Wykład 3
Kongruencje, cz. 2

Andrzej Sładek
sladek@ux2.math.us.edu.pl

Instytut Matematyki, Uniwersytet Śląski w Katowicach

1. Układy kongruencji, twierdzenie chińskie o resztach

2. Funkcja i twierdzenie Eulera

Wykład jest przewidziany na 2 godziny lekcyjne

Wykład jest przewidziany na 2 godziny lekcyjne

Tematy poruszane na wykładzie można znaleźć w:

Wykład jest przewidziany na 2 godziny lekcyjne

Tematy poruszane na wykładzie można znaleźć w:

- W. Marzantowicz, P. Zarzycki, *Elementarna teoria liczb,* PWN **2006**

Zacznijmy od prostego zadania.

Zacznijmy od prostego zadania.

Zadanie

Liczba kostek w bardzo dużej czekoladzie równa jest x. Jeśli podzielić czekoladę na 3 cześci, to zostanie 1 kostka. Przy podziale na 5 części zostaną 3 kostki, a w przypadku podziału na 7 części zostaną 2 kostki. Ile kostek ma czekolada, jeśli wiadomo, że liczba kostek jest mniejsza od 100?

Zacznijmy od prostego zadania.

Zadanie

Liczba kostek w bardzo dużej czekoladzie równa jest x. Jeśli podzielić czekoladę na 3 cześci, to zostanie 1 kostka. Przy podziale na 5 części zostaną 3 kostki, a w przypadku podziału na 7 części zostaną 2 kostki. Ile kostek ma czekolada, jeśli wiadomo, że liczba kostek jest mniejsza od 100?

Czy wiesz jak rozwiązać powyższe zadanie ?

Zacznijmy od prostego zadania.

Zadanie

Liczba kostek w bardzo dużej czekoladzie równa jest x. Jeśli podzielić czekoladę na 3 cześci, to zostanie 1 kostka. Przy podziale na 5 części zostaną 3 kostki, a w przypadku podziału na 7 części zostaną 2 kostki. Ile kostek ma czekolada, jeśli wiadomo, że liczba kostek jest mniejsza od 100?

Czy wiesz jak rozwiązać powyższe zadanie ?

Należy rozwiązać układ kongruencji

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Zacznijmy od prostego zadania.

Zadanie

Liczba kostek w bardzo dużej czekoladzie równa jest x. Jeśli podzielić czekoladę na 3 cześci, to zostanie 1 kostka. Przy podziale na 5 części zostaną 3 kostki, a w przypadku podziału na 7 części zostaną 2 kostki. Ile kostek ma czekolada, jeśli wiadomo, że liczba kostek jest mniejsza od 100?

Czy wiesz jak rozwiązać powyższe zadanie ?

Należy rozwiązać układ kongruencji

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Kiedy ten i podobne układy kongruencji mają rozwiązanie?

Twierdzenie (chińskie o resztach)

Jeśli $n_1, \ldots, n_k$ są parami względnie pierwsze oraz $r_1, \ldots, r_k$ są liczbami całkowitymi, to istnieje liczba całkowita x taka, że

$$\begin{cases} x \equiv & r_1 \pmod{n_1} \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\ x \equiv & r_k \pmod{n_k} \end{cases}$$

Liczba x jest wyznaczona jednoznacznie modulo $n_1 \cdot \ldots \cdot n_k$.

Twierdzenie (chińskie o resztach)

Jeśli $n_1, \ldots, n_k$ są parami względnie pierwsze oraz $r_1, \ldots, r_k$ są liczbami całkowitymi, to istnieje liczba całkowita x taka, że

$$\begin{cases} x \equiv & r_1 \pmod{n_1} \\ \ldots\ldots & \ldots\ldots\ldots\ldots \\ x \equiv & r_k \pmod{n_k} \end{cases}$$

Liczba x jest wyznaczona jednoznacznie modulo $n_1 \cdot \ldots \cdot n_k$.

