Liczby pierwsze i złożone

Mieszko Zimny

Koło Pasjonatów Matematyki UW

April 12, 2021

Zaczniemy od tematu, który zapewne jest w mniejszym lub większym stopniu wszystkim znany, czyli liczby pierwsze i złożone.

Zaczniemy od tematu, który zapewne jest w mniejszym lub większym stopniu wszystkim znany, czyli liczby pierwsze i złożone.

Definicja

Liczbę całkowitą większą od 1 nazywamy liczbą pierwszą, jeżeli posiada dokładnie dwa dzielniki: 1 i samą siebie.

Zaczniemy od tematu, który zapewne jest w mniejszym lub większym stopniu wszystkim znany, czyli liczby pierwsze i złożone.

Definicja

Liczbę całkowitą większą od 1 nazywamy liczbą pierwszą, jeżeli posiada dokładnie dwa dzielniki: 1 i samą siebie.
Liczbę całkowitą większą od 1, która nie jest liczbą pierwszą nazywamy liczbą złożoną.

Zaczniemy od tematu, który zapewne jest w mniejszym lub większym stopniu wszystkim znany, czyli liczby pierwsze i złożone.

Definicja

Liczbę całkowitą większą od 1 nazywamy liczbą pierwszą, jeżeli posiada dokładnie dwa dzielniki: 1 i samą siebie.
Liczbę całkowitą większą od 1, która nie jest liczbą pierwszą nazywamy liczbą złożoną.

Liczby pierwsze: 2, 3, 5, 7, 11, 13, ...

Zaczniemy od tematu, który zapewne jest w mniejszym lub większym stopniu wszystkim znany, czyli liczby pierwsze i złożone.

Definicja

Liczbę całkowitą większą od 1 nazywamy liczbą pierwszą, jeżeli posiada dokładnie dwa dzielniki: 1 i samą siebie.
Liczbę całkowitą większą od 1, która nie jest liczbą pierwszą nazywamy liczbą złożoną.

Liczby pierwsze: 2, 3, 5, 7, 11, 13, ...

Obserwacja

Każda liczba naturalna większa od 1 jest podzielna przez pewną liczbę pierwszą.

Pierwsze naturalne pytanie: Ile jest liczb pierwszych?
To pytanie zadawano sobie już w starożytności i wtedy też znaleziono odpowiedź: liczb pierwszych jest nieskończenie wiele. Pierwszy znany nam kompletny dowód tego faktu podał Euklides, z czasem pojawiło się wiele innych. My jednak zajmiemy się oryginalnym dowodem Euklidesa, ponieważ jest najprostszy.

Twierdzenie (Euklides)

Istnieje nieskończenie wiele liczb pierwszych.

Twierdzenie (Euklides)

Istnieje nieskończenie wiele liczb pierwszych.

Dowód

Załóżmy, że liczby pierwszych jest tylko skończenie wiele i oznaczmy ich liczbę przez n. Niech $p_1, p_2, \ldots p_n$ będą wszystkimi liczbami pierwszymi. Rozważmy liczbę $P = p_1 p_1 \ldots p_n + 1$. Jest to z pewnością liczba naturalna większa od 1, więc musi być podzielna przez pewną liczbą pierwszą, powiedzmy p_i. Ale p_i dzieli też $p_1 p_2 \ldots p_n$. Stąd p_i musi dzielić

$$P - p_1 p_2 \ldots p_n = p_1 p_2 \ldots p_n + 1 - p_1 p_2 \ldots p_n = 1.$$

Mamy sprzeczność, bo żadna liczba pierwsza nie może dzielić 1.

□

Podstawowe Twierdzenie Arytmetyki

Każda liczba naturalna większa od 1 może być jednoznacznie przedstawiona jako iloczyn liczb pierwszych.

Podstawowe Twierdzenie Arytmetyki

Każda liczba naturalna większa od 1 może być jednoznacznie przedstawiona jako iloczyn liczb pierwszych.

Dowód jest dość długi i żmudny i nie uważam, żeby przechodzenie przez niego było dla nas bardzo rozwijające, więć nie będę go przedstawiał.

Wiemy więc, że każda liczba naturalna n większa od 1 może zostać jednoznacznie przedstawiona w postaci

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}.$$

Podstawowe Twierdzenie Arytmetyki

Każda liczba naturalna większa od 1 może być jednoznacznie przedstawiona jako iloczyn liczb pierwszych.

