Zastosowanie liczb pierwszych

Źródło: James Orr, dostępny w internecie: www.unsplash.com.

W świecie nauki krąży anegdota, jakoby jeden z najwybitniejszych matematyków, Carl Friedrich Gauss (1777 – 1855), powiedział swego czasu, że z powodu swojej całkowitej nieprzydatności to właśnie teoria liczb jest królową matematyki. Ciekawe, co powiedziałby Gauss, gdyby się dowiedział, że to dzięki nauce o liczbach naturalnych możemy dziś przesyłać szyfrowane wiadomości (np. hasła), dzięki którym do kont bankowych i skrzynek mailowych dostęp mają tylko ich właściciele...

> **Twoje cele**
>
> - Obliczysz wybrane wartości funkcji φ Eulera.
> - Zastosujesz arytmetykę modularną.
> - Zastosujesz algorytm RSA do zakodowania i odkodowania wiadomości.

Przeczytaj

W tej lekcji skupimy się na zastosowaniu liczb pierwszych w kryptografii (gałąź wiedzy o szyfrowaniu wiadomości). Omówimy najczęściej dziś stosowany algorytm szyfrowania, jakim jest RSA. Jego nazwa pochodzi od pierwszych liter nazwisk jego twórców, czyli Rona Rivesta, Adiego Shamira oraz Leonarda Adlemana.

Zanim jednak opiszemy działanie algorytmu, wprowadzimy pojęcia matematyczne, które są przydatne do jego dokładnego omówienia.

Kongruencje i arytmetyka modularna

Przypomnijmy sobie dzielenie z resztą i bez reszty w zbiorze liczb naturalnych.

Wprowadźmy oznaczenie. Niech n będzie liczbą naturalną większą od 1. Fakt, że liczby naturalne a i b dają z dzielenia przez n tę samą resztę będziemy zapisywać następująco:

$$a \equiv b (\mathrm{mod}\ \ n).$$

Powyższy napis można odczytać jako "a przystaje do b modulo n" albo "liczby a i b przystają modulo n". Jeżeli któraś spośród liczb a i b jest mniejsza od liczby n, wówczas jest ona równa reszcie z dzielenia każdej z liczb a i b przez n.

> **Przykład 1**
>
> Ponieważ liczby 5 i 9 z dzielenia przez 2 dają resztę 1, więc prawdą jest, że $5 \equiv 9 \equiv 1 (\mathrm{mod}\ \ 2)$.
>
> Ponieważ liczby 8 i 23 z dzielenia przez 3 dają resztę 2, więc prawdą jest, że $8 \equiv 23 \equiv 2 (\mathrm{mod}\ \ 3)$.
>
> Ponieważ liczby 55 i 10 z dzielenia przez 5 dają resztę 0, więc prawdą jest, że $55 \equiv 10 \equiv 0 (\mathrm{mod}\ \ 5)$.

> Ponieważ liczby 24 i 38 z dzielenia przez 7 dają resztę 3, więc prawdą jest, że $24 \equiv 38 \equiv 3 (\mathrm{mod}\ 7)$.

Kongruencje (relacja przystawania liczb modulo) mają wiele własności analogicznych do własności relacji równości, ale nie będziemy ich tutaj szczegółowo omawiać.

Rozważmy zbiór $\mathbb{Z}_n = \{0,\ 1,\ 2,\ 3, \ldots,\ n-1\}$ wszystkich możliwych reszt z dzielenia przez liczbę naturalną n większą od 1.

W zbiorze tym zdefiniujemy dwa działania:

- dodawanie modulo n (oznaczane symbolem $+_n$),
- mnożenie modulo n (oznaczane symbolem $\cdot_n$).

Niech a i b będą liczbami ze zbioru $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$. Wówczas sumą modulo n liczb a i b nazywamy resztę z dzielenia liczby $a + b$ przez n, zaś iloczynem modulo n liczb a i b nazywamy resztę z dzielenia liczby $a \cdot b$ przez n.