Dowód. Niech $n = n_1 \cdot \ldots \cdot n_k$. Rozważmy odwzorowanie

$$\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}, \quad \varphi(x) = ((x)_{n_1}, \ldots, (x)_{n_k}) \text{ dla } x \in \mathbb{Z}_n.$$

Twierdzenie (chińskie o resztach)

Jeśli $n_1, \ldots, n_k$ są parami względnie pierwsze oraz $r_1, \ldots, r_k$ są liczbami całkowitymi, to istnieje liczba całkowita x taka, że

$$\begin{cases} x \equiv & r_1 \pmod{n_1} \\ \ldots\ldots & \ldots\ldots\ldots\ldots \\ x \equiv & r_k \pmod{n_k} \end{cases}$$

Liczba x jest wyznaczona jednoznacznie modulo $n_1 \cdot \ldots \cdot n_k$.

Dowód. Niech $n = n_1 \cdot \ldots \cdot n_k$. Rozważmy odwzorowanie

$$\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}, \quad \varphi(x) = ((x)_{n_1}, \ldots, (x)_{n_k}) \text{ dla } x \in \mathbb{Z}_n.$$

Odwzorowanie φ jest wzajemnie jednoznaczne (*dowód na tablicy*).

Twierdzenie (chińskie o resztach)

Jeśli $n_1, \ldots, n_k$ są parami względnie pierwsze oraz $r_1, \ldots, r_k$ są liczbami całkowitymi, to istnieje liczba całkowita x taka, że

$$\begin{cases} x \equiv & r_1 \pmod{n_1} \\ \ldots\ldots & \ldots\ldots\ldots\ldots \\ x \equiv & r_k \pmod{n_k} \end{cases}$$

Liczba x jest wyznaczona jednoznacznie modulo $n_1 \cdot \ldots \cdot n_k$.

Dowód. Niech $n = n_1 \cdot \ldots \cdot n_k$. Rozważmy odwzorowanie

$$\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}, \quad \varphi(x) = ((x)_{n_1}, \ldots, (x)_{n_k}) \text{ dla } x \in \mathbb{Z}_n.$$

Odwzorowanie φ jest wzajemnie jednoznaczne (*dowód na tablicy*).
Zatem

$$\varphi(x) = ((r_1)_{n_1}, \ldots, (r_k)_{n_k}) \text{ dla pewnego } x \in \mathbb{Z}_n,$$

co oznacza, że x jest rozwiązaniem danego układu kongruencji. ¶

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13$.

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13.$

Wstawiamy to do trzeciej kongruencji i wyliczamy u.
$15u + 13 \equiv 2 \pmod 7$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13.$

Wstawiamy to do trzeciej kongruencji i wyliczamy u.
$15u + 13 \equiv 2 \pmod 7 \implies u - 1 \equiv 2 \pmod 7$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13.$

Wstawiamy to do trzeciej kongruencji i wyliczamy u.
$15u + 13 \equiv 2 \pmod 7 \implies u - 1 \equiv 2 \pmod 7 \implies u \equiv 3 \pmod 7$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13.$

Wstawiamy to do trzeciej kongruencji i wyliczamy u.
$15u + 13 \equiv 2 \pmod 7 \implies u - 1 \equiv 2 \pmod 7 \implies u \equiv 3 \pmod 7 \implies u = 7s + 3$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13.$

Wstawiamy to do trzeciej kongruencji i wyliczamy u.
$15u + 13 \equiv 2 \pmod 7 \implies u - 1 \equiv 2 \pmod 7 \implies u \equiv 3 \pmod 7 \implies u = 7s + 3$
Ostatecznie $x = 15(7s + 3) + 13 = 105s + 58.$

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13.$

Wstawiamy to do trzeciej kongruencji i wyliczamy u.
$15u + 13 \equiv 2 \pmod 7 \implies u - 1 \equiv 2 \pmod 7 \implies u \equiv 3 \pmod 7 \implies u = 7s + 3$
Ostatecznie $x = 15(7s + 3) + 13 = 105s + 58.$

Odp. Liczba kostek czekolady równa jest 58.

