

3.2 The Greatest Common Divisor, Bézout, and the Euclidean Algorithm

Section 3.1 gave the constructed integers a relation $a \mid b$ and a division with remainder (Theorem 3.1.2). This section asks what two integers have in common. Here is a concrete version. A machine accepts only coins worth 12 and 42 units, and gives change in the same coins. Which amounts can be paid exactly? Paying x coins of the first kind and y of the second, with negative numbers for coins received as change, pays $12x + 42y$. So $42 - 3 \cdot 12 = 6$ can be paid, and hence every multiple of 6; and since 6 divides both 12 and 42, nothing else can. Why 6, and why exactly the multiples of 6? The answer is a theorem about every pair of integers, and its proof is the main move of this chapter.

3.2.1 Integer combinations

The amounts $12x + 42y$ form a set that deserves a name.

Definition 3.2.1. Integer Combinations

Let $a, b, n \in \mathbb{Z}$. The set of **integer combinations** of a and b is

$$a\mathbb{Z} + b\mathbb{Z} := \{ax + by : x, y \in \mathbb{Z}\},$$

and the set of **multiples** of n is $n\mathbb{Z} := \{kn : k \in \mathbb{Z}\}$.

So $n\mathbb{Z}$ is the set of $m \in \mathbb{Z}$ with $n \mid m$ (Sets, Relations, and Cardinality, Definition 2.2.1), and $a\mathbb{Z} + b\mathbb{Z}$ is written as one symbol: it is defined directly, not as a sum of two sets. Three closure properties hold for every $a, b \in \mathbb{Z}$. For $x, y, x', y', m \in \mathbb{Z}$, the ring laws of Theorem 2.3.1 and Proposition 2.3.2 (c) give

$$\begin{aligned}(ax + by) + (ax' + by') &= a(x + x') + b(y + y'), \\ -(ax + by) &= a(-x) + b(-y), \\ m(ax + by) &= a(mx) + b(my),\end{aligned}$$

so $a\mathbb{Z} + b\mathbb{Z}$ is closed under $+$, under $-$, and under multiplication by **any** integer. It contains $0 = a \cdot 0 + b \cdot 0$, $a = a \cdot 1 + b \cdot 0$ and $b = a \cdot 0 + b \cdot 1$. Taking $b = 0$ gives $n\mathbb{Z} + 0\mathbb{Z} = \{nx + 0y\} = \{xn : x \in \mathbb{Z}\} = n\mathbb{Z}$, by Proposition 2.3.2 (b) and (F6); so $n\mathbb{Z}$ has the same three properties.

Examples:

- $12\mathbb{Z} + 42\mathbb{Z}$ contains 12, 42, $30 = 42 - 12$ and $6 = 12 \cdot (-3) + 42 \cdot 1$, so it contains every multiple of 6, by the third closure property.
- $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$: it contains $1 = 2 \cdot (-1) + 3 \cdot 1$, and with it $m \cdot 1 = m$ for every $m \in \mathbb{Z}$.
- The degenerate case: $0\mathbb{Z} + 0\mathbb{Z} = \{0\}$ (the case $n = 0$ above, since $0\mathbb{Z} = \{k \cdot 0 : k \in \mathbb{Z}\} = \{0\}$ by Proposition 2.3.2 (b)). It is the only case in which $a\mathbb{Z} + b\mathbb{Z}$ has no positive element (if $a \neq 0$, one of $a, -a$ is a positive element, by Proposition 3.1.1 (h); likewise for b), and the theorem below must exclude it.

Non-example by minimal change. Allow only paying, with no change given: $\{12x + 42y : x, y \in \mathbb{N}\}$. It contains 12 and 42 and is closed under $+$, but not under $-$: it contains no negative integer, since $x, y \geq 0$ give $12x + 42y \geq 0$. Nor does it contain 6: a non-zero element has $x \geq 1$ or $y \geq 1$, so it is at least 12. The coefficients must range over all of $\mathbb{Z}$.

3.2.2 The greatest common divisor

An integer d is a **common divisor** of a and b if $d \mid a$ and $d \mid b$. Every pair has the common divisor 1 (Proposition 3.1.1 (a)). For the coins, 6 is a common divisor of 12 and 42, and the question was why it is the one that matters.

The greatest common divisor is the largest integer that divides both.

Definition 3.2.2. Greatest Common Divisor

Let $a, b \in \mathbb{Z}$. If $(a, b) \neq (0, 0)$, the **greatest common divisor** $\gcd(a, b)$ is the greatest element, for $\leq$, of the set of common divisors of a and b . We set $\gcd(0, 0) := 0$.

In words: among all integers dividing both a and b , take the largest. The definition says “the greatest element”, so it owes us a proof that there is one.