> **Przykład 2**
>
> Rozważmy zbiór $\mathbb{Z}_7 = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\}$.
>
> $0 +_7 2$ jest równe reszcie z dzielenia liczby $0 + 2 = 2$ przez 7, czyli 2.
>
> $4 +_7 2$ jest równe reszcie z dzielenia liczby $4 + 2 = 6$ przez 7, czyli 6.
>
> $4 +_7 5$ jest równe reszcie z dzielenia liczby $4 + 5 = 9$ przez 7, czyli 2.
>
> $6 +_7 2$ jest równe reszcie z dzielenia liczby $6 + 2 = 8$ przez 7, czyli 1.
>
> Cała tabliczka dodawania modulo 7 znajduje się poniżej i zawiera wszystkie możliwe sumy dwóch liczb ze zbioru $\mathbb{Z}_7 = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\}$.

$+_7$	0	1	2	3	4	5	6

0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Przykład 3

Rozważmy zbiór $\mathbb{Z}_5 = \{0,\ 1,\ 2,\ 3,\ 4\}$.

$0 \cdot_5 2$ jest równe reszcie z dzielenia liczby $0 \cdot 2 = 0$ przez 5, czyli 0.

$1 \cdot_5 3$ jest równe reszcie z dzielenia liczby $1 \cdot 3 = 3$ przez 5, czyli 3.

$3 \cdot_5 2$ jest równe reszcie z dzielenia liczby $3 \cdot 2 = 6$ przez 5, czyli 1.

$3 \cdot_5 4$ jest równe reszcie z dzielenia liczby $3 \cdot 4 = 12$ przez 5, czyli 2.

Cała tabliczka mnożenia modulo 5 znajduje się poniżej i zawiera wszystkie możliwe iloczyny dwóch liczb ze zbioru $\mathbb{Z}_5 = \{0,\ 1,\ 2,\ 3,\ 4\}$.

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Można udowodnić wiele własności działań modulo n w zbiorze $\mathbb{Z}_n = \{0,\ 1,\ 2,\ 3, \ldots,\ n-1\}$ analogicznych do własności dodawania i mnożenia w zbiorze liczb całkowitych.

Niektóre można zaobserwować na powyższych przykładach:

- zbiór $\mathbb{Z}_n = \{0,\ 1,\ 2,\ 3, \ldots,\ n-1\}$ jest zamknięty na dodawanie modulo n, co oznacza, że wynik tego działania należy do zbioru $\mathbb{Z}_n$,
- zbiór $\mathbb{Z}_n = \{0,\ 1,\ 2,\ 3, \ldots,\ n-1\}$ jest zamknięty na mnożenie modulo n, co oznacza, że wynik tego działania należy do zbioru $\mathbb{Z}_n$,
- 1 jest elementem neutralnym mnożenia modulo n,
- 0 jest elementem neutralnym dodawania modulo n,
- dodawanie modulo n jest działaniem przemiennym,
- mnożenie modulo n jest działaniem przemiennym.

Ponadto możemy wprowadzić definicje liczb (elementów) przeciwnych i liczb (elementów) odwrotnych.

> **Definicja: Liczby (elementy) przeciwne**
>
> Mówimy, że liczby a i b ze zbioru $\mathbb{Z}_n$ są liczbami przeciwnymi modulo n, jeśli ich suma modulo n jest równa 0.

> **Definicja: Liczby (elementy) odwrotne**
>
> Mówimy, że liczby a i b ze zbioru $\mathbb{Z}_n$ są liczbami odwrotnymi modulo n, jeśli ich iloczyn modulo n jest równy 1.

> **Przykład 4**
>
> W zbiorze $\mathbb{Z}_7$ parami liczb przeciwnych modulo 7 są: 1 i 6, 2 i 5, 3 i 4, bo $1 +_7 6 = 0, 2 +_7 5 = 0, 3 +_7 4 = 0$. Zero jest liczbą przeciwną do samego siebie, bo $0 +_7 0 = 0$.