Z twierdzenia chińskiego o resztach wynika, że nasz układ

$$\begin{cases} x \equiv & 1 \pmod 3 \\ x \equiv & 3 \pmod 5 \\ x \equiv & 2 \pmod 7 \end{cases}$$

ma rozwiązanie, więc spróbujmy go rozwiązać. Analizujemy pierwszą kongruencję.
$x \equiv 1 \pmod 3 \implies x = 3t + 1$

Wstawiamy tak obliczone x do drugiej kongruencji i wyliczamy t.
$3t + 1 \equiv 3 \pmod 5 \implies 3t \equiv 2 \pmod 5 \implies t \equiv 4 \pmod 5 \implies t = 5u + 4$
Zatem $x = 3(5u + 4) + 1 = 15u + 13.$

Wstawiamy to do trzeciej kongruencji i wyliczamy u.
$15u + 13 \equiv 2 \pmod 7 \implies u - 1 \equiv 2 \pmod 7 \implies u \equiv 3 \pmod 7 \implies u = 7s + 3$
Ostatecznie $x = 15(7s + 3) + 13 = 105s + 58.$

Odp. Liczba kostek czekolady równa jest 58.

Inny sposób rozwiązywania podobnych układów znajdziesz w zad. 16, zestaw 3.

I znowu proste zadanie.

I znowu proste zadanie.

Zadanie

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

I znowu proste zadanie.

Zadanie

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Do rozwiązania potrzebować będziemy tzw. funkcji Eulera.

Nazwa tej funkcji pochodzi od nazwiska szwajcarskiego matematyka L.Eulera, który żył w latach 1707-1783.

Definicja

Funkcją Eulera nazywamy funkcję

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = |U(\mathbb{Z}_n)| = |\{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = 1\}|.$$

Definicja

Funkcją Eulera nazywamy funkcję

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = |U(\mathbb{Z}_n)| = |\{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = 1\}|.$$

Własności

(1) Jeśli $\mathrm{NWD}(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

Definicja

Funkcją Eulera nazywamy funkcję

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = |U(\mathbb{Z}_n)| = |\{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = 1\}|.$$

Własności

(1) Jeśli $\mathrm{NWD}(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

(2) Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.
W szczególności $\varphi(p) = p - 1$.

Definicja

Funkcją Eulera nazywamy funkcję

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = |U(\mathbb{Z}_n)| = |\{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = 1\}|.$$

Własności

(1) Jeśli $\mathrm{NWD}(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

(2) Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.
W szczególności $\varphi(p) = p - 1$.

(3) $\sum_{d|n} \varphi(d) = n$.

Definicja

Funkcją Eulera nazywamy funkcję

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = |U(\mathbb{Z}_n)| = |\{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = 1\}|.$$

Własności

(1) Jeśli $\mathrm{NWD}(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

(2) Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.
W szczególności $\varphi(p) = p - 1$.

(3) $\sum_{d|n} \varphi(d) = n$.

Definicja

Funkcją Eulera nazywamy funkcję

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = |U(\mathbb{Z}_n)| = |\{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = 1\}|.$$

Własności

(1) Jeśli $\mathrm{NWD}(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

(2) Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.
W szczególności $\varphi(p) = p - 1$.

(3) $\sum_{d|n} \varphi(d) = n$.

Własność pierwsza mówi, że funkcja Eulera jest funkcją multiplikatywną.

Dowód własności 1: Jeśli $\mathrm{NWD}(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

Dowód własności 1: Jeśli NWD$(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

Rozważmy funkcję

$$\psi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n,\ \psi(k) = ((k)_m, (k)_n).$$

Dowód własności 1: Jeśli NWD$(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

Rozważmy funkcję

$$\psi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n,\ \psi(k) = ((k)_m, (k)_n).$$

Podobnie jak w dowodzie twierdzeni chińskiego o resztach pokazuje się, że ta funkcja jest wzjemnie jednoznaczna.

Dowód własności 1: Jeśli NWD$(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

Rozważmy funkcję

$$\psi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n,\ \psi(k) = ((k)_m, (k)_n).$$

Podobnie jak w dowodzie twierdzeni chińskiego o resztach pokazuje się, że ta funkcja jest wzjemnie jednoznaczna.
W dodatku jest to izomorfizm pierścieni, który zbiór elementów odwracalnych $U(\mathbb{Z}_{mn})$ pierścienia $\mathbb{Z}_{mn}$ przeprowadza na zbiór elementów odwracalnych $U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$ pierścienia $\mathbb{Z}_m \times \mathbb{Z}_n$ (*szczegóły na tablicy*).