Well-definedness. Let $(a, b) \neq (0, 0)$, and let D be the set of common divisors of a and b . It is non-empty, since $1 \in D$. Say $a \neq 0$ (otherwise $b \neq 0$, and the same argument runs with b). By Proposition 3.1.1 (h), one of a , $-a$ is positive; call it c . Every $d \in D$ satisfies $d \leq c$: if $d > 0$, then $d \mid c$ by Proposition 3.1.1 (d), and $d \leq c$ by Proposition 3.1.1 (e); if $d \leq 0$, then $d \leq 0 < c$. So D is bounded above, and by Proposition 2.3.6 it has a greatest element. Since $1 \in D$, that element is at least 1. Hence $\gcd(a, b) \geq 1$ **whenever** $(a, b) \neq (0, 0)$, and $\gcd(a, b) = \gcd(b, a)$, since the condition “ $d \mid a$ and $d \mid b$ ” is symmetric in a and b .

Examples:

- $\gcd(4, 6) = 2$. A positive common divisor d satisfies $d \leq 4$, by Proposition 3.1.1 (e), and $d \geq 1$, so $d \in \{1, 2, 3, 4\}$ by discreteness (Theorem 2.3.4 (c)), as in the small-primes remark of Section 3.1. Now $4 \nmid 6$ and $3 \nmid 4$, because $6 = 1 \cdot 4 + 2$ and $4 = 1 \cdot 3 + 1$ have non-zero remainders (the divisibility test after Theorem 3.1.2), while 2 divides both. So the greatest common divisor is 2.
- $\gcd(-5, 5) = 5$: the common divisors of -5 and 5 are the divisors of 5 (Proposition 3.1.1 (d) and Proposition 2.3.2 (a)), and the greatest is 5, by Proposition 3.1.1 (e).
- $\gcd(1, b) = 1$ for every $b \in \mathbb{Z}$: a common divisor d divides 1, so $d = \pm 1$ (Proposition 3.1.1 (g)), and the greater is 1.

Why the convention for $(0, 0)$. Every integer divides 0, so 0 and 0 have no greatest common divisor for $\leq$, and some value has to be chosen. The value 0 is the one that keeps clauses (c) and (e) of the theorem below true for $(0, 0)$, as the remark after it shows. It also matches Sets, Relations, and Cardinality, Example (The supremum under divisibility is the least common multiple) of *Sets, Relations, and Cardinality*, Section 2.6, where 0 is the top of $(\mathbb{N}, \mid)$, divisible by everything.

Listing divisors one by one, as in the first example, is slow. The Euclidean algorithm below replaces the list by one division per step, and Bézout’s theorem is what makes it work.

3.2.3 Bézout’s theorem

Here is the answer to the coin question for every pair of integers: the payable amounts are exactly the multiples of the greatest common divisor, and the greatest common divisor is itself payable.

Theorem 3.2.1. Bézout's Theorem

Let $a, b \in \mathbb{Z}$, not both 0, and let $S := (a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{Z}_{>0}$.

- (a) S has a least element d , and $d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$.
- (b) $d \mid a$ and $d \mid b$.
- (c) Every common divisor of a and b divides d .
- (d) $d = \gcd(a, b)$. In particular, $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.
- (e) $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Try it first (ten minutes): for $a = 12$ and $b = 42$, list the positive numbers $12x + 42y$ you can reach. Which is the least, and why should the least one divide 12?

Idea. The obvious plan starts from the greatest common divisor and tries to write it as $ax + by$. It stalls: the definition of $\gcd(a, b)$ says nothing about combinations, so there is nothing to build x and y from. The attempt on 12 and 42 suggests starting at the other end. The positive combinations 12, 42, 30, 18, 6, ... have a least element, and it was found as a combination. Why should it divide 12? Divide 12 by it. The remainder is 12 minus a multiple of a combination, so it is again a combination, and it is smaller than the least positive one. So it cannot be positive: it is 0. Once the least positive combination d is known to divide a and b , the rest is bookkeeping: every common divisor divides the combination d , so none exceeds it.

Before reading on: where is the minimality of d used, and where its positivity?

Proof.

- (a) Suppose $a \neq 0$; if $a = 0$, then $b \neq 0$, and the argument is the same with b in place of a . Both $a = a \cdot 1 + b \cdot 0$ and $-a = a \cdot (-1) + b \cdot 0$ lie in $a\mathbb{Z} + b\mathbb{Z}$, and by Proposition 3.1.1 (h) one of them is positive. So $S \neq \emptyset$. Every element of S is positive, so 0 is a lower bound, and by Proposition 2.3.6 S has a least element d . Since $d \in a\mathbb{Z} + b\mathbb{Z}$, there are $x_0, y_0 \in \mathbb{Z}$ with $d = ax_0 + by_0$.

