Kongruencje i Małe Twierdzenie Fermata

Mieszko Zimny

Koło Pasjonatów Matematyki UW

April 19, 2021

Kongruencje tak naprawdę wyrażają ideę, którą znacie ze szkoły podstawowej, mianowicie dzielenie z resztą.

Kongruencje tak naprawdę wyrażają ideę, którą znacie ze szkoły podstawowej, mianowicie dzielenie z resztą.

Definicja

Niech a i b będą liczbami całkowitymi, a m liczbą całkowitą dodatnią. 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.

Kongruencje tak naprawdę wyrażają ideę, którą znacie ze szkoły podstawowej, mianowicie dzielenie z resztą.

Definicja

Niech a i b będą liczbami całkowitymi, a m liczbą całkowitą dodatnią. 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

$$14 \equiv 2 \pmod{2}$$

$$100 \equiv 150 \pmod{5}$$

$$81 \equiv 27 \equiv 9 \equiv 3 \equiv 0 \equiv -3 \pmod{3}$$

Obserwacja

Przystawanie a i b modulo m oznacza dokładnie tyle, że a i b dają tę samą resztę z dzielenia przez m.

Obserwacja

Przystawanie a i b modulo m oznacza dokładnie tyle, że a i b dają tę samą resztę z dzielenia przez m.

W zapisie kongruencji chodzi o to, że utożsamiamy ze sobą wszystkie liczby całkowite, które dają tę samą resztę z dzielenia przez m.
To podejście okazuje się bardzo wygodne, ponieważ kongruencje możemy do pewnego stopnia traktować jak równości, tzn. mają one wiele własności takich samych, jak zwykłe równania.

Własności kongruencji

We wszystkich wzorach poniżej a, b, c, d są liczbami całkowitymi, zaś m, n liczbami całkowitymi dodatnimi.

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 $a + c \equiv b + c \pmod{m}$.
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 $a + c \equiv b + d \pmod{m}$.
7. Jeśli $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$, to $ac \equiv bd \pmod{m}$.
8. W szczególności, z powyższej własności wynika, że jeśli $a \equiv b \pmod{m}$, to $a^n \equiv b^n \pmod{m}$.

Widzimy, że kongruencje można dodawać (więc także odejmować) i mnożyć stronami. Pojawia się naturalne pytanie, czy można je też dzielić. Okazuje się, że nie, ponieważ na przykład:

$$18 \equiv 3 \pmod 3, \quad 3 \equiv 3 \pmod 3,$$

ale

$$6 \not\equiv 1 \pmod 3.$$

Na poprzednich zajęciach udowodniliśmy, że p dzieli $n^p - n$ dla $p = 2, 3, 5$. Jeżeli chcielibyśmy udowodnić teraz, że 7 dzieli $n^7 - n$, to używając kongruencji wystarczy rozważyć tylko 7 przypadków, co jest zadaniem czysto rachunkowym.

$$n \equiv 0 \pmod 7 \Rightarrow n^7 - n \equiv 0^7 - 0 = 0 \pmod 7$$

$$n \equiv 1 \pmod 7 \Rightarrow n^7 - n \equiv 1^7 - 1 = 0 \pmod 7$$

$$n \equiv 2 \pmod 7 \Rightarrow n^7 - n \equiv 2^7 - 2 = 126 = 7 \cdot 18 \equiv 0 \pmod 7$$

$$n \equiv 3 \pmod 7 \Rightarrow n^7 - n \equiv 3^7 - 3 = 2184 = 7 \cdot 312 \equiv 0 \pmod 7$$

$$n \equiv 4 \pmod 7 \Rightarrow n^7 - n \equiv 4^7 - 4 = 16380 = 7 \cdot 2340 \equiv 0 \pmod 7$$

$$n \equiv 5 \pmod 7 \Rightarrow n^7 - n \equiv 5^7 - 5 = 78120 = 7 \cdot 11160 \equiv 0 \pmod 7$$

$$n \equiv 6 \pmod 7 \Rightarrow n^7 - n \equiv 6^7 - 6 = 279930 = 7 \cdot 39990 \equiv 0 \pmod 7$$

Zadanie

Udowodnij, że liczba $93^{93} - 33^{33}$ jest podzielna przez 10.

