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

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

Solution.

(a) We have $ax_1 + by_1 = ax_2 + by_2$, so $a(x_1 - x_2) = b(y_2 - y_1)$. Since $\gcd(a, b) = 1$, this forces $x_1 - x_2$ to be a multiple of b, and $y_2 - y_1$ to be a multiple of a. So $x_1 - x_2 = kb$ for some $k \in \mathbf{Z}$ and $y_2 - y_1 = ja$ for some $j \in \mathbf{Z}$. But then $akb = bja$, so that $k = j$.

(b) From part (a) we know that any solution of $ax + by = d$ is in the set S. Conversely, let $k \in \mathbf{Z}$, then

$$a(x + kb) + b(y - ka) = ax + akb + by - bka = ax + by = d. \qquad \square$$

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

Solution.

(a) $1, 2, 3, 4, 6, 12$

(b) 1

(c) $1, 2, 3, 6$

(d) Since

$$7n + 6 = 3(2n + 3) + n - 3$$

we have

$$\gcd(2n + 3, 7n + 6) = \gcd(2n + 3, n - 3).$$

Since $2n + 3 = 2(n - 3) + 9$ we have

$$\gcd(2n + 3, n - 3) = \gcd(n - 3, 9)$$

hence the possible values of $\gcd(2n + 3, 7n + 6)$ are $1, 3, 9$.

(e) 1. $\square$

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 $c \mid b$.

Solution. We adapt the argument from Proposition 1.8.

By Bézout's Lemma, since $\gcd(a, c) = 1$ there exist $u, v \in \mathbf{Z}$ such that $ua + vc = 1$. Multiply this by b to get $uab + vcb = b$. Now $c \mid ab$ hence $c \mid uab$, and clearly $c \mid vcb$, so $c \mid uab + vcb = b$. □

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

Solution.

(a) Let $g = \gcd(m, n)$, $g' = \gcd(2m, 2n)$. By Bézout's Lemma there exist $x, y \in \mathbf{Z}$ such that $mx + ny = g$, hence $(2m)x + (2n)y = 2g$, so that applying Bézout's Lemma once more we get that $g' \mid 2g$.

Similary, there exist $u, v \in \mathbf{Z}$ such that $(2m)u + (2n)v = g'$, so $g' = 2d$ for some $d \in \mathbf{Z}$. But then $mu + nv = d$, hence $g \mid d$, so $2g \mid 2d = g'$. We conclude that $g' = 2g$.

(b) Let $g' = \gcd(2m + 1, 2n)$ and $g = \gcd(2m + 1, n)$.

It is clear that $g \mid g'$.

Now $g' \mid 2m + 1$, which is odd, so g' itself is odd, $\gcd(g', 2) = 1$. Also $g' \mid 2n$, so by 2.3 we have $g' \mid n$, so g' is a common divisor of $2m + 1$ and n, hence $g' \mid g$.

We conclude that $g' = g$.

(c) We check that the set of common divisors of m and n is equal to the set of common divisors of m and $m - n$.

If $d \mid m$ and $d \mid n$ then $d \mid m - n$.

Conversely, if $d \mid m$ and $d \mid m - n$ then $d \mid m - (m - n) = n$.

(d) Follows from (b) and (c):

$$\begin{aligned}\gcd(2m + 1, 2n + 1) &= \gcd(2m + 1, 2m + 1 - 2n - 1)\\ &= \gcd(2m + 1, 2m - 2n)\\ &= \gcd(2m + 1, m - n).\end{aligned}$$

□

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 $k \neq \ell$.

Solution.

(a)

i. If both a_n, b_n are even then define $(a_{n+1}, b_{n+1}) = (a_n/2, b_n/2)$
ii. If a_n is odd and b_n is even then define $(a_{n+1}, b_{n+1}) = (a_n, b_n/2)$
iii. If b_n is odd and a_n is even then define $(a_{n+1}, b_{n+1}) = (a_n/2, b_n)$
iv. If both a_n and b_n are odd then define $(a_{n+1}, b_{n+1}) = (a_n, (a_n - b_n)/2)$

and terminate the algorithm once $a_n \mid b_n$ or $b_n \mid a_n$, keeping a counter c of how many times the first rule was applied. In the first case, return $2^c a_n$ and in the second case, return $2^c b_n$.