- (b) Since $d \in \mathbb{Z}_{>0}$, Theorem 3.1.2 (a) gives $q, r \in \mathbb{Z}$ with $a = qd + r$ and $0 \leq r < d$. Then

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0),$$

so $r \in a\mathbb{Z} + b\mathbb{Z}$. If $r > 0$, then $r \in S$ and $r < d$, contradicting the minimality of d . Hence $r = 0$, and $a = qd$, that is, $d \mid a$. Dividing b by d in the same way gives $d \mid b$.

- (c) Let $c \mid a$ and $c \mid b$. By Proposition 3.1.1 (c), $c \mid ax_0 + by_0 = d$.
- (d) By (b), d is a common divisor of a and b . Let c be any common divisor. If $c > 0$, then $c \mid d$ by (c), and $c \leq d$ by Proposition 3.1.1 (e), since $d > 0$. If $c \leq 0$, then $c \leq 0 < d$. So d is the greatest common divisor: $d = \gcd(a, b)$ by Definition 3.2.2, and $\gcd(a, b) = ax_0 + by_0$.
- (e) ($\supseteq$) Let $k \in \mathbb{Z}$. Then $kd = k(ax_0 + by_0) = a(kx_0) + b(ky_0) \in a\mathbb{Z} + b\mathbb{Z}$. ($\subseteq$) Let $x, y \in \mathbb{Z}$. By (b), $d \mid a$ and $d \mid b$, so $d \mid ax + by$ by Proposition 3.1.1 (c), that is, $ax + by \in d\mathbb{Z}$. This proves the theorem. ■

The answer to the prompt: the minimality of d is used once, in (b), to force the remainder r to be 0. The positivity of d is used twice: to divide by d at all (Theorem 3.1.2 needs a positive divisor), and in (d), where $c \leq d$ for positive c comes from Proposition 3.1.1 (e) and for the other c from $0 < d$. (The step $r \in S$ uses the positivity of r , not of d , which is why the case $r = 0$ is split off.)

The proof of (b) is the move this chapter is built on, and we give it a name: **least positive element, then divide**. Take the least positive element d of a set closed under integer combinations; divide any element of the set by d ; the remainder lies in the set and is smaller than d , so it is 0. Section 3.3 uses the move again for common multiples, and Section 3.4 for sets closed under subtraction.

For the coins, the theorem says: the payable amounts form $12\mathbb{Z} + 42\mathbb{Z} = d\mathbb{Z}$, where d is the least positive payable amount, and $d = \gcd(12, 42)$. The Try-it-first list finds $d = 6 = 12 \cdot (-3) + 42 \cdot 1$.

Remark. Clause (c) says that $\gcd(a, b)$ is greatest also for divisibility, not only for $\leq$. For $a, b \in \mathbb{N}$, not both 0, it is the infimum of $\{a, b\}$ in $(\mathbb{N}, |)$ (Sets, Relations, and Cardinality, Definition 2.6.5): it divides both, and every $c \in \mathbb{N}$ dividing both divides it. This is the mirror image of Sets, Relations, and Cardinality, Example (The supremum under divisibility is the least common multiple), where the supremum is the least common multiple. For general $a, b \in \mathbb{Z}$, let a' be the one of $a, -a$ that lies in $\mathbb{N}$, and likewise b' (Proposition 3.1.1 (h), with $a' = 0$ if $a = 0$). Since a and $-a$ have the same divisors (Proposition 3.1.1 (d) and Proposition 2.3.2 (a)), $\gcd(a, b) = \gcd(a', b')$. With the convention $\gcd(0, 0) = 0$, clauses (c) and (e) also hold for $(0, 0)$ when d is read as 0: every integer divides 0, and $0\mathbb{Z} + 0\mathbb{Z} = \{0\} = 0\mathbb{Z}$. So 0, the top of $(\mathbb{N}, |)$, is also the infimum of $\{0, 0\} = \{0\}$.

Pairs whose greatest common divisor is 1 get a name of their own.

Definition 3.2.3. Coprime Integers

Integers $a, b \in \mathbb{Z}$ are **coprime** if $\gcd(a, b) = 1$.

For instance, 2 and 3 are coprime, and so are 1 and any b ; but 4 and 6 are not, since $\gcd(4, 6) = 2$, and neither are 0 and 0, since $\gcd(0, 0) = 0$. For coprime integers, (d) of the theorem produces 1 as a combination, and conversely:

Corollary 3.2.2. Coprime Means 1 Is a Combination

Let $a, b \in \mathbb{Z}$. Then a and b are coprime if and only if $ax + by = 1$ for some $x, y \in \mathbb{Z}$.

Proof. ($\Rightarrow$) If $\gcd(a, b) = 1$, then $(a, b) \neq (0, 0)$, since $\gcd(0, 0) = 0 \neq 1$, and Theorem 3.2.1 (d) gives $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b) = 1$.

