2 Arithmetic

Part IV of PJE

2.1 Division

Definition 2.1.1 *(p.140) A non-zero integer b* ***divides*** *integer a if there exists an integer c such that $a = bc$. We write $b|a$. We also say that a is a* ***multiple*** *of b.*

This can be written as

$$b|a \Leftrightarrow \exists c \in \mathbb{Z} : a = bc.$$

Some books will talk of b being a ***factor*** *of a.*

Example 2.1.2 *So $2|8$ since $8 = 4 \times 2$. Also $-2|8$ since $8 = (-4) \times -2$. Further $10|0$ since $0 = 0 \times 10$.*

In fact, 0 is divisible by **any** non-zero integer.

What if b does not divide a?

Example 2.1.3 *Let $b = 4043$ and $a = 166361$.*

Solution By long division,

$$\begin{array}{r@{\,}r} & 41 \\ \cline{2-2} 4043 \; \big) & 166361 \\ & 161720 \\ \cline{2-2} & 4641 \\ & 4043 \\ \cline{2-2} & 598 \end{array}$$

So $166361 = 41 \times 4043 + 598$.

That we get a remainder, 598 here, happens in general. (You have to be quite lucky if, given two randomly chosen integers, one divides the other.)

Theorem 2.1.4 ***Division Theorem****. Let a and b be integers with $b > 0$. Then there exist* ***unique*** *integers q and r such that*

$$a = bq + r \quad \textit{and} \quad 0 \leq r < b. \tag{1}$$

Proof p.191 but I repeat it here. The proof comes in two parts, existance and uniqueness.

Proof of existence of q and r. A proof of two halves, $a > 0$ and $a < 0$ (nothing to prove if $a = 0$!).

Assume $a > 0$.

Define
$$\mathcal{A} = \{k \in \mathbb{Z} : k \geq 0 \text{ and } bk \leq a\}.$$
The fact that $b \times 0 = 0 \leq a$ means that $0 \in \mathcal{A}$, in which case $\mathcal{A} \neq \varnothing$.

> **Aside** Whenever we define a set we need to immediately show it is non-empty. We don't want to waste time proving results about an empty set!

Next $b \in \mathbb{Z}$ and $b > 0$ combine to give $1 \leq b$. Thus if $k \in \mathcal{A}$ then

$$\begin{aligned} k &\leq bk \quad \text{since } 1 \leq b \\ &\leq a \quad \text{since } k \in \mathcal{A}. \end{aligned}$$

Hence all elements $k \in \mathcal{A}$ are bounded, i.e. $\mathcal{A}$ is a **bounded non-empty** set of integers. Thus $\mathcal{A}$ is a **finite** set and it would take only a finite amount of time to find its **maximum element**, $q \in \mathcal{A}$, say. Note that q being the *maximum* element in $\mathcal{A}$ means $q + 1 \notin \mathcal{A}$.

Let $r = a - bq$. Note that $q \in \mathcal{A}$ means that $bq \leq a$ which rearranges to $r \geq 0$. We need to show that $r < b$.

Assume for contradiction that $r \geq b$. Then:

$$\begin{aligned} r \geq b \quad &\Rightarrow \quad a - bq \geq b \quad \text{by definition of } r, \\ &\Rightarrow \quad b(q+1) \leq a \quad \text{on rearranging}, \\ &\Rightarrow \quad q + 1 \in \mathcal{A} \quad \text{by definition of } \mathcal{A}. \end{aligned}$$

But this contradicts the fact that $q = \max \mathcal{A} (= \max_{a \in \mathcal{A}} a)$. Hence the last assumption is false, and so $r < b$ as required.

Assume $a < 0$. Apply the above argument to the positive $-a$ to find

$$-a = bq_1 + r_1 \text{ with } 0 \leq r_1 < b.$$

- If $r_1 = 0$ then $a = b(-q_1)$ and so (1) follows with $q = -q_1$ and $r = 0$.

- If $0 < r_1 < b$ then

$$a = -bq_1 - r_1 = -b(q_1 + 1) + (b - r_1),$$

and so (1) follows with $q = -(q_1 + 1)$ and $r = b - r_1$. Note that $0 < r_1 < b$ implies that $0 < r < b$ as required.

The proof continues...

Proof of Uniqueness. Assume that for some integers a and $b > 0$ we can find **two** pairs (q_1, r_1) and (q_2, r_2) for which

$$a = bq_1 + r_1 = bq_2 + r_2 \tag{2}$$

with $0 \leq r_1, r_2 < b$.

