III LICEUM OGÓLNOKSZTAŁCĄCE

im. Adama Mickiewicza

w Tarnowie

Magdalena Ciochoń

# “Kongruencje”

Praca konkursowa pisana pod kierunkiem

mgr Agnieszki Batko

# Spis treści

# Wprowadzenie

W ubiegłorocznej edycji Małopolskiego Konkursu Prac Matematycznych przedstawiłam pracę dotyczącą liczb urojonych, które po poznaniu okazały się nie być tylko "urojonym" tworem genialnych umysłów, ale również tematem, który znajduje szerokie zastosowanie w innych dziedzinach naukowych takich jak: fizyka, chemia, mechanika kwantowa. W tym roku chciałabym zaprezentować pracę z dziedziny teorii liczb na temat "Kongruencje".
Do napisania pracy zainspirowało mnie zadanie matematyczne:

"Czy $5^{36} - 1$ dzieli się przez 13?"

Na początku pomyślałam, żeby znaleźć cechę podzielności liczby 13 i od tego zaczęłam. Po poszukiwaniach okazało się, że aby sprawdzić czy dana liczba jest podzielna przez 13 należy skreślić 3 ostatnie cyfry liczby x i od tak powstałej liczby odjąć liczbę powstałą z tych trzech skreślonych liczb. Jeżeli wynik tej różnicy jest podzielny przez 13 to oznacza, że cała liczba jest również przez nią podzielna. Jednak podczas poszukiwania tej cechy podzielności natknęłam się na pojęcie kongruencji, które okazało się być ściśle związane z powyższym zadaniem. Na początku pojęcie skojarzyło mi się z językiem polskim i gramatyką. Po dalszym poszukiwaniu okazało się, że jest to również zagadnienie matematyczne poruszane w jednym z najstarszych działów matematyki zwanym teorią liczb. Postanowiłam dowiedzieć się więcej na temat tego pojęcia, a tego co się dowiem i zrozumiem przedstawić w formie pracy matematycznej. Na końcu mojej pracy, po wnikliwej analizie kongruencji postaram się z nową wiedzą rozwiązać zadanie, które zainspirowało mnie do poznania nowego pojęcia. Mam nadzieję, że praca ta udowodni, że matematyka, jako królowa nauk potrafi być prosta, przyjemna i przydatna.

Zachęcam do lektury,

Magdalena Ciochoń

# Historia kongruencji

Dość często podczas naszej edukacji spotykamy zagadnienia, które są dla Nas trudne, jednak z czasem po poznaniu nowych pojęć stają się one o wiele łatwiejsze. Z taką sytuacją zmierzamy się w 1 klasie liceum, kiedy spotykamy równania kwadratowe, a jeszcze nie znamy funkcji kwadratowej, czy delty. Identyczną sytuację mieli matematycy zajmujący się teorią liczb. Wielkim ułatwieniem było dla nich wprowadzenie do matematyki pojęcia kongruencji. Wprowadzono je dość późno z perspektywy tego, że matematyka miała swoje zastosowanie już w czasach przed naszą erą, a zbieżność modulo (kongruencje) wprowadzono dopiero w XIX w. Pojęcie to wprowadził Gauss Carl Friedrich w swym dziele *Disquisitiones arithmeticae* (zwane także "księgą siedmiu pieczęci", gdyż składało się z siedmiu części oraz zawierało zwięzłe, cenne informacje), które było poświęcone teorii liczb i kongruencjom. Jednak warto pamiętać, że teoria przystawania liczb nie jest wyłącznie dziełem Gaussa, ale to przez niego została dopracowana, skodyfikowana i wykorzystana do rozstrzygnięcia wielu pytań związanych z podzielnością liczb. Wprowadzenie kongruencji miało ogromne korzyści w przyszłości patrząc na to, że sam pomysł na tle innych był dość prosty, a dużo ułatwił. Sama książka wprowadzająca to pojęcie dała Gausowi szansę na awans do grona cenionych matematyków na całym świecie oraz pozwoliła ona rozwinąć się innym badaczom królowej nauk.
Kongruencje w swoich twierdzeniach wykorzystali m.in. Pierre de Fermat, czy Wilson. Pierre de Fermat wykorzystał zbieżność modulo w Małym Twierdzeniu Fermata, które jest uważane za jedno z najważniejszych osiągnięć w teorii liczb. Twierdzenie to wygląda tak:

*Jeżeli p jest liczbą pierwszą, a liczbą całkowitą niepodzielną przez p, to:*

$$a^{p-1} \equiv 1 \bmod p$$

Jest ono wykorzystywane do testowania pierwszości liczb.

Jeżeli chodzi o twierdzenie Wilsona to daje ono również możliwość sprawdzenia, czy dana liczba naturalna jest liczbą pierwszą, jednak w rzeczywistości nie jest ono stosowane, gdyż nie są znane efektywne algorytmy

obliczania silni, przez co stosowanie tego twierdzenia nie jest łatwe. Samo twierdzenie ma postać:

$$(p - 1)! + 1 \equiv 0 \bmod p$$

# Od początku...

Pojęcie kongruencji jest ściśle związane z resztą z dzielenia. Przypomnijmy sobie, więc twierdzenie o dzieleniu z resztą:

$$\frac{A}{B} = K + R$$

*A* – dzielna

*B* – dzielnik

*K* – iloraz

*R* – reszta, gdzie $0 \leq R < B$

Powyższe twierdzenie możemy również przedstawić za pomocą operatora *modulo* (oznaczenia pozostawiamy takie jak są w powyższym twierdzeniu):

$$A \bmod B = R$$

*A* – dzielna

*B* – moduł

*R* – reszta

Przykłady:

