Lista Nr 02, ćwiczenia

(wyk. 15,16.X.08r)

Definicja 1. *Grupą nazywamy trójkę* $(G, *, e)$ *gdzie* $* : G \times G \longrightarrow G$ *jest działaniem dwuargumentowym,* $e \in G$ *oraz zachodzi:*

1 $\forall_{a,b,c \in G}\ a * (b * c) = (a * b) * c$ *(łączność);*
2 $\forall_{a \in G}\ e * a = a * e = a$ *(*e – element *neutralny);*
3 $\forall_{a \in G} \exists!_b\ a * b = e$, *takie* b *oznaczamy jako* $b \overset{\text{ozn.}}{=} a^{-1}$ *(*istnienie elementu *odwrotnego);*
4' $\forall_{a,b \in G}\ a * b = b * a$ *(*grupa *abelowa).*

Rzędem grupy nazywamy liczbę elementów G i oznaczamy $|G|$. Jeśli rząd jest skończony, to taką grupę nazywamy *skończoną*. Grupę G' nazywamy *podgrupą* grupy G, jeśli $G' \subseteq G$ oraz G' jest zamknięta w G na *działanie grupowe*, *jedność* i *element odwrotny*. Niech $a \in G$ – grupa skończona i $k \in \mathbb{N}$. Niech

$$a^k \overset{\text{ozn.}}{=} \underbrace{a * \ldots * a}_{k}$$

oraz

$$\langle a \rangle \overset{\text{ozn}}{=} \{a^1, a^2, a^3, \ldots\}$$

Wtedy $\langle a \rangle$ jest podgrupą grupy G. *Rząd* $\langle a \rangle$ nazywamy *rzędem elementu* a.
Dla $n \in \mathbb{N} \setminus \{0\}$ oznaczamy:

$$Z_n \overset{\text{def}}{=} \{0, 1, 2, \ldots n-1\}, \qquad a +_n b \overset{\text{def}}{=} (a+b) \bmod n, \text{ dla } a, b \in Z_n;$$
$$Z_n^* \overset{\text{def}}{=} \{a \in Z_n : a > 0 \,\&\, \mathrm{NWD}(a, n) = 1\}, \qquad a \cdot_n b \overset{\text{def}}{=} (a \cdot b) \bmod n, \text{ dla } a, b \in Z_n^*;$$
$$\phi(n) \overset{\text{ozn}}{=} |Z_n^*| \text{ – rząd grupy } Z_n^*; \qquad a =_n b \overset{\text{ozn}}{\Longleftrightarrow} a = b \bmod n, \text{ dla } a, b \in Z_n.$$

Naszym celem jest *kryptografia z kluczem publicznym RSA*, którego podstawą są własności *grupy multiplikatywnej modulo* n $(Z_n^*, \cdot_n, 1)$. Dalej $e \in \mathbb{N}$ będzie oznaczało liczbę nieparzystą.

Zad. 1 Sprawdzić, że

(a) $(Z_n, +_n, 0)$ jest grupą addytywną modulo n;

(b) $(Z_n^*, \cdot_n, 1)$ jest grupą multiplikatywną modulo n.

Zad. 2 Uzasadnić, że jeśli n jest liczbą pierwszą, to $\phi(n) = n - 1$.
Zad. 3 Jeśli p, q są liczbami pierwszymi i $n = pq$, to $\phi(n) = (p-1)(q-1)$.
Zad. 4* [1] Dla dowolnego $n > 0$ zachodzi:

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}), \quad \text{gdzie } p \text{ jest liczbą pierwszą.}$$

Zad. 5 (Lagrange) Jeśli G' jest podgrupą grupy skończonej G, to rząd G' dzieli rząd G.
Zad. 6 (Euler) Jeśli $a \in Z_n^*$, to wtedy

$$a^{\phi(n)} =_n 1.$$

Zad. 7 (Małe Twierdzenie Fermata) Jeśli p jest liczbą pierwszą oraz $1 \leqslant a < p$, to wtedy

$$a^{p-1} =_p 1.$$

[1] * oznacza zadanie trudniejsze przeznaczone dla ambitniejszych studentów.

Zad. 8* Jeśli p jest liczbą pierwszą i $e \geqslant 1$, to wtedy równanie

$$x^2 =_{p^e} 1$$

ma dokładnie dwa rozwiązania (pierwiastki z 1), $x = -1 = p^e - 1$ i $x = 1$.

Zad. 9 (Twierdzenie chińskie o resztach) Niech $n_1, n_2, \ldots, n_k$ będą liczbami dodatnimi parami względnie pierwszymi, $n = n_1 \cdot \ldots \cdot n_k$, oraz $a_i \in Z_{n_i}$ dla $i = 1, \ldots, k$. Wtedy istnieje jedyna liczba $a \in Z_n$ taka, że

$$a =_{n_i} a_i, \quad \text{dla} \quad i = 1, 2, \ldots k.$$

Wrocław, dnia 21/10/2008