Kongruencje

Tomasz Kossakowski

26 września 2025

Definicje i własności

Kongruencje stanowią bardzo wygodne narzędzie służące do badania i zapisywania rozmaitych faktów związanych z podzielnością.

Definicja 1 (dzielenie z resztą)

Dane jest $a \in \mathbb{Z}$ i $m \in \mathbb{Z}_+$. Wówczas powiemy, że a daje resztę r przy dzieleniu przez m jeśli istnieje taka liczba całkowita k, że

$$a = k \cdot m + r$$

oraz $0 \leqslant r < m$.

Na dzielenie z resztą możemy popatrzeć w inny sposób.

Definicja 2

Niech $a, b \in \mathbb{Z}$ oraz niech $m \in \mathbb{Z}_+$. Mówimy, że a przystaje do b modulo m, jeśli liczba $a - b$ dzieli się przez m. Stosujemy oznaczenie

$$a \equiv b \pmod{m}$$

i nazywamy je kongruencją.

Przykłady:

- $5 \equiv 1 \pmod{4}$, ponieważ 4 dzieli $5 - 1 = 4$
- $2025 \equiv 1 \pmod{8}$, ponieważ 8 dzieli $2025 - 1 = 2024$
- $3a \equiv a \pmod{2}$, ponieważ 2 dzieli $3a - a = 2a$.

Na kongruencje można patrzeć jak na reszty z dzielenia, np. zapis $5 \equiv 1 \pmod{4}$ informuje nas, że 5 daje taką samą resztę z dzielenia przez 4 jak 1.

Kongruencje mają wiele ciekawych własności, z których będziemy często korzystać.

Twierdzenie 1 (własności kongruencji)

Dla $a, b, c, d \in \mathbb{Z}$ oraz $m, n \in \mathbb{Z}_+$ zachodzą poniższe zależności.

1. $a \equiv a \pmod{m}$.
2. Jeśli $a \equiv b \pmod{m}$, to $b \equiv a \pmod{m}$.
3. Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$.
4. Jeśli $a \equiv b \pmod{m}$, to $a \pm c \equiv b \pm c \pmod{m}$.
5. Jeśli $a \equiv b \pmod{m}$, to $ac \equiv bc \pmod{m}$.
6. Jeśli $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$.
7. Jeśli $a \equiv b \pmod{m}$oraz $c \equiv d \pmod{m}$, to $ac \equiv bd \pmod{m}$.
8. Jeśli $a \equiv b \pmod{m}$, to $a^n \equiv b^n \pmod{m}$.

Warto tu zwrócić uwagę, iż kongruencji na ogół *nie można dzielić stronami*. Przykładowo, zachodzą kongruencje

$$18 \equiv 3 \pmod{3} \qquad \text{oraz} \qquad 3 \equiv 3 \pmod{3},$$

ale $6 \not\equiv 1 \pmod{3}$.
Gdy rozpatrujemy podzielności, często możemy dostać po pewnych przekształceniach, że $a \equiv 0 \pmod{n}$. Oznacza to wtedy, że a jest podzielne przez n (lub inaczej zapisując $n \mid a$).
Warto również wspomnieć o tzw. *resztach kwadratowych*.

Definicja 3 (reszty i nieresztу kwadratowe)

Reszta kwadratowa modulo p (gdzie p jest liczbą pierwszą) to taka liczba całkowita a, że istnieje rozwiązanie kongruencji:

$$x^2 \equiv a \pmod{p}.$$

Jeśli powyższa kongruencja nie ma rozwiązania dla pewnej liczby całkowitej a, to taką liczbę nazywamy niereszтą kwadratową modulo p.

Przykładowo rozpatrując modulo 3, resztami kwadratowymi są $\{0, 1\}$, a niereszтą kwadratową jest 2, dlatego, że gdy sprawdzimy wszystkie reszty podniesione do kwadratu:

$$n \equiv 0 \implies n^2 \equiv 0^2 \equiv 0 \pmod{3}$$
$$n \equiv 1 \implies n^2 \equiv 1^2 \equiv 1 \pmod{3}$$
$$n \equiv 2 \implies n^2 \equiv 2^2 \equiv 1 \pmod{3}$$

znajdujemy 0 i 1, ale nie ma tutaj 2.