($\Leftarrow$) Let $ax + by = 1$. Then $(a, b) \neq (0, 0)$, since otherwise $ax + by = 0 \neq 1$. So $g := \gcd(a, b) \geq 1$, and g divides a and b , hence divides $ax + by = 1$ by Proposition 3.1.1 (c). By Proposition 3.1.1 (g), $g = 1$ or $g = -1$, and $g \geq 1$ rules out -1 . So $\gcd(a, b) = 1$. ■

The direction ($\Leftarrow$) is how coprimality is usually proved: exhibit one combination equal to 1. Thus $2 \cdot (-1) + 3 \cdot 1 = 1$ shows again that 2 and 3 are coprime, with no list of divisors.

3.2.4 The Euclidean algorithm

Bézout's theorem says that $\gcd(a, b)$ is a combination of a and b , but its proof finds it as a least element, which is no way to compute it. Computing needs a step that makes the numbers smaller without changing the set of combinations. Division with remainder is that step.

Lemma 3.2.3. One Step of the Euclidean Algorithm

Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$, and let $a = qb + r$ with $q, r \in \mathbb{Z}$. Then $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z}$, and hence $\gcd(a, b) = \gcd(b, r)$.

Proof. ($\subseteq$) For $x, y \in \mathbb{Z}$, $ax + by = (qb + r)x + by = b(qx + y) + rx \in b\mathbb{Z} + r\mathbb{Z}$. ($\supseteq$) For $x, y \in \mathbb{Z}$, $bx + ry = bx + (a - qb)y = ay + b(x - qy) \in a\mathbb{Z} + b\mathbb{Z}$. So the two sets are equal. Neither pair is $(0, 0)$, since $b \neq 0$. By Theorem 3.2.1 (a) and (d), $\gcd(a, b)$ is the least element of $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{Z}_{>0}$, and $\gcd(b, r)$ is the least element of $(b\mathbb{Z} + r\mathbb{Z}) \cap \mathbb{Z}_{>0}$, the same set. So $\gcd(a, b) = \gcd(b, r)$. ■

The lemma does not need r to be the remainder; any q will do. Choosing the remainder makes the new pair smaller, and repeating the step gives a sequence. To define “repeat” without “and so on”, we use the recursion theorem.

Theorem 3.2.4. The Euclidean Algorithm

Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$. Define $(x_k, y_k) \in \mathbb{Z} \times \mathbb{N}$ for $k \in \mathbb{N}$ by $(x_0, y_0) := (a, b)$ and

$$(x_{k+1}, y_{k+1}) := \begin{cases} (y_k, r_k) & \text{if } y_k > 0, \\ (x_k, y_k) & \text{if } y_k = 0, \end{cases}$$

where, when $y_k > 0$, r_k is the remainder of x_k on division by y_k . Then:

- (a) $x_k\mathbb{Z} + y_k\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ for every $k \in \mathbb{N}$;
- (b) there is a least $K \in \mathbb{N}$ with $y_K = 0$; moreover $K \geq 1$, and $y_{k+1} < y_k$ for every $k < K$;
- (c) $x_K = \gcd(a, b)$.

The sequence is well defined. Let $G: \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Z} \times \mathbb{N}$ send (x, y) to (y, r) , where r is the remainder of x on division by y , if $y > 0$, and to (x, y) if $y = 0$. This is a function: the remainder exists and is unique by Theorem 3.1.2 (a), and it lies in $\mathbb{N}$ because $r \geq 0$ (Theorem 2.3.4 (b)). The recursion theorem (Sets, Relations, and Cardinality, Theorem 2.3.1, read on $\mathbb{N} = \omega$ as Theorem 1.5.1 by Corollary 1.7.3 (b)), with $X = \mathbb{Z} \times \mathbb{N}$, starting value (a, b) and step $(k, (x, y)) \mapsto G(x, y)$, gives exactly one sequence with the two displayed properties.

Idea. Part (a) is Lemma 3.2.3, once per step, carried along by induction. For (b), the second entries are natural numbers that drop at each step while they are positive, and a set of natural numbers has a least element, which cannot be positive. For (c), at the first index K

with $y_K = 0$, the invariant (a) reads $a\mathbb{Z} + b\mathbb{Z} = x_K\mathbb{Z}$, and Bézout's theorem identifies the gcd as the least positive element of this set.

Proof.

