KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Uniwersytety Młodzieżowe Matematyczne

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Arytmetyka modulo w pracy z uczniem zdolnym

Agnieszka Kozak

Zakład Dydaktyki Matematyki
Instytut Matematyki
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
e-mail: akozak@hektor.umcs.lublin.pl

Projekt realizowany przez Uniwersytet Rzeszowski w partnerstwie z Uniwersytetem Jagiellońskim oraz Państwową Wyższą Szkołą Zawodową w Chełmie

Wprowadzenie - trochę wzorów

Definicja przystawania liczb

Dwie liczby całkowite a i b przystają modulo n jeśli dają tę samą resztę przy dzieleniu przez n.

$$a \equiv b \pmod{n}$$

lub równoważnie

$$a - b \equiv 0 \pmod{n}$$

Przykład

Liczby -18, 12 przystają modulo 5,

Przykład

Liczby $-18,\ 12$ przystają modulo 5,

$$12 = 2 \cdot 5 + 2$$

Przykład

Liczby $-18,\ 12$ przystają modulo 5,

$$12 = 2 \cdot 5 + 2$$

$$-18 = 4 \cdot (-5) + 2,$$

co zapisujemy następująco:

Przykład

Liczby $-18,\ 12$ przystają modulo 5,

$$12 = 2 \cdot 5 + 2$$

$$-18 = 4 \cdot (-5) + 2,$$

co zapisujemy następująco:

$$-18 \equiv 12 \pmod 5.$$

Własności kongruencji

$$a \equiv a,$$

Jeżeli

$$a \equiv b \pmod{n} \text{ i } b \equiv c \pmod{n}, \text{ to } a \equiv c \pmod{n},$$

Jeżeli

$$a \equiv b \pmod{n} \text{ i } c \equiv d \pmod{n}, \text{ to,}$$

$$a + c \equiv b + d \pmod{n}$$

$$a - c \equiv b - d \pmod{n}$$

$$a \cdot c \equiv b \cdot d \pmod{n}$$

Zastosowania kongruencji - pomocne wzory

Małe twierdzenie Fermata

$$\bigwedge_{a\in\mathbb{N}} \bigwedge_{p\in\mathbb{P},} p \nmid a, \quad a^{p-1} \equiv 1 \pmod{p}$$

Zastosowania kongruencji - pomocne wzory

Małe twierdzenie Fermata

$$\bigwedge_{a\in\mathbb{N}} \bigwedge_{p\in\mathbb{P},} p \nmid a, \quad a^{p-1} \equiv 1 \pmod{p}$$

Twierdzenie Eulera

$$\bigwedge_{a\in\mathbb{N}} \bigwedge_{m\in\mathbb{N},m>1} NWD(a,m) = 1, \quad a^{\varphi(m)} \equiv 1 \pmod{m},$$

gdzie $\varphi(m)$ jest funkcją Eulera, której wartością jest ilość liczb całkowitych od 1 do m, które są względnie pierwsze z m.

Zatem Małe Twierdzenie Fermata jest wnioskiem z Twierdzenia Eulera. Mamy bowiem $\varphi(p) = p - 1$, gdy p jest liczbą pierwszą.

Zatem Małe Twierdzenie Fermata jest wnioskiem z Twierdzenia Eulera. Mamy bowiem $\varphi(p) = p - 1$, gdy p jest liczbą pierwszą.

Funkcja Eulera - wzór

Niech $m = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$ będzie rozkładem liczby m na czynniki pierwsze, wówczas

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

Zatem Małe Twierdzenie Fermata jest wnioskiem z Twierdzenia Eulera. Mamy bowiem $\varphi(p) = p - 1$, gdy p jest liczbą pierwszą.