- 4 mod 6 = 4

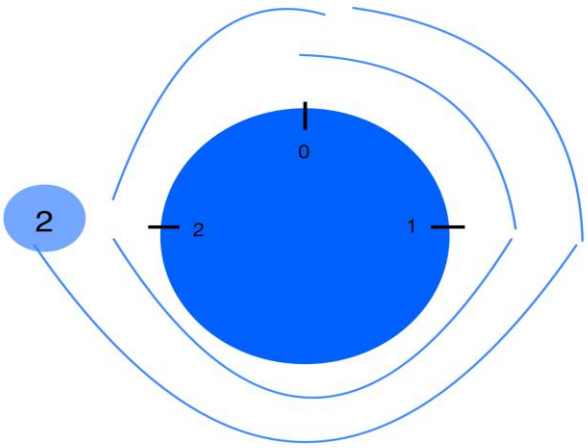
- 6 mod 5 = 1
- 14 mod 2 = 0
- - 8 mod 3 = 1
- -10 mod 5 = 0

# Wizualizacja operacji modulo na tarczy zegara

Przejdźmy od razu do przykładu:

*5 mod 3 = ...*

W tym przypadku nasz moduł wynosi 3. Zatem możliwe reszty z dzielenia przez tę liczbę to: 0,1,2 – konstruujemy, więc zegar o takiej wielkości. Następnie przesuwamy wskazówkę zegara o tyle ile wynosi dzielna, czyli w tym przypadku o 5.



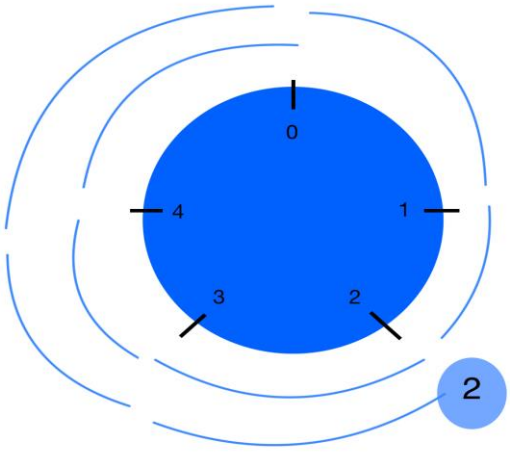

Postępując zgodnie z powyższymi krokami otrzymujemy następującą sekwencję: 1,2,0,1,2. Sekwencja kończy się na liczbie 2, więc jest ona rozwiązaniem powyższej operacji modulo. Zatem: *5 mod 3 = 2.*

*Ważne! Jeżeli dzielna jest liczbą dodatnią poruszamy się zgodnie z ruchem wskazówek zegara, jeżeli ujemna – przeciwnie.*

Przeanalizujmy jeszcze jeden przykład:

*-8 mod 5 = …*

W tym przykładzie nasz moduł wynosi 5. Zatem możliwe reszty z dzielenia przez tę liczbę to: 0,1,2,3,4 – konstruujemy, więc zegar o takiej wielkości. Następnie przesuwamy wskazówkę zegara o –8.




Otrzymujemy następującą sekwencję: 4,3,2,1,0,4,3,2. Ostatnią liczbą sekwencji jest 2, zatem: *-8 mod 5 = 2.*

INNE PRZYKŁADY DO SAMODZIELNEGO ROZWIĄZANIA:

Rozwiąż podane operacje modulo za pomocą wizualizacji na tarczy:

- *9 mod 4 =...*
- -3 mod 2 =...
- -12 mod 10 =…

Należy, jednak pamiętać, że operacja modulo to nie to samo co zbieżność modulo (kongruencje), ale pojęcia te są ze sobą ściśle związane, co postaram się pokazać po wprowadzeniu następnego pojęcia.

# Definicja kongruencji (przystawania modulo)

Kiedy pomiędzy liczbami zachodzi kongruencja?

O dwóch danych liczbach całkowitych a i b mówimy, że przystają do siebie według modułu m (czyli zachodzi pomiędzy nimi kongruencja), jeżeli różnica tych liczb jest podzielna przez liczbę naturalną m. Relację tę zapisujemy symbolicznie w taki sposób:

$$a \equiv b \ (mod n)$$

Powyższe wyrażenie czytamy w następujący sposób: A jest przystające do B modulo C.

Inaczej mówiąc, aby kongruencja była prawdziwa musi zajść równość:

$$a - b = kn, \text{ gdzie } k \in Z$$

Wiadome jest również to, że aby dana zbieżność modulo była prawdziwa liczby całkowite a i b muszą dawać tę samą resztę z dzielenia przez *m* – innymi słowy liczby te muszą należeć do tej samej klasy równoważności.

Powyższy zapis oznacza również, że reszta z dzielenia a przez n jest równa b, czyli $a = kn+b$.

*Przykładowe zadanie:*

Sprawdź czy dana kongruencja jest prawdziwa?

a. $16 \equiv -14 \ (mod 5)$

Rozwiązanie:

$16 - (-14) = 30 = 5 \cdot 6$

Jak widać różnica liczb 16 i –14 jest podzielna przez 5, zatem ta kongruencja jest prawdziwa.

b. $27 \equiv 12 \ (mod 7)$

Rozwiązanie:

$27 - 12 = 15 = 7 \cdot 2 + 1$

Jak widać różnica liczb 27 i 12 nie jest podzielna przez 7, zatem ta kongruencja jest fałszywa.

c. *4 ≡ -81 (mod3)*

Rozwiązanie:

$$\frac{-81}{3} = -27$$

$$\frac{4}{3} = 1 \cdot 3 + 1$$

Reszta z dzielenia 4 przez 3 wynosi 1, a liczby –81 przez 3 wynosi 0, więc reszty z dzielenia są różne - co oznacza, że kongruencja jest nieprawdziwa.

INNE PRZYKŁADY DO SAMODZIELNEGO ROZWIĄZANIA:

Sprawdź czy dana kongruencja jest prawdziwa?

- *14 ≡ 8 (mod 3)*
- *-18≡ -12 (mod 9)*
- *28 ≡ 12 (mod 4)*

**Zatem, czy operacja modulo jest tym samym co zbieżność modulo (kongruencje)?**

*A mod B = R* - operacja modulo

$a \equiv b \pmod{n}$ - zbieżność modulo

Zapisy wyglądają bardzo podobnie, jednak nie są to te same rzeczy, co postaram się teraz pokazać:

Weźmy sobie na przykład kongruencje: *7 ≡ 1(mod3)*, czy ten zapis jest tożsamy z zapisem: *7 mod 3 = 1*?