- (a) We use Logic and Proof, Axiom 4.2.1 (through Corollary 1.7.3 (b)) on k , for $P(k)$: “ $x_k\mathbb{Z} + y_k\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ ”. The base case $P(0)$ holds since $(x_0, y_0) = (a, b)$. Suppose $P(k)$. If $y_k > 0$, then $x_k = q_k y_k + r_k$ for some $q_k \in \mathbb{Z}$, and Lemma 3.2.3 with x_k, y_k in place of a, b gives

$$x_{k+1}\mathbb{Z} + y_{k+1}\mathbb{Z} = y_k\mathbb{Z} + r_k\mathbb{Z} = x_k\mathbb{Z} + y_k\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}.$$

If $y_k = 0$, then $(x_{k+1}, y_{k+1}) = (x_k, y_k)$, and $P(k+1)$ is $P(k)$.

- (b) The set $Y := \{y_k : k \in \mathbb{N}\} \subseteq \mathbb{N}$ is non-empty and has the lower bound 0, so it has a least element y_m (Proposition 2.3.6). If $y_m > 0$, then $y_{m+1} = r_m < y_m$ by the definition of the step and Theorem 3.1.2 (a), contradicting the choice of y_m . So $y_m = 0$, and the set $\{k \in \mathbb{N} : y_k = 0\}$ is non-empty, with lower bound 0. Let K be its least element (Proposition 2.3.6). Then $K \neq 0$, since $y_0 = b > 0$; so $K \geq 1$. For $k < K$, $y_k \neq 0$ by the choice of K , so $y_k > 0$ (as $y_k \in \mathbb{N}$, Theorem 2.3.4 (b)), and $y_{k+1} = r_k < y_k$.
- (c) Since $K \geq 1$, $K-1 \in \mathbb{N}$ and $K-1 < K$, so $y_{K-1} > 0$ by (b), and the definition of the step gives $x_K = y_{K-1} > 0$. By (a) with $k = K$, and since $y_K = 0$,

$$a\mathbb{Z} + b\mathbb{Z} = x_K\mathbb{Z} + 0\mathbb{Z} = x_K\mathbb{Z}.$$

The least positive element of $x_K\mathbb{Z}$ is x_K : it lies in the set $(x_K = 1 \cdot x_K)$, and every positive element mx_K is divisible by x_K , so $x_K \leq mx_K$ by Proposition 3.1.1 (e). Since $b > 0$, $(a, b) \neq (0, 0)$, and by Theorem 3.2.1 (a) and (d), the least element of $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{Z}_{>0}$ is $\gcd(a, b)$. Hence $x_K = \gcd(a, b)$. ■

In practice the sequence is written as a chain of divisions, each dividing the previous divisor by the previous remainder, until a remainder is 0; then $x_K = y_{K-1}$, the last non-zero second entry, is the gcd. If $K \geq 2$, it is the last non-zero remainder r_{K-2} ; if $K = 1$, it is b , and then $b \mid a$. Exercise B3 shows that at most b divisions are needed.

To find coefficients x, y with $\gcd(a, b) = ax + by$, we run the identity of Lemma 3.2.3 backwards.

Algorithm. Back-substitution. Write out the divisions $x_k = q_k y_k + r_k$ for $k = 0, \dots, K-1$, so that $x_{k+1} = y_k$ and $y_{k+1} = r_k$. Start from $\gcd(a, b) = x_K = 1 \cdot x_K + 0 \cdot y_K$, a combination of the last pair. Then, for $k = K-1, K-2, \dots, 0$ in turn, rewrite a combination $ux_{k+1} + vy_{k+1} = uy_k + vr_k$ of the pair with index $k+1$ as one of the pair with index k , by substituting $r_k = x_k - q_k y_k$:

$$uy_k + v(x_k - q_k y_k) = vx_k + (u - q_k v)y_k,$$

the identity in the proof of Lemma 3.2.3. After $k = 0$, the combination is one of $x_0 = a$ and $y_0 = b$. Multiply it out to check it. (By hand, the step $k = K-1$ changes nothing, since $r_{K-1} = 0$; so one starts from the last division with a non-zero remainder, as in the example below.)

The procedure only computes; nothing rests on it. That some x, y exist is [Theorem 3.2.1](#) (d), and the final multiplication checks the particular x, y found.

Example. Two runs of the algorithm

Compute $\gcd(252, 198)$ and $\gcd(-35, 15)$, and write each as a combination of the two numbers.

Solution. The pair $(252, 198)$. The chain of divisions is

$$252 = 1 \cdot 198 + 54,$$

$$198 = 3 \cdot 54 + 36,$$

$$54 = 1 \cdot 36 + 18,$$

$$36 = 2 \cdot 18 + 0.$$

In the notation of the theorem, (x_k, y_k) runs through $(252, 198)$, $(198, 54)$, $(54, 36)$, $(36, 18)$, $(18, 0)$, so $K = 4$ and $\gcd(252, 198) = x_4 = 18$. Back-substitution, from the third division up:

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 = 54 - (198 - 3 \cdot 54) = 4 \cdot 54 - 198 \\ &= 4 \cdot (252 - 198) - 198 = 4 \cdot 252 - 5 \cdot 198. \end{aligned}$$

Check: $4 \cdot 252 = 1008$, $5 \cdot 198 = 990$, and $1008 - 990 = 18$.

