6. Определение за приведена (редуцирана) система остатъци.

Множеството от цели числа $\{a_i\}_{i=\overline{1,\varphi(m)}}^{}$, наричаме приведена система, ако за всеки $i,j = \overline{1,m}$, $(a_i, a_j) = 1$, броят на елементите в $\varphi(m)$, $a_i \not\equiv a_j \pmod m$.

7. Формула за функцията на Ойлер

$$\varphi(m) = m \prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

8. Теорема на Ферма-Ойлер.

$a^{\varphi(m)} \equiv 1 \pmod m$, ако $(a, m) = 1$.

9. Определение за показател

Минимално число m, такова че $a^m \equiv 1 \pmod m$, където $(a, m) = 1$, наричаме показател на a по модул m, $\|a\|_m$ по модул m.

10. Свойства на показателите.

За всяко $\|a\| = m$ по модул m, $a^i \not\equiv a^j \pmod m$, за $i \neq j$, $i, j = \overline{1, m}$.

За всяко $\|a\| = m$ по модул m, $a^{bm} \equiv 1 \pmod m$, където $b \in \mathbb{N}$.

За всяко $\|a\| = m$ по модул m, $m \mid \varphi(m)$

За всяко $\|a\| = m$ по модул m, $\|a^b\| = \frac{m}{(m,b)}$, за $b \in \mathbb{N}$ по модул m.

Ако $(m, b) = 1$, $\|a^b\| = m$ по модул m.

За всяко $\|a\| = m$ по модул m, ако $\|a\| = mb$ по модул m, тогава $\|a^m\| = b$.

За всяко $\|a\| = m$ по модул m, ако $\|b\| = c$ по модул m и $(m, c) = 1$, то $\|ab\| = mc$ по модул m.

Ако $\|a_i\| = m_i$ по модул m, $i = \overline{1, s}$ и за $\forall i \neq j$, $(m_i, m_j) = 1$, $i, j = \overline{1, s}$, тогава

$$\left\| \prod_{i=1}^{i=s} a_i \right\| = \prod_{i=1}^{i=s} m_i$$

11. Определение за примитивен корен

Ако $(a, m) = 1$ и $\|a\| = \varphi(m)$ по модул m, тогава a наричаме примитивен корен по модул m.

12. Определение за индекс

Нека $g^m \equiv a \pmod p$, $0 \le m \le p-2$, тогава числото m се нарича индекс на числото a по модул p при основа примитивен корен g.

$m = ind_g a \pmod p$.

Ако $m = ind_g a$, $g^b \equiv a \pmod p$, тогава $m \equiv b \pmod{p-1}$.

Ако $a \equiv b \pmod p$, тогава $ind_g a \equiv ind_g b \pmod{p-1}$

Ако $P \times \prod_{i=1}^{i=m} a_i$, тогава $ind_g \prod_{i=1}^{i=m} a_i \equiv \sum_{i=1}^{i=m} ind_g a_i \pmod{p-1}$