2. Számelmélet gyakorlat (2009/2010)

Néhány megoldás

1. Euklideszi Algoritmussal: $1521 = 4 \cdot 372 + 33$, $372 = 11 \cdot 33 + 9$, $33 = 3 \cdot 9 + 6$, $9 = 1 \cdot 6 + \boxed{3}$, $6 = 2 \cdot 3 + 0$. Az $1521x + 372y = (1521, 372)$ diofantikus egyenlet egy megoldását leolvashatjuk az EA lépéseiből a maradékok kifejezésével: Legyen $a = 1521$ és $b = 372$. Ekkor $33 = a - 4b$, $9 = b - 11 \cdot 33 = b - 11(a - 4b) = -11a + 45b$, $6 = 33 - 3 \cdot 9 = (a - 4b) - 3(-11a + 45b) = 34a - 139b$, és végül $3 = 9 - 1 \cdot 6 = (-11a + 45b) - (34a - 139b) = -45a + 184b = 1521(-45) + 372 \cdot 184$, vagyis $x = -45$, $y = 184$.

2. Szerepelt előadáson.

3. Legyen $(a, b) = 5$ és $d = (a+b, a-b)$. Ekkor nyilván $5 \mid d$ és $d \mid (a+b)+(a-b) = 2a$, $d \mid (a + b) - (a - b) = 2b$, amiből $d \mid (2a, 2b) = 2(a, b) = 10$. Tehát $d = 5$ vagy $d = 10$. Mindkettő lehet, mert például $a = 5$, $b = 10$ esetén $d = 5$, és $a = 15$, $b = 25$ esetén $d = 10$.

$(a + 2b, 4a - b)$ vizsgálata teljesen hasonló.

4. (a): $n^3 - n + 3 = (n - 1)n(n + 1) + 3$ így osztható 3-mal, tehát, ha prím, akkor csak ± 3 lehet, amiből $n = -2, -1, 0, 1$.

(b): Ha $n^3 - 27 = (n - 3)(n^2 + 3n + 9)$ prím, akkor valamelyik tényező ± 1. A második tényező nem lehet ± 1 egész n esetén. Ha az első 1, akkor $n = 4$ és a második tényező 37, prím. Ha az első tényező -1, akkor $n = 2$ és a második tényező 19, prím.

(c): $n^8 + n^7 + \cdots + n + 1 = n^6(n^2 + n + 1) + n^3(n^2 + n + 1) + (n^2 + n + 1) = (n^6 + n^3 + 1)(n^2 + n + 1)$ nem lehet prím, mert egyik tényező sem lehet -1, ha pedig valamelyik 1, akkor a másik is 1.

5. Világos, hogy $a^{(n,k)} - 1 \mid d = (a^n - 1, a^k - 1)$. Legyenek $x, y \in \mathbb{Z}$ egész számok, melyekre $nx + ky = (n, k)$. Mivel $n, k > 0$, ezért x és y előjele különböző. Áttérve $x' = x$ és $y' = -y$-ra azonos előjelű megoldását kapjuk az $nx' - ky' = (n, k)$ egyenletnek. Feltehető, hogy $x', y' > 0$, mert minden m-re $x' + mk$ és $y' + mn$ is megoldás. Ekkor

$$(a^{nx'} - 1) - (a^{ky'} - 1) = a^{nx'} - a^{ky'} = a^{ky'}(a^{nx'-ky'} - 1) = a^{ky'}(a^{(n,k)} - 1).$$

Mivel $d \mid a^{nx'} - 1 (= (a^n - 1)((a^n)^{x'-1} + \cdots + a^n + 1))$, $d \mid a^{ky'} - 1$, és nyilván $(d, a^{ky'}) = 1$, ezért $d \mid a^{(n,k)} - 1$, vagyis $d = a^{(n,k)} - 1$.