1) [20 points] Use the *Extended Euclidean Algorithm* to write the GCD of 83 and 61 as a linear combination of themselves. *Show work!*

[**Hint:** You should get 1 for the GCD!]

Solution. We have:

$$\begin{array}{rcrcrcrcrl}
83 & = & 1 & \cdot & 83 & + & 0 & \cdot & 61 & \\
61 & = & 0 & \cdot & 83 & + & 1 & \cdot & 61 & \text{(mult. by } -1) \\
22 & = & 1 & \cdot & 83 & + & (-1) & \cdot & 61 & \text{(mult. by } -2) \\
17 & = & (-2) & \cdot & 83 & + & 3 & \cdot & 61 & \text{(mult. by } -1) \\
5 & = & 3 & \cdot & 83 & + & (-4) & \cdot & 61 & \text{(mult. by } -3) \\
2 & = & (-11) & \cdot & 83 & + & 15 & \cdot & 61 & \text{(mult. by } -2) \\
\boxed{1} & = & 25 & \cdot & 83 & + & (-34) & \cdot & 61 & \text{(mult. by } -2) \\
0 & & & & & & & & &
\end{array}$$

So, $\gcd(83, 61) = 1 = 25 \cdot 83 + (-34) \cdot 61.$ □

2) [20 points] Express 2023 in base 5, i.e., write

$$2023 = \boxed{?} + \boxed{?} \cdot 5 + \boxed{?} \cdot 5^2 + \boxed{?} \cdot 5^3 + \cdots$$

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:

$$\begin{aligned}
2023 &= 5 \cdot 404 + 3 \\
404 &= 5 \cdot 80 + 4 \\
80 &= 5 \cdot 16 + +0 \\
16 &= 5 \cdot 3 + 1 \\
3 &= 5 \cdot 0 + 3.
\end{aligned}$$

So,

$$2023 = \boxed{3} + \boxed{4} \cdot 5 + \boxed{0} \cdot 5^2 + \boxed{1} \cdot 5^3 + \boxed{3} \cdot 5^4.$$

□

3) Prove that for all positive integers n, we have $\gcd(n, n+2)$ is either 1 or 2.

Proof. Let $d \stackrel{\text{def}}{=} \gcd(n, n+2)$. Then, $d \mid (n+2) - n = 2$. So, since $d > 0$, we must have that $d = 1$ or $d = 2$. $\square$

4) [20 points] Let $a, b \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$, then $\gcd(a, b^2) = 1$.

Proof. By *Bezout's Lemma*, we have that there are $u, v \in \mathbb{Z}$ such that $1 = au + bv$. Squaring this expression, we obtain

$$1 = a^2u^2 + 2abuv + b^2v^2 = a \cdot (au^2 + 2buv) + b^2 \cdot v^2.$$

Since $au^2 + 2buv, v^2 \in \mathbb{Z}$, we have that 1 is an (integral) linear combination of a and b^2, and thus $\gcd(a, b^2) \mid 1$, and hence $\gcd(a, b^2) = 1$.

Alternative proof: Let $d > 1$ such that $d \mid a, b^2$. [We need to derive a contradiction.] Then there is p prime such that $p \mid d$, and hence $p \mid a, b^2$. By *Euclid's Lemma* we have that $p \mid b$. Hence, we have that $p \mid a, b$ and so $1 < p \leq \gcd(a, b) = 1$, a contradiction. $\square$

5) [20 points] Prove that if $\gcd(a, b) = 1$, $a \mid c$, and $b \mid c$, then $ab \mid c$.

[**Hint:** This was a HW problem. *Carefully state any previous result you use!*]

Proof. We have that $n = aa_1$ [as $a \mid n$]. Since $b \mid n$, we have that $b \mid aa_1$, and by Corollary 1.40, we have that $b \mid a_1$, i.e., $a_1 = a_2b$. Thus, $n = aba_2$, and therefore $ab \mid n$.

Alternative proof: Since $a \mid c$ and $b \mid c$, we can write, $c = a_1a = b_1b$ for some $a_1, b_1 \in \mathbb{Z}$. By *Bezout's Lemma*, there are $u, v \in \mathbb{Z}$ such that $1 = ua + vb$. Multiplying by c we have $c = uac + vbc = ua(bb_1) + vb(aa_1) = ab(ub_1 + va_1)$. Since $ub_1 + va_1 \in \mathbb{Z}$ (as $u, v, a_1, b_1 \in \mathbb{Z}$), we have that $ab \mid c$.

$\square$