Jak widać kongruencja jest prawdziwa, gdyż 7-1 = 6 = 2 · 3. Operacja modulo jest również poprawna, więc może te zapisy są równoważne? Sprawdźmy to jeszcze może na jednym przykładzie:

Tym razem weźmy sobie kongruencje: *26 ≡ 11(mod5)* i sprawdźmy czy jest to równoważne zapisowi *26 mod 5 = 11*. Kongruencja tym razem jest również prawdziwa (26 – 11 = 15 = 5 · 3), jednak operacja modulo już nie jest prawdziwa, ponieważ *26 mod 5 = 1*.

Już drugi przykład pokazał nam, że nie są to te same pojęcia, jednak są one ze sobą w jakiś sposób powiązane.

# Podstawowe własności

Zacznijmy od trzech praw, które wskazują, że relacja kongruencji modulo m jest relacją równoważności:

1.PRAWO TOŻSAMOŚCI (ZWROTNOŚĆ)

Prawo to mówi nam, że każda liczba całkowita przystaje według każdego naturalnego modułu:

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

Dowód: Różnica między tymi samymi liczbami całkowitymi zawsze wynosi 0, a ta liczba jest podzielna przez każde naturalne m.

2.PRAWO SYMETRII

Każda kongruencja $a \equiv b \pmod{m}$ jest równoważna kongruencji $b \equiv a \pmod{m}$.

Dowód: $a - b$ i $b - a$ są zawsze albo jednocześnie podzielne lub jednocześnie niepodzielne przez m

3.PRAWO PRZECHODNIOŚCI

Jeżeli $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$ to $a \equiv c \pmod{m}$.

Dowód: $a - c = (a - b) + (b - c)$

Następne cztery dotyczą arytmetyki kongruencji. Mówią one, że relacja kongruencji jest zgodna z dodawaniem, odejmowaniem i mnożeniem, a to

oznacza, że kongruencje wolno dodawać, odejmować, mnożyć, a nawet potęgować stronami.

UWAGA! Nie mamy prawa dzielić stronami kongruencji! (chociaż są przypadki, w których jest to dopuszczalne - odwrotność modulo m, prawo skracania).

1.Jeżeli $a \equiv b \pmod m$ i c $\equiv d \pmod m$ to $a + c \equiv b + d \pmod m$.

Dowód: $(a + c) - (b + d) = (a - b) + (c - d)$

2. Jeżeli $a \equiv b \pmod m$ i c $\equiv d \pmod m$ to $a - c \equiv b - d \pmod m$

Dowód: $(a - c) - (b - d) = (a - b) - (c - d)$

3. Jeżeli $a \equiv b \pmod m$ i c $\equiv d \pmod m$ to $ac \equiv bd \pmod m$

Dowód: $ac - bd = (a - b) \cdot c + (c - d) \cdot b$

4. Jeżeli $a \equiv b \pmod m$ to $a^k \equiv b^k \pmod m$

# Cechy podzielności a kongruencja

Już w szkole podstawowej poznajemy cechy podzielności liczb, ale nie wykazujemy ich. A to właśnie dzięki kongruencjom jesteśmy wstanie w miarę prosty sposób wykazać te cechy podzielności liczb oraz w trudniejszych przypadkach ocenić czy dana liczba jest podzielna przez drugą. Jednak zanim spróbujemy udowodnić dane cechy podzielności musimy poznać następne twierdzenie. Twierdzenie to brzmi:

*Jeżeli f(x) będzie wielomianem o współczynnikach całkowitych to kongruencja*

$a \equiv b \pmod m$ *pociąga za sobą kongruencję* $f(a) \equiv f(b) \pmod m$

Na początku spróbujmy udowodnić cechę podzielności przez 9, która brzmi: dana liczba x jest podzielna przez 9, jeżeli suma jej cyfr jest podzielna przez 9.

Zacznijmy od symbolicznego zapisania liczby w systemie dziesiątkowym, czyli w postaci wielomianu:

[1] $$A = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n$$

$a_0 + a_1 + a_2 + \ldots + a_n$ - *kolejne cyfry liczby A*

Następnie znając ogólny wzór wielomianu *[f(X) = $a_n \cdot X^n + \ldots + a^1 \cdot X + a^0$]* możemy stwierdzić, że w tym przypadku

[2] $A = f(10)$, *gdzie A jest dowolną liczbą naturalną*

Następnym krokiem w udowadnianiu tej cechy jest zauważenie, że:

[3] $10 \equiv 1 \pmod 9$

Dzięki temu spostrzeżeniu możemy zastosować wcześniej poznane twierdzenie:

[4] $a \equiv b \pmod m \Rightarrow f(a) \equiv f(b) \pmod m$

Zatem:

[5] $10 \equiv 1 \pmod 9 \Rightarrow f(10) \equiv f(1) \pmod 9$

Następnie wiedząc już, że $A = f(10)$ oraz [1] zauważamy, że:

[6] $f(1) = a_0 + a_1 + a_2 + \ldots + a_n$

Teraz możemy podstawić [2] i [6] do drugiej części [5]:

[7] $A \equiv a_0 + a_1 + a_2 + \ldots + a_n \pmod 9$

$a_0 + a_1 + a_2 + \ldots + a_n$ *są sumą kolejnych cyfr liczby A*

Patrząc na [7] od razu stwierdzamy, że aby jakaś liczba A była podzielna przez 9 to suma jej kolejnych cyfr musi być podzielna przez 9.

Teraz możemy spróbować udowodnić cechę podzielności liczby 11. Aby to zrobić postępujemy bardzo podobnie jak wcześniej. Dlatego też zacznijmy od przypomnienia cechy podzielności: dana liczba jest podzielna przez 11 jeżeli różnica między sumą cyfr liczby x stojących na miejscach nieparzystych (licząc od prawej), a sumą cyfr na miejscach parzystych jest podzielna przez 11.

