1) [25 points] Use the *Extended Euclidean Algorithm* to write the GCD of 69 and 48 as a linear combination of themselves. *Show work!*
[**Hint:** You should get 3 for the GCD!]

Solution. We have:

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

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

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

i.e.,

$$3 = 7 \cdot 69 + (-10) \cdot 48.$$

□

2) [15 points] Express 194 in base 3. *Show work!*

Solution. We have:

$$\begin{aligned} 194 &= 3 \cdot 64 + 2 \\ 64 &= 3 \cdot 21 + 1 \\ 21 &= 3 \cdot 7 + 0 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 3 \cdot 0 + 2. \end{aligned}$$

So, $194 = 2 + 1 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 = (21012)_3$. □

3) [30 points] Let $r, r', m \in \mathbb{Z} \setminus \{0\}$. Prove that if $(r, m) = (r', m) = 1$, then $(rr', m) = 1$.
[**Note:** 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.] $\square$

4) [30 points] Let $a, b, c \in \mathbb{Z} \setminus \{0\}$. Prove that if $a \mid bc$ and $d = (a, b)$, then $a \mid dc$.
[**Hint:** I shouldn't have to say this, but use *Bezout's Theorem.*]

Proof. By Bezout's Theorem, there are $r, s \in \mathbb{Z}$ such that:

$$d = ra + sb.$$

Also, since $a \mid bc$, there is $k \in \mathbb{Z}$ such that $bc = ak$. Then:

$$dc = c(ra + sb) = (cr)a + s(bc) = (cr)a + s(ak) = (cr + sk)a.$$

Since $cr + sk \in \mathbb{Z}$, we have that $a \mid dc$. $\square$