The pair $(-35, 15)$. The first entry may be negative; only the second must be positive. The remainder of -35 on division by 15 is 10 , not -5 :

$$-35 = (-3) \cdot 15 + 10,$$

$$15 = 1 \cdot 10 + 5,$$

$$10 = 2 \cdot 5 + 0.$$

So $\gcd(-35, 15) = 5$, and

$$5 = 15 - 10 = 15 - (-35 + 3 \cdot 15) = (-1) \cdot (-35) + (-2) \cdot 15.$$

Check: $(-1) \cdot (-35) = 35$, $(-2) \cdot 15 = -30$, and $35 - 30 = 5$.

Warning. Bézout coefficients are **not** unique. From $18 = 4 \cdot 252 - 5 \cdot 198$ and $11 \cdot 252 = 2772 = 14 \cdot 198$,

$$18 = (4 - 11) \cdot 252 + (-5 + 14) \cdot 198 = (-7) \cdot 252 + 9 \cdot 198.$$

So “the” coefficients of $\gcd(a, b)$ means nothing by itself; when a computation needs particular ones, they are those produced by back-substitution, and any other pair works as well.

Quick check. Compute $\gcd(0, -6)$ and $\gcd(84, 35)$.

Solution. $\gcd(0, -6) = 6$. Every integer divides 0, so the common divisors of 0 and -6 are the divisors of -6 , which are those of 6 (Proposition 3.1.1 (d) and Proposition 2.3.2 (a)). The positive ones are at most 6 (Proposition 3.1.1 (e)), and 6 is one of them. (The theorem does not apply directly to $(0, -6)$, since its second entry is negative; it does apply to $(0, 6)$, with the one division $0 = 0 \cdot 6 + 0$.)

$\gcd(84, 35) = 7$, by the chain $84 = 2 \cdot 35 + 14$, $35 = 2 \cdot 14 + 7$, $14 = 2 \cdot 7 + 0$.

3.2.5 Exercises

3.2.5.1 A. Check your understanding

Exercise. A1

These questions are about the proof of [Theorem 3.2.1](#).

- (a) Where is the minimality of d used?
- (b) Run the proof on $(a, b) = (12, 42)$: find d , x_0 , y_0 , and the divisions of (b).
- (c) Which step fails for $(a, b) = (0, 0)$?
- (d) State the idea of the proof in two sentences.

Solution.

- (a) Once, in (b): the remainder r of a on division by d is a combination of a and b , and if it were positive it would be an element of S smaller than d . Minimality forces $r = 0$.
- (b) The set S contains $6 = 12 \cdot (-3) + 42 \cdot 1$. Every element of $12\mathbb{Z} + 42\mathbb{Z}$ is divisible by 6, since $6 \mid 12$ and $6 \mid 42$ (Proposition 3.1.1 (c)), so every element of S is at least 6 (Proposition 3.1.1 (e)). Hence $d = 6$, with $x_0 = -3$ and $y_0 = 1$. The divisions of (b) are $12 = 2 \cdot 6 + 0$ and $42 = 7 \cdot 6 + 0$: both remainders are 0, as the proof predicts.
- (c) Step (a): $0\mathbb{Z} + 0\mathbb{Z} = \{0\}$, so $S = \emptyset$, and Proposition 2.3.6 does not apply. There is no d to divide by.
- (d) Take the least positive integer combination d of a and b . Dividing a (or b) by d leaves a remainder that is again a combination and smaller than d , so it is 0; thus d is a common divisor, and since every common divisor divides the combination d , it is the greatest.

3.2.5.2 B. Practice

Exercise. B1

Run the Euclidean algorithm on $(1001, 357)$, and use back-substitution to write $\gcd(1001, 357)$ as $1001x + 357y$ with $x, y \in \mathbb{Z}$.

Solution. The chain of divisions is

$$1001 = 2 \cdot 357 + 287,$$

$$357 = 1 \cdot 287 + 70,$$

$$287 = 4 \cdot 70 + 7,$$

$$70 = 10 \cdot 7 + 0,$$

so $\gcd(1001, 357) = 7$ by [Theorem 3.2.4](#) (c). Back-substitution:

$$7 = 287 - 4 \cdot 70 = 287 - 4 \cdot (357 - 287) = 5 \cdot 287 - 4 \cdot 357$$

$$= 5 \cdot (1001 - 2 \cdot 357) - 4 \cdot 357 = 5 \cdot 1001 - 14 \cdot 357.$$

Check: $5 \cdot 1001 = 5005$, $14 \cdot 357 = 4998$, and $5005 - 4998 = 7$. Hence $x = 5$, $y = -14$ works.