Podobnie jak wyżej zacznijmy od symbolicznego zapisania liczby w systemie dziesiętnym:

[1] $A = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n$

$a_0 + a_1 + a_2 + \ldots + a_n$ - *kolejne cyfry liczby A*

Z tego wynika, że:

[2] $A = f(10)$

Następnie musimy znaleźć odpowiednią kongruencje, którą będziemy mogli wykorzystać w dalszej części udowadniania:

[3] $10 \equiv -1 \pmod{11}$

Po raz kolejny korzystając z twierdzenia: $a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m}$ oraz [3] dochodzimy do wniosku, że:

[4] $10 \equiv -1 \pmod{m} \Rightarrow f(10) \equiv f(-1) \pmod{11}$

Wiemy, że $A = f(10)$, ale musimy jeszcze wyliczyć wartość $f(-1)$, co robimy przez podstawienie pod X z wyrażenia [1] - 1, czyli:

[5] $f(-1) = a_0 - a_1 + a_2 - a_{3\ldots}$

Mając już te wszystkie informacje podstawimy [5] i [2] do drugiej części [4]:

[6] $A \equiv a_0 - a_1 + a_2 - a_{3\ldots} \pmod{11}$

Patrząc na [6] zaraz stwierdzamy, że wcześniej zapisana cecha podzielności jest prawidłowa.

Jak widać nie jest to takie trudne. W ramach ćwiczeń można jeszcze udowodnić cechę podzielności liczby 13 i 7.

# Odwrotność modulo

Teraz wróćmy do pojęcia wspomnianego w rozdziale “Podstawowe własności”: odwrotności modulo. Jak już wcześniej wspomniałam w kongruencjach można dodawać, odejmować oraz mnożyć stronami. Teraz zajmijmy się możliwością obustronnego dzielenia przez daną liczbę całkowitą.

Jak wiemy dzielenie to mnożenie przez odwrotność, a iloczyn danej liczby i jej odwrotności jest zawsze równy 1, np.:

Przykładowa liczba: 6

Odwrotność przykładowej liczby: 1/6

Iloczyn przykładowej liczby i jej odwrotności: $6 \cdot 1/6 = 1$

Tak samo jest w kongruencjach: aby dana liczba całkowita była odwracalna modulo to musi istnieć jej odwrotność. Jeżeli ten warunek zostanie spełniony to zachodzi wtedy kongruencja:

$$ax \equiv 1 \pmod{n}$$

x - odwrotność liczby a modulo n

Warto jeszcze zauważyć, że jeżeli a jest odwracalna modulo n to:

$$ax \equiv b \pmod{n} \Leftrightarrow x \equiv ba^{-1} \pmod{n}$$

*Jak oznaczamy odwrotność liczby a modulo m?*

W matematyce odwrotność liczby a modulo m oznaczamy $a^{-1} \equiv b \pmod{n}$, gdy wiemy o jaki moduł chodzi; lub po prostu $a^{-1}$.

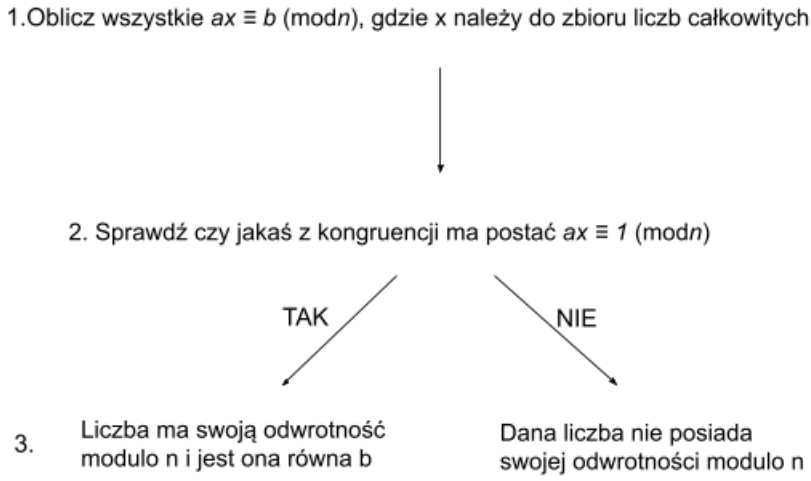
*Kiedy dana liczba a ma swoją odwrotność modulo n?*

Twierdzenie: Liczba a ma odwrotność modulo n wtedy i tylko wtedy, gdy liczby a i n są względnie pierwsze, czyli największy wspólny dzielnik tych liczb jest równy 1 – *NWD (a , n) = 1.*

Zatem nie każda liczba a ma swoją odwrotność modularną n.

*Jak znaleźć odwrotność modularną?*

Zacznijmy od długiej, ale niewymagającej poznawania następnych pojęć metody, którą zwie się METODĄ NAIWNĄ, która została wyjaśniona na poniższym grafie:




Przykłady:

- Oblicz: $4^{-1} \pmod 7 \Rightarrow a = 4, n = 7$

  Krok 1:

  $4 \cdot 0 \equiv 0 \pmod 7$

  $4 \cdot 1 \equiv 4 \pmod 7$

**4 · 2 ≡ 1 (mod 7)**

4 · 3 ≡ 5 (mod 7)

4 · 4 ≡ 2 (mod 7)

4 · 5 ≡ 6 (mod 7)

4 · 6 ≡ 3 (mod 7)

Krok 2 i 3:

Patrząc na kongruencję trzecią z kolei możemy stwierdzić, że podana liczba w przykładzie posiada odwrotność modulo n, która jest równa **2**.

- Oblicz: $5^{-1} \pmod 6 \Rightarrow a = 5, n = 7$

Krok 1:

5 · 0 ≡ 0 (mod 6)

5 · 1 ≡ 5 (mod 6)

5 · 2 ≡ 4 (mod 6)

5 · 3 ≡ 3 (mod 6)

5 · 4 ≡ 2 (mod 6)

**5 · 5 ≡ 1 (mod 6)**

Krok 2 i 3:

W tym przypadku kongruencja o postaci $ax \equiv 1 \pmod n$ znajduje się w ostatniej linijce. Zatem odwrotność modulo n w tym przypadku jest równa **5**.