Funkcja Eulera - wzór

Niech $m = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$ będzie rozkładem liczby m na czynniki pierwsze, wówczas

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

Twierdzenie Wilsona

Jeśli p jest liczbą pierwszą, to $(p-1)! \equiv -1 \pmod{p}$

Zastosowania kongruencji - zadania

Zadanie 1

Sprawdź, że:

$$\text{a) } 2 \cdot 26! \equiv -1 \pmod{29}, \quad \text{b) } 18! \equiv -1 \pmod{437}$$

Zastosowania kongruencji - zadania

Zadanie 1

Sprawdź, że:

$$\text{a) } 2 \cdot 26! \equiv -1 \pmod{29}, \quad \text{b) } 18! \equiv -1 \pmod{437}$$

Zadanie 2

1. Oblicz resztę z dzielenia 5^{138} przez 11;
2. Wyznacz ostatnia cyfrę liczby 7^{100}.

Zadanie 3

Wykaż, że:

1. $$\bigwedge_{n\in\mathbb{N}} 31|2^{5n}-1;$$
2. $$\bigwedge_{n\in\mathbb{N}} 13|1+3^{3n+1}+9^{3n+1};$$
3. $$10|53^{53}-33^{33}.$$

Zadanie 4

Liczby naturalne $a_1, a_2, \ldots, a_{2011}$ spełniają warunek $a_1 + a_2 + \ldots + a_{2011} = 2011^{2011}$. Wyznacz resztę z dzielenia liczby $a_1^3 + a_2^3 + \ldots + a_{2011}^3$ przez 6.

Zastosowania kongruencji - rozwiązania zadań

Zadanie 1 - rozwiązanie

Zastosowania kongruencji - rozwiązania zadań

Zadanie 1 - rozwiązanie

a) Z Twierdzenia Wilsona otrzymujemy:

$$28! \equiv -1 \pmod{29},$$

stąd

$$2 \cdot 26! \cdot 27 \cdot 28 \equiv -2 \pmod{29}.$$

Zastosowania kongruencji - rozwiązania zadań

Zadanie 1 - rozwiązanie

a) Z Twierdzenia Wilsona otrzymujemy:

$$28! \equiv -1 \pmod{29},$$

stąd

$$2 \cdot 26! \cdot 27 \cdot 28 \equiv -2 \pmod{29}.$$

Zastosowania kongruencji - rozwiązania zadań

Zadanie 1 - rozwiązanie

a) Z Twierdzenia Wilsona otrzymujemy:

$$28! \equiv -1 \pmod{29},$$

stąd

$$2 \cdot 26! \cdot 27 \cdot 28 \equiv -2 \pmod{29}.$$

Ponieważ

$$28 \equiv -1 \pmod{29},$$

oraz

$$27 \equiv -2 \pmod{29},$$

to

$$28 \cdot 27 \equiv 2 \pmod{29},$$

to

$$28 \cdot 27 \equiv 2 \pmod{29},$$

a zatem

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

to

$$28 \cdot 27 \equiv 2 \pmod{29},$$

a zatem

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

b) Zauważmy, że $437 = 19 \cdot 23$. Zatem rozwiązanie tego zadania będzie polegało na wykazaniu dwóch kongruencji:

$$18! \equiv -1 \pmod{19},$$

$$18! \equiv -1 \pmod{23}.$$

to

$$28 \cdot 27 \equiv 2 \pmod{29},$$

a zatem

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

b) Zauważmy, że $437 = 19 \cdot 23$. Zatem rozwiązanie tego zadania będzie polegało na wykazaniu dwóch kongruencji:

$$18! \equiv -1 \pmod{19},$$

$$18! \equiv -1 \pmod{23}.$$

Ponieważ 19 i 23 są liczbami pierwszymi to powyższy układ kongruencji implikuje przystawanie

$$18! \equiv -1 \pmod{19 \cdot 23}$$

co zakończy zadanie.