W zbiorze $\mathbb{Z}_7$ parami liczb odwrotnych modulo 7 są: 2 i 4, 3 i 5, bo $2 \cdot_7 4 = 1$, $3 \cdot_7 5 = 1$.
Jedynka jest liczbą odwrotną do samej siebie, bo $1 \cdot_7 1 = 1$. Podobnie liczba 6 jest odwrotna sama do siebie, bo $6 \cdot_7 6 = 1$.

Funkcja φ Eulera

Funkcja φ przyporządkowuje liczbie naturalnej n liczbę liczb względnie pierwszych z n, które nie są od niej większe.

Przykład 5

$\varphi(10)$ oznacza liczbę liczb naturalnych nie większych od 10, które są z dziesiątką względnie pierwsze.
Są to liczby: $1, 3, 7, 9$ i jest ich 4, zatem $\varphi(10) = 4$.

$\varphi(11)$ oznacza liczbę liczb naturalnych nie większych od 11, które są z jedenastką względnie pierwsze.
Są to liczby: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ i jest ich 10, zatem $\varphi(11) = 10$.

Zauważmy, że liczb względnie pierwszych z liczbą 11 jest znacznie więcej, niż liczb względnie pierwszych z liczbą 10, pomimo że obie liczby różnią się tylko o 1. Powodem tego jest fakt, że liczba 11 jest liczbą pierwszą, czyli poza jedynką nie ma dzielników mniejszych od siebie.

Ponieważ liczba pierwsza p nie ma poza jedynką dzielników mniejszych niż p, zatem wszystkie liczby naturalne mniejsze niż p są z nią względnie pierwsze. Wynika stąd, że dla każdej liczby pierwszej p zachodzi

$$\varphi(p) = p - 1$$

Przykład 6

Wyznaczymy $\varphi(49)$.

Zauważmy, że liczba 49 jest kwadratem liczby pierwszej 7 ($49 = 7^2$).

Zatem jedyne liczby nie większe od liczby 49, które nie są z nią względnie pierwsze to wielokrotności liczby 7, czyli $7 = 7 \cdot 1, 14 = 7 \cdot 2, 21 = 7 \cdot 3, 28 = 7 \cdot 4, 35 = 7 \cdot 5, 42 = 7 \cdot 6, 49 = 7 \cdot 7$. Jest ich dokładnie 7.

Zatem $\varphi(49) = 49 - 7 = 42$.

Przykład 7

Wyznaczymy $\varphi\left(p^2\right)$ dla dowolnej liczby pierwszej p.

Zauważmy, że jedyne liczby nie większe od p^2, które nie są względnie pierwsze z p^2 to wielokrotności liczby p, czyli liczby p, $2p$, $3p$, $4p$, $\ldots$, $(p-1)p$, p^2. Jest ich dokładnie p.

Zatem $\varphi\left(p^2\right)$ możemy otrzymać odejmując od liczby wszystkich liczb naturalnych od 1 do p^2 liczbę wielokrotności liczby p nie większych od liczby p^2, zatem $\varphi\left(p^2\right) = p^2 - p = p(p-1)$.

Przykład 8

Wyznaczymy $\varphi(pq)$ dla dowolnych liczby pierwszych p i q.

Zauważmy, że jedyne liczby nie większe od pq, które nie są względnie pierwsze z pq to wielokrotności liczby p i wielokrotności liczby q, czyli liczby p, $2p$, $3p$, $4p$, $\ldots$, $(q-1)p$, qp oraz liczby q, $2q$, $3q$, $4q$, $\ldots$, $(p-1)q$, pq.

Tych pierwszych jest dokładnie p, zaś tych drugich dokładnie q, ale liczba pq jest wielokrotnością i liczby p, i liczby q, co oznacza, że razem tych liczb jest $(p+q-1)$.

Zatem $\varphi(pq)$ możemy otrzymać odejmując od liczby wszystkich liczb naturalnych od 1 do pq liczbę wielokrotności liczby p nie większych od liczby pq oraz liczbę wielokrotności liczby q mniejszych od pq.

