“Czy mamy dość teorii liczb?” - rozwiązania

Mateusz Jocz

1. Udowodnić, że dla liczby pierwszej p istnieje takie n naturalne, że

$$p|2^n - n$$

Źródło: Staszic

2. Udowodnić, że dla liczby pierwszej p istnieje nieskończenie wiele liczb naturalnych n takich, że

$$p|2^n - n$$

Źródło: Staszic

Rozwiązanie:

(a) Jeżeli $p = 2$ to teza jest spełniona dla $n = 2$. Dalej zakładamy że $p \neq 2$.

(b) Z małego twierdzenia Fermata mamy:

$$2^{p-1} \equiv 1 \mod p$$

Teraz na mocy *lematu o rzędzie* otrzymujemy $\text{ord}(2,p)|p-1$. Z tego wynika, że liczby $\text{ord}(2,p)$ i p są względnie pierwsze.

(c) Wykażemy, że teza jest spełniona dla pewnego $n = kd$, gdzie k jest całkowite, a $d = \text{ord}(2,p)$. Dla każdego k, z definicji rzędu d, mamy:

$$(2^d)^k \equiv 1^k \mod p$$

$$2^n \equiv 1 \mod p$$

(d) Rozważmy zbiór liczb $A = \{0, d, 2d, \ldots, (p-1)d\}$. Wiemy, że p jest względnie pierwsze z d. Jeżeli istniałyby dwie liczby h i l $(0 \leq l < h < p)$, takie że hd i ld dawałyby takie same reszty z dzielenia przez p to mielibyśmy $p|d(h-l) \Rightarrow p|h-l$, sprzeczność. Zatem liczby ze zbioru A dają różne reszty z dzielenia przez p, a skoro w A jest tyle samo liczb, co w zbiorze wszystkich reszt, to liczby z A dają wszystkie reszty z dzielenia przez p, w szczególności dla pewnego $m \in \{0, 1, 2, \ldots, p-1\}$ mamy:

$$md \equiv 1 \mod p$$

(e) Definiujemy

$$n := md$$

gdzie m, d określone są wyżej. Udowodniliśmy, że

$$2^n \equiv 1 \mod p \text{ oraz } n \equiv 1 \mod p$$

Stąd wynika, że

$$p|2^n - n$$

Istnieje więc liczba n spełniająca warunki zadania, pozostaje dowieść, że takich liczb jest nieskończenie wiele.

(f) Niech z będzie dowolną liczbą naturalną, $d = \text{ord}(2, p)$, jak wyżej, a n będzie takie, że $n \equiv 2^n \equiv 1 \mod p$. Zauważmy że:

$$n + zpd \equiv n \equiv 1 \mod p$$

$$2^{n+zpd} = 2^n \cdot (2^d)^{zp} \equiv 1 \cdot 1^{zp} = 1 \mod p$$

$$2^{n+zpd} - (n + zpd) \equiv 0 \mod p$$

Ponieważ z może być dowolną liczbą naturalną to otrzymujemy nieskończenie wiele rozwiązań postaci $n + zpd$.

3. Rozstrzygnąć, dla jakich $k \in \mathbb{N}$ istnieje liczba naturalna n, będąca kwadratem liczby naturalnej i zaczynająca się w zapisie dziesiętnym k jedynkami.
Źródło: Mathlinks

Rozwiązanie:

(a) Dla $k = 0$ taka liczba oczywiście istnieje, na przykład $n = 4 = 2^2$.

