

Funkcja Eulera i szyfrowanie RSA

Stefan Sokołowski

Elbląg, 10 maja 2025

1 Funkcja φ Eulera

Definicja funkcji φ Eulera:

$\varphi(n) \stackrel{\text{def}}{=} \text{liczba takich } k \in \{1, 2, \dots, n\}, \text{ że } \text{nwd}(k, n) = 1$

czyli liczba liczb między 1 a n (włącznie) względnie pierwszych z n .

Obliczanie wartości funkcji φ Eulera:

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

gdzie $p_1, p_2, \dots, p_k$ są wszystkimi pierwszymi dzielnikami liczby n .

Twierdzenie Eulera:

Jeśli n i a są względnie pierwsze i $n \geq 2$, to

$$a^{\varphi(n)} \equiv_n 1$$

Zadanie 1:

Policzyć resztę z dzielenia liczby 49^{1500} przez 300.

Rozwiązanie:

Najpierw policzmy $\varphi(300)$. Jej dzielnikami pierwszymi są 2, 3 i 5:

$$\varphi(300) = 300 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 300 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 80$$

Wobec tego z twierdzenia Eulera mamy $49^{80} = 49^{\varphi(300)} \equiv_{300} 1$, bo 49 i 300 są liczbami względnie pierwszymi. Dlatego

$$\begin{aligned} 49^{1500} &= 49^{80 \cdot 18 + 60} = (49^{80})^{18} \cdot 49^{60} \equiv_{300} 1^{18} \cdot 49^{60} \\ &= 49^{60} = (49^2)^{30} = 2401^{30} \equiv_{300} 1^{30} = 1 \end{aligned}$$

Zadanie 2:

Policzyć następujące reszty z dzielenia:

- | | | |
|---------------------------------|-----------------------------|-------------------------------|
| (a) $8^{1000000}$ przez 63 | (d) 7^{2021} przez 13 | (g) 1111^{111111} przez 59. |
| (b) $110^{10^{25}}$ przez 73 | (e) 28^{123456} przez 41; | |
| (c) $77^{2 \cdot 7^7}$ przez 17 | (f) 57^{666666} przez 29; | |
-

2 Szyfrowanie RSA

Założmy, że

- (a) p i q są różnymi (dużymi) liczbami pierwszymi, $r = p \cdot q$;
wtedy funkcja Eulera wyraża się tak: $\varphi(r) = (p-1) \cdot (q-1)$;
- (b) $e \in \{2, 3, \dots, r-1\}$ jest względnie pierwsze z $\varphi(r)$.

Klucz jawny i szyfrowanie:

Kluczem jawnym jest para (r, e) (czynniki p i q **nie są** ujawniane). Szyfrowanie liczby $L \in \{1, 2, \dots, r-1\}$:

$$L \mapsto C = L^e \bmod r$$

Klucz tajny i odszyfrowywanie:

Kluczem tajnym jest para (r, d) , gdzie d jest odwrotnością liczby e modulo $\varphi(r)$:

$$e \cdot d \equiv_{\varphi(r)} 1 \tag{1}$$

Znając p i q możemy wyznaczyć $\varphi(r)$, a następnie d (przez rozszerzony algorytm Euklidesa); ale znając tylko r nie możemy tego zrobić, bo rozkład r na iloczyn $p \cdot q$ jest trudny obliczeniowo.

Odszyfrowanie dokonuje się przez:

$$C \mapsto L' = C^d \bmod r$$

Zadanie 3:

Wyznaczyć wzór na szyfrowanie kluczem publicznym (jawnym) oraz wzór na odszyfrowywanie w oparciu o liczby pierwsze $p = 19$ i $q = 47$ oraz liczbę $e = 5$. Zilustrować szyfrowanie oraz odszyfrowywanie liczb 413 oraz 38.

Rozwiązanie:

Liczymy iloczyn $r = pq = 19 \cdot 47 = 893$. Ogłaszamy parę $(r, e) = (893, 5)$ jako **klucz jawny**. Dla wyznaczenia klucza tajnego należy znaleźć takie d , żeby

$$5 \cdot d + 828 \cdot k = 1 \quad \text{dla pewnego } k$$

Z rozszerzonego algorytmu Euklidesa wynika, że $d = 497$. Wobec tego za **klucz tajny** będzie służyć para $(r, e) = (893, 497)$.

Szyfrowanie liczby 413:

$$C \equiv_{893} 413^5 \equiv_{893} 580$$

Odszyfrowywanie liczby 580:

$$\begin{aligned} L &\equiv_{893} 580^{497} \equiv_{893} (580^{10})^{49} \cdot 580^7 \equiv_{893} 788^{49} \cdot 737 \equiv_{893} (788^{10})^4 \cdot 788^9 \cdot 737 \\ &\equiv_{893} 465^4 \cdot 761 \cdot 737 \equiv_{893} 766 \cdot 53 \equiv_{893} 413 \end{aligned}$$

Szyfrowanie liczby 38:

$$C \equiv_{893} 38^5 \equiv_{893} 171$$

Odszyfrowywanie liczby 171:

$$\begin{aligned} L &\equiv_{893} 171^{497} \equiv_{893} (171^{10})^{49} \cdot 171^7 \equiv_{893} 874^{49} \cdot 608 \equiv_{893} (874^{10})^4 \cdot 874^9 \cdot 608 \\ &\equiv_{893} 380^4 \cdot 779 \cdot 608 \equiv_{893} 209 \cdot 342 \equiv_{893} 38 \end{aligned}$$

Zadanie 4:

Wyznaczyć wzór na szyfrowanie oraz wzór na odszyfrowywanie RSA jeśli

(a) $p = 17, q = 59, e = 5$

(b) $p = 23, q = 31, e = 29$

W każdym z tych przypadków wyliczyć zaszyfrowaną postać liczby $L = 300$ oraz odszyfrowaną postać wyniku tego szyfrowania.