Przykłady

Ćwiczenie 1 (Matura podstawowa, czerwiec 2025)**.** Wykaż, że dla każdej nieparzystej liczby naturalnej n liczba $3n^2 + 2n + 7$ jest podzielna przez 4.

Rozwiązanie 1. Oczywiście moglibyśmy to zadanie zrobić metodą „szkolną”, jednak rozwiążemy je używając kongruencji.
Dowolna liczba całkowita nieparzysta podzielona przez 4 daje resztę 1 lub 3, zatem rozpatrzmy 2 przypadki:

1. Gdy $n \equiv 1 \pmod 4$, wtedy $3n^2 + 2n + 7 \equiv 3 \cdot 1^2 + 2 \cdot 1 + 7 = 12 \equiv 0 \pmod 4$, zatem $4 \mid 3n^2 + 2n + 7$.
2. Gdy $n \equiv 3 \pmod 4$, wtedy $3n^2 + 2n + 7 \equiv 3 \cdot 3^2 + 2 \cdot 3 + 7 = 40 \equiv 0 \pmod 4$, zatem $4 \mid 3n^2 + 2n + 7$.

W obu przypadkach wyszło, że $4 \mid 3n^2 + 2n + 7$, co należało udowodnić.

Ćwiczenie 2. Znajdź wszystkie takie liczby pierwsze p, dla których liczba p^2+2 także jest pierwsza.

Rozwiązanie 2. Zauważmy, że jeżeli liczba p nie dzieli się przez 3, to $p \equiv 1 \pmod 3$ lub $p \equiv 2 \pmod 3$. Stąd w obu przypadkach dostajemy $p^2 \equiv 1 \pmod 3$. A zatem

$$p^2 + 2 \equiv 0 \pmod 3$$

co oznacza, że liczba $p^2 + 2$ jest podzielna przez 3. Ponadto liczba $p^2 + 2$ jest większa od 3, gdyż p – jako liczba pierwsza – jest nie mniejsza od 2. Wobec tego liczba $p^2 + 2$ musi być złożona. Jeśli z kolei liczba p dzieli się przez 3, to musi być równa 3, gdyż jest to liczba pierwsza. Wtedy $3^2 + 2 = 11$ również jest liczbą pierwszą. Wobec tego jedyną liczbą p spełniającą warunki zadania jest $p = 3$.

Zadania

Zadanie 1. Wyznacz reszty z dzielenia (podaj najmniejsze naturalne a, b, c, d, e, f spełniające poniższe kongruencje):

1. $5 \equiv a \pmod 2$
2. $17 \equiv b \pmod 5$
3. $-4 \equiv c \pmod 6$
4. $123 \equiv d \pmod{20}$
5. $8 \cdot 421 \equiv e \pmod 4$
6. $7^9 \equiv f \pmod 8$.

Rozwiązanie 1. Korzystamy z własności kongruencji.

1. $5 \equiv a \pmod 2$, $\quad 5 = 2 \cdot 2 + 1 \Rightarrow a = 1$.
2. $17 \equiv b \pmod 5$, $\quad 17 = 5 \cdot 3 + 2 \Rightarrow b = 2$.
3. $-4 \equiv c \pmod 6$, $\quad -4 + 6 = 2 \Rightarrow c = 2$.
4. $123 \equiv d \pmod{20}$, $\quad 123 = 20 \cdot 6 + 3 \Rightarrow d = 3$.
5. $8 \cdot 421 \equiv e \pmod 4$, $\quad 8 \equiv 0 \pmod 4 \Rightarrow 8 \cdot 421 \equiv 0 \cdot 421 = 0 \pmod 8 \Rightarrow e = 0$.
6. $7^9 \equiv f \pmod 8$, $\quad 7 \equiv -1 \pmod 8 \Rightarrow 7^9 \equiv (-1)^9 \equiv -1 \equiv 7 \pmod 8 \Rightarrow f = 7$.

Zadanie 2. Wyznacz resztę z dzielenia liczby 2^{50} przez 3.

Rozwiązanie 2. Zauważmy, że

$$2 \equiv -1 \pmod 3,$$

czyli

$$2^{50} \equiv (-1)^{50} = 1 \pmod 3.$$

Czyli reszta z dzielenia tej liczby to 1.

Zadanie 3. Udowodnić, że dla dowolnej liczby całkowitej nieujemnej n liczba

$$3^{4^n} + 23$$

dzieli się przez 13.

