyć wszystkie nieujemne liczby całkowite n, dla których liczba $2^n + 105$ jest kwadratem liczby całkowitej.

   Rozwiązanie: Jeśli n jest nieparzyste, to $2^n + 105 \equiv 2 \pmod 3$, więc $2^n + 105$ nie jest kwadratem. Dla $n = 2k$ mamy $2^{2k} + 105 = a^2$ tylko jeśli $(a - 2^k)(a + 2^k) = 105$, skąd $2^k < \frac{105}{2}$, czyli $k \leq 5$. Bezpośrednio sprawdza się, że odpowiedź brzmi $n \in \{4, 6, 8\}$.

3. [57OM] Wyznaczyć wszystkie liczby całkowite dodatnie k, dla których liczba $3^k + 5^k$ jest potęgą liczby całkowitej o wykładniku naturalnym większym od 1.

   Rozwiązanie: Jedno rozwiązanie: $3^1 + 5^1 = 2^3$; $3^{2n} + 5^{2n} \equiv 2 \pmod 4$, więc k musi być nieparzyste; $3^{2n+1} + 5^{2n+1} \equiv 8 \pmod{16}$, więc $3^k + 5^k$ może być tylko sześcianem; dla $n > 1$, $3^{2n+1} + 5^{2n+1} \bmod 9 = 5^{2n+1} \bmod 9 \in \{2, 5, 8\}$, ale $m^3 \bmod 9 \in \{0, 1, 8\}$, przez co $3|k$; wreszcie $3^{6n+3} + 5^{6n+3} \equiv 5 \pmod 7$, ale $m^3 \bmod 7 \in \{0, 1, 6\}$, więc nie ma więcej rozwiązań.

4. [59OM] Wyznaczyć najwiekszą możliwą długość ciągu kolejnych liczb całkowitych, z których każdą można przedstawić w postaci $x^3 + 2y^2$ dla pewnych liczb całkowitych x, y.

   Rozwiązanie: $x^3 \bmod 8 \in \{0, 1, 3, 5, 7\}$, $2y^4 \bmod 8 \in \{0, 2\}$, zatem $x^3 + 2y^4 \bmod 8 \in \{0, 1, 2, 3, 5, 7\}$. Odpowiedź: 5.

Algorytm Euklidesa

1. [59OM] Dana jest liczba całkowita dodatnia n niepodzielna przez 3. Udowodnić, że istnieje liczba m o następującej włąsności: Każda liczba całkowita nie mniejsza niż m jest sumą cyfr pewnej wielokrotności liczby n.

   Rozwiązanie: Bez utraty ogólności możemy założyć, że n jest niepodzielna przez 10. Jeśli kn ma sumę cyfr a, zaś ln ma sumę cyfr b, to o ile N jest dostatecznie duże, $(10^N k + l)n$ ma sumę cyfr $a + b$. Wystarczy zatem wskazać dwie wielokrotności n, których sumy cyfr są liczbami względnie pierwszymi i zastosować algorytm Euklidesa. Aby znaleźć te wielokrotności, wybierzmy k niepodzielne przez 3 i takie, by cyfra jedności liczby kn była różna od zera, a cyfra dziesiątek — różna od 9. Następnie ustalmy l niepodzielne przez 3 i takie, by najbardziej znacząca cyfra liczby ln była równa 9. Niech N oznacza liczbę cyfr liczby ln, zaś a i b odpowiednio sumy cyfr liczb kn i ln; ponieważ kn i ln nie są podzielne przez 3, tę własność mają również ich sumy cyfr a i b. Pozostaje zauważyć, że $(10^N k + l)n$ ma sumę cyfr równą $a + b$, a suma cyfr liczby $(10^{N-1} k + l)n$ wynosi $a + b - 9$, i że te sumy cyfr są względnie pierwsze.

Mateusz Kwaśnicki