(b) WLOG $k > \ell$, otherwise swap them. Set $(a_0, b_0) = (2^{2^k}+1, 2^{2^\ell}+1)$ and apply the above algorithm.

By (iv), we have

$$\gcd(a_0, b_0) = \gcd(2^{2^k}+1, 2^{2^k-1} - 2^{2^\ell-1}).$$

Applying (ii) $2^{2^\ell-1}$-times results in

$$\gcd(a_0, b_0) = \gcd(2^{2^k}+1, 2^{2^k-2^\ell} - 1).$$

Apply (iv) to get

$$\gcd(a_0, b_0) = \gcd(2^{2^k}+1, 2^{2^k-1} - 2^{2^k-2^\ell-1} + 1).$$

Apply (iv) again to get

$$\gcd(a_0, b_0) = \gcd(2^{2^k}+1, 2^{2^k-1} - 2^{2^k-2^\ell-1}).$$

Apply (ii) $2^{2^k-2^\ell-1}$-times to get

$$\gcd(a_0, b_0) = \gcd(2^{2^k}+1, 2^{2^\ell} - 1).$$

Note that, since we have never applied (i), we have shown:

$$\gcd(2^{2^k}+1, 2^{2^\ell}+1) = \gcd(2^{2^k}+1, 2^{2^\ell} - 1).$$

Let

$$d \mid \gcd(2^{2^k}+1, 2^{2^\ell}+1).$$

The above implies

$$d \mid \gcd(2^{2^k}+1, 2^{2^\ell} - 1).$$

In particular

$$d \mid 2^{2^\ell}+1 \quad \text{and} \quad d \mid 2^{2^\ell} - 1.$$

Since $2^{2^\ell}+1 = (2^{2^\ell}-1)+2$ this is only possible if $d = 1$ or $d = 2$. Since $2^{2^\ell}+1$ is odd, $d = 2$ is impossible. Hence $d = 1$. This implies

$$\gcd(2^{2^k}+1, 2^{2^\ell}+1) = 1. \qquad \square$$

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).

Solution.

(a) We proceed by induction on $n > 1$.

Base case: $n = 2$ is a prime number.

Induction step: let $n > 1$ be arbitrary but fixed and suppose that every $k \leqslant n$ factors into a product of primes. Consider the integer $n + 1$. If it is prime, we are done. Otherwise it must have some divisor $a \notin \{1, n+1\}$. Write $n+1 = ab$, then both a and b are $\leqslant n$. By the induction hypothesis, both a and b factor into products of primes, and therefore so does $n + 1$.

(b) The existence part of the Fundamental Theorem of Arithmetic follows directly: if $n > 1$ then n can be written as a product of finitely many prime numbers. Order these in non-decreasing order, so that

$$n = q_1 q_2 \dots q_t,$$

where q_i are prime and $q_i \leqslant q_{i+1}$ for all i. Now collect any of the prime factors that are equal to get

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

where p_i are prime, $p_i < p_{i+1}$ for all i, and $e_i \in \mathbf{Z}_{\geqslant 1}$. □

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 $\mathbf{S}^1$.

Solution.

(a) 0: 1; 1: 10; 2: 5; 3: 10; 4: 5; 5: 2; 6: 5; 7: 10; 8: 5; 9: 10.

(b) 1: 1; 3: 4; 7: 4; 9: 2.

(c) These are complex 5-th roots of unity, that is complex roots of $z^5 = 1$. Let $\zeta = e^{(2\pi i)/5}$, then they are $\{\zeta, \zeta^2, \zeta^3, \zeta^4\}$. (The other root is 1, which has order 1 in the group.)

(d) 2 has infinite order in $\mathbf{C}^\times$ because $2^n = 1$ has no solutions with $n \in \mathbf{Z}_{\geqslant 1}$.

(e) Choose $\theta \in (0, 2\pi)$ such that $\dfrac{\theta}{2\pi} \notin \mathbf{Q}$, then $z = e^{i\theta}$ has infinite order. □

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 $\gcd(a, b)$.