Dowód własności 1: Jeśli NWD$(n, m) = 1$, to $\varphi(nm) = \varphi(n)\varphi(m)$.

Rozważmy funkcję

$$\psi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n,\ \psi(k) = ((k)_m, (k)_n).$$

Podobnie jak w dowodzie twierdzeni chińskiego o resztach pokazuje się, że ta funkcja jest wzjemnie jednoznaczna.
W dodatku jest to izomorfizm pierścieni, który zbiór elementów odwracalnych $U(\mathbb{Z}_{mn})$ pierścienia $\mathbb{Z}_{mn}$ przeprowadza na zbiór elementów odwracalnych $U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$ pierścienia $\mathbb{Z}_m \times \mathbb{Z}_n$ (*szczegóły na tablicy*).
Zatem

$$\varphi(mn) = |U(\mathbb{Z}_m \times \mathbb{Z}_n)| = |U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)| = \varphi(m)\varphi(n). \quad ¶$$

Dowód własności 2: Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.

Dowód własności 2: Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.

$$\mathbb{Z}_{p^k} = \{0,\ 1,\ 2,\ ...,\ 1 \cdot p,\ p+1,\ ...,\ 2 \cdot p,\ 2p+1,\ ...,\ (p^{k-1}-1) \cdot p,\ ...,\ p^k - 1\}.$$

Czerwonym kolorem zaznaczono elementy $\mathbb{Z}_{p^k}$, które nie są względnie pierwsze p.

Jak widać jest ich

Dowód własności 2: Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.

$$\mathbb{Z}_{p^k} = \{0,\ 1,\ 2,\ ...,\ 1 \cdot p,\ p+1,\ ...,\ 2 \cdot p,\ 2p+1,\ ...,\ (p^{k-1}-1) \cdot p,\ ...,\ p^k - 1\}.$$

Czerwonym kolorem zaznaczono elementy $\mathbb{Z}_{p^k}$, które nie są względnie pierwsze p.

Jak widać jest ich p^{k-1}.

Dowód własności 2: Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.

$$\mathbb{Z}_{p^k} = \{0,\ 1,\ 2,\ ...,\ 1\cdot p,\ p+1,\ ...,\ 2\cdot p,\ 2p+1,\ ...,\ (p^{k-1}-1)\cdot p,\ ...,\ p^k-1\}.$$

Czerwonym kolorem zaznaczono elementy $\mathbb{Z}_{p^k}$, które nie są względnie pierwsze p.

Jak widać jest ich p^{k-1}.

Zatem

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1). \quad ¶$$

Dowód własności 3: $\sum_{d|n} \varphi(d) = n$.

Dowód własności 3: $\sum_{d|n} \varphi(d) = n$.

Dla $d|n$ niech

$$X_d = \{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = d\}.$$

Dowód własności 3: $\sum_{d|n} \varphi(d) = n$.

Dla $d|n$ niech

$$X_d = \{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = d\}.$$

Ponieważ

$$\mathrm{NWD}(k, n) = d \iff \mathrm{NWD}(\frac{k}{d}, \frac{n}{d}) = 1,$$

więc $|X_d| = \varphi(\frac{n}{d})$.

Dowód własności 3: $\sum_{d|n} \varphi(d) = n$.

Dla $d|n$ niech

$$X_d = \{k \in \mathbb{Z}_n : \mathrm{NWD}(k, n) = d\}.$$

Ponieważ

$$\mathrm{NWD}(k, n) = d \iff \mathrm{NWD}(\frac{k}{d}, \frac{n}{d}) = 1,$$

więc $|X_d| = \varphi(\frac{n}{d})$.

Jeżeli $1 = d_1 < \ldots < d_s = n$ są wszystkimi dzielnikami liczby n, to $e_i = \frac{n}{d_i}$, $i = 1, \ldots, s$, są również wszystkimi dzielnikami liczby n.

Dowód własności 3: $\sum_{d|n} \varphi(d) = n$.