Zadanie

Udowodnij, że liczba $93^{93} - 33^{33}$ jest podzielna przez 10.

Rozwiązanie:

Mamy oczywiście

$$93^{93} \equiv 3^{93} \pmod{10}$$

oraz

$$33^{33} \equiv 3^{33} \pmod{10}.$$

Zadanie

Udowodnij, że liczba $93^{93} - 33^{33}$ jest podzielna przez 10.

Rozwiązanie:

Mamy oczywiście

$$93^{93} \equiv 3^{93} \pmod{10}$$

oraz

$$33^{33} \equiv 3^{33} \pmod{10}.$$

Zauważmy, że

$$3^4 = 81 \equiv 1 \pmod{10},$$

Zadanie

Udowodnij, że liczba $93^{93} - 33^{33}$ jest podzielna przez 10.

Rozwiązanie:
Mamy oczywiście

$$93^{93} \equiv 3^{93} \pmod{10}$$

oraz

$$33^{33} \equiv 3^{33} \pmod{10}.$$

Zauważmy, że

$$3^4 = 81 \equiv 1 \pmod{10},$$

a stąd

$$3^{93} = 3^{92} \cdot 3 = (3^4)^{23} \cdot 3 \equiv 1^{23} \cdot 3 = 3 \pmod{10}$$

oraz

$$3^{33} = 3^{32} \cdot 3 = (3^4)^8 \cdot 3 \equiv 1^8 \cdot 3 = 3 \pmod{10},$$

co kończy dowód.

Zadanie

Wyznacz dwie ostatnie cyfry liczby 2021^{2021}.

Zadanie

Wyznacz dwie ostatnie cyfry liczby 2021^{2021}.

Rozwiązanie:

Mamy

$$2021 \equiv 21 \pmod{100}$$

$$2021^2 \equiv 21^2 = 441 \equiv 41 \pmod{100}$$

$$2021^3 = 2021^2 \cdot 2021 \equiv 41 \cdot 21 = 861 \equiv 61 \pmod{100}$$

$$2021^4 = 2021^3 \cdot 2021 \equiv 61 \cdot 21 = 1281 \equiv 81 \pmod{100}$$

$$2021^5 = 2021^4 \cdot 2021 \equiv 81 \cdot 21 = 1701 \equiv 1 \pmod{100}.$$

Stąd

$$2021^{2021} = 2021^{2020} \cdot 2021 = (2021^5)^{404} \cdot 2021 \equiv 21 \pmod{100}.$$

Zadanie

Wyznacz wszystkie liczby całkowite dodatnie n, dla których liczba $2^n - 1$ jest podzielna przez 7.

Zadanie

Wyznacz wszystkie liczby całkowite dodatnie n, dla których liczba $2^n - 1$ jest podzielna przez 7.

Rozwiązanie:
Mamy:

$$2^1 \equiv 2 \pmod 7$$

$$2^2 \equiv 4 \pmod 7$$

$$2^3 \equiv 1 \pmod 7.$$

Stąd łatwo zauważyć, że 2^n daje resztę 1 z dzielenia przez 7 wtedy i tylko wtedy, gdy n jest podzielne przez 3.

Zadanie

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

Zadanie

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

Rozwiązanie:
Znów, gdy nie wiadomo, jak zacząć zadanie, warto zobaczyć, co dzieje sie dla małych wartośći p.

