Bevezetés a számításelméletbe II.

10. gyakorlat, 2007. április 18.

Koblinger Egmont <egmont@cs.bme.hu>

Számelmélet III. – Csoportelmélet

103. Teljes maradékrendszer-e modulo 77 az 1, 11, 21, ... 761 számhalmaz?

104. Redukált maradékrendszer-e modulo 32 az 5, 15, 25, ..., 155 számhalmaz?

105. Legyen n osztható k-val. Bizonyítsuk be, hogy $\varphi(n)$ is osztható $\varphi(k)$-val.

106. Mivel kongruens mod 77 az 1998^{1979} szám?

107. Mi $7^{6^{5^{4^{3^2}}}}$ utolsó számjegye a 10-es számrendszerben?

108. Kiszámítandó $(((43^{43})^{43})^{43})^{43}$ modulo 49.

109. Biz. be, hogy a $10^n + 3$ alakú számok között végtelen sok osztható 13-mal.

110. Legyen a p prím esetén $a_1, a_2, \ldots, a_{p-1}$ RMR (mod p). Biz: $a_1^{p-2}, a_2^{p-2}, \ldots, a_{p-1}^{p-2}$ szintén RMR (mod p).

111. Adjuk meg az összes 1, 2, 3, illetve 4 elemű nem izomorf csoport műveletttábáját.

112. Értelmezzük az egész számok halmazán az $a \star b = a + b + 1$ képlettel megadott műveletet. Mutasd meg, hogy $(\mathbb{Z}, \star)$ csoport. Milyen korábbról ismert csoporttal izomorf $(\mathbb{Z}, \star)$?

113. Határozzuk meg az alábbi alakzatok szimmetriacsoportját.
    (a) szabályos háromszög;
    (b) paralelogramma;
    (c) téglalap;
    (d) deltoid;
    (e) kocka;
    (f) tetraéder.

114. A G csoport e egységére és x, y elemeire $x^2 = e$ és $xyx^{-1} = y^3$. Bizonyítsuk be, hogy $y^8 = e$.

115. Az alábbi következtetések közül melyek teljesülnek minden csoportban?
    (a) $ax = ay \Rightarrow x = y$;
    (b) $xa = ya \Rightarrow x = y$;
    (c) $xa = ay \Rightarrow x = y$;
    (d) $abx = aby \Rightarrow x = y$;
    (e) $axb = ayb \Rightarrow x = y$;
    (f) $bxa = ayb \Rightarrow x = y$;
    (g) $ax = 1 \Rightarrow x = a^{-1}$;
    (h) $abx = 1 \Rightarrow x = a^{-1}b^{-1}$;
    (i) $abx = 1 \Rightarrow x = b^{-1}a^{-1}$.

116. Legyen $a_1, \ldots a_{\varphi(m)}$ az m-nél kisebb, m-hez relatív prím pozitív egészek halmaza. Hasonlóan legyen $b_1, \ldots b_{\varphi(n)}$ az n-nél kisebb, n-hez relatív prím pozitívak halmaza.
    (a) Mutassuk meg, hogy minden $1 \leq i \leq \varphi(m)$ és $1 \leq j \leq \varphi(n)$ esetén pontosan egy olyan mn-nél kisebb x szám van, amelyre $x \equiv a_i(m)$ és $x \equiv b_j(n)$.
    (b) Mutassuk meg, hogy az így kapott x relatív prím mn-hez.
    (c) Bizonyítsuk be, hogy ha m és n relatív prímek, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.