1) [20 points] Use the *Extended Euclidean Algorithm* to write the GCD of 117 and 69 as a linear combination of themselves. *Show work!*

[**Hint:** You should get 3 for the GCD!]

Solution. We have:

$$\begin{aligned}
117 &= 1 \cdot 117 + 0 \cdot 69 \\
69 &= 0 \cdot 117 + 1 \cdot 69 && \text{(mult. by } -1) \\
48 &= 1 \cdot 117 + -1 \cdot 69 && \text{(mult. by } -1) \\
21 &= -1 \cdot 117 + 2 \cdot 69 && \text{(mult. by } -2) \\
6 &= 3 \cdot 117 + -5 \cdot 69 && \text{(mult. by } -3) \\
3 &= -10 \cdot 117 + 17 \cdot 69
\end{aligned}$$

So, $\gcd(117, 69) = 3 = -10 \cdot 117 + 17 \cdot 69$.

□

2) [20 points] Express 2022 in base 7, i.e., write

$$2022 = \boxed{?} + \boxed{?} \cdot 7 + \boxed{?} \cdot 7^2 + \boxed{?} \cdot 7^3 + \cdots$$

with the blanks in $\{0, 1, 2, 3, 4, 5, 6\}$. *Show work!*

[**Note:** Trial and error is not acceptable here! You have to use some algorithm that always works, like the one I showed you in class.]

Solution. We have:

$$\begin{aligned}
2022 &= 7 \cdot 288 + 6 \\
288 &= 7 \cdot 41 + 1 \\
41 &= 7 \cdot 5 + 6 \\
5 &= 7 \cdot 0 + 5.
\end{aligned}$$

So,

$$2022 = 6 + 1 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^3.$$

□

3) [20 points] Prove the following statements using only the definition of divisibility.

[**Note:** These were given as exercises in class. These are short and simple!]

(a) Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Since $a \mid b$, we have that $b = a \cdot k$ for some $k \in \mathbb{Z}$, and since $b \mid c$, we have that $c = b \cdot l$, for some $l \in \mathbb{Z}$. Then,

$$c = b \cdot l = (a \cdot k) \cdot l = a \cdot (k \cdot l),$$

and since $k \cdot l \in \mathbb{Z}$, since $k, l \in \mathbb{Z}$, we have that $a \mid c$. □

(b) Prove that if $a \mid b$, then $a \mid -b$ and $-a \mid b$.

Proof. Since $a \mid b$, we have that $b = a \cdot k$ for some $k \in \mathbb{Z}$. Then, we have that $-b = (-k) \cdot a$ and $b = (-k) \cdot (-a)$. Since $-k \in \mathbb{Z}$, since $k \in \mathbb{Z}$, we have that $a \mid -b$ and $-a \mid b$. □

4) [20 points] Let $a, b, d \in Z$. Prove that if d is a common divisor of a and b, then $d \mid \gcd(a, b)$.

[**Note:** This was proved in class.]

Proof. Since d is a common divisor of a and b, we have that $a = a_1 d$ and $b = b_1 d$ for some $a_1, b_1 \in \mathbb{Z}$. By *Bezout's Lemma* there are $s, t \in \mathbb{Z}$ such that:

$$\gcd(a, b) = sa + tb = s(a_1 d) + t(b_1 d) = (sa_1 + tb_1)d.$$

Since $sa_1 + tb_1 \in \mathbb{Z}$, we have that $d \mid \gcd(a, b)$. □

5) [20 points] Let $r, r', m \in \mathbb{Z}$. Prove that if $\gcd(r, m) = \gcd(r', m) = 1$, then $\gcd(rr', m) = 1$.

[**Hint:** This was a HW problem.]

Proof. Suppose that p is a prime such that p divides both rr' and m. [This would mean that $p \mid (rr', m)$, and hence we need to get a contradiction.] Since p is prime, *Euclid's Lemma* tells us that either $p \mid r$ or $p \mid r'$. But that means that p is a common divisor of either r and m [as $p \mid m$ by assumption] or r' and m. But both are impossible as the respective GCDs are 1. Therefore, there is no prime common divisor of rr' and m. Thus $(rr', m) = 1$ [as if it was not one, this GCD would have a prime factor which would also be a common divisor.]

Alternative solution: By Bezout's Lemma, there are $s, t, s', t' \in \mathbb{Z}$ such that

$$1 = sr + tm, \qquad 1 = s'r' + t'm.$$

Multiplying these we get:

$$\begin{aligned} 1 &= ss'rr' + st'rm + s'tr'm + tt'm^2 \\ &= (ss')(rr') + (st'r + s'tr' + tt'm)m. \end{aligned}$$

By Problem 1.56 [done in class], we have that $(rr', m) = 1$. □