co zakończy zadanie. Pierwsza kongruencja jest oczywista ze wzoru Wilsona dla $p = 19$. Druga jest również konsekwencją tego wzoru dla $p = 23$. Mamy bowiem

co zakończy zadanie. Pierwsza kongruencja jest oczywista ze wzoru Wilsona dla $p = 19$. Druga jest również konsekwencją tego wzoru dla $p = 23$. Mamy bowiem

$$22! \equiv -1 \pmod{23}.$$

co zakończy zadanie. Pierwsza kongruencja jest oczywista ze wzoru Wilsona dla $p = 19$. Druga jest również konsekwencją tego wzoru dla $p = 23$. Mamy bowiem

$$22! \equiv -1 \pmod{23}.$$

Stąd

$$18! \cdot 22 \cdot 21 \cdot 20 \cdot 19 \equiv -1 \pmod{23}.$$

co zakończy zadanie. Pierwsza kongruencja jest oczywista ze wzoru Wilsona dla $p = 19$. Druga jest również konsekwencją tego wzoru dla $p = 23$. Mamy bowiem

$$22! \equiv -1 \pmod{23}.$$

Stąd

$$18! \cdot 22 \cdot 21 \cdot 20 \cdot 19 \equiv -1 \pmod{23}.$$

Ostatecznie ponieważ

$$22 \cdot 21 \cdot 20 \cdot 19 \equiv 1 \pmod{23}$$

dostajemy drugą kongruencję.

Zadanie 2 - rozwiązanie

Zadanie 2 - rozwiązanie

1. Z Małego Twierdzenia Fermata otrzymujemy:

$$5^{10} \equiv 1 \pmod{11},$$

Zadanie 2 - rozwiązanie

1. Z Małego Twierdzenia Fermata otrzymujemy:

$$5^{10} \equiv 1 \pmod{11},$$

co daje nam

$$\left(5^{10}\right)^{13} \equiv 1 \pmod{11}.$$

Zadanie 2 - rozwiązanie

1. Z Małego Twierdzenia Fermata otrzymujemy:

$$5^{10} \equiv 1 \pmod{11},$$

co daje nam

$$\left(5^{10}\right)^{13} \equiv 1 \pmod{11}.$$

Ponieważ $5^{138} = 5^{130} \cdot 5^8$, pozostaje nam sprawdzić do jakiej liczby przystaje 5^8 modulo 11.

Mnożąc stronami kongruencję

$$5^2 \equiv 3 \pmod{11}$$

Mnożąc stronami kongruencję

$$5^2 \equiv 3 \pmod{11}$$

i korzystając z prawa skracania, dostajemy

$$5^8 \equiv 4 \pmod{11}.$$

Mnożąc stronami kongruencję

$$5^2 \equiv 3 \pmod{11}$$

i korzystając z prawa skracania, dostajemy

$$5^8 \equiv 4 \pmod{11}.$$

A zatem

$$5^{138} \equiv 4 \pmod{11}.$$

2. Wyznaczenie ostatniej cyfry danej liczby to wyznaczenie jej reszty z dzielenia przez 10. A zatem chcemy wiedzieć do czego przystaje 7^{100} modulo 10. Skorzystamy w tym celu z Twierdzenia Eulera. Założenia tego twierdzenia sa spełnione, bowiem $\mathrm{NWD}(7, 10) = 1$.

2. Wyznaczenie ostatniej cyfry danej liczby to wyznaczenie jej reszty z dzielenia przez 10. A zatem chcemy wiedzieć do czego przystaje 7^{100} modulo 10. Skorzystamy w tym celu z Twierdzenia Eulera. Założenia tego twierdzenia sa spełnione, bowiem $\mathrm{NWD}(7, 10) = 1$. Obliczamy wartość funkcji $\varphi(10)$.

$$\varphi(10) = 10 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4,$$

2. Wyznaczenie ostatniej cyfry danej liczby to wyznaczenie jej reszty z dzielenia przez 10. A zatem chcemy wiedzieć do czego przystaje 7^{100} modulo 10. Skorzystamy w tym celu z Twierdzenia Eulera. Założenia tego twierdzenia sa spełnione, bowiem NWD$(7, 10) = 1$. Obliczamy wartość funkcji $\varphi(10)$.