Dla $d|n$ niech

$$X_d = \{k \in \mathbb{Z}_n : \text{NWD}(k, n) = d\}.$$

Ponieważ

$$\text{NWD}(k, n) = d \iff \text{NWD}(\frac{k}{d}, \frac{n}{d}) = 1,$$

więc $|X_d| = \varphi(\frac{n}{d})$.

Jeżeli $1 = d_1 < ... < d_s = n$ są wszystkimi dzielnikami liczby n, to $e_i = \frac{n}{d_i}$, $i = 1, ..., s$, są również wszystkimi dzielnikami liczby n.

Zauważmy, że

$$\{1, ..., n\} = X_{e_1} \dot{\cup} ... \dot{\cup} X_{e_s}.$$

Dowód własności 3: $\sum_{d|n} \varphi(d) = n$.

Dla $d|n$ niech

$$X_d = \{k \in \mathbb{Z}_n : \text{NWD}(k, n) = d\}.$$

Ponieważ

$$\text{NWD}(k, n) = d \iff \text{NWD}(\frac{k}{d}, \frac{n}{d}) = 1,$$

więc $|X_d| = \varphi(\frac{n}{d})$.

Jeżeli $1 = d_1 < ... < d_s = n$ są wszystkimi dzielnikami liczby n, to $e_i = \frac{n}{d_i}$, $i = 1, ..., s$, są również wszystkimi dzielnikami liczby n.

Zauważmy, że

$$\{1, ..., n\} = X_{e_1} \dot{\cup} ... \dot{\cup} X_{e_s}.$$

Zatem

$$n = |X_{e_1}| + ... + |X_{e_s}| = \varphi(e_1) + ... + \varphi(e_s) = \sum_{d|n} \varphi(d). \quad ¶$$

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z},\ n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $\quad a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.
Zatem funkcja

$$\psi : U(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n),\ \psi(x) = (a \cdot x)_n$$

jest poprawnie określona.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.
Zatem funkcja

$$\psi : U(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n),\ \psi(x) = (a \cdot x)_n$$

jest poprawnie określona.
Pokażemy (*na tablicy*), że jest ona wzajemnie jednoznaczna.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.
Zatem funkcja

$$\psi : U(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n),\ \psi(x) = (a \cdot x)_n$$

jest poprawnie określona.
Pokażemy (*na tablicy*), że jest ona wzajemnie jednoznaczna.
Zatem jeżeli $U(\mathbb{Z}_n) = \{x_1, ..., x_{\varphi(n)}\}$, to również $U(\mathbb{Z}_n) = \{(a \cdot x_1)_n, ..., (a \cdot x_{\varphi(n)})_n\}$.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.
Zatem funkcja

$$\psi : U(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n),\ \psi(x) = (a \cdot x)_n$$

jest poprawnie określona.
Pokażemy (*na tablicy*), że jest ona wzajemnie jednoznaczna.
Zatem jeżeli $U(\mathbb{Z}_n) = \{x_1, ..., x_{\varphi(n)}\}$, to również $U(\mathbb{Z}_n) = \{(a \cdot x_1)_n, ..., (a \cdot x_{\varphi(n)})_n\}$.
Stąd

$$x_1 \cdot ... \cdot x_{\varphi(n)} = (a \cdot x_1)_n \cdot ... \cdot (a \cdot x_{\varphi(n)})_n$$

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.
Zatem funkcja

$$\psi : U(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n),\ \psi(x) = (a \cdot x)_n$$

jest poprawnie określona.
Pokażemy (*na tablicy*), że jest ona wzajemnie jednoznaczna.
Zatem jeżeli $U(\mathbb{Z}_n) = \{x_1, ..., x_{\varphi(n)}\}$, to również $U(\mathbb{Z}_n) = \{(a \cdot x_1)_n, ..., (a \cdot x_{\varphi(n)})_n\}$.
Stąd

$$x_1 \cdot ... \cdot x_{\varphi(n)} = (a \cdot x_1)_n \cdot ... \cdot (a \cdot x_{\varphi(n)})_n = (a^{\varphi(n)})_n \cdot x_1 \cdot ... \cdot x_{\varphi(n)},$$

(*mnożenie w* $U(\mathbb{Z}_n)$).

