# Exam 1

**1)** [15 points] Use the *Extended Euclidean Algorithm* to write the GCD of 235 and 185 as a linear combination of themselves. *Show the computations explicitly!* [**Hint:** You should get 5 for the GCD!]

*Solution.* We have:

$$\begin{aligned} 235 &= 185 \cdot 1 + 50 \\ 185 &= 50 \cdot 3 + 35 \\ 50 &= 35 \cdot 1 + 15 \\ 35 &= 15 \cdot 2 + 5 \\ 15 &= 5 \cdot 3 + 0, \end{aligned}$$

So, the GCD is 5.
Now:

$$\begin{aligned} 5 &= 35 + (-2) \cdot 15 \\ &= 35 + (-2) \cdot (50 - 35) \\ &= (-2) \cdot 50 + 3 \cdot 35 \\ &= (-2) \cdot 50 + 3 \cdot (185 - 3 \cdot 50) \\ &= 3 \cdot 185 + (-11) \cdot 50 \\ &= 3 \cdot 185 + (-11) \cdot (235 - 185) \\ &= (-11) \cdot 235 + 14 \cdot 185. \end{aligned}$$

□

**2)** [15 points] If $a$ and $b$ are positive integers such that $ab = 3321$ and $\gcd(a, b) = 3$, then what is $\operatorname{lcm}(a, b)$?

*Solution.* $\operatorname{lcm}(a, b) = ab / \gcd(a, b) = 3321/3 = 1107$. □

**3)** [15 points] Let $a$ and $b$ be positive integers with $(a, b) = d$. Prove that $(a/d, b/d) = 1$.

*Proof.* By Theorem 1.35 [which I called *Bezout's Theorem*], we have that there are $r, s \in \mathbb{Z}$ such that

$$ra + bs = d.$$

Dividing this equation by $d$, we have:

$$r\left(\frac{a}{d}\right) + s\left(\frac{b}{d}\right) = 1.$$

By Problem 1.56 [done in class], this implies that $(a/d, b/d) = 1$. □

**4)** [20 points] Find the remainder of $10001 \cdot 674378^{584} - 3728382$ when divided by 5. *Show your computations explicitly!*

*Solution.* First, remember that if $a = d_k d_{k-1} \cdots d_0$ [$d_i$'s the digits of $a$], then $a \equiv d_0 \pmod 5$. We first deal with the power: $674378 \equiv 3 \pmod 5$. Now we find the exponent in base 5:

$$\begin{aligned} 584 &= 5 \cdot 116 + 4 \\ 116 &= 5 \cdot 23 + 1 \\ 23 &= 5 \cdot 4 + 3 \\ 4 &= 5 \cdot 0 + 4 \end{aligned}$$

So, $584 = (4314)_5$, and $674378^{584} \equiv 3^{4+3+1+4} = 3^{12} = 3^{2+2\cdot 5} \equiv 3^{2+2} = 81 \equiv 1 \pmod 5$. So:

$$\begin{aligned} 10001 \cdot 674378^{584} - 3728382 &\equiv 10001 \cdot 2 - 3728382 \\ &\equiv 1 \cdot 1 - 2 \\ &\equiv -1 \equiv 4 \pmod 5. \end{aligned}$$

Hence, the remainder is 4. □

**5)** [20 points] Give the set of all integer solutions of the system

$$\begin{aligned} x &\equiv 4 \pmod{15}, \\ 3x &\equiv 11 \pmod{14}. \end{aligned}$$

*Solution.* We do it by substitution. The first equation gives that $x = 15n + 4$ for some $n \in \mathbb{Z}$. Substituting in the second equation, we have

$$3 \cdot (4 + 15n) \equiv 11 \pmod{14} \quad \Rightarrow \quad 45n \equiv -1 \pmod{14} \quad \Rightarrow \quad 3n \equiv -1 \pmod{14}$$

Multiplying by 5, we get $n \equiv -5 \equiv 9 \pmod{14}$, so $n = 9 + 14k$ for some $k \in \mathbb{Z}$. Then, $x = 15 \cdot (9 + 14k) + 4 = 139 + 210k$, for $k \in \mathbb{Z}$. □

**6)** [15 points] Prove that 1234567 is not a perfect square.

*Proof.* We look modulo 4: $1234567 \equiv 67 \equiv 3 \pmod 4$. But the squares modulo 4 are 0 and 1 only [as $0^2 \equiv 0 \pmod 4$, $1^2 \equiv 1 \pmod 4$, $2^2 \equiv 0 \pmod 4$, and $3^2 \equiv 1 \pmod 4$], so 1234567 is not a perfect square. □