Zatem
$\varphi(pq) = pq - (p + q - 1) = pq - p - q + 1 = p(q - 1) - (q - 1) = (q - 1)(p - 1$
.

Przykład 9

Wyznaczymy wartość funkcji φ dla wybranych liczb naturalnych:

$\varphi(20)$ – liczby względnie pierwsze z liczbą 20 i nie większe od niej to 1, 3, 7, 9, 11, 13, 17, 19, zatem $\varphi(20) = 8$

$\varphi(25)$ – liczba 25 jest kwadratem liczby 5, więc możemy wykorzystać zależność z przykładu 7: $\varphi(25) = 25 - 5 = 20$

$\varphi(35)$ – liczba 35 jest iloczynem dwóch liczb pierwszych (5 i 7), więc możemy skorzystać z zależności z przykładu 8:
$\varphi(35) = \varphi(5 \cdot 7) = (5 - 1)(7 - 1) = 4 \cdot 6 = 24$

Twierdzenie: Twierdzenie Eulera

Jeśli a i m są względnie pierwszymi liczbami naturalnymi dodatnimi, to m dzieli liczbę

$$a^{\varphi(m)} - 1.$$

Równoważnie twierdzenie można sformułować następująco:

Jeśli a i m są względnie pierwszymi liczbami naturalnymi dodatnimi, to

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m).$$

Dowód powyższego twierdzenia pominiemy, ale ma ono zasadnicze znaczenie w algorytmie RSA.

Przykład 10

Rozważmy $a = 22$ i $m = 35$. Ponieważ $a = 2 \cdot 11$ i $m = 5 \cdot 7$, więc liczby 22 i 35 są względnie pierwsze.

Na mocy twierdzenia Eulera $22^{\varphi(35)} \equiv 1 (\mathrm{mod}\ \ 35)$.

Ponieważ $\varphi(35) = \varphi(5 \cdot 7) = (5-1)(7-1) = 4 \cdot 6 = 24$, więc
$22^{24} \equiv 1 (\mathrm{mod}\ \ 35)$, co oznacza, że liczba 22^{24} z dzielenia przez 35 daje resztę 1.

Szyfrowanie RSA

Opiszemy teraz krok po kroku działanie algorytmu RSA.

1. Losujemy dwie liczby pierwsze p i q.
2. Obliczamy iloczyn liczb p i q: $n = p \cdot q$.
3. Obliczamy $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.
4. Wybieramy liczbę J, która spełnia warunki: $1 < J < \varphi(n)$ oraz J jest względnie pierwsze z $\varphi(n)$ (J nie jest dzielnikiem $\varphi(n)$).
5. Szyfrogramem (który zostaje przesłany) liczby m jest liczba c obliczona ze wzoru $c \equiv m^J (\mathrm{mod}\ \ n)$.
6. Obliczamy T tak, aby $T \cdot J \equiv 1 (\mathrm{mod}\, \varphi(n))$.
7. Aby odkodować otrzymany szyfrogram c, obliczamy resztę z dzielenia liczby c^T przez n. Z własności kongruencji wynika, że $m = c^T (\mathrm{mod}\ \ n)$.

Parę liczb $(n,\ J)$ nazywamy **kluczem publicznym** (jawnym), zaś parę $(n,\ T)$ nazywamy **kluczem prywatnym** (tajnym).