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.
Zatem funkcja

$$\psi : U(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n),\ \psi(x) = (a \cdot x)_n$$

jest poprawnie określona.
Pokażemy (*na tablicy*), że jest ona wzajemnie jednoznaczna.
Zatem jeżeli $U(\mathbb{Z}_n) = \{x_1, ..., x_{\varphi(n)}\}$, to również $U(\mathbb{Z}_n) = \{(a \cdot x_1)_n, ..., (a \cdot x_{\varphi(n)})_n\}$.
Stąd

$$x_1 \cdot ... \cdot x_{\varphi(n)} = (a \cdot x_1)_n \cdot ... \cdot (a \cdot x_{\varphi(n)})_n = (a^{\varphi(n)})_n \cdot x_1 \cdot ... \cdot x_{\varphi(n)},$$

(*mnożenie w* $U(\mathbb{Z}_n)$).

Skracając lewą i prawą stronę powyższej równości (w grupie $U(\mathbb{Z}_n)$) przez $x_1 \cdot ... \cdot x_{\varphi(n)}$ mamy

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.
Zatem funkcja

$$\psi : U(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n),\ \psi(x) = (a \cdot x)_n$$

jest poprawnie określona.
Pokażemy (*na tablicy*), że jest ona wzajemnie jednoznaczna.
Zatem jeżeli $U(\mathbb{Z}_n) = \{x_1, ..., x_{\varphi(n)}\}$, to również $U(\mathbb{Z}_n) = \{(a \cdot x_1)_n, ..., (a \cdot x_{\varphi(n)})_n\}$.
Stąd

$$x_1 \cdot ... \cdot x_{\varphi(n)} = (a \cdot x_1)_n \cdot ... \cdot (a \cdot x_{\varphi(n)})_n = (a^{\varphi(n)})_n \cdot x_1 \cdot ... \cdot x_{\varphi(n)},$$

(*mnożenie w* $U(\mathbb{Z}_n)$).

Skracając lewą i prawą stronę powyższej równości (w grupie $U(\mathbb{Z}_n)$) przez $x_1 \cdot ... \cdot x_{\varphi(n)}$ mamy

$$(a^{\varphi(n)})_n = 1 \text{ (oczywiście w } \mathbb{Z}_n),$$

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dowód. Jeżeli $x \in U(\mathbb{Z}_n)$, to $(a \cdot x)_n \in U(\mathbb{Z}_n)$.
Zatem funkcja

$$\psi : U(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n),\ \psi(x) = (a \cdot x)_n$$

jest poprawnie określona.
Pokażemy (*na tablicy*), że jest ona wzajemnie jednoznaczna.
Zatem jeżeli $U(\mathbb{Z}_n) = \{x_1, ..., x_{\varphi(n)}\}$, to również $U(\mathbb{Z}_n) = \{(a \cdot x_1)_n, ..., (a \cdot x_{\varphi(n)})_n\}$.
Stąd

$$x_1 \cdot ... \cdot x_{\varphi(n)} = (a \cdot x_1)_n \cdot ... \cdot (a \cdot x_{\varphi(n)})_n = (a^{\varphi(n)})_n \cdot x_1 \cdot ... \cdot x_{\varphi(n)},$$

(*mnożenie w* $U(\mathbb{Z}_n)$).

Skracając lewą i prawą stronę powyższej równości (w grupie $U(\mathbb{Z}_n)$) przez $x_1 \cdot ... \cdot x_{\varphi(n)}$ mamy

$$(a^{\varphi(n)})_n = 1 \text{ (oczywiście w } \mathbb{Z}_n),$$

co oznacza

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad ¶$$

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to przyjmuje szczególną postać, gdy $n = p \in P$.

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z},\ n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to przyjmuje szczególną postać, gdy $n = p \in P$.

Wniosek - Małe Twierdzenie Fermata

Jeśli $a \in \mathbb{Z},\ p \in \mathbb{P},\ p \not| a$, to $a^{p-1} \equiv 1 \pmod{p}$.

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to przyjmuje szczególną postać, gdy $n = p \in P$.

Wniosek - Małe Twierdzenie Fermata

Jeśli $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid a$, to $a^{p-1} \equiv 1 \pmod{p}$.