Solution.

(a) Let H be a subgroup of G. If $H = \{0\}$ then we can take $m = 0$ and we are done.

Otherwise, there exists $h \in H$ with $h \neq 0$. Then also $-h \in H$, since H is a subgroup. One of $\pm h$ is positive.

Therefore the set

$$S = \{h \in H : \ h > 0\}$$

is a nonempty subset of $\mathbf{N}$, hence by the Well-Ordering Principle it has a minimal element m.

I claim that $H = m\mathbf{Z}$. First, since $m \in H$ and H is a subgroup, $m\mathbf{Z} \subseteq H$. Suppose there exists $h \in H$ such that $h \notin m\mathbf{Z}$. WLOG h is positive (otherwise replace it with $-h$). By the Division Algorithm $h = qm + r$ with $0 \leqslant r < m$. But $r \neq 0$ since $h \notin m\mathbf{Z}$. On the hand, $r = h - qm \in H$ with $r < m$, contradicting the minimality of m.

(b) We want to prove that $\langle a, b \rangle = m\mathbf{Z}$, where $m = \gcd(a, b)$.

First note that $m \mid a$ so $a \in m\mathbf{Z}$, and $m \mid b$ so $b \in m\mathbf{Z}$. We conclude that $m\mathbf{Z}$ is a subgroup of $\mathbf{Z}$ that contains a and b, so $\langle a, b \rangle \subseteq m\mathbf{Z}$.

In the other direction, by Bézout's Lemma there exist $u, v \in \mathbf{Z}$ such that $m = ua + vb$. But $a \in \langle a, b \rangle$ so $ua \in \langle a, b \rangle$, and similarly $vb \in \langle a, b \rangle$, hence $m \in \langle a, b \rangle$. We conclude that $\langle a, b \rangle$ is a subgroup of $\mathbf{Z}$ that contains m, so $m\mathbf{Z} \subseteq \langle a, b \rangle$. □

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 $\gcd(m, n) = 1$, 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.

Solution.

(a) Write $k = sm = tn$, then

$$k(a + b) = ka + kb = sma + tnb = s(ma) + t(nb) = s \cdot 0 + t \cdot 0 = 0,$$

hence the order of $a + b$ is a divisor of k.

(b) Let ℓ be the order of $a + b$. We know from part (a) that $\ell \mid mn$. Since $\gcd(m, n) = 1$, we can write $\ell = \ell_1 \ell_2$ where $\ell_1 \mid m$ and $\ell_2 \mid n$. Write $m = \ell_1 m_1$, $n = \ell_2 n_2$.

Then from $\ell(a + b) = 0$ we get $\ell a = -\ell b$, so $\ell_1 \ell_2 a = -\ell_1 \ell_2 b$, so

$$0 = m\ell_2 a = m_1 \ell_1 \ell_2 a = -m_1 \ell_1 \ell_2 b = -m\ell_2 b.$$

We conclude that $m\ell_2 b = 0$, therefore $n \mid m\ell_2$ (since b has order n). But $\gcd(n, m) = 1$, so $n \mid \ell_2$, so $n = \ell_2$.

In a similar way we obtain that $m = \ell_1$, so $\ell = \ell_1 \ell_2 = mn$.

(c) Let $G = \mathbf{Z}/2\mathbf{Z}$, $a = b = 1$, then a and b each has order 2, but $a + b = 0$ has order $1 \neq 2 = \mathsf{lcm}\,(2, 2)$.

(d) If $k = 1$ then the neutral element $0 \in G$ has order k.

If $k \geqslant 2$, consider the prime factorisation

$$k = q_1^{e_1} \ldots q_r^{e_r}.$$

Fix $j \in \{1, \ldots, r\}$. Since $q_j \mid k = \mathsf{lcm}\,(m, n) \mid mn$, then q_j divides m or n. In fact, $q_j^{e_j}$ divides m or n. Hence an appropriate power c_j of a or b has order $q_j^{e_j}$. Letting $c = c_1 \ldots c_r$, part (b) gives us that c has order k. □