Rozwiązanie 3. Mamy $3^4 = 81 \equiv 3 \pmod{13}$ skąd wynika, że

$$\begin{aligned} 3^{4^n} + 23 = (3^4)^{4^{n-1}} + 23 \equiv 3^{4^{n-1}} + 23 \equiv \ldots \equiv \\ \equiv 3^4 + 23 \equiv 3^1 + 23 = 26 \equiv 0 \pmod{13}. \end{aligned}$$

Stąd teza.

Zadanie 4. Udowodnić, że liczba $93^{93} - 33^{33}$ dzieli się przez 10.

Rozwiązanie 4. Zauważmy, że zachodzą kongruencje $93 \equiv 3 \pmod{10}$, $33 \equiv 3 \pmod{10}$ oraz $3^4 = 81 \equiv 1 \pmod{10}$. Wobec tego

$$93^{93} \equiv 3^{93} = (3^4)^{23} \cdot 3 \equiv 3 \pmod{10}$$

oraz

$$33^{33} \equiv (3^4)^8 \cdot 3 \equiv 3 \pmod{10}.$$

Wobec tego, mamy $93^{93} \equiv 33^{33} \pmod{10}$, co jest równoważne tezie zadania.

Zadanie 5 (VI OM-I-10)**.** Wykazać, że liczba $53^{53} - 33^{33}$ jest podzielna przez 10.

Rozwiązanie 5. Ponieważ $53 \equiv 3 \pmod{10}$, $33 \equiv 3 \pmod{10}$, $3^4 \equiv 1 \pmod{10}$, więc

$$53^{53} \equiv 3^{53} \equiv (3^4)^{13} \cdot 3 \equiv 3 \pmod{10},$$

$$33^{33} \equiv 3^{33} \equiv (3^4)^8 \cdot 3 \equiv 3 \pmod{10},$$

zatem

$$53^{53} - 33^{33} \equiv 0 \pmod{10}.$$

Zadanie 6. Liczby całkowite a, b, c mają tę własność, że liczby $ab - 1, bc - 1$ i $ca - 1$ są podzielne przez pewną liczbę pierwszą p. Wykaż, że liczba

$$a^2 + b^2 + c^2 - 3$$

również jest podzielna przez p.

Rozwiązanie 6. Dane podzielności możemy zapisać równoważnie jako

$$ab \equiv 1 \pmod{p}, \quad bc \equiv 1 \pmod{p}, \quad ca \equiv 1 \pmod{p}.$$

Mamy

$$a^2 \equiv a^2 \cdot bc \equiv ab \cdot ac \equiv 1 \pmod{p}.$$

W sposób analogiczny wykazujemy, że $b^2 \equiv c^2 \equiv 1 \pmod{p}$. Stąd

$$a^2 + b^2 + c^2 - 3 \equiv 1 + 1 + 1 - 3 \equiv 0 \pmod{p},$$

co należało wykazać.

Zadanie 7. W pewnej klasie jest mniej niż 40 osób. Gdy uczniowie chcieli podzielić się na grupy 5-osobowe, 4 osoby zostały bez grupy. Gdy natomiast chcieli podzielić się na grupy 6-osobowe, 5 osób zostało bez grupy. Ilu uczniów jest w tej klasie?

Rozwiązanie 7. Dołączmy do klasy jeszcze jednego ucznia; wtedy będzie można uczniów podzielić na grupy pięcioosobowe, a także na grupy sześcioosobowe, więc liczba uczniów będzie podzielna przez 30. Wobec tego liczba uczniów wyniesie dokładnie 30. Początkowo jest więc 29 uczniów.

Zadanie 8. Wyznacz reszty kwadratowe modulo 3, 4, 5 i 8.

Rozwiązanie 8. Reszta kwadratowa modulo p to liczba całkowita r taka, że istnieje $x \in \mathbb{Z}$ z $x^2 \equiv r \pmod{p}$.

Modulo 3: możliwe reszty z dzielenia liczby przez 3: $0, 1, 2$.

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4 \equiv 1 \pmod{3}.$$

Zatem reszty kwadratowe modulo 3 to

$$\{0, 1\}.$$

Modulo 4: reszty: $0, 1, 2, 3$.

