1) [20 points] Use the *Extended Euclidean Algorithm* to write the GCD of 117 and 66 as a linear combination of themselves. *Show work!*

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

Solution. We have:

$$\begin{aligned} 117 &= 66 \cdot 1 + 51 \\ 66 &= 51 \cdot 1 + 15 \\ 51 &= 15 \cdot 3 + 6 \\ 15 &= 6 \cdot 2 + \boxed{3} \longleftarrow \text{GCD} \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

So,

$$\begin{aligned} 3 &= 15 + (-2) \cdot 6 \\ &= 15 + (-2) \cdot [51 + (-3) \cdot 15] \\ &= 7 \cdot 15 + (-2) \cdot 51 \\ &= 7 \cdot [66 + (-1) \cdot 51] + (-2) \cdot 51 \\ &= 7 \cdot 66 + (-9) \cdot 51 \\ &= 7 \cdot 66 + (-9) \cdot [117 + (-1) \cdot 66] \\ &= 16 \cdot 66 + (-9) \cdot 117. \end{aligned}$$

□

2) [20 points] Express 2020 in base 5, i.e., write

$$2020 = \boxed{?} + \boxed{?} \cdot 5 + \boxed{?} \cdot 5^2 + \boxed{?} \cdot 5^3 + \cdots$$

with the blanks in $\{0, 1, 2, 3, 4\}$. *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:

$$\begin{aligned} 2020 &= 5 \cdot 404 + 0 \\ 404 &= 5 \cdot 80 + 4 \\ 80 &= 5 \cdot 16 + 0 \\ 16 &= 5 \cdot 3 + 1 \\ 3 &= 5 \cdot 0 + 3. \end{aligned}$$

So,

$$2020 = 0 + 4 \cdot 5 + 0 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4.$$

□

3) [20 points] Prove that $\sqrt{6}$ is not a rational number, i.e., that $\sqrt{6}$ is not of the form a/b, with $a, b \in \mathbb{Z}_{>0}$.

[**Hint:** We've proved in class that $\sqrt{2}$ is not rational. This is *very* similar.]

Proof. Suppose $\sqrt{6} = a/b$, with $a, b \in \mathbb{Z}_{>0}$ and $\gcd(a, b) = 1$. Then, $\sqrt{6}\, b = a$, and so $6b^2 = a^2$. Therefore, since $2 \mid 6b^2$, we have that $2 \mid a^2$. Since 2 is prime, by Euclid's Lemma we have that $2 \mid a$. So, $a = 2a_1$, and then $6b^2 = (2a_1)^2 = 4a_1^2$. Then, $3b^2 = 2a_1^2$. So, $2 \mid 3b^2$ and since 2 is prime and $2 \nmid 3$ by Euclid's Lemma, we have that $2 \mid b^2$, and hence $2 \mid b$ [by Euclid's Lemma again]. But then $2 \mid a$ and $2 \mid b$, which is a contradiction as $\gcd(a, b) = 1$.

□

4) [20 points] Let $n \in \mathbb{Z}$ and suppose that $3 \nmid n$. Prove that $\gcd(n, n + 3) = 1$.

[**Note:** In the HW you've proved that for all $n \in \mathbb{Z}$, we have $\gcd(n, n + 1) = 1$. This is similar.]

Proof. Let $d = \gcd(n, n + 3)$. Then, $d \mid n$ and $d \mid (n + 3)$, and hence $d \mid (n + 3) - n = 3$, by the Basic Lemma. So either $d = 1$ or $d = 3$. If $d = 3$, then $d = 3 \mid n$, a contradiction, so $d = 1$. □

5) [20 points] Let a, b, and n be integers. [You may assume they are non-zero, if you wish.] Prove that if $a \mid n$, $b \mid n$, and $\gcd(a, b) = 1$, then $ab \mid n$.

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

Proof. Let $n = aa_1$ and $n = bb_1$, with $a_1, b_1 \in \mathbb{Z}$, since $a, b \mid n$. Now, by Bezout's Theorem, we have $1 = sa + tb$. Multiplying by n we have

$$n = san + tbn = sa(bb_1) + tb(aa_1) = ab(sb_1 + ta_1).$$

Since $sb_1 + ta_1 \in \mathbb{Z}$, as $\mathbb{Z}$ is closed under addition and multiplication, we have that $ab \mid n$. $\square$