Exercise. B2

Let $a, b \in \mathbb{Z}$. Prove that $\gcd(a, b) = \gcd(-a, b)$, and that $\gcd(a, 0) = a$ if $a \in \mathbb{Z}_{>0}$.

Solution. First claim. If $(a, b) = (0, 0)$, then also $(-a, b) = (0, 0)$, and both sides are 0 by convention. Otherwise $(-a, b) \neq (0, 0)$ as well, since $-a = 0$ would give $a = -(-a) = -0 = 0$ (Proposition 2.3.2 (a); $-0 = 0$ because $0 + 0 = 0$ and the inverse is unique). By Proposition 3.1.1 (d), $c \mid a$ implies $c \mid -a$, and $c \mid -a$ implies $c \mid -(-a) = a$ (Proposition 2.3.2 (a)). So a and $-a$ have the same divisors, the pairs (a, b) and $(-a, b)$ have the same common divisors, and the greatest is the same ([Definition 3.2.2](#)).

Second claim. Let $a > 0$. Every integer divides 0 (Proposition 3.1.1 (a)), so the common divisors of a and 0 are the divisors of a . Among them is a itself. A positive divisor c satisfies $c \leq a$ by Proposition 3.1.1 (e), and a non-positive one satisfies $c \leq 0 < a$. So a is the greatest, and $\gcd(a, 0) = a$.

Exercise. B3: The algorithm stops quickly

In the notation of [Theorem 3.2.4](#), prove that $y_k \leq b - k$ for every $k \in \mathbb{N}$ with $k \leq K$. Deduce that $K \leq b$: the algorithm stops after at most b divisions.

Solution. We use Logic and Proof, Axiom 4.2.1 (through Corollary 1.7.3 (b)) on k , for $P(k)$: “if $k \leq K$, then $y_k \leq b - k$ ”. The base case $P(0)$ is $y_0 = b = b - 0$. Suppose $P(k)$, and let $k + 1 \leq K$. Then $k < K$, so $k \leq K$ and $P(k)$ gives $y_k \leq b - k$. By [Theorem 3.2.4](#) (b), $y_{k+1} < y_k$, so $y_{k+1} + 1 \leq y_k$ by discreteness (Theorem 2.3.4 (c)), that is, $y_{k+1} \leq y_k - 1$. Hence $y_{k+1} \leq b - k - 1 = b - (k + 1)$, which is $P(k + 1)$.

With $k = K$: $0 = y_K \leq b - K$, so $K \leq b$. Each index $k < K$ is one division, so there are $K \leq b$ of them.

3.2.5.3 C. Going deeper

Exercise. C1: Exit check: Bézout

Let $a, b \in \mathbb{Z}$, not both 0, and let $S := (a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{Z}_{>0}$. Prove that S has a least element d ; that $d \mid a$ and $d \mid b$; that every common divisor of a and b divides d ; and that $d = \gcd(a, b)$.

Solution. S has a least element. Say $a \neq 0$ (otherwise exchange the roles of a and b). Both $a = a \cdot 1 + b \cdot 0$ and $-a = a \cdot (-1) + b \cdot 0$ are combinations of a and b , and one of them is positive (Proposition 3.1.1 (h)); so $S \neq \emptyset$. It is bounded below by 0, so it has a least element d (Proposition 2.3.6), and $d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$.

d divides a and b . Divide a by $d > 0$ (Theorem 3.1.2 (a)): $a = qd + r$ with $0 \leq r < d$. Then $r = a(1 - qx_0) + b(-qy_0)$ is a combination of a and b . If $r > 0$, then $r \in S$ and $r < d$, against the minimality of d . So $r = 0$ and $d \mid a$. The same argument with b gives $d \mid b$.

Common divisors divide d . If $c \mid a$ and $c \mid b$, then $c \mid ax_0 + by_0 = d$ (Proposition 3.1.1 (c)).

d is the gcd. d is a common divisor. A common divisor $c > 0$ divides $d > 0$, so $c \leq d$ (Proposition 3.1.1 (e)); a common divisor $c \leq 0$ satisfies $c < d$. So d is the greatest common divisor (Definition 3.2.2).

