Kurs M.D. - W 8a
Forma - wykład
Tryb - on-line

Wykład oczupełniający!

Temat . Liczby pierwsze, kongruencje i zastosowanie w kryptografii na przykładzie systemu RSA.

Wprowadzenie

RSA (od Rivest - Shamir - Adleman) jest algorytmem, który pozwala w dobie współczesnych komputerów w sposób zadowalający szyfrować i deszyfrować wiadomości.
Jest to tzw. algorytm asymetryczny, co oznacza że korzysta on z dwóch różnych KLUCZY.
Jak pokażemy dalej, konstrukcja tych kluczy jak i procedury szyfrowania - deszyfrowania wykorzystuje: liczby pierwsze i ich własności (Podstawowe twierdzenie arytmetyki), relację mod i jej własności (Tw. Eulera).

Dalej przedstawimy te zagadnienia ilustrując je odpowiednimi przykładami.

Liczby pierwsze.

Niech $\mathbb{N}$ oznacza zbiór l. całkowitych dodatnich ($\equiv$ naturalnych)

Def 1 (dzielnik)

Powiemy, że liczba $d \in \mathbb{N}$ jest dzielnikiem liczby $n \in \mathbb{N}$, co zapisujemy $d | n$, jeśli

$$n = d \cdot k, \text{ dla pewnej } k \in \mathbb{N}.$$

Def 2 (l. pierwsza)

Każdą liczbę całkowitą ~~dodatnią~~ $n \geq 2$, której jedynymi dzielnikami są: 1 oraz n nazywamy liczbą PIERWSZĄ.

Uwaga 1.

Przyjmujemy (patrz też dalej), że $n = 1$ nie jest l. pierwszą. Zatem najmniejszą jest liczba 2.

Każdą liczbę $n \in \mathbb{N} \setminus \{1\}$, która nie jest pierwsza będziemy nazywali liczbą złożoną.

Przykład 1

7 – pierwsza, $15 = 3 \cdot 5$ – złożona

Uwaga 2.

Liczby pierwsze można wyznaczyć za pomocą algorytmu zwanego Sito Eratostenesa (S.E.)

Algorytm S.E.

(i) ze zbioru $A_n = \{2, 3, \ldots, n\}$ $(n > 2)$

wybieramy najmniejszą, czyli 2 i wykreślamy wszystkie jej wielokrotności większe od niej samej

$$A_{17} = \{2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17\}$$

$$\downarrow$$

$$A^{(i)} = \{2, 3, 5, 7, 9, 11, 13, 15, 17\}$$

(ii) ze zbioru $A^{(i)}$ wybieramy najmniejszą, czyli 3 i powtarzamy krok (i)

$$A^{(ii)} = \{2, 3, 5, 7, 11, 13, 17\}$$

Procedurę (i) powtarzamy aż liczba k, której wielokrotności wykreślamy, będzie spełniała warunek $k > \sqrt{n}$, czyli $k > \sqrt{17}$. Dlatego $A^{(ii)}$ – wszystkie liczby pierwsze ze zbioru A_n.

Uwaga).

Wyróżnia się wiele rodzajów liczb pierwszych: np. Liczby MERSENNEa, bliźniacze, lustrzane i inne.

Nie ma natomiast wzoru, który uwzględniałby wszystkie L.P.

Niektóre można opisać, np. dla kolejnych $n \in \mathbb{N}$

$(n=1,2,3,4)$ $F(n) = 2^{2^n} + 1$ są pierwsze (ale nie dla wszystkich!) np. $n=5$

$(n=1,2,\dots,40)$ $F(n) = n^2 - n + 41$ są pierwsze.

Tw1 (o nieskończoności zbioru l. pierwszych)

Zbiór liczb pierwszych P nie jest skończony. Mówimy, że jest nieskończony.

Dowód. (Euklides).

Przypuśćmy, że tak nie jest, czyli $P = \{p_1, p_2, \dots, p_k\}$, a inne każda liczba $n \in \mathbb{N} \setminus P$ jest złożona.