Przykład 11

Przyporządkujmy literom alfabetu liczby wg poniższego wzoru:

a	b	c	d	e	f	g	h	i	j	k	l

01	02	03	04	05	06	07	08	09	10	11	12

$ł$	m	n	o	p	r	s	t	u	w	y	z
13	14	15	16	17	18	19	20	21	22	23	24

Zaszyfrujemy słowo “rak”:

1. Wybieramy liczby pierwsze $p = 3$ i $q = 11$.
2. Obliczamy $n = 3 \cdot 11 = 33$.
3. Obliczamy $\varphi(33) = (3-1)(11-1) = 20$.
4. Wybieramy J większe od 1 i mniejsze od 20 względnie pierwsze z 20. Niech $J = 3$.
5. Odczytujemy liczby odpowiadające literom słowa “rak”:

Litera	r	a	k
Liczba odpowiadająca (z tabeli powyżej)	18	01	11
I etap szyfrowania – podnoszenie do potęgi $J = 3$	$18^3 = 5832$	$1^3 = 1$	$11^3 = 1331$
II etap szyfrowania – obliczanie reszty z dzielenia przez 33	$5832 \equiv 24 (\mathrm{mod}\ 33)$	$1 \equiv 1 (\mathrm{mod}\ 33)$	$1331 \equiv 11 (\mathrm{mod}\ 33$
Liczby do przesłania	24	01	11

Zatem szyfrogram do przesłania to 24 01 11.

Przykład 12

Chcemy odczytać szyfrogram 09 03 26, znając klucz publiczny $(n,\ J) = (33, 3)$.

6. Osoba, która chce szyfrogram odczytać, potrzebuje klucza prywatnego, czyli takiej liczby T, dla której $J \cdot T \equiv 1 (\mathrm{mod}\ \varphi(n))$. W naszym przypadku $3T \equiv 1 (\mathrm{mod}\ 20)$.
   Ponieważ $3 \cdot 7 = 21 \equiv 1 (\mathrm{mod}\ 20)$, więc $T = 7$.
7. Możemy deszyfrować wiadomość:

Otrzymane liczby	09	03	
I etap szyfrowania – podnoszenie do potęgi $T = 7$	$9^7 = 4782969$	$3^7 = 2187$	$26^7 = 8031$
II etap szyfrowania – obliczanie reszty z dzielenia przez 33	$4782969 \equiv 15 (\mathrm{mod}\ 33)$	$2187 \equiv 9 (\mathrm{mod}\ 33)$	803181017
Liczby po odszyfrowaniu	15	09	05
Litery odpowiadające odszyfrowanym liczbom	n	i	e

Otrzymana wiadomość to "*nie*" – wstrzymujemy się zatem z działaniem, o którym była mowa z nadawcą szyfrogramu...

W przykładzie 12, aby odczytać treść szyfrogramu, potrzebowaliśmy wartości T. Znając klucz publiczny, mogliśmy ją obliczyć.

Można w takim razie zadać pytanie, na czym polega szyfrowanie, skoro wszystko można obliczyć...
Zwróć uwagę na to, że aby wyznaczyć T, potrzebowaliśmy $\varphi(n)$, czyli rozkład liczby n na czynniki pierwsze.
Skuteczność algorytmu RSA opiera się na tym, że nawet superkomputery mają problemy z rozkładaniem naprawdę dużych liczb na czynniki pierwsze. Gdy ktoś chce włamać się do jakiejś bazy danych i potrzebuje złamać hasło, musi zrobić to na tyle szybko, aby nikt nie zdążył się zorientować, a rozkładanie liczby na czynniki pierwsze może zająć przynajmniej kilka dni. Z tego też powodu ciągle trwają poszukiwania coraz większych liczb pierwszych – im większe liczby pierwsze p i q pomnożymy, tym większą liczbę n otrzymamy. Zaś im większe n, tym trudniej rozłożyć je na czynniki.

> **Przykład 13**
>
> Spróbuj rozłożyć na czynniki pierwsze liczby:
>
> **a)** 2627,
>
> **b)** 56153.
>
> Udało się? Ile czasu Ci to zajęło?
>
> Odpowiedzi:
>
> **a)** $37 \cdot 71 = 2627$,
>
> **b)** $241 \cdot 233 = 56153$.

> **Ciekawostka**
>
> Największa odkryta dotąd (styczeń 2019) liczba pierwsza to $2^{82589933} - 1$ i liczy sobie 24 862 048 cyfr w zapisie dziesiętnym. Wyobraź sobie rozkład na czynniki liczb będących iloczynem liczb pierwszych tego rzędu.

