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

1. Bármely véges részbenrendezett halmazt egyértelműen meghatározza a fedési relációja.

2. (Euklideszi algoritmus) Tetszőleges nemnulla a, b egész számokon végrehajtva az euklideszi algoritmust az véges számú lépésben véget ér, és 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 $\operatorname{lnko}(a, b) \mid c$. 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 a t egész szám alkalmas megválasztásával.

$$x = x_0 + \frac{b}{\operatorname{lnko}(a, b)} \cdot t$$
$$y = y_0 - \frac{a}{\operatorname{lnko}(a, b)} \cdot t$$

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

6. (Primitív gyökök prímmodulusra) Ha p prím, és $d \mid p - 1$, 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 számelméleti függvények esetén $F(n) = \sum_{d|n} f(d)$ akkor és csak akkor teljesül minden n természetes számra, ha $f(n) = \sum_{d|n} F(d)\,\mu\left(\frac{n}{d}\right)$ 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 is 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 a 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 párosságúak és egymáshoz relatív prímek.

11. (Gyökvonás komplex számokból) Minden nemnulla komplex számnak pontosan n különböző n-edik gyöke van. A $z = r(\cos\varphi + i\sin\varphi)$ trigonometrikus alakban megadott komplex szám n-edik gyökei:

$$\sqrt[n]{z} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right) \qquad (k = 0, 1, \ldots, n-1).$$

12. Minden euklideszi gyűrű főideálgyűrű.

13. Minden főideálgyűrű Gauss-gyűrű. (Elegendő az irreducibilis faktorizáció egzisztenciáját igazolni.)

14. (Irreducibilis polinomok a valós számtest felett) Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom melynek diszkriminánsa negatív.

15. (Schönemann-Eisenstein–féle irreducibilitási kritérium) Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre $p \nmid a_n, p \mid a_{n-1}, \ldots, p \mid a_1, p \parallel a_0$, akkor f irreducibilis a racionális számok teste felett.

16. (Lagrange-interpoláció) Bármely T test, és tetszőlegesen adott $c_1, \ldots, c_{n+1}$ páronként különböző, és $d_1, \ldots, d_{n+1}$ (nem feltétlenül különböző) T-beli elemek esetén létezik pontosan egy olyan $f \in T[x]$ legfeljebb n-edfokú polinom, melyre $f(c_i) = d_i$ $(i = 1, \ldots, n+1)$.

17. (Gyök multiplicitása és a derivált kapcsolata) Ha $k \geq 1$ és a c komplex szám k-szoros gyöke az $f \in \mathbb{C}[x]$ polinomnak, akkor $k - 1$-szeres gyöke f'-nek. (Ha $k = 1$, akkor c nem gyöke f'nek.)

18. (Cardano-képlet) Az $x^3 + px + q = 0$ $(p, q \in \mathbb{C})$ harmadfokú egyenlet minden megoldása megkapható az alábbi képlet segítségével:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

A két köbgyök értékét úgy kell (és lehet is!) megválasztani, hogy a szorzatuk $-\frac{p}{3}$ legyen. Ha u és v a két köbgyök egy-egy ilyen értéke, akkor az $x^3 + px + q$ polinom három gyöke (multiplicitással): $u + v, u\varepsilon + v\varepsilon^2, u\varepsilon^2 + v\varepsilon$, ahol ε egy primitív harmadik egységgyök.

19. (A szimmetrikus polinomok alaptétele) Bármely szimmetrikus polinom felírható az elemi szimmetrikus polinomok polinomjaként.

20. (Testbővítés, véges testek) Ha $f \in \mathbb{Z}_p[x]$ egy n-edfokú irreducibilis polinom, akkor $\mathbb{Z}_p[x]/(f)$ egy p^n-elemű test, amelyben az f polinomnak van gyöke.