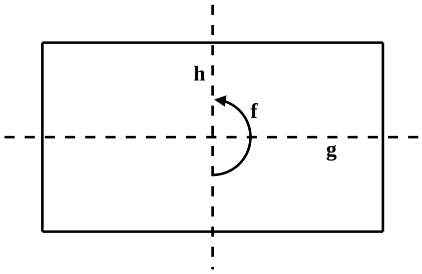
Bevezetés a számításelméletbe II.
2005. ÁPRILIS 21.
10. gyakorlat: Euler-Fermat tétel, algebrai alapfogalmak

1. Számítsuk ki az alábbi értékeket:
   (a) $d(12)$, $\phi(12)$, $\sigma(12)$,
   (b) $d(2004)$, $\phi(2004)$, $\sigma(2004)$.
2. Mennyi $\phi(9)$, $\phi(133)$, $\phi(540)$, $\phi(7!)$?
3. **ZH!** Milyen n értékekre igaz, hogy $\phi(n)$ páratlan? (és milyen n-ekre lesz $d(n)$ páratlan?)
4. Az Euler-féle ϕ függvény tulajdonságait felhasználva,
   (a) bizonyítsuk be, hogy $11 \mid n^{11} + 10n$,
   (b) igazoljuk, hogy ha n nem osztható 17-tel, akkor $n^8 + 1$ vagy $n^8 - 1$ biztosan osztható 17-tel,
   (c) számítsuk ki 108^{182} ill. 5^{17} maradékát 19-cel osztva,
   (d) bizonyítsuk be, hogy $42 \mid n^7 - n$.
5. Bizonyítsuk be, hogy
   (a) $39^{14} - 1$ osztható 5-tel,
   (b) $333^{444} + 444^{333}$ osztható 7-tel,
   (c) $4^{90} + 1$ osztható 17-tel!
6. Kiszámítandó $(((43)^{43})^{43})^{43}$ modulo 49.
7. Oldjuk meg az alábbi kongruenciákat:
   (a) $49^{49} \equiv x \pmod{15}$,
   (b) $3^{80}x \equiv 23 \pmod{100}$.
8. Határozzuk meg az utolsó
   (a) három jegyét számjegyét 403^{402}-nek,
   (b) két számjegyét $29^{39^{49}}$-nek,
   (c) számjegyét $7^{6^{5^{4^{3^2}}}}$-nek!
9. Csoportot alkotnak-e az alábbi halmazon definiált műveletek? Ha igen, akkor vizsgáljuk meg, hogy a csoport kommutatív-e?
   (a) {egész számok, összeadás},
   (b) {páratlan számok, összeadás},
   (c) {páros számok, összeadás},
   (d) {2×2-es mátrixok, mátrixszorzás},
   (e) {n-edik komplex egységgyökök, szorzás},
10. $a^2 = 1 \quad \forall a \in G$-re $\Longrightarrow G$ – Abel-csoport.
11. Írjuk fel az alábbi csoportok Cayley-táblázatát! Melyek izomorfak egymással?
    (a) {mod 4 maradékosztályok, összeadás}
    (b) {mod 8 redukált maradékosztályok, szorzás}
    (c) A téglalap szimmetriacsoportja: (szimmetriacsoport = a rajzot önmagába vivő egybevágósági transzformációk halmaza a kompozícióra, mint műveletre nézve!)



    (d) A „füles négyzet” szimmetriacsoportja: