Wzory i twierdzenia:

1. Małe Twierdzenie Fermata
2. Twierdzenie Eulera

Jeżeli i , to dzieli liczbę . Innymi słowy: . Jest to silniejsza wersja Małego Twierdzenia Fermata.

1. Funkcja Eulera

Przypisuje zadanej liczbie naturalnej liczbę liczb względnie z nią pierwszych mniejszych od niej samej.

# Podstawowe operacje arytmetyczne

**Treść:** Napisać program, który wykonuje operacje arytmetyczne (mod, +, -, \*, ^) w *Zp* dla dowolnego *p*. Proszę pamiętać, że:

* mod - oznacza wyliczenie reszty modulo z dzielenia liczby X przez *p*,
* +, -, \*, ^ - oznaczają dodawanie, odejmowanie, mnożenie i potęgowanie modulo *p*.

**Rozwiązanie:** Napisałem program w .NET (C#), w którym stworzyłem klasę Modular – zawiera ona przeciążenia operatorów dodawania, odejmowania, mnożenia i potęgowania. Jest też w stanie wyświetlić tabliczki dodawania i mnożenia dla ciała o zadanej charakterystyce. Klasa Modular radzi sobie również z elementami przeciwnymi. Program obsługuje teoretycznie nieskończenie wielkie liczby (struktura BigInteger).

# Metody szukania generatorów w ciele

**Treść:** Znajdź możliwie wiele metod szukania generatorów ciała Z*p* - bądź w stanie wytłumaczyć/omówić te metody. Ile jest generatorów ciała Zp?

**Rozwiązanie:**

Liczbę generatorów (elementów pierwotnych) w ciele można znaleźć za pomocą poniższego wzoru:

gdzie jest funkcją Eulera.

1. Generator (element pierwotny) ciała generuje grupę cykliczną, która jest grupą multiplikatywną tego ciała. Oznacza to, że jeśli jest elementem pierwotnym ciała , jesteśmy w stanie zapisać każdy niezerowy (gdyż zero istnieje w każdym ciele) element tego ciała w następującej postaci , gdzie jest pewną dodatnią liczbą całkowitą.

Aby więc znaleźć wszystkie generatory w ciele wystarczy sprawdzić wszystkie jego kolejne elementy i to, jakie generują grupy cykliczne. Jeśli dany element generuje grupę cykliczną o liczności (czyli wszystkie elementy niezerowe), jest on generatorem.

1. Można również skorzystać z tzw. Małego Twierdzenia Fermata, które jest opisane poniższym wzorem:

gdzie jest pewną liczbą pierwszą. Jeśli powyższe równanie jest prawdziwe dla elementu w ciele , należy sprawdzić wykonać kolejne obliczenia:

W przypadku uzyskania wyniku rząd elementu jest mniejszy od , a więc nie jest generatorem. W przypadku uzyskania wyniku rząd elementu jest równy , a więc element jest generatorem.

1. Np. dla . Szukamy elementów, które w tej potędze dają .
2. Odwrotność multiplikatywna generatora też jest generatorem.
3. - kolejne generatory, gdzie jest względnie pierwsze z , jest pierwszym znalezionym generatorem.

# Odwrotność multiplikatywna modulo

**Treść:** Znajdź implementację obliczania odwrotności multiplikatywnej modulo p oraz modulo n (gdzie n jest iloczynem dwóch liczb pierwszych) - bądź w stanie wytłumaczyć/omówić te metody

**Rozwiązanie:**

Odwrotnością multiplikatywną liczby modulo nazywamy liczbę , która spełnia poniższe równanie:

gdzie i muszą być wzlędnie pierwsze, inaczej odwrotność liczby modulo nie istnieje. Rozwiązanie tego problemu sprowadza się do rozwiązania równania diofantycznego.

Kolejne kroki algorytmu obliczania odwrotności multiplikatywnej liczby modulo

1. Sprawdzenie istnienia odwrotności multiplikatywnej liczby modulo dokonywane jest poprzez sprawdzenie, czy następująca równość jest spełniona:

Jeśli powyższa równość jest prawdziwa, liczba modulo posiada swoją odwrotność multiplikatywną i można kontynuować do kroku nr 2. W przeciwnym wypadku algorytm kończy działanie.

1. Zastosowanie Rozszerzonego Algorytmu Euklidesa w celu rozwiązania równania .

Innym podejściem jest skorzystanie ze wzoru (pod warunkiem, że i są względnie pierwsze:

gdzie jest funkcją Eulera.

Dowód:

# Podzielność liczb

**Treść:** Podzielność liczby *a* prze *b* oznacza, że *b* dzieli *a* (zapis: *b*|*a*) bez reszty, tj. *a* = *k* \* *a* +0, gdzie *k* jest pewną liczbą całkowitą. Udowodnij, że warunkiem podzielności liczby dziesiętnej przez 5 jest ostatnia cyfra równa 0 albo 5. Wyprowadź regułę podzielności przez 11.

**Rozwiązanie:** System liczbowy, z którego korzystamy na co dzień jest systemem pozycyjnym o podstawie . Każdą liczbę w tym systemie można więc zapisać w następujący sposób:

gdzie:

– liczba cyfr w liczbie

Taką reprezentację można łatwo uogólnić do wielomianu:

stąd:

## Podzielność przez 5

Zapis liczby można uprościć, wyciągając wspólny czynnik przed nawias:

Powyższa reprezentacja liczby całkowitej w systemie pozycyjnym o podstawie pokazuje, że liczba jest zawsze podzielna przez , a więc jest zawsze podzielna przez . Oznacza to, że aby było podzielne przez , wystarczy, żeby było podzielne przez , a więc wynosiło lub .

## Podzielność przez 11

Kongruencja:

stąd:

Liczba jest podzielna przez wtedy i tylko wtedy, gdy po odjęciu sumy cyfr z pozycji parzystych od sumy cyfr z pozycji nieparzystych otrzymany wynik będzie podzielny przez 11.

TODO:

- program do szukania wszystkich generatorów w ciele Zp

- program do liczenia odwrotności multiplikatywnej modp, modn