(b) Dla $k \geq 1$ mamy:

$$\underbrace{33\ldots3}_{k-1\ razy}\ 4^2 = (\frac{10^{k-1} - 1}{3} \cdot 10 + 4)^2 =$$

$$= \frac{10^{2k-2} - 2 \cdot 10^{k-1} + 1}{9} \cdot 10^2 + 8 \cdot 10 \cdot \frac{10^{k-1} - 1}{3} + 16 =$$

$$= \frac{10^{2k}}{9} - 20 \cdot \frac{10^k}{9} + \frac{100}{9} + 24 \cdot \frac{10^k}{9} - \frac{240}{9} + \frac{90}{9} + 6 =$$

$$= \frac{10^{2k}}{9} - \frac{10^k}{9} + 5 \cdot \frac{10^k}{9} - \frac{50}{9} + 6 =$$

$$= \frac{10^k - 1}{9} \cdot 10^k + 5 \cdot \frac{10^{k-1} - 1}{9} \cdot 10 + 6 =$$

$$= \underbrace{11\ldots1}_{k\ razy}\ \underbrace{55\ldots5}_{k-1\ razy}\ 6$$

Stąd już widzimy, że o ile $k \geq 1$ to taka liczba n dla każdego k istnieje.

(c) Ostatecznie liczba naturalna n o wymaganych własnościach istnieje dla wszystkich $k \in \mathbb{N}$, *c.k.d.*

(d) Oczywiście istnieją też inne przykłady podobnych liczb, np.:

$$\underbrace{33\ldots3}_{k+1\ razy}{}^2 = \underbrace{11\ldots1}_{k\ razy}0\underbrace{88\ldots8}_{k\ razy}9$$

$$\underbrace{33\ldots3}_{k-1\ razy}\ 45^2 = \underbrace{11\ldots1}_{k\ razy}\ \underbrace{88\ldots8}_{k-2\ razy}\ 9025$$

(e) **Komentarz:** Takie rozwiązanie narzuca się, jeżeli pomyśli się, że liczba $111111\ldots$ jest prawie równa $10^{2k} \cdot 1/9$, a przecież ta liczba jest kwadratem liczby $10^k \cdot 1/3$ równej $333333\ldots$. Potem te "prawie" trzeba oczywiście sformalizować...

4. * Udowodnić, że równanie

$$x^2 + y^2 + z^2 = (x - y)(y - z)(z - x)$$

ma nieskończenie wiele rozwiązań w liczbach naturalnych x, y, z.
Źródło: Mathlinks

Rozwiązanie:

(a) Niech k będzie dowolną liczbą całkowitą dodatnią. Rozważmy rozwiązania postaci:

$$(x, y, z) = (\ (2k-1)(6k^2+1), 2k(6k^2+1), (2k+1)(6k^2+1)\ )$$

Obliczamy, że lewa strona równania jest równa:

$$x^2+y^2+z^2 = (2k-1)^2(6k^2+1)^2 + (2k)^2(6k^2+1)^2 + (2k+1)^2(6k^2+1)^2 =$$

$$= (6k^2+1)^2(4k^2-4k+1+4k^2+4k^2+4k+1) = (6k^2+1)^2(12k^2+2) = 2(6k^2+1)^3$$

Natomiast prawa strona równania wynosi:

$$(x-y)(y-z)(z-x) = (6k^2+1)(2k-1-2k)\cdot(6k^2+1)(2k-2k-1)\cdot(6k^2+1)(2k+1-2k+1) =$$

$$= (6k^2+1)^2 \cdot 2(6k^2+1) = 2(6k^2+1)^3$$

Widzimy, że obie strony równania są równe. Ponieważ k jest dowolną liczbą całkowitą dodatnią i dla różnych k wartości liczby $z = (2k+1)(6k^2+1)$ są różne, to otrzymaliśmy nieskończoną liczbę rozwiązań postaci

$$(x, y, z) = (\ (2k-1)(6k^2+1), 2k(6k^2+1), (2k+1)(6k^2+1)\ )$$

Koniec dowodu – punkt następny służy tylko objaśnieniu i nie potrzeba go pisać np. na olimpiadzie.