- Oblicz: $2^{-1} \pmod 4 \Rightarrow a = 2, n = 4$

Krok 1:

2 · 0 ≡ 0 (mod 4)

2 · 1 ≡ 2 (mod 4)

2 · 2 ≡ 0 (mod 4)

2 · 3 ≡ 2 (mod 4)

Krok 2 i 3:

Jak widać z powyższych obliczeń wynika, że podana liczba nie posiada odwrotności modulo n.

- $1878^{-1} \pmod{673}$ - przykład ten zostanie obliczony w dalszej części

Postępowanie w tym przykładzie jest takie same, ale bardzo pracochłonne (trzeba byłoby obliczyć aż 673 kongruencji). Jak można się domyślać istnieje szybsza metoda, ale aby z niej skorzystać musimy poznać rozszerzony algorytm Euklidesa.

**ROZSZERZONY ALGORYTM EUKLIDESA**

Zacznijmy od tego, że algorytm ten pozwala nam wyznaczać największy wspólny dzielnik (NWD), czyli największą liczbę naturalną, która dzieli obie te liczby bez reszty. Można również stwierdzić, że jest to najważniejsze narzędzie rachunkowe w elementarnej teorii liczb.

W szkole poznajemy również taki algorytm, jednak jest on trudniejszy i bardziej pracochłonny - wymaga rozkładu na czynniki pierwsze, a przy dużych liczbach nie jest on prosty i szybki. Natomiast dzięki algorytmowi Euklidesa możemy obejść te trudności; zamiast rozkładu na czynniki pierwsze wykorzystuje on wielokrotne dzielenie z resztą. Na początku zacznijmy od poznania dwóch twierdzeń:

Twierdzenie 1:

*"Jeżeli dla liczb całkowitych a, b, q, r zachodzi równość a = qb + r, to*

*NWD(a,b) = NWD (b,r)."*

Twierdzenie 2 (Algorytm Euklidesa)

*"Dane są liczby całkowite a i b, przy czym b ≠ 0. Wykonujemy kolejne dzielenia z resztą:*

$$\begin{cases} a = qb + r, \\ b = q_1 r + r_1, \\ r = q_2 r_1 + r_2, \\ r_1 = q_3 r_2 + r_3, \\ \dots \end{cases}$$

*Wówczas ciąg reszt r, $r_1$, $r_2$, … jest ściśle malejącym ciągiem liczb całkowitym nieujemnych. Ostatnia niezerowa reszta jest NWD (a, b)."*

Przykłady:

- NWD (1878,673) = ?

$$\begin{cases} 1878 = 2 \cdot 673 + 532 \\ 673 = 532 \cdot 1 + 141 \\ 532 = 141 \cdot 3 + 109 \\ 141 = 109 \cdot 1 + 32 \\ 109 = 32 \cdot 3 + 13 \\ 32 = 13 \cdot 2 + 6 \\ \mathbf{13 = 6 \cdot 2 + 1} \\ 6 = 6 \cdot 1 + 0 \end{cases}$$

Ostatnią niezerową liczbą jest 1, zatem według twierdzenia 2:

**NWD (1878,673) = 1**.

Dla ułatwienia powyższe wyliczenia można zapisywać w taki sposób:

1878 : 673 = 2, reszty 532

673 : 532 = 1, reszty 141

532 : 141 = 3, reszty 109

141 : 109 = 1, reszty 32

109 : 32 = 3, reszty 13

32 : 13 = 2, reszty 6

**13 : 6 = 2, reszty 1**

6 : 1 = 6, reszty 0

**NWD(1878, 673) = 1**

- NWD (2000,1628) = ?

$$\begin{cases} 2000 = 1 \cdot 1628 + 372 \\ 1628 = 372 \cdot 4 + 140 \\ 372 = 140 \cdot 2 + 92 \\ 140 = 92 \cdot 1 + 48 \\ 92 = 48 \cdot 1 + 44 \\ \mathbf{48 = 44 \cdot 1 + 4} \\ 44 = 4 \cdot 11 + 0 \end{cases}$$

Zatem: **NWD (2000,1628) = 4**

Znając już rozszerzony algorytm Euklidesa możemy wrócić do obliczania odwrotności modulo za pomocą niego oraz algorytmu odwrotnego do niego.

Przykłady:

- Oblicz $71^{-1}$ (mod 22) za pomocą algorytmu Euklidesa:

$$\begin{cases} 71 = 22 \cdot 3 + 5 \\ 22 = 5 \cdot 4 + 2 \\ \mathbf{5 = 2 \cdot 2 + 1} \\ 2 = 2 \cdot 1 + 0 \end{cases}$$

$5 = 71 - 22 \cdot 3$

$2 = 22 - 5 \cdot 4$

$1 = 5 - 2 \cdot 2$

Trzecia linia mówi nam o tym, że istnieje $71^{-1}$ (mod 22), zatem możemy teraz za pomocą odwrotnego algorytmu Euklidesa wyliczyć tą odwrotność:

$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (22 - 5 \cdot 4) = 5 - 2 \cdot 22 + 8 \cdot 5 = 9 \cdot 5 - 2 \cdot 22 =$

$9 \cdot (71 - 22 \cdot 3) - 2 \cdot 22 = 9 \cdot 71 - 29 \cdot 22$

Zatem: $71^{-1} \equiv 9$ (mod 22)

- Oblicz $1878^{-1}$ (mod 673) za pomocą algorytmu Euklidesa:

$$\begin{cases} 1878 = 673 \cdot 2 + 532 \\ 673 = 532 \cdot 1 + 141 \\ 532 = 141 \cdot 3 + 109 \\ 141 = 109 \cdot 1 + 32 \\ 109 = 32 \cdot 3 + 13 \\ 32 = 13 \cdot 2 + 6 \\ \mathbf{13 = 6 \cdot 2 + 1} \\ 6 = 1 \cdot 6 + 0 \end{cases}$$

Odwrócony algorytm Euklidesa:

$1 = 13 - 6 \cdot 2 = 13 - 2 \cdot (32 - 13 \cdot 2) = 5 \cdot 13 - 2 \cdot 32 = 5 \cdot (109 - 32 \cdot 3) - 2 \cdot 32 =$