Dowód jest dość długi i żmudny i nie uważam, żeby przechodzenie przez niego było dla nas bardzo rozwijające, więć nie będę go przedstawiał.
Wiemy więc, że każda liczba naturalna n większa od 1 może zostać jednoznacznie przedstawiona w postaci

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}.$$

A co z liczbami ujemnymi? Jeżeli n jest ujemną liczbą całkowitą mniejszą od -1, to oczywiście $-n$ jest dodatnią liczbą całkowitą większą od 1, a stąd

$$n = -p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_m}.$$

Podstawowe Twierdzenie Arytmetyki

Każda liczba naturalna większa od 1 może być jednoznacznie przedstawiona jako iloczyn liczb pierwszych.

Dowód jest dość długi i żmudny i nie uważam, żeby przechodzenie przez niego było dla nas bardzo rozwijające, więć nie będę go przedstawiał.
Wiemy więc, że każda liczba naturalna n większa od 1 może zostać jednoznacznie przedstawiona w postaci

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}.$$

A co z liczbami ujemnymi? Jeżeli n jest ujemną liczbą całkowitą mniejszą od -1, to oczywiście $-n$ jest dodatnią liczbą całkowitą większą od 1, a stąd

$$n = -p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_m}.$$

Zatem każda liczba całkowita jest albo równa 0 albo równa 1, albo równa -1, albo postaci

$$(-1)^k p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_m}.$$

Definicja

Liczby całkowite m, n nazywamy względnie pierwszymi, gdy ich największy wspólny dzielnik wynosi 1.

Zadanie

Wyznacz wszystkie pary liczb całkowitych (x, y), dla których

$$(x - 2y - 1)(x - y + 1) = 5.$$

Zadanie

Wyznacz wszystkie pary liczb całkowitych (x, y), dla których

$$(x - 2y - 1)(x - y + 1) = 5.$$

Rozwiązanie:
Jedyne sposoby na zapisanie liczby 5 jako iloczynu dwóch liczb całkowitych, to (uwzględniając kolejność):

$$5 = 5 \cdot 1 = 1 \cdot 5 = (-5) \cdot (-1) = (-1) \cdot (-5).$$

Zadanie

Wyznacz wszystkie pary liczb całkowitych (x, y), dla których

$$(x - 2y - 1)(x - y + 1) = 5.$$

Rozwiązanie:
Jedyne sposoby na zapisanie liczby 5 jako iloczynu dwóch liczb całkowitych, to (uwzględniając kolejność):

$$5 = 5 \cdot 1 = 1 \cdot 5 = (-5) \cdot (-1) = (-1) \cdot (-5).$$

Stąd, aby podania w zadaniu równość zachodziła, musi być spełniony któryś z poniższych układów równań:

$$\begin{cases} x - 2y - 1 = 5 \\ x - y + 1 = 1 \end{cases} \quad \begin{cases} x - 2y - 1 = 1 \\ x - y + 1 = 5 \end{cases}$$

$$\begin{cases} x - 2y - 1 = -5 \\ x - y + 1 = -1 \end{cases} \quad \begin{cases} x - 2y - 1 = -1 \\ x - y + 1 = -5 \end{cases}$$

Dostajemy z nich kolejno rozwiązania:

$$x = -6, y = -6, \quad x = 6, y = 2,$$

$$x = 0, y = 2, \quad x = -12, y = -6.$$

W każdym przypadku dostajemy liczby całkowite, więc mamy odpowiedź: istnieją cztery takie pary - $(-6, -6)$, $(6, 2)$, $(0, 2)$, $(-12, -6)$.

Zadanie

Czy istnieją dodatnie liczby całkowite m, n, k spełniające równanie

$$6^m \cdot 12^n = 18^k?$$

Zadanie

Czy istnieją dodatnie liczby całkowite m, n, k spełniające równanie

$$6^m \cdot 12^n = 18^k?$$

Rozwiązanie:
Po rozłożeniu obu stron na czynniki pierwsze, dostajemy

$$2^m \cdot 3^m \cdot 3^n \cdot 2^{2n} = 2^k \cdot 3^{2k}$$

$$2^{m+2n} \cdot 3^{m+n} = 2^k \cdot 3^{2k}.$$

Skoro rozkład na czynniki pierwsze jest jednoznaczny, to musi być spełniony układ równań

$$\begin{cases} m + 2n = k \\ m + n = 2k \end{cases}$$

Skoro $n > 0$, to musi być $m + 2n > m + n$. Z drugiej strony, skoro $k > 0$, to musi być $2k > k$. Dostajemy sprzeczość, co dowodzi, że liczby o podanych własnościach nie istnieją.

Zadanie

Znaleźć wszystkie pary (x, y) liczb całkowitych dodatnich takie, że

$$2^x + 2^y = 2^{100}.$$

Zadanie

Znaleźć wszystkie pary (x, y) liczb całkowitych dodatnich takie, że

$$2^x + 2^y = 2^{100}.$$

Rozwiązanie:

Jeżeli $x = y$, to równanie sprowadza się do

$$2 \cdot 2^x = 2^{100}$$

$$2^{x+1} = 2^{100},$$

zatem $x = 99$ i dostajemy parę $(99, 99)$.