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4 \equiv 0, \quad 3^2 \equiv 9 \equiv 1 \pmod{4}.$$

Reszty kwadratowe modulo 4:

$$\{0, 1\}.$$

Modulo 5: reszty: $0, 1, 2, 3, 4$.

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 4, \quad 4^2 \equiv 16 \equiv 1 \pmod{5}.$$

Reszty kwadratowe modulo 5:

$$\{0, 1, 4\}.$$

Modulo 8: reszty: $0, 1, 2, 3, 4, 5, 6, 7$.

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 1, \quad 4^2 \equiv 16 \equiv 0 \pmod{8}$$

$$5^2 \equiv 25 \equiv 1, \quad 6^2 \equiv 36 \equiv 4, \quad 7^2 \equiv 49 \equiv 1 \pmod{8}.$$

Reszty kwadratowe modulo 8:

$$\{0, 1, 4\}.$$

Zadanie 9. Znajdź wszystkie liczby całkowite x, y spełniające równanie

$$x^2 - 3y^2 = 1001.$$

Rozwiązanie 9. *Odpowiedź:* Liczby spełniające dane równanie nie istnieją.
Skoro liczby $x^2 - 3y^2$ oraz 1001 są sobie równe, to w szczególności dają tę samą resztę z dzielenia przez 3. Możemy więc kolejno zapisać

$$x^2 - 3y^2 \equiv 1001 \pmod{3},$$

$$x^2 - 0y^2 \equiv 2 \pmod{3},$$

$$x^2 \equiv 2 \pmod{3}.$$

Ostatnia kongruencja to sprzeczność, gdyż 2 jest niereszą kwadratową *modulo 2*, co dowodzi, że szukane liczby nie istnieją.

Zadanie 10. Rozstrzygnąć, czy istnieją takie liczby całkowite: $a_1, a_2, \ldots, a_{10}$, które spełniają równość

$$a_1^4 + a_2^4 + \cdots + a_9^4 + a_{10}^4 = 201200002013.$$

Wskazówka: rozważ modulo 16.

Rozwiązanie 10. Zauważmy, że dla dowolnej liczby całkowitej a spełniony jest następujący fakt

$$a^4 \equiv 0 \pmod{16} \qquad \text{lub} \qquad a^4 \equiv 1 \pmod{16}.$$

Wtedy możliwe reszty z dzielenia wyrażenia $a_1^4 + a_2^4 + \cdots + a_9^4 + a_{10}^4$ przez 16 należą do zbioru $\{0, 1, \ldots, 10\}$.
Ponieważ $201200002013 \equiv 13 \pmod{16}$, więc takie liczby $a_1, a_2, \ldots, a_{10}$ nie istnieją.

Zadanie 11. Udowodnić, że dla nieskończenie wielu liczb całkowitych dodatnich n liczba $7 \cdot 2^n + 1$ jest złożona.

Rozwiązanie 11. Wystarczy wskazać nieskończenie wiele n, dla których $7 \cdot 2^n + 1$ ma dzielnik właściwy. Weźmy wszystkie n postaci $n = 6k + 3$ ($k \in \mathbb{N}$). Wtedy modulo 3 mamy

$$2^6 \equiv 1 \pmod 3 \quad \Longrightarrow \quad 2^{6k+3} \equiv (2^6)^k \cdot 2^3 \equiv 1 \cdot (-1) \equiv -1 \pmod 3,$$

a zatem

$$7 \cdot 2^{6k+3} + 1 \equiv 7 \cdot (-1) + 1 \equiv -6 \equiv 0 \pmod 3.$$

Ponieważ dla $k \geqslant 0$ zachodzi $7 \cdot 2^{6k+3} + 1 \geqslant 7 \cdot 8 + 1 = 57 > 3$, liczba ta nie jest równa 3, a więc – mając dzielnik 3 – musi być złożona. Takich n (równe 3 mod 6) jest nieskończenie wiele, co kończy dowód.

Zadanie 12. Udowodnić, że równanie $x^3+y^3+z^3 = 2005^2$ nie ma rozwiązań w liczbach całkowitych.