$-17 \cdot 32 + 5 \cdot 109 = -17 (141 - 109 \cdot 1) + 5 \cdot 109 = -17 \cdot 141 + 22 \cdot 109 =$

$-17 \cdot 141 + 22 (532 - 141 \cdot 3) = 22 \cdot 532 - 83 \cdot 141 = 22 \cdot 532 - 83 \cdot (673 - 532) =$

$105 \cdot 532 - 83 \cdot 673 = 105 \cdot (1878 - 673 \cdot 2) - 83 \cdot 673 = 105 \cdot 1878 - 293 \cdot 673$

Więc: $1878^{-1} \equiv 105$ (mod 673)

- Oblicz $23^{-1}$ (mod 51):

$$\begin{cases} 51 = 23 \cdot 2 + 5 \\ 23 = 5 \cdot 4 + 3 \\ 5 = 3 \cdot 1 + 2 \\ 3 = 2 \cdot 1 + 1 \\ 2 = 2 \cdot 1 + 0 \end{cases}$$

Następnie tak jak poprzednio stosujemy odwrócony algorytm Euklidesa:

$1 = 3 - 2 \cdot 1 = 3 - 1 \cdot (5 - 3 \cdot 1) = 2 \cdot 3 - 5 \cdot 1 = 2 \cdot (23 - 5 \cdot 4) - 5 \cdot 1 = 2 \cdot 23 - 9 \cdot 5 = 2 \cdot 23 - 9 \cdot (51 - 23 \cdot 2) = 20 \cdot 23 - 9 \cdot 51$

Rozwiązanie: $23^{-1} \equiv 20 \pmod{51}$

INNE PRZYKŁADY DO SAMODZIELNEGO ROZWIĄZANIA:

Oblicz na podstawie algorytmu Euklidesa i algorytmu do niego odwrotnego:

- $35^{-1} \pmod{144}$
- $10^{-1} \pmod{9999}$
- $37^{-1} \pmod{99}$

PAMIĘTAJ! Nie każda liczba ma swoją odwrotność modulo!

Znając już odwrotność modulo warto poznać jeszcze dwa twierdzenia, które w jakiś sposób wiążą się z dzieleniem obustronnym kongruencji - chociaż jak wiemy nie można dzielić obustronnie kongruencji.

Pierwsze z nich nazywa się prawem skracania i brzmi:

*Jeżeli NWD (c, n) = 1, czyli c i n są liczbami względnie pierwszymi i $ac \equiv bc \pmod{n}$ to $a \equiv b \pmod{n}$.*

Przykład:

Mając taką kongruencję: $27 \equiv 102 \pmod{25}$ możemy zastosować prawo skracania, gdyż spełnia ona warunki twierdzenia. Zatem powyższą kongruencję możemy przedstawić tak: $3 \cdot 9 \equiv 34 \cdot 3 \pmod{25}$, a następnie po zastosowaniu prawa skracania "nowa postać" kongruencji wygląda tak: $9 \equiv 34 \pmod{25}$.

Drugie twierdzenie brzmi:

*Jeżeli wszystkie trzy liczby w kongruencji a ≡ b (mod m) są podzielne przez liczbę d to zachodzi:*

$$\frac{a}{d} \equiv \frac{b}{d}(mod\frac{m}{d})$$

Przykład:

Powyższe twierdzenie możemy wykorzystać przy kongruencji: 36 ≡ 92 (mod 8), ponieważ wszystkie liczby kongruencji (a = 36, b = 92, m = 8) są podzielne przez 4.

Zatem: 36 ≡ 92 (mod 8) ⇒ 9 ≡ 23 (mod 2).

# Trzy najważniejsze twierdzenia

Znając już podstawy z zakresu kongruencji możemy przejść do omówienia trzech ważnych twierdzeń znanych i wybitnych matematyków. Zacznijmy od tych dwóch, dzięki którym przynajmniej formalnie możemy szybko się dowiedzieć czy dana liczba jest pierwsza.

Pierwsze twierdzenie sformułował Fermat, słynny matematyk z epoki nowożytnej, który z zawodu był prawnikiem, ale w wolnym czasie zajmował się matematyką - głównie w zakresie: geometrii (uznawany jest za ojca geometrii analitycznej), rachunku prawdopodobieństwa, rachunku różniczkowego, czy teorii liczb. Twierdzenie to nazywamy Małym Twierdzeniem Fermata (warto wspomnieć, że sam Fermat nigdy nie opublikował dowodu na swoje odkrycie, co jest typowe dla czasów nowożytnych - pierwszy dowód przedstawił Euler). To samo twierdzenie niezależnie od Fermata odkrył Leibniz, a brzmi ono:

*Jeżeli p jest liczbą pierwszą i p nie jest dzielnikiem liczby całkowitej a, to:*

$$a^{p-1} \equiv 1 \bmod p$$

Za odkrywcę następnego ważnego twierdzenia uznaje się już nie aż tak znanego Johna Wilsona, które opublikował w je 1770 r. (chociaż twierdzenie znali już al – Hajsam (X/XIw.), czy Leibniz (XVIIw.), a dowód tego twierdzenia przedstawił dopiero Langrange) Twierdzenie to od nazwiska jego twórcy nazywa się Twierdzeniem Wilsona i brzmi ono:

*Dla każdej liczby pierwszej p zachodzi kongruencja:*

$$(p - 1)! \equiv -1 \bmod p$$

Przypomnienie: znak "!" w matematyce oznacza silnię. Obliczamy ją w następujący sposób: $n!=1\cdot2\cdot3\cdot\ldots\cdot(n-1)\cdot n$

Ostatnim twierdzeniem, które chciałabym przedstawić w tym rozdziale jest twierdzenie Eulera. Twórca tego twierdzenia – Leonhard Euler – jest uznawany za jednego z najważniejszych matematyków w całej historii. Jego dokonania matematyczne dotyczyły prawie wszystkich dziedzin nauki. Twierdzenie Eulera brzmi:

Jeżeli a, m są liczbami względnie pierwszymi [NWD (a, m) = 1] to zachodzi kongruencja:

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

W twierdzeniu pojawia się symbol $\varphi(m)$, który nazywamy funkcją Eulera (funkcja "fi"). Funkcja Eulera to ilość liczb naturalnych od 1 do m, które są względnie pierwsze z m, funkcję tę określa wzór:

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_s}\right)$$

Gdzie $p_1$, $p_2$,…, $p_s$ są kolejnymi czynnikami rozkłady liczby m na czynniki pierwsze. (czyli $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$).