Zadanie

Znaleźć wszystkie pary (x, y) liczb całkowitych dodatnich takie, że

$$2^x + 2^y = 2^{100}.$$

Rozwiązanie:

Jeżeli $x = y$, to równanie sprowadza się do

$$2 \cdot 2^x = 2^{100}$$

$$2^{x+1} = 2^{100},$$

zatem $x = 99$ i dostajemy parę $(99, 99)$.

Załóżmy teraz, że $x \neq y$. Bez straty ogólności $x < y$. Po podzieleniu równania stronami przez 2^x, dostajemy

$$1 + 2^{y-x} = 2^{100-x}$$

Zadanie

Znaleźć wszystkie pary (x, y) liczb całkowitych dodatnich takie, że

$$2^x + 2^y = 2^{100}.$$

Rozwiązanie:
Jeżeli $x = y$, to równanie sprowadza się do

$$2 \cdot 2^x = 2^{100}$$

$$2^{x+1} = 2^{100},$$

zatem $x = 99$ i dostajemy parę $(99, 99)$.
Załóżmy teraz, że $x \neq y$. Bez straty ogólności $x < y$. Po podzieleniu równania stronami przez 2^x, dostajemy

$$1 + 2^{y-x} = 2^{100-x}$$

Jednka lewa strona tego równania jest nieparzysta, a prawa parzysta. Otrzymujemy sprzeczność, z czego wynika, że w tym przypadku nie ma rozwiązań, a jedyną parą spełniającą warunki zadania jest $(99, 99)$.

Zadanie

Wyznacz wszystkie liczby pierwsze p, q, r, dla których

$$pq + 3 = 3p + q + r.$$

Zadanie

Wyznacz wszystkie liczby pierwsze p, q, r, dla których

$$pq + 3 = 3p + q + r.$$

Rozwiązanie:
Przekształcając dane równanie, dostajemy

$$pq + 3 - 3p - q = r$$

$$(p - 1)(q - 3) = r.$$

Zadanie

Wyznacz wszystkie liczby pierwsze p, q, r, dla których

$$pq + 3 = 3p + q + r.$$

Rozwiązanie:
Przekształcając dane równanie, dostajemy

$$pq + 3 - 3p - q = r$$

$$(p-1)(q-3) = r.$$

Skoro r jest liczbą pierwszą, to musi być spełniony któryś z poniższych układów:

$$\begin{cases} p-1=1 \\ q-3=r \end{cases} \qquad \begin{cases} p-1=r \\ q-3=1 \end{cases}$$

W pierwszym przypadku z pierwszego równania mamy $p = 2$, a z drugiego wynika, że q i r muszą być liczbami różnej parzystości. Skoro są pierwsze, to jedna z nich musi być równa 2. Musi być to r, ponieważ jest mniejsza. Wówczas $q = 5$ i dostajemy rozwiązanie $(p, q, r) = (2, 5, 2)$.
W drugim przypadku z drugiego równania dostajemy $q = 4$, co nie jes liczbą pierwszą. Zatem w tym przypadku nie ma rozwiązań.

Zadanie

Udowodnij, że jeśli liczba pierwsza p jest większa od 3, to liczba $p^2 - 1$ jest podzielna przez 24.

Zadanie

Udowodnij, że jeśli liczba pierwsza p jest większa od 3, to liczba $p^2 - 1$ jest podzielna przez 24.

Rozwiązanie:
Mamy

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

Skoro p jest liczbą pierwszą większą od 3, to jest nieparzysta, więc $p + 1$ i $p - 1$ są dwiema kolejnymi liczbami parzystymi. Jedna z nich musi być podzielna przez 4, a więc ich iloczyn jest podzielny przez $4 \cdot 2 = 8$. Ponadto, p jest niepodzielna przez 3, a zatem któraś z liczb $p + 1$, $p - 1$ musi być podzielna przez 3. Stąd już wynika, że $p^2 - 1$ jest podzielna przez $8 \cdot 3 = 24$.

Zadanie

Wyznacz wszystkie liczby pierwsze p, dla których liczby $4p^2 + 1$ oraz $6p^2 + 1$ także są pierwsze.

Zadanie

Wyznacz wszystkie liczby pierwsze p, dla których liczby $4p^2 + 1$ oraz $6p^2 + 1$ także są pierwsze.