Rozwiązanie 12. Rozważmy równanie

$$x^3 + y^3 + z^3 = 2005^2.$$

Będziemy badać je modulo 9. Przypomnijmy fakt dotyczący sześcianów całkowitych:

$$n^3 \equiv 0, 1, 8 \pmod 9 \quad \text{dla każdego } n \in \mathbb{Z}.$$

Można też zapisać $8 \equiv -1 \pmod 9$, więc reszty sześcianów modulo 9 należą do zbioru

$$\{0, 1, -1\}.$$

Zatem suma trzech sześcianów modulo 9 może przyjmować wartości:

$$0+0+0 = 0, \quad 1+0+0 = 1, \quad 1+1+0 = 2, \quad 1+1+1 = 3, \quad \ldots, \quad (-1)+(-1)+(-1) = -3 \equiv 6 \pmod 9.$$

Zbiór możliwych reszt sumy trzech sześcianów modulo 9 to:

$$\{-3, -2, -1, 0, 1, 2, 3\} \equiv \{0, 1, 2, 3, 6, 7, 8\} \pmod 9.$$

Obliczmy resztę liczby 2005^2 modulo 9. Najpierw

$$2005 \equiv 2 + 0 + 0 + 5 = 7 \pmod 9,$$

więc

$$2005^2 \equiv 7^2 = 49 \equiv 4 \pmod 9.$$

Ale 4 nie należy do zbioru możliwych reszt sumy trzech sześcianów modulo 9. Oznacza to, że równanie

$$x^3 + y^3 + z^3 = 2005^2$$

nie ma rozwiązań w liczbach całkowitych.

Zadania dodatkowe

Zadanie 13. Wyznaczyć wszystkie liczby pierwsze p, dla których liczba $3^p + 4^p$ jest podzielna przez 181.

Rozwiązanie 13. Podstawienie kilku przykładowych wartości p prowadzi do odkrycia pierwszego rozwiązania: $3^5 + 4^5 = 243 + 1024 = 1267 = 181 \cdot 7$. To sugeruje, by zbadać liczbę $3^p + 4^p$ przy podstawieniu $p = 5k + \ell$ (dla k będącej liczbą całkowitą nieujemną oraz $\ell \in \{0, 1, 2, 3, 4\}$). Mamy $3^5 \equiv -4^5 \pmod{181}$, stąd

$$3^{5k} \equiv (-1)^k \cdot 4^{5k} \pmod{181}.$$

Możemy więc napisać

$$3^p + 4^p = 3^{5k+\ell} + 4^{5k+\ell} = 3^{5k} \cdot 3^\ell + 4^{5k} \cdot 4^\ell \equiv$$
$$\equiv (-1)^k \cdot 4^{5k} \cdot 3^\ell + 4^{5k} \cdot 4^\ell = 4^{5k} \left[(-1)^k \cdot 3^\ell + 4^\ell\right] \pmod{181}.$$

Liczba 181 jest pierwsza, a zatem nie ma dzielników większych od 1 wspólnych z 4^{5k}. Jeśli więc $3^p + 4^p$ dzieli się przez 181, to musi zachodzić kongruencja

$$(-1)^k \cdot 3^\ell + 4^\ell \equiv 0 \pmod{181}.$$

Dla k nieparzystego oraz $\ell = 0$ warunek ten jest oczywiście spełniony, zaś dla pozostałych k, ℓ nie zachodzi. Sprawdzamy bowiem, że $3^0 + 4^0 \neq 0 \pmod{181}$,

$$1 \leqslant (-1)^k \cdot 3^\ell + 4^\ell \leqslant 180 \quad \text{dla } \ell = 1, 2, 3$$

oraz

$$\pm 3^4 + 4^4 = \pm 81 + 256 \neq 0 \pmod{181}.$$

Wykazaliśmy zatem, że liczba $3^p + 4^p$ dzieli się przez 181 wtedy i tylko wtedy, gdy p jest postaci $5k$ dla pewnej dodatniej liczby nieparzystej k. Ponieważ p ma być liczbą pierwszą, rozwiązanie $p = 5$, odgadnięte na wstępie, jest jedynym rozwiązaniem zadania.

Zadanie 14. Wykazać, że dla nieskończenie wielu liczb całkowitych dodatnich n, liczba $1+2^{4^n}+2^{5^n}$ jest złożona.