Inaczej mówiąc funkcja $\varphi(M)$ mówi nam o ilości liczb mniejszych od M lub równych M niemających z nią żadnych wspólnych dzielników (NWD = 1). Na przykład, jeśli chcemy wyznaczyć wartość funkcji $\varphi(6)$ to musimy sprawdzić, ile liczb całkowitych ze zbioru {1,2,3,4,5,6} nie ma z 6 wspólnego dzielnika większego od 1.

Spróbujmy zatem na początku wyliczyć $\varphi(6)$ bez wzoru, aby lepiej zrozumieć czym jest ta funkcja:

**NWD (6,1) = 1**

NWD (6,2) = 2

NWD (6,3) = 3

NWD (6, 4) = 2

**NWD (6, 5) = 1**

NWD (6, 6) = 6

Jak widać są dwie liczby ze zbioru {1,2,3,4,5,6} nie mają z 6 wspólnego dzielnika większego od 1. Zatem $\varphi(6) = 2$.

Wyznaczmy jeszcze $\varphi(5)$ za pomocą wzoru:

$$\Phi(5) = 5(1 - \frac{1}{5}) = 4$$

Warto zapamiętać, że jeżeli p jest liczbą pierwszą to $\varphi(p) = p - 1$ (np. $\varphi(11) = 10$)

Poznaliśmy już trzy najważniejsze twierdzenia, choć z pewnością istnieją jeszcze inne, które są równie istotne (np. chińskie twierdzenie o resztach, twierdzenie Lagrange'a).

Podczas poznawania Małego Twierdzenia Fermata miałam wrażenie, że jest ono ściśle związane z zadaniem, które pozwoliło mi się zainteresować tematem kongruencji - sprawdźmy to.

Przypomnienie treści **NIEZWYKŁEGO ZADANIA**:

*"Czy $5^{36} - 1$ jest podzielne przez 13?"*

Na podstawie Małego Twierdzenia Fermata stwierdzamy, że:

$5^{12} \equiv 1 \mod 13$

Następnie obustronnie podnosimy powyższą kongruencję do potęgi 3:

$5^{36} \equiv 1 \mod 13$

A teraz wystarczy obustronnie odjąć 1:

$5^{36} - 1 \equiv 0 \mod 13$

Kongruencja ta pokazuje, że dzieląc liczba $5^{36} - 1$ przez 13 otrzymujemy resztę 0. Zatem liczba ta jest podzielna przez 13.

Udało się! Okazało się, że zadanie to można rozwiązać szybko i prosto, dzięki zastosowaniu twierdzenia Fermata, choć zapewne istnieje jeszcze mnóstwo sposobów rozwiązania tego problemu matematycznego.

Na koniec przejdźmy do innych zadań, które pozwolą zastosować dwa inne wyżej poznane twierdzenia:

1.Udowodnij, że $53^{53} - 33^{33}$ jest podzielna przez 10.

Aby to udowodnić, trzeba dowieść, że:

$53^{53} \equiv 33^{33} \pmod{10}$

Wiedząc, że 53 i 10 są względnie pierwsze wyznaczamy $\varphi(10)$ i stosując twierdzenie Eulera wyznaczamy potrzebną kongruencje:

$$10 = 5 \cdot 2$$

$$\phi(10) = 10 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 4$$

$a^{\varphi(m)} \equiv 1 \pmod{m} \Rightarrow 53^4 \equiv 1 \pmod{10}$

Dzięki wyżej wyznaczonej kongruencji oraz $53 \equiv 3 \pmod{10}$ możemy wywnioskować, że:

$53^{53} = 53 \cdot (53^4)^{13} \equiv 3 \cdot 1^{13} \equiv 3 \pmod{10}$

Tak samo postępujemy z liczbą $33^{33}$:

$33 \equiv 3 \pmod{10}$

$a^{\varphi(m)} \equiv 1 \pmod{m} \Rightarrow 33^4 \equiv 1 \pmod{10}$

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

Zatem z twierdzenia: $a \equiv b \pmod{m} \wedge c \equiv b \pmod{m} \Rightarrow a \equiv c \pmod{m}$ możemy wnioskować, że:

$53^{53} \equiv 3 \pmod{10} \wedge 33^{33} \equiv 3 \pmod{10} \Rightarrow 53^{53} \equiv 33^{33} \pmod{10}$

Ten wniosek kończy dowód.

2.Sprawdź, czy kongruencja: $2 \cdot 26! \equiv -1 \pmod{29}$ jest prawdziwa.

Aby rozwiązać to zadanie trzeba skorzystać z Twierdzenia Wilsona, z którego wynika, że:

$(p - 1)! \equiv -1 \bmod p \Rightarrow 28! \equiv -1 \bmod 29$

Następnie możemy przekształcić powyższą kongruencję do takiej postaci:

$26! \cdot 27 \cdot 28 \equiv -1 \bmod 29$

Teraz mnożymy obustronnie przez 2, aby doprowadzić kongruencję do postaci podobnej w treści zadania:

$2 \cdot 26! \cdot 27 \cdot 28 \equiv -2 \bmod 29$

Następnie wyliczamy dwie kongruencje:

$27 \equiv -2 \bmod 29$

$28 \equiv -1 \bmod 29$

Teraz możemy obie te kongruencje podstawić do tej wcześniejszej:

$2 \cdot 26! \cdot (-2) \cdot (-1) \equiv -2 \bmod 29$

Ostatnim krokiem jest podzielenie powyższej kongruencji obustronnie przez 2:

$2 \cdot 26! \equiv -1 \pmod{29}$

Zatem kongruencja z zadania jest prawdziwa.