Zadanie

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

Rozwiązanie:
Znów, gdy nie wiadomo, jak zacząć zadanie, warto zobaczyć, co dzieje sie dla małych wartośći p.

p	$2^p + 3^p$
2	25
3	91
5	$1267 = 7 \cdot 181$

To sugeruje, aby rozpatrzeć wyrażenie $3^p + 4^p$ w zależności od reszty z dzielenia przez 5 dawanej przez p.

Niech $p = 5k + m$, gdzie $m \in \{0, 1, 2, 3, 4\}$. Mamy

$$3^p + 4^p = 3^{5k} \cdot 3^m + 4^{5k} \cdot 4^m.$$

Niech $p = 5k + m$, gdzie $m \in \{0, 1, 2, 3, 4\}$. Mamy

$$3^p + 4^p = 3^{5k} \cdot 3^m + 4^{5k} \cdot 4^m.$$

Zauważmy, że

$$3^5 \equiv -4^5 \pmod{181},$$

a stąd

$$3^{5k} \cdot 3^m + 4^{5k} \cdot 4^m \equiv (-1)^k \cdot 4^{5k} \cdot 3^m + 4^{5k} \cdot 4^m \equiv$$

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

Liczby 181 oraz 4^{5k} są względnie pierwsze, więc 181 dzieli $\equiv 4^{5k} \cdot \left[(-1)^k \cdot 3^m + 4^m\right]$ wtedy i tylko wtedy, gdy dzieli $\left[(-1)^k \cdot 3^m + 4^m\right]$. Powyższa równość zachodzi oczywiście dla $m = 0$ i k nieparzystego. Pozostaje rozpatrzeć pozostałe przypadki.

$$3^1 + 4^1 = 7$$

$$-3^1 + 4^1 = 1$$

$$3^2 + 4^2 = 25$$

$$-3^2 + 4^2 = 7$$

$$3^3 + 4^3 = 91$$

$$-3^3 + 4^3 = 37$$

$$3^4 + 4^4 = 337$$

$$-3^4 + 4^4 = 175$$

Żadna z otrzymanych liczb nie dzieli się przez 181, więc ostatecznie warunki zadania spełnia tylko $p = 5$.

Oznaczenie

Jeżeli n jest liczbą całkowitą dodatnią, to $n!$ (n silnia) oznacza iloczyn wszystkich liczb całkowitych od 1 do n:

$$n! = 1 \cdot 2 \cdot \ldots \cdot n.$$

Dodatkowo przyjmujemy $0! = 1$.

Małe Twierdzenie Fermata

Dla każdej liczby całkowitej n i każdej liczby pierwszej p, liczba $n^p - n$ jest podzielna przez p.

Małe Twierdzenie Fermata

Dla każdej liczby całkowitej n i każdej liczby pierwszej p, liczba $n^p - n$ jest podzielna przez p.

Dowód 1:
Jeżeli n jest podzielna przez p, to teza jest oczywista, bo wówczas także n^p jest podzielna przez p. Załóżmy dalej, że n jest względnie pierwsza z p. Mamy

$$n^p - n = n(n^{p-1} - 1).$$

Zatem w tym przypadku liczba p dzieli $n^p - n$ wtedy i tylko wtedy, gdy dzieli $n^{p-1} - 1$.

Najpierw pokażemy, że liczby ze zbioru {n, 2n, 3n, . . . (p-1)n} dają różne reszty z dzielenia przez p.

Najpierw pokażemy, że liczby ze zbioru {n, 2n, 3n, ... (p-1)n} dają różne reszty z dzielenia przez p.
Gdyby kn i ln dla pewnych $k, l \in \{1, 2, \ldots, (p-1)\}$ dawały tę samą resztę z dzielenia przez p, to $p|(kn - ln) = (k-l)n$. Skoro p jest względnie pierwsze z n, to p musi dzielić $k - l$. Ale $k, l \in \{1, 2, \ldots, (p-1)\}$, a więc

$$k - l \in \{-(p-2), -(p-3), \ldots p-3, p-2\}.$$

Jedyna liczba podzielna przez p w tym zbiorze to 0, zatem musi być $k = l$. To dowodzi, że istotnie dla $k \neq l$, $k, l \in \{1, 2, \ldots, (p-1)\}$ liczby kn i ln dają różne liczby z dzielenia przez p.

