

# 1. Emlékeztető

**1.1. Definíció.** Egy  $g$  számot primitív gyöknek nevezünk modulo  $m$ , ha

$$o_m(g) = \varphi(m).$$

Pl. modulo 17 összesen 8 darab primitív gyök van. Ezek: 3, 5, 6, 7, 10, 11, 12 és 14.

**1.1. Tétel.** Ha  $p$  prím, akkor modulo  $p$  létezik primitív gyök.

**1.2. Tétel.** Egy  $g$  szám akkor és csak akkor primitív gyök modulo  $m$ , ha  $1, g, g^2, \dots, g^{\varphi(m)-1}$  redukált maradékrendszer modulo  $m$ .

**1.3. Tétel.** Az  $m > 1$  modulusra nézve akkor és csak akkor létezik primitív gyök, ha  $m = p^\alpha, 2p^\alpha, 2$  vagy 4, ahol  $p > 2$  prím és  $\alpha > 0$  egész szám.

**1.4. Tétel.** Legyen a modulus egy  $p$  prímszám.

(i) Egy primitív gyök  $i$ -edik hatványa akkor és csak akkor primitív gyök, ha  $(i, p-1) = 1$ .

(ii) A páronként inkongruens primitív gyökök száma  $\varphi(p-1)$ .