6. Számelemélet gyakorlat (2009/2010)

1. $o_{77}(155) = 1$, mert $155 \equiv 1 \ (77)$.

$o_{100}(199) = 2$, mert $199 \equiv -1 \ (100)$.

$o_{65}(2) = 12$, mert $2^6 = 64 \equiv -1 \ (65)$ és így $2^{12} \equiv 1 \ (65)$. Kisebb rend nem jöhet szóba, mert a rend osztója 12-nek.

$o_{47}(43) = 46$, mert $\varphi(47) = 46$, ezért a lehetséges rendek $1, 2, 23, 46$. $43^2 \equiv (-4)^2 = 16 \not\equiv 1 \ (47)$, $(-4)^5 = -1024 \equiv -37 \equiv 10 \ (47)$, amiből $(-4)^{23} = ((-4)^5)^4(-4)^3 \equiv 10000 \cdot (-64) \equiv (-11)30 \not\equiv -330 \equiv -1 \ (47)$.

2. Legyen p prím és $o_p(a) = 3$.

(a) $a^3 \equiv 1 \ (p)$, vagyis $p \mid a^3 - 1 = (a-1)(a^2+a+1)$, de $p \nmid a - 1$, mert akkor 1 lenne a rendje, ezért $p \mid 1 + a + a^2$.

(b) $(1+a)^2 = 1 + 2a + a^2 \equiv a \ (p)$ az (a) rész miatt és persze $a \not\equiv 1 \ (p)$. Mivel $a^3 \equiv 1 \ (p)$, ezért $o_p(1+a) \mid 6$, tehát $o_p(1+a)$ még lehet 3 vagy 6. $(1+a)^3 \equiv a(1+a) = a+a^2 \equiv -1 \ (p)$ az (a) rész miatt és $-1 \not\equiv 1 \ (p)$, mert akkor $p = 2$ lenne, de akkor nem lenne 3 rendű elem.

3.

4.

5. A 2 primitív gyök mod 13.

(a) $3x^5 \equiv 2 \ (13)$, $\mathrm{ind}3 + 5 \cdot \mathrm{ind}x \equiv \mathrm{ind}2 \ (\varphi(13) = 12)$, $4 + 5 \cdot \mathrm{ind}x \equiv 1 \ (12)$, $5 \cdot \mathrm{ind}x \equiv -3 \equiv -15 \ (12)$, $\mathrm{ind}x \equiv -3 \equiv 9 \ (12)$, amiből $x \equiv 5 \ (13)$.

(c) $4x^7 + 7x^4 \equiv 0 \ (13)$. Az $x \equiv 0 \ (13)$ megoldás. Ha $13 \nmid x$, akkor $4x^3 \equiv -7 \equiv 6 \ (13)$, $\mathrm{ind}4 + 3 \cdot \mathrm{ind}x \equiv \mathrm{ind}6 \ (12)$, $2 + 3 \cdot \mathrm{ind}x \equiv 5 \ (12)$, $3 \cdot \mathrm{ind}x \equiv 3 \ (12)$, $\mathrm{ind}x \equiv 1 \ (4)$, tehát $\mathrm{ind}x \equiv 1, 5, 9 \ (12)$, amiből $x \equiv 2, 6, 5 \ (13)$.

6.