Niech r_k oznacza resztę z dzielenia liczby kn przez p dla $k \in \{1, 2, \ldots, p-1\}$. Pokazaliśmy, że liczby r_k są parami różne. Co więcej, każda z nich jest różna od zera, bo n i k są względnie pierwsze z p. W takim razie są to wszystkie możliwe niezerowe reszty z dzielenia przez p:

$$\{r_1, r_2, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}.$$

Niech r_k oznacza resztę z dzielenia liczby kn przez p dla $k \in \{1, 2, \ldots, p-1\}$. Pokazaliśmy, że liczby r_k są parami różne. Co więcej, każda z nich jest różna od zera, bo n i k są względnie pierwsze z p. W takim razie są to wszystkie możliwe niezerowe reszty z dzielenia przez p:

$$\{r_1, r_2, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}.$$

Wobec tego

$$n \cdot (2n) \cdot \ldots \cdot ((p-1)n) \equiv r_1 r_2 \ldots r_{p-1} = (p-1)! \pmod{p}$$

$$(p-1)! n^{p-1} \equiv (p-1)! \pmod{p}.$$

Niech r_k oznacza resztę z dzielenia liczby kn przez p dla $k \in \{1, 2, \ldots, p-1\}$. Pokazaliśmy, że liczby r_k są parami różne. Co więcej, każda z nich jest różna od zera, bo n i k są względnie pierwsze z p. W takim razie są to wszystkie możliwe niezerowe reszty z dzielenia przez p:

$$\{r_1, r_2, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}.$$

Wobec tego

$$n \cdot (2n) \cdot \ldots \cdot ((p-1)n) \equiv r_1 r_2 \ldots r_{p-1} = (p-1)! \pmod{p}$$

$$(p-1)! n^{p-1} \equiv (p-1)! \pmod{p}.$$

W takim razie p dzieli liczbę

$$(p-1)! n^{p-1} - (p-1)! = (p-1)!(n^{p-1} - 1).$$

Ale p i $(p-1)!$ są względnie pierwsze, stąd p dzieli $n^{p-1} - 1$.

□

Dowód 2:
Tak jak wcześniej, szybko udowadniamy przypadek, gdy $p|n$ i w dalszej części dowodu zakładamy, że n i p są względnie pierwsze. Najpierw udowodnimy, że istnieje liczba całkowita dodatnia $k \leq p-1$ taka, że $n^k \equiv 1 \pmod{p}$.

Dowód 2:
Tak jak wcześniej, szybko udowadniamy przypadek, gdy $p|n$ i w dalszej części dowodu zakładamy, że n i p są względnie pierwsze.
Najpierw udowodnimy, że istnieje liczba całkowita dodatnia $k \leq p-1$ taka, że $n^k \equiv 1 \pmod{p}$.
Rozważmy reszty z dzielenia przez p liczb

$$n, n^2, n^3, \ldots, n^{p-1}$$

przez p. Oczywiście wszystkie one są niezerowe. Jeżeli wszystkie są różne, to są to wszystkie niezerowe reszty z dzielenia przez p, więc pewna z nich musi być równa 1. Jeżeli natomiast pewnie dwa z nich są równe, powiedzmy reszty z dzielenia n^{k_1} i n^{k_2}, $k_1 < k_2$, to p dzieli

$$n^{k_2} - n^{k_1} = n^{k_1}(n^{k_2-k_1} - 1).$$

Skoro n i p są względnie piersze, to p dzieli $n^{k_2-k_1} - 1$, czyli $n^{k_2-k_1}$ daje resztę 1 z dzielenia przez p i oczywiście $k_2 - k_1 \leq p-1$.

