"B" tételek

Az itt szereplő tételeket be kell bizonyítani, a bizonyításhoz a korábban kimondott tételeket, segédtételeket, lemmákat fel lehet használni.

1. Legyen A egy nemüres halmaz. Ha $\rho \subseteq A \times A$ ekvivalenciareláció, akkor A/ρ osztályozás az A halmazon. Ha pedig $C \subseteq P(A)$ osztályozás, akkor az $a\rho b \iff \exists B \in C : a, b \in B$ formulával definiált reláció ekvivalenciareláció az A halmazon. A most megadott "ekvivalenciareláció $\mapsto$ osztályozás" illetve "osztályozás $\mapsto$ ekvivalenciareláció" megfeleltetések egymás inverzei.

2. (Euklideszi algoritmus.) Tetszőleges nemnulla a, b egész számokon végrehajtva az euklideszi algoritmust az véges lépésben véget ér, és az utolsó nemzérus osztási maradéka a és b legnagyobb közös osztóját adja.

3. (Diofantoszi egyenlet) Tetszőleges adott nemzéró a, b, c egész számok esetén az $ax + by = c$ diofantoszi egyenlet akkor és csak akkor oldható meg, ha $ln.k.o.(a, b)|c$. Ha (x_0, y_0) egy megoldás, akkor bármely t egész számra az alábbi (x, y) pár is megoldás, továbbá minden megoldás előáll ilyen alakban t alkalmas megválasztásával.

$$x = x_0 + \frac{b}{ln.k.o(a,b)}t$$

$$y = y_0 - \frac{a}{ln.k.o(a,b)}t$$

4. (Kínai maradéktétel) Ha az $x \equiv a_i \pmod{m_i}$, $(1 \leq i \leq k)$ lineáris kongruenciarendszerben a modulusok páronként relatív prímek, akkor a kongruenciarendszer megoldható, és általános megoldása $x \equiv \sum_{i=1}^{k} a_i M_i y_i \pmod{M}$, ahol $M = m_1, \ldots, m_k$, $M_i = \frac{M}{m_i}$ és y_i megoldása az $M_i y_i \equiv 1 \pmod{m_i}$ kongruenciának.

5. (Euler-Fermat–tétel) Tetszőleges a, m egész számok esetén ha $m \geq 2$ és $ln.k.o.(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

6. (Primitív gyökök prímmodulusra) Ha p prím, és $d|p-1$, akkor pontosan $\varphi(d)$ számú inkongruens d-edrendű egész szám létezik modulo p. Következésképp összesen $\varphi(p-1)$ számú inkongruens primitív gyök létezik modulo p.

7. (Négyzetes reciprocitás tétele) Ha p és q különböző páratlan prímek, akkor

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

8. (Möbius-féle megfordítási képlet) Tetszőleges f és F esetén $F(n) = \sum_{d|n} f(d)$ akkor és csak akkor teljesül minden n természetes számra, ha $f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d})$ teljesül minden n természetes számra.

9. (Tökéletes számok) Egy páros szám akkor és csak akkor tökéletes, ha $2^{p-1}(2^p - 1)$ alakú, és itt $2^p - 1$ prímszám (ez pedig csak akkor lehetséges, ha p maga prím).

10. (Primitív pitagoraszi számhármasok) Ha (x, y, z) primitív pitagoraszi számhármas, akkor x és y közül az egyik páros, a másik páratlan. Ha mondjuk x páros, akkor a számhármas megkapható $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$ alakban, ahol $m > n > 0$, továbbá m és n különböző parosságúak és egymáshoz relatív prímek.