(b) *W jaki sposób możemy znaleźć właśnie taką postać rozwiązania?*

i. Na początku stwierdzamy, że trzy niewiadome to trochę za dużo. Spróbujmy ograniczyć się do dwóch. Warto więc aby (x, y, z) był jakimś ciągiem, którego wyrazy możemy zapisać za pomocą dwóch niewiadomych. Jako jeden z pierwszych nasuwa nam się ciąg arytmetyczny. Różnicę naszego ciągu oznaczmy przez r. Prawdziwe są równości:

$$x = y - r \quad \text{i} \quad z = y + r$$

Po podstawieniu tych równości możemy zredukować równanie

$$x^2+y^2+z^2 = (x-y)(y-z)(z-x)$$

do postaci:

$$3y^2 = 2r^2(r-1)$$

ii. Z powyższego równania możemy wyliczyć y:

$$y = \sqrt{\frac{2r^2(r-1)}{3}} = r\sqrt{\frac{2(r-1)}{3}}$$

Jeżeli teraz znajdziemy nieskończenie wiele takich r całkowitych dodatnich, że $r\sqrt{\frac{2(r-1)}{3}}$ jest całkowite (oczywiście jest też wtedy dodatnie) i przyjmiemy

$$r_y := r\sqrt{\frac{2(r-1)}{3}},\ r_x := r_y - r,\ r_z := r_y + r$$

to trójka (r_x, r_y, r_z) będzie rozwiązaniem naszego wyjściowego równania.

iii. Kiedy $\sqrt{\frac{2(r-1)}{3}}$ może być całkowite?
Żeby było to całkowite, wystarczy, żeby r było postaci $r = 6k^2+1$, gdzie $k \in \mathbb{Z}_+$ – wtedy $\sqrt{\frac{2(r-1)}{3}} = 2k$.
Przyjmujemy więc takie r i wyliczamy

$$r_y = 2k(6k^2+1),\ r_x = (2k-1)(6k^2+1),\ r_z = (2k+1)(6k^2+1)$$

5. * Znajdź wszystkie liczby naturalne n takie, że

$$n^2|3^n+1$$

Źródło: Staszic

Rozwiązanie:

(a) Załóżmy, że dla pewnego $n>1$ teza jest spełniona. Wtedy możemy n przedstawić w postaci: $n=k\cdot p$, gdzie p jest **najmniejszym** pierwszym dzielnikiem liczby n, a k jest pewną liczbą całkowitą dodatnią.

(b) Zauważmy, że $3 \not| n$ i tym samym $p \neq 3$. Sensowny jest więc napis $\text{ord}(3,p)$ Zauważmy, że:

$$3^n \equiv -1 \mod p$$

$$3^{2n} \equiv 1 \mod p$$

Na mocy *lematu o rzędzie* mamy $\text{ord}(3,p)|2n = 2pk$. Z drugiej strony z (wniosku z) *lematu o rzędzie* wynika że $\text{ord}(3,p)|p-1$, czyl $\text{ord}(3,p)$ jest względnie pierwsze z p. Zatem $\text{ord}(3,p)|2k$.

(c) Niech d będzie największym wspólnym dzielnikiem liczb $\text{ord}(3,p)$ i k.
Możliwe są dwa przypadki: $\text{ord}(3,p)=d$ lub $\text{ord}(3,p)=2d$. W obu przypadkach, jeżeli $d \geq p$, to $\text{ord}(3,p) \geq p$ i otrzymujemy sprzeczność z $\text{ord}(3,p)|p-1$. Stąd wynika $d<p$.

(d) Liczby $d<p$ i p są dzielnikami n, przy czym p jest najmniejszym dzielnikiem pierwszym, więc $d=1$ (kluczowy moment) i tym samym

$$\text{ord}(3,p)=1 \text{ lub } \text{ord}(3,p)=2$$

korzystając z definicji rzędu otrzymujemy

$$3^1 \equiv 1 \mod p \text{ lub } 3^2 \equiv 1 \mod p$$

$$p|2 \text{ lub } p|8$$

A więc $p=2$, $n=2k$, czyli $4|n^2$. Zauważmy, że jeśli n jest parzyste to $3^n \equiv 1 \mod 4$. Liczba 3^n+1 nie może więc być podzielna przez 4. Sprzeczność.

(e) Pozostaje nam przypadek gdy $n=1$. Łatwo zauważyć, że teza jest teraz spełniona. Jest to więc jedyne rozwiązanie.