Przykład

$\varphi(200) =$

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to przyjmuje szczególną postać, gdy $n = p \in P$.

Wniosek - Małe Twierdzenie Fermata

Jeśli $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid a$, to $a^{p-1} \equiv 1 \pmod{p}$.

Przykład

$\varphi(200) = \varphi(2^3 5^2) =$

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to przyjmuje szczególną postać, gdy $n = p \in P$.

Wniosek - Małe Twierdzenie Fermata

Jeśli $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid a$, to $a^{p-1} \equiv 1 \pmod{p}$.

Przykład

$\varphi(200) = \varphi(2^3 5^2) = \varphi(2^3)\varphi(5^2) =$

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to przyjmuje szczególną postać, gdy $n = p \in P$.

Wniosek - Małe Twierdzenie Fermata

Jeśli $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid a$, to $a^{p-1} \equiv 1 \pmod{p}$.

Przykład

$\varphi(200) = \varphi(2^3 5^2) = \varphi(2^3)\varphi(5^2) = 2^2(2-1)5^1(5-1) =$

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to przyjmuje szczególną postać, gdy $n = p \in P$.

Wniosek - Małe Twierdzenie Fermata

Jeśli $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid a$, to $a^{p-1} \equiv 1 \pmod{p}$.

Przykład

$\varphi(200) = \varphi(2^3 5^2) = \varphi(2^3)\varphi(5^2) = 2^2(2-1)5^1(5-1) = 80$

Spójrzmy jeszcze raz na twierdzenie Eulera.

Twierdzenie Eulera

Jeśli $a \in \mathbb{Z}$, $n \in \mathbb{N}$ oraz $\mathrm{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to przyjmuje szczególną postać, gdy $n = p \in P$.

Wniosek - Małe Twierdzenie Fermata

Jeśli $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid a$, to $a^{p-1} \equiv 1 \pmod{p}$.

Przykład

$\varphi(200) = \varphi(2^3 5^2) = \varphi(2^3)\varphi(5^2) = 2^2(2-1)5^1(5-1) = 80$

Zatem $3^{80} \equiv 1 \pmod{200}$.

Wróćmy do naszego zadania.

Wróćmy do naszego zadania.

Zadanie

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Wróćmy do naszego zadania.

Zadanie

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Rozwiązanie.
Należy znaleźć resztę z dzielenia liczby 3^{14404} przez 1000.

Wróćmy do naszego zadania.

Zadanie

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Rozwiązanie.
Należy znaleźć resztę z dzielenia liczby 3^{14404} przez 1000.
Obliczmy

$$\varphi(1000) = \varphi(2^3 5^3) = \varphi(2^3)\varphi(5^3) = 400.$$

Wróćmy do naszego zadania.

Zadanie

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Rozwiązanie.
Należy znaleźć resztę z dzielenia liczby 3^{14404} przez 1000.
Obliczmy

$$\varphi(1000) = \varphi(2^3 5^3) = \varphi(2^3)\varphi(5^3) = 400.$$

Zatem

$$3^{14404} = 3^{400 \cdot 36 + 4} = (3^{400})^{36} 3^4 \equiv 3^4 \pmod{1000},$$

bo $3^{400} \equiv 1 \pmod{1000}$ na podstawie twierdzenia Eulera.

Wróćmy do naszego zadania.

Zadanie

Znajdź trzy ostatnie cyfry liczby 3^{14404}.

Rozwiązanie.
Należy znaleźć resztę z dzielenia liczby 3^{14404} przez 1000.
Obliczmy

$$\varphi(1000) = \varphi(2^3 5^3) = \varphi(2^3)\varphi(5^3) = 400.$$

Zatem

$$3^{14404} = 3^{400 \cdot 36 + 4} = (3^{400})^{36} 3^4 \equiv 3^4 \pmod{1000},$$

bo $3^{400} \equiv 1 \pmod{1000}$ na podstawie twierdzenia Eulera.

Ponieważ $3^4 = 81$, więc
ostatnie trzy cyfry liczby 3^{14404} to 081.

I to już koniec wykładu 3!

Dziękuję za uwagę