Bierzemy liczbę

$$n \stackrel{df}{=} p_1 p_2 \cdots p_k + 1.$$ Jasne, że

$n \notin P$ (bo $n > p_j$, $j = 1 \dots k$)

Ponieważ

$$n = (p_2 \cdot \ldots \cdot p_k)p_1 + 1 \quad \text{oraz} \quad p_1 \geq 2$$

oznacza to, że p_1 nie dzieli n.
Podobnie $p_2, \ldots, p_k$ nie dzielą n.
Weźmy dzielnik $1<d$ liczby n mniejszy od n.
Wtedy albo d jest liczbą pierwszą, albo ma dzielnik będący liczbą pierwszą. Ale jak pokazaliśmy wyżej jest to niemożliwe. Uzyskana sprzeczność dowodzi, że zdanie „P jest zbiorem skończonym" jest fałszywe.

$\emptyset$.

ZAD 1.
Udowodnić, że każda l. naturalna $n>1$ ma co najmniej jeden dzielnik będący liczbą pierwszą.

Tw 2 (Podstawowe Tw. Arytmetyki)

Dla każdej liczby naturalnej $n>1$, ~~dla każdej~~ mamy:
albo $n \in \mathbb{P}$, albo

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \quad \text{gdzie } p_1, \ldots, p_k \in \mathbb{P}$$
$$\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$$

i ponadto przedstawienie jest jedyne, czyli

gdyby $p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdot \ldots \cdot q_r^{\beta_r}$, to

$k = r$, $p_i = q_i$ $i = 1..k$

$\alpha_i = \beta_i$

//.

Przykład 2 (rozkład liczby - faktoryzacja)

Weźmy $n = 135$. Czytając zbiór $\mathbb{P}$ od najmniejszej będziemy identyfikować dzielniki n i jej kolejnych wielokrotności tych dzielników:

135	$\cancel{2}$ 3	$\cancel{2}$, 3
wielokrotnie ← 45	3	$\cancel{2}$, 3
15	3	$\cancel{2}$, 3
5	5	$\cancel{2}$, $\cancel{3}$, 5
1		

$135 = 3^3 \cdot 5$

Def 3 (liczby względnie pierwsze)

Powiemy, że $n, m \in \mathbb{N} \setminus \{1\}$ są względnie pierwsze, piszemy $(n,m) = 1$, jeśli $\text{NWD}(n,m) = 1$

gdzie $NWD(a,b)$ oznacza największą liczbę $d \in \mathbb{N}$,

że $d|a$ oraz $d|b$.

Uwaga.

Algorytm Euklidesa wyznaczania $NWD(a,b)$

Niech $a,b \in \mathbb{N} \setminus \{1\}$. Możemy założyć, że $a>b$.

Wtedy $a = k_1 b + r_1$, gdzie $k_1 \in \mathbb{N}$

$r_1 \in \{0,1,\ldots,b-1\}$.

Jeśli $r_1 = 0$, to

$$NWD(a,b) = b.$$

Jeśli $r_1 > 0$, to mamy

$$b = k_2 \cdot r_1 + r_2, \quad r_2 \in \{0,1,\ldots,r_1-1\}$$

$k_2 \in \mathbb{N}$

Jeśli $r_2 = 0$, to po podstawieniu otrzymamy

$$a = k_1 b + r_1 = k_1(k_2 r_1) + r_1 =$$

$$= r_1(k_1 k_2 + 1) \text{ i } NWD(b,r_1) = r_1,$$

dlatego $NWD(a,b) = r_1$. Procedura zakończy się

po skończonej ilości kroków, bo $\ldots < r_2 < r_1$.

P.3.

Znajdź NWD(282, 78)

$282 = 3 \cdot 78 + 48$ $\qquad r_1 = 48$

$78 = 1 \cdot 48 + 30$ $\qquad r_2 = 30$

$48 = 1 \cdot 30 + 18$ $\qquad r_3 = 18$

$30 = 1 \cdot 18 + 12$ $\qquad r_4 = 12$

$18 = 1 \cdot 12 + 6$ $\qquad r_5 = 6$

$12 = 2 \cdot 6 + 0$ $\qquad r_6 = 0$

Zatem $\underline{NWD(282, 78) = 6}$.

Def 4 (Funkcja Eulera φ)

Dla każdej $n \in \mathbb{N}$, niech

$$\varphi(n) \overset{df}{=} \#\{1 \le d < n : (d, n) = 1\},$$

$d < n$

czyli jest to liczba wszystkich względnie pierwszych z n.