Słownik

liczby względnie pierwsze

mówimy, że liczby naturalne k i m są względnie pierwsze, jeśli ich największym wspólnym dzielnikiem jest 1

liczba pierwsza

liczba naturalna, która ma dokładnie 2 różne dzielniki: 1 i samą siebie

szyfrogram

wiadomość, która została zaszyfrowana

deszyfrować

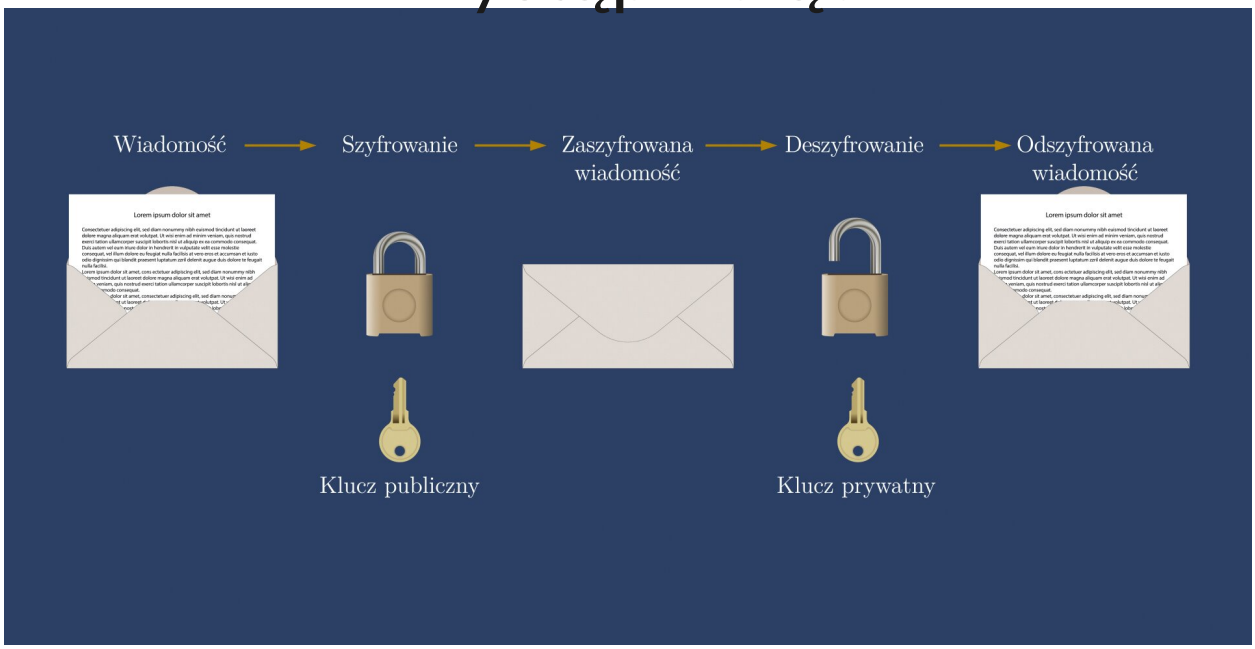
odszyfrowywać wiadomość, która wcześniej została zaszyfrowana

Animacja

Polecenie 1

Przeanalizuj sposób działania algorytmu RSA na podstawie informacji zawartych w animacji.

Wystąpił błąd



Film dostępny pod adresem /preview/resource/RAyAiAW77C6IR

Film nawiązujący do treści lekcji dotyczącej zastosowania liczb pierwszych.

Polecenie 2

Polecenie 3

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Ćwiczenie 2

Ćwiczenie 3

Ćwiczenie 4

Ćwiczenie 5

Ćwiczenie 6

Ćwiczenie 7

Znajdź klucz prywatny, gdy klucz publiczny stanowią liczby $(n,\ J) = (91,\ 29)$.