Niech teraz k będzie najmniejszą taką liczbą całkowitą dodatnią, że $n^k \equiv 1 \pmod{p}$. Pokażemy, że $k|(p-1)$.

Niech teraz k będzie najmniejszą taką liczbą całkowitą dodatnią, że $n^k \equiv 1 \pmod{p}$. Pokażemy, że $k|(p-1)$.
Rozważmy następujące zbiory: dla każdego $r \in \{1, 2, \ldots, p-1\}$ zbiór A_r składa się z reszt z dzielenia przez p liczb rn, rn^2, $\ldots$, rn^k. Oczywiście $A_r \subseteq \{1, 2, \ldots, p-1\}$. Udowodnimy teraz kilka własności zbiorów A_r.

Niech teraz k będzie najmniejszą taką liczbą całkowitą dodatnią, że $n^k \equiv 1 \pmod{p}$. Pokażemy, że $k|(p-1)$.
Rozważmy następujące zbiory: dla każdego $r \in \{1, 2, \ldots, p-1\}$ zbiór A_r składa się z reszt z dzielenia przez p liczb rn, rn^2, $\ldots$, rn^k. Oczywiście $A_r \subseteq \{1, 2, \ldots, p-1\}$. Udowodnimy teraz kilka własności zbiorów A_r.
1. Każdy ze zbiorów A_r ma dokładnie k elementów.

Niech teraz k będzie najmniejszą taką liczbą całkowitą dodatnią, że $n^k \equiv 1 \pmod{p}$. Pokażemy, że $k|(p-1)$.
Rozważmy następujące zbiory: dla każdego $r \in \{1, 2, \ldots, p-1\}$ zbiór A_r składa się z reszt z dzielenia przez p liczb rn, rn^2, ..., rn^k. Oczywiście $A_r \subseteq \{1, 2, \ldots, p-1\}$. Udowodnimy teraz kilka własności zbiorów A_r.
1. Każdy ze zbiorów A_r ma dokładnie k elementów.
Gdyby było

$$rn^{k_1} \equiv rn^{k_2} \pmod{p},$$

to $p|rn^{k_1}(n^{k_2-k_1}-1)$. Stąd $n^{k_2-k_1}$ daje resztę 1 z dzielenia przez p. Ale $k_2 - k_1 < k$, a założyliśmy, że k jest najmniejszą liczbą całkowitą dodatnią taką, że $n^k \equiv 1 \pmod{p}$. Dostaliśmy sprzeczność, co dowodzi, że istotnie otrzymywane reszty są parami różne.

2. Dla dwóch różnych $r_1, r_2 \in \{1, 2, \ldots, p-1\}$ zbiory A_{r_1}, A_{r_2} są albo równe albo rozłączne.

2. Dla dwóch różnych $r_1, r_2 \in \{1, 2, \ldots, p-1\}$ zbiory A_{r_1}, A_{r_2} są albo równe albo rozłączne.
Załóżmy, że A_{r_1} i A_{r_2} nie są rozłączne, tzn. istnieją $k_1, k_2 \in \{1, 2, \ldots k\}$ takie, że

$$r_1 n^{k_1} \equiv r_2 n^{k_2} \pmod{p}.$$

Stąd wynika, że

$$r_1 n^{k_1+m} \equiv r_2 n^{k_2+m} \pmod{p}$$

dla dowolnej dodatniej liczby całkowitej m. To już dowodzi, że zbiory A_{r_1} i A_{r_2} są równe.

3. $A_1 \cup A_2 \cup \ldots \cup A_{p-1} = \{1, 2, \ldots, p-1\}$

3. $A_1 \cup A_2 \cup \ldots \cup A_{p-1} = \{1, 2, \ldots, p-1\}$
Niech $r \in \{1, 2, \ldots, p-1\}$. Wówczas

$$rn^k \equiv r \pmod{p},$$

więc $r \in A_r$.

