Topics: Divisibility, abelian groups.

2.1. Note that the statement of Bézout's Lemma (Proposition 1.7) does not mention uniqueness of solutions. There's an excellent reason for this, as we are about to discover.

Suppose $a, b \in \mathbf{Z}_{\geqslant 1}$ are coprime, that is $\gcd(a, b) = 1$. Let $d \in \mathbf{Z}$.

(a) Suppose $(x_1, y_1), (x_2, y_2) \in \mathbf{Z}^2$ are two solutions of the equation $ax + by = d$.
Prove that there exists $k \in \mathbf{Z}$ such that $x_1 - x_2 = kb$ and $y_1 - y_2 = -ka$.

(b) Prove that if $(x, y) \in \mathbf{Z}^2$ is a solution of $ax + by = d$, then the solution set of this equation is

$$S = \{(x + kb, y - ka) \in \mathbf{Z}^2 : \ k \in \mathbf{Z}\}.$$

2.2. For integer n find all the possible values of:

(a) $\gcd(n, 12)$,

(b) $\gcd(n, n + 1)$,

(c) $\gcd(n, n + 6)$,

(d) $\gcd(2n + 3, 7n + 6)$,

(e) $\gcd(n^2, n + 1)$.

2.3. Prove the following generalisation of Proposition 1.8:
If $a, b, c \in \mathbf{Z}_{\geqslant 1}$ are such that $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

2.4 (GCD properties)**.** Prove that for any integers m and n we have

(a) $\gcd(2m, 2n) = 2\gcd(m, n)$;

(b) $\gcd(2m + 1, 2n) = \gcd(2m + 1, n)$;

(c) $\gcd(m, n) = \gcd(m, m - n)$;

(d) $\gcd(2m + 1, 2n + 1) = \gcd(2m + 1, m - n)$.

2.5 (Binary GCD Algorithm)**.**

(a) Using 2.4, construct a recursive algorithm for finding $\gcd(a, b)$ for all positive integers a and b as follows: set $(a_0, b_0) = (a, b)$, then for any $n \geqslant 0$:

i. If a_n and b_n are both even then define $(a_{n+1}, b_{n+1}) =$
ii. If a_n is odd and b_n is even then define $(a_{n+1}, b_{n+1}) =$
iii. If b_n is odd and a_n is even then define $(a_{n+1}, b_{n+1}) =$
iv. If a_n and b_n are both odd then define $(a_{n+1}, b_{n+1}) =$

Complete the above definitions. When should the algorithm stop and what should it return?

(b) Using part (a), find $\gcd\left(2^{2^k} + 1, 2^{2^\ell} + 1\right)$ for positive integers $k \neq \ell$.

2.6.

(a) Use the Principle of (Strong) Mathematical Induction to prove that: Every integer $n > 1$ can be written as a product of finitely many prime numbers.

(b) Show that part (a) implies the existence part of the Fundamental Theorem of Arithmetic (Theorem 1.10).

2.7.

(a) Find the order of each element in the group $\mathbf{Z}/10\mathbf{Z}$.

(b) Find the order of each element in the group $(\mathbf{Z}/10\mathbf{Z})^\times$.

(c) Find all the elements of order 5 in the group $\mathbf{C}^\times$.

(d) Give an example of an element of infinite order in the group $\mathbf{C}^\times$.

(e) Give an example of an element of infinite order in the group $\mathbf{S}^1$.

2.8. Let $G = \mathbf{Z}$ with the usual addition.

(a) Prove that given any subgroup H of G, there exists an integer $m \geqslant 0$ such that $H = m\mathbf{Z}$.

(b) Let $a, b \in \mathbf{Z}_{\geqslant 1}$ and let $H = \langle a, b \rangle$. Prove that in this setting, the integer m from part (a) is $\mathsf{gcd}\,(a, b)$.

2.9. Let G be an abelian group (denoted additively) and let $a, b \in G$ be elements of finite orders m, n. Let $k = \mathsf{lcm}\,(m, n)$.

(a) Prove that the order of $a + b$ divides k.

(b) Prove that if $\mathsf{gcd}\,(m, n) = 1$, then the order of $a + b$ is $k = \mathsf{lcm}\,(m, n) = mn$.

(c) Give an example where the order of $a + b$ is strictly less than k.

(d) Show that there exists some element $c \in G$ of order k.