$$\varphi(10) = 10 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4,$$

a zatem

$$7^4 \equiv 1 \pmod{10}$$

i stąd

$$7^{100} \equiv 1 \pmod{10}.$$

Zadanie 3 - rozwiązanie

1. Wiemy, że
$$2^5 \equiv 1 \pmod{31},$$
a zatem mnożąc stronami tę kongruencję n-krotnie dostajemy
$$2^{5n} \equiv 1 \pmod{31}.$$
2. W zadaniu tym wyznaczamy reszty z dzielenia przez 13 poszczególnych składników, a następnie pokazujemy, że sumują się one do 13. Mamy więc
$$9^3 \equiv 1 \pmod{13}$$
i podobnie jak w zadaniu poprzednim
$$9^{3n} \equiv 1 \pmod{13}, \quad 3^{3n} \equiv 1 \pmod{13},$$

stąd

$$9^{3n+1} \equiv 9 \pmod{13}$$

oraz

$$3^{3n+1} \equiv 3 \pmod{13}.$$

Widzimy zatem, ze otrzymane reszty sumują się dla dowolnego n do 13.

3. W zadaniu tym chcemy udowodnić, że

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

Zauważmy, że

$$53 \equiv 3 \pmod{10}$$

a zatem

$$53^{53} \equiv 3^{53} \pmod{10}.$$

Korzystając z Twierdzenia Eulera (podobnie jak w zadaniu 2) otrzymujemy

$$3^4 \equiv 1 \pmod{10}$$

i stąd

$$3^{53} = 3^{52+1} \equiv 3 \pmod{10}.$$

Ostatecznie, ponieważ

$$3^{33} = 3^{22+1} \equiv 3 \pmod{10}$$

dostajemy

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

Zadanie 4 - rozwiązanie, [4], zad.1.45

Na wstępie zauważmy, że liczba $a^3 - a$, gdzie $a \in \mathbb{N}$ jest zawsze podzielna przez 6, ponieważ jest iloczynem kolejnych liczb naturalnych. A zatem $a^3 \equiv a \pmod 6$ oraz

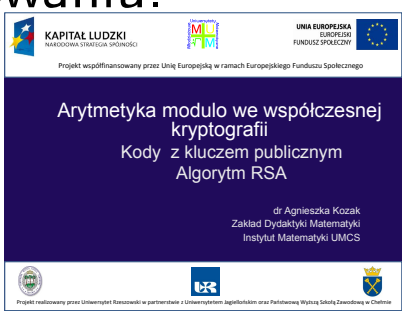
$$a_1^3 + a_2^3 + \ldots + a_{2011}^3 \equiv a_1 + a_2 + \ldots + a_{2011} \equiv 2011^{2011} \pmod 6 = 1,$$

ponieważ

$$2011 \equiv 1 \pmod 6, \quad 2011 = 335 \cdot 6 + 1.$$

Arytmetyka modulo we współczesnej kryptologii
Kody z kluczem publicznym, algorytm RSA

Uwagi wprowadzające:
Szyfr jest pewną funkcja matematyczną. Najczęściej przy szyfrowaniu używało się funkcji dwukierunkowej tzn. takiej, że funkcja odwrotna do niej jest równie łatwa w stosowaniu jak dana funkcja. Zmiana nastąpiła w latach 70 - tych XX wieku. W prezentacji pokażemy, dlaczego funkcja modulo znalazła zastosowanie w kodowaniu.



Patrz plik Prez2.pdf

Literatura

1. Richard Courant, Herbert Robbins "Co to jest matematyka?" Wyd. Prószyński i S-ka, Warszawa 1998
2. Wacław Marzantowcz, Piotr Zarzycki "Elementy teorii liczb" Wyd. Naukowe UAM, Poznań 1999
3. Henryk Pawłowski "Zadania z olimpiad matematycznych z całego świata", Oficyna Wydawnicza Tutor, Toruń 1997
4. Simon Singh "Księga szyfrów", Wyd. Albatros-Andrzej Kuryłowicz, 2001