Rozwiązanie 14. Wykażemy, że jeśli n jest dodatnią liczbą nieparzystą, to badana liczba jest podzielna przez 7; skoro $1 + 2^{4^n} + 2^{5^n} > 7$, to wyniknie z tego teza zadania. Dla $n = 1$ dostajemy liczbę $1+2^4+2^5 = 49$, która oczywiście dzieli się przez 7. Załóżmy dalej, że n jest liczbą nieparzystą większą od 1.
Zauważmy, iż $2^4 \equiv 2 \pmod{7}$, skąd

$$2^{4^n} = (2^4)^{4^{n-1}} \equiv 2^{4^{n-1}} \pmod{7}$$

i analogicznie

$$2^{4^n} \equiv 2^{4^{n-2}} \pmod{7}.$$

Podobnie $2^5 \equiv 4 = 2^2 \pmod{7}$, a więc

$$2^{5^n} = (2^5)^{5^{n-1}} \equiv 2^{5^{n-1} \cdot 2} = (2^{5^{n-1}})^2 \pmod{7}$$

oraz

$$2^{5^{n-1}} \equiv (2^{5^{n-2}})^2 \pmod{7}.$$

Ostatnie dwie kongruencje prowadzą do wniosku, że

$$2^{5^n} \equiv (2^{5^{n-2}})^4 = (2^4)^{5^{n-2}} \equiv 2^{5^{n-2}} \pmod{7}.$$

Wobec tego wykazaliśmy, iż

$$1 + 2^{4^n} + 2^{5^n} \equiv 1 + 2^{4^{n-2}} + 2^{5^{n-2}} \pmod{7},$$

a zatem

$$1 + 2^{4^n} + 2^{5^n} \equiv 1 + 2^{4^1} + 2^{5^1} = 49 \equiv 0 \pmod{7}.$$

Rozwiązanie jest zakończone.

Zadanie 15. Dane są liczby całkowite dodatnie a, b, c, d, e, f takie, że

$$a + b = c + d = e + f = 101.$$

Udowodnić, że liczby $\frac{ace}{bdf}$ nie można zapisać w postaci ułamka $\frac{m}{n}$, gdzie m, n są liczbami całkowitymi dodatnimi o sumie mniejszej niż 101.

Rozwiązanie 15. Zapiszmy liczbę $\frac{ace}{bdf}$ w postaci ułamka nieskracalnego $\frac{m}{n}$; istnieje zatem taka liczba całkowita dodatnia k, że

$$ace = k \cdot m \quad \text{oraz} \quad bdf = k \cdot n.$$

Dalej, mamy

$$a \equiv -b \pmod{101}, \quad c \equiv -d \pmod{101}, \quad e \equiv -f \pmod{101},$$

a zatem

$$ace \equiv -bdf \pmod{101},$$

czyli $ace + bdf = k \cdot (m+n)$ dzieli się przez 101. Z drugiej strony, 101 jest liczbą pierwszą i każda z liczb a, b, c, d, e, f należy do zbioru $\{1, 2, \ldots, 100\}$. W konsekwencji, ace oraz bdf nie dzielą się przez 101, a zatem k także nie dzieli się przez 101. Doszliśmy więc do wniosku, iż $101 \mid m+n$, co pociąga za sobą $m+n \geqslant 101$; stąd teza.

Zadanie 16. Udowodnić, że dla dowolnej liczby całkowitej dodatniej n liczba $73^{6^n} - 37^{6^n}$ dzieli się przez 35.

Rozwiązanie 16. Chcemy pokazać, że dla dowolnego $n \in \mathbb{Z}_{>0}$ mamy $73^{6^n} - 37^{6^n} \equiv 0 \pmod{35}$. Ponieważ $35 = 5 \cdot 7$ i $\mathrm{NWD}(5,7) = 1$, wystarczy udowodnić podzielność przez 5 oraz przez 7.
Krok 1: podzielność przez 5.
Zauważmy, że

$$73 \equiv 3 \pmod{5}, \quad 37 \equiv 2 \pmod{5}.$$

Zatem

$$73^{6^n} - 37^{6^n} \equiv 3^{6^n} - 2^{6^n} \pmod{5}.$$

Ponieważ 6^n jest liczbą parzystą, oznaczmy $6^n = 2m$. Wtedy

$$3^{6^n} = 3^{2m} = (3^2)^m = 9^m \equiv 4^m \pmod{5},$$
$$2^{6^n} = 2^{2m} = (2^2)^m = 4^m \pmod{5}.$$

Stąd

$$3^{6^n} - 2^{6^n} \equiv 0 \pmod{5}.$$

Krok 2: podzielność przez 7.

