1) [20 points] Use the *Extended Euclidean Algorithm* to write the GCD of 78 and 44 as a linear combination of themselves. *Show work!*
[**Hint:** You should get 2 for the GCD!]

Solution. We have:

$$78 = 44 \cdot 1 + 34$$

$$44 = 34 \cdot 1 + 10$$

$$34 = 10 \cdot 3 + 4$$

$$10 = 4 \cdot 2 + 2$$

$$4 = 2 \cdot 2 + 0.$$

So,

$$\begin{aligned} 2 &= 10 + (-2) \cdot 4 \\ &= 10 + (-2) \cdot [34 + (-3) \cdot 10] \\ &= 7 \cdot 10 + (-2) \cdot 34 \\ &= 7 \cdot [44 + (-1)34] + (-2) \cdot 34 \\ &= 7 \cdot 44 + (-9) \cdot 34 \\ &= 7 \cdot 44 + (-9) \cdot [78 + (-1) \cdot 44] \\ &= 16 \cdot 44 + (-9) \cdot 78. \end{aligned}$$

□

2) [20 points] Express 355 in base 4. *Show work!*

Solution. We have:

$$355 = 4 \cdot 88 + 3$$

$$88 = 4 \cdot 22 + 0$$

$$22 = 4 \cdot 5 + 2$$

$$5 = 4 \cdot 1 + 1$$

$$1 = 4 \cdot 0 + 1.$$

So,

$$355 = 3 + 0 \cdot 4 + 2 \cdot 4^2 + 1 \cdot 4^3 + 1 \cdot 4^4.$$

$\square$

3) [20 points] Let $a, b \in \mathbb{Z} \setminus \{0\}$. Prove that $(a, b) \neq 1$ if and only if there is a prime p such that $p \mid a$ and $p \mid b$.

Proof. Suppose $(a, b) = d \neq 1$. So, $d \geq 2$ and hence it's either prime or a product of primes, and hence divisible by some prime p. Since $p \mid d$ and $d \mid a, b$, we have that $p \mid a, b$.

Conversely, suppose that $p \mid a, b$. Then, p is a common divisor greater than one, so $(a, b) > 1$. $\square$

4) [20 points] Let $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ with $a \mid c$, $b \mid d$ and $(c, d) = 1$. Prove that $(a, b) = 1$.

Proof. Suppose $e > 0$ with $e \mid a$ and $e \mid b$. Since $e \mid a$ and $a \mid c$, we have $e \mid c$. Similarly, since $e \mid b$ and $b \mid d$, we get $e \mid d$. So, $e > 0$ and $e \mid c, d$. Since $(c, d) = 1$, we have that $e = 1$. So, the only positive common divisor of a and b is 1, and hence $(a, b) = 1$.

[Alternatively, since $a \mid c$ and $b \mid d$, there are $k, l \in \mathbb{Z}$ such that $c = ak$, $d = bl$. Since $(c, d) = 1$, by Bezout's Theorem, there are $r, s \in \mathbb{Z}$ such that

$$rc + sd = 1 \quad \Rightarrow \quad rak + sbl = 1 \quad \Rightarrow \quad (rk)a + (sl)b = 1.$$

Since 1 is a linear combination of a and b, we have $(a, b) = 1$.]

$\square$

5) [20 points] Prove that if $(a, b) = d$, then $(a/d, b/d) = 1$.
[**Hint:** This was a HW problem.]

Proof. By Bezout's Theorem, we have:

$$ar + bs = d, \qquad \text{for some } r, s \in \mathbb{Z}.$$

Dividing by d we get:

$$\frac{a}{d}r + \frac{b}{d}s = 1.$$

[Note that $a/d, b/d \in \mathbb{Z}$, as d is a common divisor.] Then, since the linear combination gives 1, the GCD is 1 [we have the converse to Bezout's Theorem in this case]. So, $(a/d, b/d) = 1$. $\square$