3. $A_1 \cup A_2 \cup \ldots \cup A_{p-1} = \{1, 2, \ldots, p-1\}$
Niech $r \in \{1, 2, \ldots, p-1\}$. Wówczas

$$rn^k \equiv r \pmod{p},$$

więc $r \in A_r$.
Podzieliliśmy więc $(p-1)$-elementowy zbiór $\{1, 2, \ldots p-1\}$ na pewną liczbę rozłącznych podzbiorów k-elementowych. Stąd $p - 1 = km$ dla pewnego $m \in \mathbb{Z}$, a zatem

$$n^{p-1} = (n^k)^m \equiv 1^m = 1 \pmod{p},$$

co kończy dowód.

□

Dowód 3:
Bez straty ogólności możemy założyć, że n jest dodatnie, bo to pokrywa wszystkie możliwe reszty z dzielenia przez p.

Dowód 3:
Bez straty ogólności możemy założyć, że n jest dodatnie, bo to pokrywa wszystkie możliwe reszty z dzielenia przez p.
Rozpatrzmy wszystkie możliwe kolorowania koła podzielonego na p części za pomocą n kolorów. Kolorowania, które możemy na siebie nałożyć po obrócenia koła traktujemy jako różne.

Dowód 3:
Bez straty ogólności możemy założyć, że n jest dodatnie, bo to pokrywa wszystkie możliwe reszty z dzielenia przez p.
Rozpatrzmy wszystkie możliwe kolorowania koła podzielonego na p części za pomocą n kolorów. Kolorowania, które możemy na siebie nałożyć po obrócenia koła traktujemy jako różne.
Wszystkich kolorowań jest n^p. Kolorowań jednokolorowych jest, oczywiście, n.

Dowód 3:
Bez straty ogólności możemy założyć, że n jest dodatnie, bo to pokrywa wszystkie możliwe reszty z dzielenia przez p.
Rozpatrzmy wszystkie możliwe kolorowania koła podzielonego na p części za pomocą n kolorów. Kolorowania, które możemy na siebie nałożyć po obrócenia koła traktujemy jako różne.
Wszystkich kolorowań jest n^p. Kolorowań jednokolorowych jest, oczywiście, n.
Rozważmy teraz kolorowanie używające co najmniej dwóch kolorów. Mając jedno takie kolorowanie możemy je obracać, otrzymując inne. Pokażemy, że każdy obrót o $\frac{k}{p} \cdot 360^\circ$ dla $k \in \{0, 1, 2, \ldots, p-1\}$ daje inne kolorowanie.

Wybierzmy dowolne kolorowanie danego koła. Niech α będzie najmniejszym niezerowym kątem takim, że obrót o α daje znów to samo kolorowanie. Oczywiście $\alpha = \frac{k}{p} \cdot 360^\circ$ dla pewnego $k \in \mathbb{N}$. Niech $p = mk + r$, gdzie $m \in \mathbb{Z}$, $r \in \{0, 1, \ldots, k-1\}$. Zauważmy, że wówczas obrót koła o kąt $\frac{r}{p} \cdot 360^\circ$ także daje to samo kolorowanie. Skoro α była najmniejszym niezerowym kątem dającym to samo kolorowanie, to musi być $r = 0$, a stąd

$$km = p.$$

Stąd mamy $k = 1$ lub $k = p$. W pierwszym przypadku kolorowanie jest jednokolorowe, a w drugim to samo kolorowanie otrzymywane jest dopiero po obrocie koła o pełne 360°.