$$73 \equiv 3 \pmod{7}, \qquad 37 \equiv 2 \pmod{7},$$

więc rozważamy $3^{6^n} - 2^{6^n}$ modulo 7. Wykonamy proste obliczenia potęg modulo 7:

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8 \equiv 1 \pmod{7}.$$

Zatem $2^3 \equiv 1 \pmod{7}$, a więc $2^6 = (2^3)^2 \equiv 1^2 \equiv 1 \pmod{7}$. Dla dowolnego $n \geqslant 1$

$$2^{6^n} = \left(2^6\right)^{6^{n-1}} \equiv 1^{6^{n-1}} \equiv 1 \pmod{7}.$$

Analogicznie dla 3:

$$3^1 \equiv 3, \quad 3^2 \equiv 9 \equiv 2, \quad 3^3 \equiv 3 \cdot 2 \equiv 6,$$
$$3^4 \equiv 3 \cdot 6 \equiv 18 \equiv 4, \quad 3^5 \equiv 3 \cdot 4 \equiv 12 \equiv 5, \quad 3^6 \equiv 3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}.$$

Stąd $3^6 \equiv 1 \pmod{7}$, więc podobnie jak poprzednio

$$3^{6^n} = \left(3^6\right)^{6^{n-1}} \equiv 1^{6^{n-1}} \equiv 1 \pmod{7}.$$

Wynika stąd, że $3^{6^n} - 2^{6^n} \equiv 0 \pmod{7}$.
Wniosek: Skoro wyrażenie jest podzielne i przez 5, i przez 7, to jest podzielne przez 35. Zatem dla każdego $n \geqslant 1$

$$73^{6^n} - 37^{6^n} \equiv 0 \pmod{35}.$$

Uwaga: Zależności $2^6 \equiv 1 \pmod{7}$ i $3^6 \equiv 1 \pmod{7}$ wynikają błyskawicznie z *małego twierdzenia Fermata*, które przedstawione jest w zadaniu 18.

Zadanie 17. Wykazać, że dla dowolnej liczby naturalnej n liczba

$$\frac{n^{44}+n^{33}+n^{22}+n^{11}+1}{n^4+n^3+n^2+n+1}$$

jest liczbą naturalną.

Rozwiązanie 17. Tezę możemy zapisać równoważnie w postaci

$$n^{44}+n^{33}+n^{22}+n^{11}+1 \equiv 0 \pmod{n^4+n^3+n^2+n+1}.$$

Dla ułatwienia zapisu przyjmijmy, że $n^4+n^3+n^2+n+1 = S$.
Na początku zauważmy, że

$$\begin{aligned} n^{10}-1 &= (n-1)(n^9+n^8+n^7+n^6+n^5+n^4+n^3+n^2+n+1) = \\ &= (n-1)(n^5-1)(n^4+n^3+n^2+n+1) \equiv 0 \pmod{S}. \end{aligned}$$

Wynika stąd, że:

$$\begin{aligned} &n^{10} \equiv 1 \pmod{S}, \qquad n^{11} \equiv n \pmod{S}, \qquad n^{22} \equiv n^2 \pmod{S}, \\ &n^{33} \equiv n^3 \pmod{S}, \qquad n^{44} \equiv n^4 \pmod{S}. \end{aligned}$$

Po dodaniu stronami dostajemy, że

$$n^{44}+n^{33}+n^{22}+n^{11}+1 \equiv n^4+n^3+n^2+n+1 \equiv 0 \pmod{n^4+n^3+n^2+n+1},$$

co kończy dowód.

Zadanie 18. Udowodnić *małe twierdzenie Fermata:*
Jeśli p jest liczbą pierwszą, zaś a liczbą całkowitą dodatnią niepodzielną przez p, to a^{p-1} daje resztę 1 z dzielenia przez p.