Ćwiczenie 8

Klucz publiczny to $(n,\ J) = (55,\ 27)$. Znajdź klucz prywatny i rozszyfruj szyfrogram “$17\ 24\ 01$”. Literom odpowiadają liczby z przykładu 11.

Dla nauczyciela

Autor: Sebastian Guz

Przedmiot: Matematyka

Temat: Zastosowanie liczb pierwszych

Grupa docelowa:

III etap edukacyjny, liceum ogólnokształcące, technikum, zakres rozszerzony

Podstawa programowa:

Treści nauczania – wymagania szczegółowe:

I. Liczby rzeczywiste.

Zakres podstawowy. Uczeń:

2) przeprowadza proste dowody dotyczące podzielności liczb całkowitych i reszt z dzielenia nie trudniejsze niż: a) dowód podzielności przez 24 iloczynu czterech kolejnych liczb naturalnych, b) dowód własności: jeśli liczba przy dzieleniu przez 5 daje resztę 3, to jej trzecia potęga przy dzieleniu przez 5 daje resztę 2;

Kształtowane kompetencje kluczowe:

- kompetencje w zakresie rozumienia i tworzenia informacji;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii
- kompetencje cyfrowe
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się

Cele operacyjne:

Uczeń:

- oblicza wybrane wartości funkcji φ Eulera,
- stosuje arytmetykę modularną,
- wykorzystuje algorytm RSA do zakodowania i odkodowania wiadomości.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- odwrócona klasa;
- dyskusja;
- opis ustny.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. Nauczyciel prosi uczniów o zapoznanie się z zagadnieniami, które będą poruszane podczas lekcji.

Faza wstępna:

1. Nauczyciel prosi wybraną osobę o odczytanie tematu lekcji tj. „Zastosowanie liczb pierwszych", a następnie określa cele i kryteria sukcesu.
2. Nauczyciel prosi uczniów, aby zgłaszali swoje propozycje pytań do wspomnianego tematu. Jedna osoba może zapisywać je na tablicy. Gdy uczniowie wyczerpią pomysły, a pozostały jakieś ważne kwestie do poruszenia, nauczyciel je dopowiada.

Faza realizacyjna:

1. Nauczyciel dzieli uczniów na 4-osobowe grupy. Uczniowie w grupach zapoznają się z informacjami w sekcji „Przeczytaj". Analizują przedstawione przykłady i notują pytania. Następnie przedstawiają pytania na forum klasy. Odpowiadają na nie uczniowie z innych grup. Nauczyciel wyjaśnia ewentualne wątpliwości.
2. Uczniowie wykonują wspólnie na forum klasy ćwiczenia nr 1-2.
3. Kolejne ćwiczenia nr 3-5 uczniowie wykonują w parach. Następnie konsultują swoje rozwiązania z inna parą uczniów i ustalają jedną wersję odpowiedzi, zapisują problemy, które napotkali podczas rozwiązywania ćwiczeń.
4. Uczniowie wykonują indywidualnie ćwiczenia 6, 7 i 8, ale następnie porównują swoje odpowiedzi z kolegą lub koleżanką.

Faza podsumowująca:

1. Omówienie ewentualnych problemów z rozwiązaniem ćwiczeń z sekcji „Sprawdź się".

2. Nauczyciel przypomina temat zajęć: „Zastosowanie liczb pierwszych” i podsumowuje przebieg zajęć. Wskazuje mocne i słabe strony pracy uczniów.

Praca domowa:

1. Uczniowie opracowują FAQ (minimum 3 pytania i odpowiedzi prezentujące przykład i rozwiązanie) do tematu lekcji („Zastosowanie liczb pierwszych”).

Materiały pomocnicze:

- Liczby pierwsze i liczby złożone
- Czy liczby pierwsze zdradzą swoje tajemnice?

Wskazówki metodyczne:

- Medium w sekcji „Animacja” można potraktować jako zadania domowe dotyczące analizy problemu w temacie „Zastosowanie liczb pierwszych”.