

Első ZH**2025. január 8. 10:05–11:45****PÓT-feladatsor**

Minden megoldást indoklással kell alátámasztani. (Az előadáson és a gyakorlaton elhangzott állításokra szabad hivatkozni azok pontos megfogalmazása után. **A tanult módszerek következetes alkalmazása elég indoklás.**)

Használható: Egy A4-es lap két oldalára saját kezűleg írt „puska” és nem programozható számológép (de minden részletszámításnak, ahogy órán tanultuk, szerepelnie kell a beadott lapokon). **Felhasználható idő: 100 perc.**

1. feladat (5+5 = 10 pont)

Add meg a következő számpárok legnagyobb közös osztóit!

(a) Add meg $11^4 - 1$ és $11^6 - 1$ legnagyobb közös osztóját!

(b) Add meg $11^4 + 1$ és $11^6 + 1$ legnagyobb közös osztóját! (Vigyázat! Itt $+$ jelek vannak!)

(**Tipp:** $\text{luko}(a+1, b+1) = \text{luko}(a-b, b+1)$, ezel szemben: $\text{luko}(a-1, b+1) = \text{luko}(a+b, b+1)$, vagy másik módon: $\text{luko}(a-1, b+1) = \text{luko}(a-1, a+b)$, sokszor érdemes az utóbbit használni.)

2. feladat (5+5 = 10 pont)

Oldd meg a következő kongruenciákat!

(a) $11x \equiv 360 \pmod{13}$

(b) $13x \equiv 360 \pmod{11}$

3. feladat (10 pont)

Alaszkában kutyaszánversenyt tartanak. Kizárólag kétféle kutyafoogat indul: olyan, melyet pontosan 11 alaszkai malamut, vagy olyan, melyet pontosan 13 szibériai husky húz. Mindkét fajta szán indult a versenyen, és összesen 360 szánhúzó kutya volt a helyszínen (mind valamelyik szán elé befogva). Hány malamut és hány husky lehetett a helyszínen? (Több megoldás is van, mindet add meg.)

4. feladat (5+5 = 10 pont)

Számítsuk ki az alábbiakat:

(a) $12^{11^{10}} \pmod{13}$;

(b) $11^{45} \pmod{23}$;

5. feladat (10 pont)

RSA titkosításánál $p = 7$, $q = 13$ és $e = 5$. Mi lehetett az eredeti üzenet, ha $c = 2$ a titkosított üzenet?