Zatem, jeżeli mamy dane kolorowanie używające co najmniej dwóch kolorów, to przy obracaniu koła o $\frac{k}{p} \cdot 360^\circ$ to kolorowanie się nie powtórzy. Ten sam argument możemy zastosować dla kolorowń powstałych po obrocie wyjściowego kolorwania o $\frac{1}{p} \cdot 360^\circ$, $\frac{2}{p} \cdot 360^\circ$, ... Zatem istotnie każdy obrót o $\frac{k}{p} \cdot 360^\circ$ dla $k \in \{0, 1, 2, \ldots, p-1\}$ daje inne kolorowanie. Jak już wspomnieliśmy, wszystkich kolorowań jest n^p, a kolorowań jednokolorowych n. Kolorowań co najmniej dwukolorowych jest więc $n^p - n$ i właśnie pokazaliśmy, że ich zbiór może zostać podzielony na pewną liczbę rozłącznych p-elementowych podzbiorów. Stąd

$$p | n^p - n,$$

czego należało dowieść.

□

Zadanie

Dana jest liczba pierwsza $p > 2$. Wykaż, że istnieje nieskończenie wiele takich dodatnich liczb całkowitych n, że liczba $2^n - n$ jest podzielna przez p.

Zadanie

Dana jest liczba pierwsza $p > 2$. Wykaż, że istnieje nieskończenie wiele takich dodatnich liczb całkowitych n, że liczba $2^n - n$ jest podzielna przez p.

Rozwiązanie:
Oczywiście p jest względnie pierwsza z 2, więc z Małego Twierdzenia Fermata

$$2^{p-1} \equiv 1 \pmod{p},$$

a więc także

$$2^{k(p-1)} \equiv 1 \pmod{p}$$

dla dowolnej liczby naturalnej k.

Zadanie

Dana jest liczba pierwsza $p > 2$. Wykaż, że istnieje nieskończenie wiele takich dodatnich liczb całkowitych n, że liczba $2^n - n$ jest podzielna przez p.

Rozwiązanie:
Oczywiście p jest względnie pierwsza z 2, więc z Małego Twierdzenia Fermata

$$2^{p-1} \equiv 1 \pmod{p},$$

a więc także

$$2^{k(p-1)} \equiv 1 \pmod{p}$$

dla dowolnej liczby naturalnej k.Ponadto, oczywiście

$$k(p-1) \equiv -k \pmod{p},$$

czyli

$$2^{k(p-1)} - k(p-1) \equiv 1 + k \pmod{p}.$$

Jeżeli więc będzie $k \equiv -1 \pmod{p}$, to otrzymamy liczbę podzielną przez p. Zatem warunki zadania spełniają wszystkie liczby powstaci $n = (p-1)(pm-1)$ dla pewnego całkowitego, dodatniego n, których jest, oczywiście, nieskończenie wiele.

Zadanie

Dana jest liczba pierwsza p oraz takie dodatnie liczby całkowite m, n, że

$$m \equiv n \pmod{p(p-1)}.$$

Udowodnij, że $m^m \equiv n^n \pmod{p}$.

Zadanie

Dana jest liczba pierwsza p oraz takie dodatnie liczby całkowite m, n, że

$$m \equiv n \pmod{p(p-1)}.$$

Udowodnij, że $m^m \equiv n^n \pmod{p}$.

Rozwiązanie:

Jeżeli n jest podzielna przez p, to także m jest podzielna przez p i wtedy teza jest oczywista. Załóżmy więc, że n jest względnie pierwsza z p.

Zadanie

Dana jest liczba pierwsza p oraz takie dodatnie liczby całkowite m, n, że

$$m \equiv n \pmod{p(p-1)}.$$

Udowodnij, że $m^m \equiv n^n \pmod{p}$.

Rozwiązanie:
Jeżeli n jest podzielna przez p, to także m jest podzielna przez p i wtedy teza jest oczywista. Załóżmy więc, że n jest względnie pierwsza z p.
Bez straty ogólności $m > n$. Wówczas z warunku z zadania wynika, że

$$m = k(p-1) + n$$

dla pewnej liczby naturalnej k. Wówczas

$$m^m \equiv n^m = (n^{p-1})^k \cdot n^n \equiv n^n \pmod{p},$$

co kończy rozwiązanie zadania.