Rozwiązanie 18. Po pierwsze wykazujemy, że liczby ze zbioru $\{a, 2a, \ldots, (p-1)a\}$ dają różne reszty z dzielenia przez p. Załóżmy bowiem, że liczby ka i la dają tę samą resztę, czyli $p \mid ka-la = a(k-l)$. Skoro liczba a jest niepodzielna przez p, to $p \mid k-l$. Ale mamy $1 \leqslant k, l \leqslant p-1$, więc

$$-p+2 = 1-(p-1) \leqslant k-l \leqslant (p-1)-1 = p-2.$$

Jedyną liczbą podzielną przez p w przedziale $[-p+2, p-2]$ jest 0, zatem $k-l=0$, czyli $k=l$.
Niech r_i oznacza resztę z dzielenia liczby $i \cdot a$ przez p, dla $i = 1, 2, \ldots, p-1$. Wykazaliśmy powyżej, że zbiór reszt $\mathcal{R} = \{r_1, \ldots, r_{p-1}\}$ ma $p-1$ różnych elementów. Żadna z liczb $i \cdot a$ nie dzieli się przez p, zatem $\mathcal{R}$ jest zawarty w zbiorze $\{1, 2, \ldots, p-1\}$. Zbiory te mają tyle samo elementów, więc

$$\{r_1, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}.$$

Wobec tego

$$(1 \cdot a) \cdot (2 \cdot a) \cdot \ldots \cdot ((p-1) \cdot a) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1} \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p},$$

czyli $(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}$, więc $p \mid (p-1)! \cdot (a^{p-1}-1)$. Liczba p jest pierwsza i p nie dzieli $(p-1)!$, więc $p \mid a^{p-1}-1$, innymi słowy a^{p-1} daje resztę 1 z dzielenia przez p, co było do udowodnienia.

Zadanie 19. Znajdź wszystkie takie pary dodatnich liczb całkowitych (n, m), dla których zachodzi równość

$$1! + 2! + 3! + \ldots + n! = m^2.$$

Rozwiązanie 19. *Odpowiedź:* Jedynymi rozwiązaniami danego równania są pary $(n, m) = (1, 1)$ i $(3, 3)$.
Zauważmy, że dla $n \geqslant 5$, liczba $n! = 1 \cdot 2 \cdot \ldots \cdot n$ jest podzielna zarówno przez 2 jak i przez 5. Wynika stąd, że liczba ta jest podzielna także przez 10. A więc dla $n \geqslant 5$ mamy

$$1! + 2! + \cdots + n! \equiv 1! + 2! + 3! + 4! = 1 + 2 + 6 + 24 = 33 \equiv 3 \pmod{10}.$$

Pozostaje zauważyć, że dla każdego m liczba m^2 nie daje reszty 3 z dzielenia przez 10. Wnioskujemy stąd, że dla $n \geqslant 5$ równanie nie ma rozwiązań.
Sprawdzając $n = 1, 2, 3, 4$, wnioskujemy, że pary $(n, m) = (1, 1), (3, 3)$ są jedynymi rozwiązaniami danego równania.

Zadanie 20. Udowodnić *chińskie twierdzenie o resztach:*
Dla dodatnich liczb całkowitych względnie pierwszych a_1 i a_2 oraz liczb całkowitych $0 \leqslant r_1 < a_1$, $0 \leqslant r_2 < a_2$ istnieje dokładnie jedna liczba $0 \leqslant n < a_1 \cdot a_2$ taka, że n daje resztę r_1 z dzielenia przez a_1 i resztę r_2 z dzielenia przez a_2.

Rozwiązanie 20. Jeżeli liczby k i l dają te same reszty zarówno z dzielenia przez a_1, jak i przez a_2, to znaczy, że $a_1 \mid k - l$ i $a_2 \mid k - l$, czyli $a_1 \cdot a_2 \mid k - l$, gdyż liczby a_1, a_2 są względnie pierwsze. Zatem liczby k i l różnią się o wielokrotność liczby $a_1 \cdot a_2$.
Wynika stąd, że każde dwie różne z liczb $0, 1, \ldots, a_1 \cdot a_2 - 1$ dają różne reszty z dzielenia przez a_1 lub różne reszty z dzielenia przez a_2. Możliwych par (reszta z dzielenia przez a_1, reszta z dzielenia przez a_2) jest $a_1 \cdot a_2$; tyle samo, ile liczb $0, 1, \ldots, a_1 \cdot a_2 - 1$. To oznacza, że w zbiorze tych liczb każda para reszt występuje dokładnie raz. Innymi słowy, dla każdych zadanych r_1 i r_2 znajdziemy dokładnie jedną liczbę n ze zbioru $\{0, 1, \ldots, a_1 \cdot a_2 - 1\}$ taką, że n daje resztę r_1 przy dzieleniu przez a_1 i resztę r_2 przy dzieleniu przez a_2. To kończy dowód.