P.3. Niech $n = 15$, wtedy jej dzielniki to: $\overbrace{1, 2, 3, \dots 14}^{14}$

$\{1, 2, 4, 7, 8, 11, 13, 14\}$

oraz każdy z nich jest względnie pierwszy z 15,

zatem $\varphi(15) = 8$.

8

Zauważmy, że mamy rozkład (faktoryzację!)

$15 = 3 \cdot 5$ oraz

$$15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8 = \varphi(15).$$

Twierdzenie 3 (o funkcji Eulera)

Dla funkcji Eulera φ mamy

① $\varphi(p) = p-1, \quad p \in P$

② $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right)$

③ $(m,n)=1$, to $\varphi(mn) = \varphi(m)\varphi(n)$

Niech teraz dana będzie faktoryzacja (Tw. 2)

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

Wtedy z ③

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r})$$

Ale z ② $\quad \varphi(p_j^{\alpha_j}) = p_j^{\alpha_j}\left(1-\frac{1}{p_j}\right)$,

dlatego

$$\varphi(n) = \left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\right)\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \cdots \left(1-\frac{1}{p_r}\right)$$

Skut

$$\boxed{\varphi(n) = n\prod_{j=1}^{r}\left(1-\frac{1}{p_j}\right)}$$

Jt do ogólnej postaci wzoru na f. Eulera.

ZAD2

Udowodnij, że dla $p \in P$, $\alpha \geq 1$

$$\varphi(p^{\alpha}) = p^{\alpha}\left(1-\frac{1}{p}\right).$$

Kongruencja i Tw. Eulera.

Przypomnijmy, że dla $d \in \mathbb{N} \setminus \{1\}$, oraz $n \in \mathbb{Z}$, $r_d(n)$ oznacza resztę z dzielenia n przez d, czyli

$$n = kd + r_d(n), \quad r_d(n) \in \{0, 1, .., d-1\}.$$

Wtedy piszemy

$$n \equiv r_d(n) \pmod{d}$$

Jeśli teraz dla $n, m \in \mathbb{Z}$,

$$r_d(n) = r_d(m),$$ to piszemy

$$n \equiv m \pmod{d}.$$

Z def. wynika, iż

$$n \equiv m \pmod{d} \iff d \mid n-m.$$

Dalej będzie potrzebne następujące tw.

<u>Tw. 4 (Eulera o kongruencji)</u>

Dla dowolnych $a, n \in \mathbb{N}$, takich że $(a,n) = 1$ mamy

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

Przed dowodem pokażmy praktyczne zastosowanie tego wzoru.

<u>P.4.</u> Oblicz $13^{101} \underbrace{\pmod{16}}_{\to \text{ obliczyć liczbę!}}$.

<u>Obserwacja 1.</u> $(13, 16) = 1$

<u>Obserwacja 2</u> $\varphi(16) = 8$

Zahn z Tv. 4

$$13^8 \equiv 1 \pmod{16}$$

Z drugiej strony

$$101 = 12\cdot 8 + 5 \text{, dlatego}$$

$$13^{101} = 13^{\frac{101}{8}\cdot 8} = \left(13^8\right)^{\frac{101}{8}} =$$

$$= \left(13^8\right)^{12+\frac{5}{8}} = \left(13^8\right)^{12} \cdot 13^5$$

Ale $\left(13^8\right)^{12} \equiv 1^{12} \pmod{16}$

$$\parallel$$

$$\equiv 1$$

Wyżej $13^5 = 13^{1+4} = 13\cdot 13^4 =$

$$= 13\cdot\left(13^2\right)^2 \equiv (13\cdot\quad) \pmod{16}$$

Ale $13^2 = 169 \equiv 9 \pmod{16}$

$$\left(13^2\right)^2 \equiv 9^2 \equiv 1 \pmod{16}$$

Dlatego $13^{101} \equiv 13^5 \equiv (13\cdot 1) \equiv 13 \pmod{16}$

Powyższy przykład pokazuje, że trzeba go poprawić, bowiem wyliczenie liczby 13^{101} jest kłopotliwe!
(pamiętajmy ile to jest 2^{64}!).

WPROWADZENIE do algorytmu RSA

Jesteśmy przygotowani, aby zrozumieć podstawy szyfrowania opartego na algorytmie RSA.

