1. tétel

Lineáris kongruenciák:

D: Legyen $a,b \in \mathbb{Z}$ és m pozitív egész. Azt mondjuk, hogy a kongruens b-vel modulo m, ha: $m \mid a-b$.

jel: $a \equiv b \ (m)$

T: 1) $\forall a$-ra : $a \equiv a \ (m)$ reflexív

2) $a \equiv b \ (m) \Rightarrow b \equiv a \ (m)$ szimmetrikus

3) $a \equiv b \ (m) \wedge b \equiv c \ (m) \Rightarrow a \equiv c \ (m)$ tranzitív

} ekvivalenciareláció

4) $a \equiv b \ (m) \wedge c \equiv d \ (m) \Rightarrow a+c \equiv b+d \ (m) \wedge a-c \equiv b-d \ (m)$

5) $a \equiv b \ (m) \wedge c \equiv d \ (m) \Rightarrow ac \equiv bd \ (m)$

6) $a \equiv b \ (m) \Rightarrow a+c \equiv b+c \ (m) \wedge a-c \equiv b-c \ (m)$

7) $a \equiv b \ (m) \Rightarrow ac \equiv bc \ (m)$

8) $a \equiv b \ (m) \Rightarrow a^n \equiv b^n \ (m)$

9) Legyen f egy egész együtthatós polinom. Ekkor:
$a \equiv b (m) \Rightarrow f(a) \equiv f(b) \ (m)$

T: Legyenek $a,b \in \mathbb{Z}$ és m pozitív egész. Ekkor az $ax \equiv b \ (m)$ kongruenciát lineáris kongruenciának nevezzük, és ennek egy megoldásán olyan s számot ($s \in \mathbb{Z}$) értünk, amelyet az x helyére téve a kongruencia fennáll.

T: Az $ax \equiv b \ (m)$ kongruenciának $\Leftrightarrow \exists$ megoldása, ha $(a,m) \mid b$

Euler-Fermat tétel:

T: $(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \ (m)$

D: (Euler-féle φ függvény) Tetszőleges n pozitív egészek esetén $\varphi(n)$ az $1,2 \dots n$ számok közül az n-hez relatív prímek számát jelenti.

T: „Kis" Fermat-tétel:

- Ha p prím és $(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \ (p)$
- Ha p prím $\Rightarrow \forall a \in \mathbb{Z}$ esetén $a^p \equiv a \ (p)$.

Kvadratikus reciprocitás:

T.: Gauss-lemma

Legyen $(a,p)=1$ és tekintsük az $a, 2a, \dots, \frac{p-1}{2}a$ számok modulo p vett legkisebb pozitív maradékait. Jelölje v ezek közül a $\frac{p}{2}$-nél nagyobbak számát. Ekkor $\left(\frac{a}{p}\right) = (-1)^v$

T.: Kvadratikus reciprocitási tétel:

Ha $p>2$ és $q>2$ különböző prím $\Rightarrow$

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \quad \text{azaz} \quad \left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right), & \text{ha } p \equiv q \equiv -1 \ (4) \\ \left(\frac{p}{q}\right), & \text{egyébként.} \end{cases}$$

Legendre szimbólum:

D.: Legyen $p>2$ prím, $(a,p)=1$. Az a számot aszerint nevezzük kvadratikus maradéknak, ill. kvadratikus nemmaradéknak modulo p, hogy az $x^2 \equiv a \ (p)$ kongruencia megoldható-e vagy sem. Az $a \equiv 0 \ (p)$ számokat nem soroljuk sem a kvadratikus maradékok, sem a kvadratikus nemmaradékok közé.

D.: Az $\left(\frac{a}{p}\right)$ Legendre szimbólumot a következőképpen értelmezzük:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ kvadratikus maradék mod } p \\ -1, & \text{ha } a \text{ kvadratikus nemmaradék mod } p. \end{cases}$$

T.: 1) $a \equiv b \ (p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv 1 \ (4) \\ -1, & \text{ha } p \equiv -1 \ (4) \end{cases}$

Magasabb fokú kongruenciák:

D.: Az $f = a_0 + a_1 x + \dots + a_n x^n$ polinom modulo m vett foka k, ha $a_k \not\equiv 0 \ (m)$, de minden $i>k$ esetén $a_i \equiv 0 \ (m)$. Ha minden i-re $a_i \equiv 0 \ (m)$, azaz f minden együtthatója $0 \ (m) \Rightarrow f$-nek modulo m nincs foka.

T.: Ha p prím és az f polinom modulo p vett foka $k \Rightarrow$ az $f(x) \equiv 0 \ (p)$ kongruencia megoldásszáma legfeljebb k.

D.: Legyen $(a,m)=1$. A ℓ pozitív egészt az a rendjének nevezzük modulo m, ha $a^\ell \equiv 1 \ (m)$, de $\forall \ 0 < i < \ell$ esetén $a^i \not\equiv 1 \ (m)$

Primitív gyök:

D.: Egy g számot primitív gyöknek nevezünk modulo m, ha $o_m(g) = \varphi(m)$

T.: Egy g szám $\Leftrightarrow$ primitív gyök az m modulusra nézve, ha $1, g, g^2 \dots g^{\varphi(m)-1}$ redukált maradékrendszert alkotnak modulo m.

T.: Ha p prím $\Rightarrow$ modulo p létezik primitív gyök.

Diszkrét logaritmus (index):

D.: Legyen g primitív gyök mod p $\wedge$ $(a,p)=1$. Ekkor az a-nak a g alapú diszkrét logaritmusán vagy indexén azt a $0 \le \ell \le p-2$ számot értjük, amelyre $a \equiv g^\ell \ (p)$.

jel.: $\operatorname{ind}_{p,g}(a)$

Def.: Jacobi szimbólum:

Legyen $m > 1$ páratlan szám, $m = p_1 \cdot \dots \cdot p_r$, ahol p_i számok pozitív prímek. Legyen továbbá $(a,m)=1$. Ekkor az $\left(\frac{a}{m}\right)$ Jacobi-szimbólumot mint az $\left(\frac{a}{p_i}\right)$ Legendre szimbólumok szorzatát értelmezzük. $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_r}\right)$

T.: I. $a \equiv b \ (m) \Rightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

II. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$; $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

III. $\left(\frac{-1}{m}\right) = \begin{cases} 1, \text{ha } m \equiv 1 \ (4) \\ -1, \text{ha } m \equiv -1 \ (4) \end{cases}$

IV. $\left(\frac{2}{m}\right) = \begin{cases} 1, \text{ha } m \equiv \pm 1 \ (8) \\ -1, \text{ha } m \equiv \pm 3 \ (8) \end{cases}$

V. $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), \text{ha } n \equiv m \equiv -1 \ (4) \\ \left(\frac{n}{m}\right), \text{egyébként} \end{cases}$