Rozwiązanie:
Jeżeli nie wiadomo jak zacząć, dobrym pomysłem jest po prostu policzenie wartości $4p^2 + 1$ i $6p^2 + 1$ dla małych wartości p, aby zobaczyć, co się dzieje.

Zadanie

Wyznacz wszystkie liczby pierwsze p, dla których liczby $4p^2 + 1$ oraz $6p^2 + 1$ także są pierwsze.

Rozwiązanie:
Jeżeli nie wiadomo jak zacząć, dobrym pomysłem jest po prostu policzenie wartości $4p^2 + 1$ i $6p^2 + 1$ dla małych wartości p, aby zobaczyć, co się dzieje.

p	$4p^2 + 1$	$6p^2 + 1$
2	17	25
3	37	55
5	101	151
7	197	295

Zadanie

Wyznacz wszystkie liczby pierwsze p, dla których liczby $4p^2 + 1$ oraz $6p^2 + 1$ także są pierwsze.

Rozwiązanie:
Jeżeli nie wiadomo jak zacząć, dobrym pomysłem jest po prostu policzenie wartości $4p^2 + 1$ i $6p^2 + 1$ dla małych wartości p, aby zobaczyć, co się dzieje.

p	$4p^2 + 1$	$6p^2 + 1$
2	17	25
3	37	55
5	101	151
7	197	295

Możemy zauważyć, że w każdym wierszu znajduje się liczba podzielna przez 5.

Możemy więc sformułować hipotezę: dla każdej liczby pierwszej p jedna z liczb p, $4p^2+1$, $6p^2+1$ jest podzielna przez 5.
Udowodnienie tej hipotezy praktycznie natychmiast rozwiązałoby nasze zadanie, ale nie wiadomo, jak się za to zabrać. Możemy za to rozważyć hipotezę dużo mocniejszą, ale potencjalnie prostszą do udowodnienia: dla każdej liczby naturalnej n jedna z liczb n, $4n^2+1$, $6n^2+1$ jest podzielna przez 5.
To już jest łatwe do zweryfikowania.

Zadanie

Udowodnij, że dla każdej liczby całkowitej dodatniej n liczba $n^2 - n$ jest podzielna przez 2.

Zadanie

Udowodnij, że dla każdej liczby całkowitej dodatniej n liczba $n^2 - n$ jest podzielna przez 2.

Rozwiązanie:
Mamy

$$n^2 - n = n(n-1).$$

Jedna z liczb n, $n-1$ musi być podzielna przez 2, więc ich iloczyn także.

Zadanie

Udowodnij, że dla każdej liczby całkowitej dodatniej n liczba $n^3 - n$ jest podzielna przez 3.

Zadanie

Udowodnij, że dla każdej liczby całkowitej dodatniej n liczba $n^3 - n$ jest podzielna przez 3.

Rozwiązanie:
Mamy

$$n^3 - n = n(n^2 - 1) = (n-1)n(n+1)$$

i kończymy rozumowanie podobnie jak poprzednio.

Zadanie

Czy dla każdej liczby całkowitej dodatniej n liczba $n^4 - n$ jest podzielna przez 4?

Zadanie

Czy dla każdej liczby całkowitej dodatniej n liczba $n^4 - n$ jest podzielna przez 4?

Rozwiązanie:
Nie, dla $n = 2$ dostajemy

$$2^4 - 2 = 16 - 2 = 14.$$

Zadanie

Czy dla każdej liczby całkowitej dodatniej n liczba $n^5 - n$ jest podzielna przez 5?

Zadanie

Czy dla każdej liczby całkowitej dodatniej n liczba $n^5 - n$ jest podzielna przez 5?

Rozwiązanie:
Mamy

$$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n-1)n(n+1)(n^2+1).$$

Zadanie

Czy dla każdej liczby całkowitej dodatniej n liczba $n^5 - n$ jest podzielna przez 5?

Rozwiązanie:
Mamy

$$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n-1)n(n+1)(n^2+1).$$

Jeżeli n daje resztę 0, 1 lub 4, to odpowiedź jest pozytywna.
Pozostają nam przypadki, gdy $n = 5k + 2$ lub $n = 5k + 3$.
Wówczas jednak mamy

$$n^2 + 1 = (5k+2)^2 + 1 = 25k^2 + 20k + 5$$

$$n^2 + 1 = (5k+3)^2 + 1 = 25k^2 + 20k + 10.$$

Otrzymujemy liczby podzielne przez 5, zatem w tym przypadku odpowiedź jest pozytywna.

Powstaje naturalne pytanie: czy dla każdej liczby pierwszej p liczba $n^p - n$ jest zawsze podzielna przez p? Okazuje się to prawdą, jest to tzw. Małe Twierdzenie Fermata, które planuję udowodnić na następnym spotkaniu.