Założenia

1) Algorytm jest asymetryczny, czyli wymaga dwóch różnych kluczy: PuK (klucz publiczny)
PrK (klucz prywatny).

2) Niech S – nadawca
R – odbiorca
wiadomości M.

3) R dysponuje PuK & PrK. Celem pozyskania wiadomości M od R przekazuje on PuK (stąd „PUBLICZNY").

4) S koduje wiadomość M za pomocą PuK.

5) R dekoduje wiadomość M zaszyfrowaną do C za pomocą PrK.

Konstrukcja kluczy PuK & PrK

α) ustalmy dwie (duże) liczby pierwsze p, q (i zachowujemy je w tajemnicy)

β) definiujemy wartość mod: $n = p \cdot q$ dla obu kluczy

γ) Obliczamy $\varphi(n) = (p-1)(q-1)$ (Tw. Eulera).

δ) Wybieramy liczbę e:

$$1 < e < \varphi(n) \quad \& \quad (e, \varphi(n)) = 1$$

$\underline{\underline{e}}$ będzie współdefiniować PuK wraz z $\underline{\underline{n}}$

ε) wyznaczamy d: $de \equiv 1 \pmod{\varphi(n)}$,

czyli $de = k\varphi(n) + 1$ dla $k \in \mathbb{N}$

lub $\underbrace{d = \frac{1 + k\varphi(n)}{e}}$

d będzie współdefiniować PrK wraz z n

Proces szyfrowania – deszyfrowania.

zaszyfrowana wiadomość ($M \to m$) PuK (e,n) $m<n$

$c \equiv m^e \pmod n$

$\boxed{R}$ $\boxed{S}$

PuK (e,n)

PrK (d,n)

PuK (e,n)

$M \longrightarrow m \; (\in \mathbb{N})$

schemat wypełniania (PADDING SCHEME)

R odbiera $c = m^e \pmod n$ znając e oraz c.

Deszyfruje kluczem PrK (d,n):

$$c = m^e \pmod n \iff c^d \equiv m^{ed} \pmod n$$

Ale $d = \frac{1+k\varphi(n)}{e}$ dla p. $k \in \mathbb{N}$, wiec

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot m^{k\varphi(n)}$$

Jeśli $(m,n)=1$, to z Tw. Eulera

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

i dalej $m^{k\varphi(n)} \equiv (m^{\varphi(n)})^k \equiv 1^k \equiv 1 \pmod n$,

skąd

$$c^d \equiv m^{ed} \equiv m \pmod n$$

Jeśli m i n nie są wzgl. pierwsze, to rozkładamy m na czynniki pierwsze i stosujemy powyższe dla tych czynników.

Zatem: $m^{k\varphi(n)} \equiv 1 \pmod n$

i dalej

$$c^d \equiv m^{ed} \equiv m \pmod n$$

co daje wynik.

Przykład liczby RSA

Załóżmy: $p = 61$, $q = 53$, $n = p \cdot q = 3233$

$M \to m = 123$

Konstrukcja kluczy:

$$\varphi(pq) = (61-1)(53-1) = 3120$$

PuK: $e > 1$ i $(e, 3120) = 1$ np.

$$e = 17$$

mamy: $(e, n) = (17, 3233)$

PrK: d: $de \equiv 1 \pmod{\varphi(n)}$

$$d = \frac{k \cdot 3120 + 1}{17}, \text{ dla } k = 15,$$

w dalsze $d = 2753$

mamy $(d, n) = (2753, 3233)$.

Szyfrowanie PuK wiadomości M:

$$M \to m(=123) \longrightarrow c \equiv m^e \pmod{n},$$

czyli $c = 123^{17} \pmod{3233}$

Deszyfrujemy c PvK:

Krok 1. Odbieramy c:

$c = 855 \pmod{3233}$

ZAD. Wyznacz c(!).

Krok 2. Używamy klucza PvK:

$m \equiv c^d \pmod{n}$:

$m = 855^{2753} \pmod{3233}$

Więc, że $d = \frac{k \cdot 3120 + 1}{17}$ $(k = 15)$, skąd

i z tw. Eulera

$m = 855^{2753} \equiv 855^{k \cdot 3120}$

ZAD. Proszę wykazać, że ~~855~~

$855^{k \cdot 3120}\Big|_{k=15} \equiv 123 \pmod{3233}$