Marking scheme. (10 points) - 2: shows $S \neq \emptyset$, with a reason that covers $a < 0$ or $b < 0$ (for instance, one of $a, -a$ is a positive combination). - 1: obtains the least element by a cited well-ordering result for sets of integers bounded below. - 3: divides a by d and writes the remainder as a combination of a and b . - 2: uses the minimality of d to force the remainder to be 0, for a and for b . - 2: shows every common divisor divides d , and deduces that d is the greatest (with the case of non-positive divisors). Fatal errors (0 for the step): assuming that the gcd is a combination of a and b (circular); citing Theorem 3.2.4 (c) or the gcd clause of Lemma 3.2.3 (both are proved from Theorem 3.2.1, so this is circular); “ d divides a because d is the least positive combination”, with no division step. A second route goes through the Euclidean algorithm, with back-substitution, by induction on the number of steps. Citing Theorem 3.2.4 (a), (b) and the equality $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z}$ of Lemma 3.2.3 is allowed; if the invariant used is “the common divisors are unchanged”, it must be proved directly from $r = a - qb$. The invariant earns the 3 points for the division, and termination earns the 2 points for minimality. The answer must still identify the gcd with the least element d of S ($d \leq \gcd(a, b)$ since $\gcd(a, b) \in S$; $\gcd(a, b) \mid d$ since the gcd divides every combination). The rest is marked as written.

Exercise. C2: Scaling the gcd

Let $a, b \in \mathbb{Z}$ and $k \in \mathbb{Z}_{>0}$. Prove that $\gcd(ka, kb) = k \gcd(a, b)$.

Solution (Hint 1). Use the description of $a\mathbb{Z} + b\mathbb{Z}$ in Theorem 3.2.1 (e), and the description of the gcd as a least element in (a) and (d).

Solution (Hint 2). If $(a, b) \neq (0, 0)$ and $d := \gcd(a, b)$, first show $(ka)\mathbb{Z} + (kb)\mathbb{Z} = (kd)\mathbb{Z}$.

Solution. If $(a, b) = (0, 0)$, then $(ka, kb) = (0, 0)$ by Proposition 2.3.2 (b), and both sides are 0: $\gcd(0, 0) = 0 = k \cdot 0$.

Otherwise let $d := \gcd(a, b)$, so $d \geq 1$. Say $a \neq 0$ (otherwise $b \neq 0$; exchange the roles of a and b); then $ka \neq 0$, since $k \neq 0$ and $\mathbb{Z}$ has no zero divisors (Proposition 2.3.5 (f)). So $(ka, kb) \neq (0, 0)$, and Theorem 3.2.1 applies to both pairs.

The combinations. For $x, y \in \mathbb{Z}$, $(ka)x + (kb)y = k(ax + by)$. As x, y range over $\mathbb{Z}$, $ax + by$ ranges over $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ (Theorem 3.2.1 (e)), so

$$(ka)\mathbb{Z} + (kb)\mathbb{Z} = \{k(md) : m \in \mathbb{Z}\} = \{m(kd) : m \in \mathbb{Z}\} = (kd)\mathbb{Z}.$$

The least positive element. $kd > 0$ by (O4), and $kd = 1 \cdot kd \in (kd)\mathbb{Z}$. Every positive element $m(kd)$ of $(kd)\mathbb{Z}$ is divisible by kd , so $kd \leq m(kd)$ by Proposition 3.1.1 (e). So kd is the least element of $((ka)\mathbb{Z} + (kb)\mathbb{Z}) \cap \mathbb{Z}_{>0}$, and by Theorem 3.2.1 (a) and (d), $\gcd(ka, kb) = kd = k \gcd(a, b)$.

For instance, $\gcd(12, 42) = 6 \gcd(2, 7) = 6$, since 2 and 7 are coprime ($2 \cdot (-3) + 7 \cdot 1 = 1$, Corollary 3.2.2).

Marking scheme. (10 points) - 2: treats $(a, b) = (0, 0)$ by the convention, and checks $(ka, kb) \neq (0, 0)$ otherwise, with a reason (no zero divisors). - 4: shows $(ka)\mathbb{Z} + (kb)\mathbb{Z} = (kd)\mathbb{Z}$, citing Theorem 3.2.1 (e) for (a, b) . - 2: shows that kd is the least positive element of $(kd)\mathbb{Z}$. - 2: concludes $\gcd(ka, kb) = kd$ through Theorem 3.2.1 (a), (d) for (ka, kb) . Fatal errors (0 for the step): asserting that every common divisor of ka and kb is k times a common divisor of a and b (false: 1 divides $6 = 3 \cdot 2$ and $9 = 3 \cdot 3$, and 1 is not 3 times an integer); using prime factorizations, which this section does not have. A second route, showing kd is a common divisor and every common divisor c divides kd because $c \mid (ka)x_0 + (kb)y_0 = kd$, earns the same total: 2 for treating $(a, b) = (0, 0)$ by the convention and checking $(ka, kb) \neq (0, 0)$ otherwise (no zero divisors); 3 for showing kd is a common divisor and a combination $(kd = (ka)x_0 + (kb)y_0$ with $ax_0 + by_0 = d$ from Theorem 3.2.1); 3 for every common divisor dividing kd ; 2 for concluding kd is the greatest ($kd > 0$, rule (e) for positive divisors, and the non-positive divisors) via Definition 3.2.2.