PODOBNE ZADANIA DO ROZWIĄZANIA PRZEZ CZYTELNIKA:

1. Sprawdź, czy kongruencja: $18! \equiv -1 \pmod{437}$ jest prawdziwa?

2.Ustal, czy liczba $48^{77} - 1$ jest podzielne przez 8.

3.Wyznacz ostatnią cyfrę liczby $7^{100}$. Wskazówka: jeżeli chcemy wyznaczyć ostatnią cyfrę jakiejś liczby to musimy wyznaczyć jej resztę z dzielenia przez 10.

Klucz odpowiedzi do tych zadań znajdują się na końcu pracy.

# Podsumowanie

Kongruencje to z pewnością temat, któremu warto poświęcić czas. Daje on nam możliwość poznania jednego z najstarszych działów matematyki, którym jest teoria liczb, a dział ten jak mówił Carl Friedrich Gauss jest królową matematyki (“Matematyka jest królową nauk, a teoria liczb królową matematyki”). W mojej pracy poruszyłam tylko podstawy dotyczące tego obszernego zagadnienia. Pominęłam np. chińskie twierdzenie o liczbach, czy układy kongruencji liniowych. Jestem pewna, że powrócę do tych zagadnień, bo są naprawdę bardzo interesujące.

Kongruencje mają szerokie zastosowanie w kryptografii, ale warto je poznać choćby po to, by móc szybciej dochodzić do rozwiązań pewnych problemów. Mam nadzieję, że samą pracą zachęcę do poznania tak ciekawego tematu czytelników. Bardzo się cieszę, że dzięki znalezionemu zadaniu matematycznemu mogłam poznać kongruencje i napisać pracę na ich temat. Na początku pisania wydawały się dość skomplikowane, jednak po poznaniu stały się o wiele łatwiejsze.

W tym miejscu mojej pracy chciałabym także podziękować za ogromne wsparcie i pomoc mojej nauczycielki.

Magdalena Ciochoń

# Bibliografia

*Matematyka olimpijska. Algebra i teoria liczb* Adam Neugebauer
*Teoria liczb. Markowe wykłady z matematyki* Marek Zakrzewski

*Encyklopedia szkolna – matematyka Wydawnictwa Greg*

*"Teoria liczb" Wacław Sierpiński*

Strony internetowe:

http://matwbn.icm.edu.pl/ksiazki/mon/mon19/mon1903.pdf

https://pl.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/congruence-modulo

http://www.ftj.agh.edu.pl/~lenda/cicer/gauss2.htm

http://www.ftj.agh.edu.pl/~lenda/number_theory/A31.pdf

http://knm.katowice.pl/licea/kolko/14.11.2011_beata_lojan/pliki/kongruencje.pdf

https://eszkola.pl/matematyka/kongruencja-10776.html

https://histmag.org/Carl-Friedrich-Gauss-krol-liczb-10685

https://www.zse-2.krakow.pl/zse2/pozalekcyjne/matematyka/gauss.htm

https://histmag.org/Carl-Friedrich-Gauss-krol-liczb-10685

https://docplayer.pl/12207692-Kongruencje-oraz-przyklady-ich-zastosowan.html

http://www.ftj.agh.edu.pl/~lenda/cicer/gauss2.htm

http://zasobyip2.ore.edu.pl/pl/publications/download/10813?link=header

https://pl.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/euler-s-totient-function-phi-function

# Klucz odpowiedzi

1. Tak, jest prawdziwa. (Skorzystaj z Twierdzenia Wilsona)
2. Tak, jest podzielne przez 8. (Skorzystaj z Małego twierdzenia Fermata)
3. Ostatnią cyfrą liczby $7^{100}$ jest 1. (Skorzystaj z Twierdzenie Eulera)

# Opinia Opiekuna pracy

## OCENA PRACY MAGDALENY CIOCHOŃ – uczennicy klasy 2a III LO w Tarnowie

Magdalena Ciochoń jest uczennicą klasy drugiej o profilu humanistycznym, piszę o tym we wstępie, gdyż mając na uwadze, że w zeszłorocznej edycji konkursu po raz pierwszy uczestniczyła, to tegoroczny powrót do podjęcia próby napisania kolejnej pracy uważam za sukces, zarówno uczennicy, jak i swój sukces edukacyjny.

Znajdujemy się obecnie w związku z pandemią w trudnej sytuacji i pomimo możliwości kontaktu dzięki platformom, nauka a szczególnie rozwijanie umiejętności znacząco wykraczających poza podstawę programową w klasach humanistycznych jest mocno ograniczona. Tegoroczna praca Magdaleny w całości jest pracą indywidualną. Czas wolny, który w chwili obecnej jest mocno ograniczony dla młodzieży uczącej się zdalnie, Magdalena poświęciła na opracowywanie kolejnych zagadnień do pracy. Moja pomoc ograniczyła się do weryfikacji bibliografii, udzielaniu wskazówek i odpowiedzi na stawiane pytania. Ubolewam nad brakiem możliwości stacjonarnych spotkań, brakiem wspólnej analizy zagadnień i rozwiązywania zadań na tradycyjnej szkolnej tablicy, co jak rok wcześniej, umożliwiało nam stawianie kolejnych pytań i szukania na nich odpowiedzi.

Temat jaki wybrała Magdalena, nie jest tematem łatwym, często staje się on problematyczny dla osób, które swoją przyszłość łączą z naukami matematycznymi, jednak moja uczennica jako ambitna, ciekawa i uparcie dążąca do odpowiedzi wykazała się determinacją w dążeniu do rozwiązania zadania, które zupełnie przypadkiem trafiło w jej ręce podczas naszych wspólnych zajęć.

Magdalena przedstawia Państwu pracę, która w całości została opracowana przez nią samą, przy minimalnym moim wkładzie i ingerencji w jej formę lub zakres materiału w niej zawarty.

Życzę Państwu miłej lektury pracy autorstwa duszy humanistycznej, ale posiadającej „pierwiastek” matematyczny.