4. Számelmélet gyakorlat (2009/2010)
Néhány megoldás

1. Ha 3, 36, és 64 ugyanannak mod m maradékosztálynak az elemei, akkor bármely kettő különbsége osztható m-mel: $m \mid 36-3=33$, $m \mid 64-3=61$ és $m \mid 64-36=28$. Mivel $(33,61)=1$, ezért csak $m=1$ lehetséges, vagyis amikor minden egész szám egy mod m maradékosztályba tartozik.

2. (a) Hamis, például $1,2,3,4,5,6$ redukált maradékrendszer mod 7, de mod 14 nem az, mert például $(2,14)=2\neq 1$.

(b) Igaz. Legyen $r_1,\ldots,r_k$ redukált maradékrendszer mod 14. Ahhoz, hogy megmutassuk ez egy mod 7 redukált maradékrendszer is, a következőket kell meggondolnunk:

(i) $k=\varphi(7)$,

(ii) $r_i \not\equiv r_j \ (7)$, ha $i\neq j$,

(iii) $(r_i,7)=1$ minden i-re.

(i) $\varphi(14)=\varphi(7)$. (iii) Ha $(r_i,14)=1$, akkor nyilván $(r_i,7)=1$ is teljesül. (ii) Indirekt tegyük fel, hogy $r_i \equiv r_j \ (7)$, vagyis hogy $7 \mid r_i-r_j$. Ekkor azonban r_i vagy r_j páros, ami nem lehet, mert nem lenne reletív prím 14-hez, ellentmondás.

3. $\varphi(82)=\varphi(2)\varphi(41)=(2-1)(41-1)$, $\varphi(1000)=\varphi(2^3)\varphi(5^3)=(2^3-2^2)(5^3-5^2)=4\cdot 100=400$, $\varphi(2009)=\varphi(7^2)\varphi(41)=(7^2-7)(41-1)=1680$.

4. $\varphi(n)$ az $A=\{k: 1\leq k\leq n \text{ és } (k,n)=1\}$ halmaz elemszáma, $d(n)$ a $B=\{\ell: 1\leq \ell\leq n \text{ és } \ell \mid n\}$ halmaz elemszáma. $A\cup B\subseteq\{1,\ldots,n\}$ és $A\cap B=\{1\}$. $\varphi(n)+d(n)=|A|+|B|=|A\cup B|+|A\cap B|\leq n+1$.

Egyenlőség csak a prímekre és a 4-re áll fenn. Ha p prím, akkor $\varphi(p)=p-1$ és $d(p)=2$, $\varphi(4)=2$ és $d(4)=3$. Ha $m=m_0m_1$ egy öszetett szám, $1<m_0,m_1<m$ és $2<m_1$, akkor $2m_0$ se nem osztója m-nek, se nem relatív prím m-hez, vagyis egyik halmaznak sem eleme, így $\varphi(m)+d(m)\leq m$.

5. Vizsgáljuk meg az $\frac{1}{n},\frac{2}{n},\ldots,\frac{n}{n}$ törteket. Mindet egyszerűsítsük le amennyire csak lehet. A kapott $\frac{k}{d}$ alakú törtekről a következőket tudjuk: 1) Páronként különbözők, mert az eredeti törtek is ilyenek voltak. 2) $d \mid n$ és $(k,d)=1$, mert nem tudtunk tovább egyszerűsíteni. 3) Ha $d' \mid n$ és $(k',d')=1$, $1\leq k'\leq d'$, akkor $\frac{k'}{d'}$ megjelenik a törtjeink között, mert a $\frac{k'\frac{n}{d'}}{n}$ tört egyszerűsítettje.

Kaptuk tehát, hogy n darab olyan $\langle k,d\rangle$ párunk van, melyre $1\leq k\leq d$, $d \mid n$ és $(k,d)=1$. A szummával pontosan ezeket a párokat számoltuk meg.

6. Ha $11 \mid a$, akkor $a^{30}\equiv 0 \ (11)$, ha $11 \nmid a$, akkor az Euler-Fermat Tétel szerint $a^{10}\equiv 1 \ (11)$, amiből $a^{30}\equiv 1 \ (11)$. Tehát a^{30},b^{30},c^{30} közül mindegyik 0 vagy 1 maradékot ad 11-gyel osztva. Ha az összegük osztható 11-gyel, akkor csak $11 \mid a$, $11 \mid b$ és $11 \mid c$ lehetséges, amiből nyilván következik, hogy $11^{30} \mid a^{30}+b^{30}+c^{30}$.

7. Tegyük fel, hogy $23 \nmid a^{88}-b^{88}$. Ha $23 \mid a$, akkor $23 \mid a^{88}$, így $23 \nmid b^{88}$, amiből $23 \nmid b$ és hasonlóan fordítva. Még azt kell megmutatnunk, hogy az egyikük biztosan osztható 23-mal. Ha $23 \nmid a$ és $23 \nmid b$, akkor az Euler-Fermat Tétel szerint $a^{22}\equiv b^{22}\equiv 1 \ (23)$, amiből $a^{88}\equiv b^{88}\equiv 1 \ (23)$, vagyis $23 \mid a^{88}-b^{88}$, ellentmondás.

A fordított implikáció teljesen hasonlóan bizonyítható.