Exam 1

1) [15 points] Use the *Extended Euclidean Algorithm* to write the GCD of 186 and 69 as a linear combination of themselves. *Show the computations explicitly!* [**Hint:** You should get 3 for the GCD!]

Solution. We have:

$$\begin{aligned} 186 &= 69 \cdot 2 + 48 \\ 69 &= 48 \cdot 1 + 21 \\ 48 &= 2 \cdot 21 + 6 \\ 21 &= 6 \cdot 3 + 3 \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

So, $\gcd(186, 69) = 3$. Now:

$$\begin{aligned} 3 &= 1 \cdot 21 + (-3) \cdot 6 \\ &= 1 \cdot 21 + (-3) \cdot [48 + (-2) \cdot 21] \\ &= 7 \cdot 21 + (-3) \cdot 48 \\ &= 7 \cdot [68 + (-1) \cdot 48] + (-3) \cdot 48 \\ &= 7 \cdot 68 + (-10) \cdot 48 \\ &= 7 \cdot 68 + (-10) \cdot [186 + (-2) \cdot 69] \\ &= (-10) \cdot 186 + 27 \cdot 69, \end{aligned}$$

i.e.,

$$3 = (-10) \cdot 186 + 27 \cdot 69.$$

$\square$

2) [13 points] Compute the LCM of 186 and 69 [the same numbers above!].

Solution. We have the $\operatorname{lcm}(186, 69) = (186 \cdot 69)/\gcd(186, 69) = (186 \cdot 69)/3 = 62 \cdot 69 = 4278.$ $\square$

3) [15 points] Let $a, b, c \in \mathbb{Z}$. Let $a, b, c \in \mathbb{Z}$. Prove that if $a \mid b$, then $a \mid (b \cdot c)$. [This is as simple as it gets! Don't make it hard!]

Proof. By definition, if $a \mid b$, then there is $k \in \mathbb{Z}$ such that $b = a \cdot k$. So, $b \cdot c = (a \cdot k) \cdot c = a \cdot (k \cdot c)$. Since, $k \cdot c \in \mathbb{Z}$ [as $k, c \in \mathbb{Z}$], we have, by definition of divisibility, that $a \mid (b \cdot c)$. $\square$

4) [15 points] Find the remainder of the division of 674378^{584} when divided by 5. *Show your computations explicitly!*

Solution. Note that $674378 \equiv 3 \pmod 5$, so $674378^{584} \equiv 3^{584}$.

Now, we write 584 in base 5:

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

i.e., $584 = 4 \cdot 5^0 + 1 \cdot 5 + 3 \cdot 5^2 + 4 \cdot 5^3$. Hence, by *Femat's Little Theorem*:

$$674378^{584} \equiv 3^{584} \equiv 3^{4+1+3+4} = 3^{12} \pmod 5.$$

Now, $12 = 2 \cdot 5^0 + 2 \cdot 5^1$, and hence:

$$674378^{584} \equiv 3^{584} \equiv 3^{4+1+3+4} = 3^{12} \equiv 3^{2+2} = 3^4 = 81 \equiv 1 \pmod 5.$$

[Here is another way:

$$674378^{584} \equiv 3^{584} \equiv (3^2)^{292} = 9^{292} \equiv (-1)^{292} = 1 \pmod 5.]$$

$\square$

5) [12 points] Let $a = 2^5 \cdot 3^2 \cdot 11^4 \cdot 13$ and $b = 3^2 \cdot 5 \cdot 11^3$.

(a) Compute the prime factorization of $\gcd(a, b)$.

Solution.

$$\gcd(a, b) = 3^2 \cdot 11^3.$$

$\square$

(b) Compute the prime factorization of $\operatorname{lcm}(a, b)$.

Solution.

$$\operatorname{lcm}(a, b) = 2^5 \cdot 3^2 \cdot 5 \cdot 11^4 \cdot 13.$$

□

6) [15 points] Give the set of all solutions of the system

$$\begin{aligned} x &\equiv 4 \pmod{15} \\ x &\equiv 22 \pmod{33} \end{aligned}$$

[**Hint:** The system *does* have solution(s)!]

Solution. Note that $\gcd(15, 33) = 3$ and $3 \mid (4 - 22)$, so, indeed, the system has solution.

The first equation implies that $x = 15k + 4$ for some $k \in \mathbb{Z}$. Substituting in the second equation, we get $15k + 4 \equiv 22 \pmod{33}$, i.e.,

$$15k \equiv 18 \pmod{33}.$$

Dividing by 3 [i.e., $\gcd(15, 33)$] we get

$$5k \equiv 6 \pmod{11}.$$

Now, $1 = 11 + \boxed{-2} \cdot 5$, so multiplying by -2, we get

$$k \equiv -12 \equiv -1 \equiv 10 \pmod{11}.$$

Hence, $k = 11 \cdot l - 1$, for some $l \in \mathbb{Z}$, and thus $x = 165l - 11$ [or $k = 11 \cdot l + 10$ and $x = 165l + 154$]. □

7) [15 points] Prove that there are no integers x and y such that

$$x^2 + y^2 = 1{,}000{,}000{,}000{,}003.$$

[**Hint:** What happens modulo 4?]

Proof. If x and y are integers satisfying the equation, then

$$x^2 + y^2 \equiv 1{,}000{,}000{,}000{,}003 \equiv 3 \pmod{4}.$$

Now, modulo 4, we have that z is congruent to either 0, 1, 2 or 3, and hence z^2 is congruent to either 0 or 1 [as $4 \equiv 0 \pmod{4}$ and $9 \equiv 1 \pmod{4}$]. So, x^2 and y^2 are both also either 0 or 1, and hence the possible sums are 0, 1 or 2 modulo 4, but never 3 modulo 4. So, there can be no integers x and y such that

$$x^2 + y^2 \equiv 3 \pmod{4},$$

and hence there can be no integers x and y such that that

$$x^2 + y^2 = 1{,}000{,}000{,}000{,}003.$$

□