Without loss of generality (w.l.o.g.), we may assume $r_1 \leq r_2$, (so, if this doesn't hold, simply relabel the remainders) in which case

$$0 \leq r_1 = a - bq_1 \leq r_2 = a - bq_2 < b.$$

Even at their extremes of $r_1 = 0$ and $r_2 = b - 1$ the difference $r_2 - r_1$ can be no larger than $b - 1$, that is

$$\begin{aligned} 0 &\leq (a - bq_2) - (a - bq_1) < b \\ \text{i.e. } 0 &\leq b(q_1 - q_2) < b. \end{aligned}$$

From the first inequality $0 \leq b(q_1 - q_2)$ with $b > 0$ we deduce that $q_1 - q_2 \geq 0$.

From the second inequality $b(q_1 - q_2) < b$ and $b > 0$ we deduce $q_1 - q_2 < 1$. But $q_1 - q_2$ is an integer so $q_1 - q_2 < 1$ means $q_1 - q_2 \leq 0$.

From $q_1 - q_2 \geq 0$ and $q_1 - q_2 \leq 0$ we conclude $q_1 = q_2$. From (2) we then deduce $r_1 = r_2$. ■

Definition 2.1.5 *We call q the **quotient** and r the **remainder**.*

Note that we demand that the remainder is **non-negative**.

> **Aside concerning the proof**: In the proof we claim 'If $\mathcal{A}$ is a **finite** set then it would take only a finite amount of time to find its maximum element'. An algorithm for such a search would be: take any two elements, compare and keep the largest, pick another element and compare these two. Continue.

This argument would **not** work for an *infinite* set. For example

$$\left\{0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, ..., \frac{n-1}{n}, ...\right\}$$

is an infinite set bounded above (by 1) but which has no maximal element.

Example 2.1.6 *What is the quotient and remainder on dividing* $= -166361$ *by* $b = 4043$?

Solution From the first part of this example we have, on multiplying by -1,

$$\begin{aligned} -166361 &= (-41) \times 4043 - 598 \\ &= (-42) \times 4043 + 4043 - 598 \\ &= (-42) \times 4043 + 3445, \end{aligned}$$

all because the remainder has to be *non-negative.* Thus $q = -42$ and $r = 3445$. ■

Definition 2.1.7 *(p.140) Let* a *and* b *be integers, at least one of which is non-zero. Then the* ***greatest common divisor of*** a ***and*** b *is the unique* ***positive*** *integer* d *such that*

i) $d|a$ *and* $d|b$ *, i.e.* d *is* ***a*** *common divisor,*

ii) if $c|a$ *and* $c|b$ *then* $c \le d$*, so* d *is the* ***greatest*** *of all such common divisors.*

Notation We write $\gcd(a, b)$, or even just (a, b), for the greatest common divisor. (In lectures I will write (a, b), while in the notes I will keep to $\gcd(a, b)$).

Note In some books you will find hcf (representing ***highest common factor***) in place of gcd.

Example 2.1.8 *Calculate* $\gcd(12, 30)$.

Solution The *set* of common divisors is

$$D(12, 30) = \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

The *greatest* of all these divisors is 6. Hence $\gcd(12, 30) = 6$. ■

Question Does the gcd of two integers always exist?

Definition 2.1.9 *For $a \in \mathbb{Z}$, let $D(a)$ be the set of divisors of a, so*

$$D(a) = \{d \in \mathbb{Z} : d|a\}.$$

Note that $1 \in D(a)$ so $D(a) \neq \varnothing$.

If $a = 0$ then $D(0) = \mathbb{Z} \setminus \{0\}$ since every non-zero integer divides 0.

If $a \neq 0$ then the largest divisor of a is $|a|$ so $\max D(a) = |a|$.

Definition 2.1.10 *For $a, b \in \mathbb{Z}$ let*

$$D(a, b) = D(a) \cap D(b)$$

be the set of common divisors of a and b.

Note that $1 \in D(a, b)$ so $D(a, b) \neq \varnothing$. Thus, *if* $\max D(a, b)$ exists *then* $\gcd(a, b) = \max D(a, b)$.

Special cases.

- If $a = b = 0$ then $D(0, 0) = D(0) = \mathbb{Z} \setminus \{0\}$. This has no maximal element so in this case we **define** $\gcd(0, 0) = 0$.
- If $a = 0$ and $b \neq 0$ then $D(0) = \mathbb{Z} \setminus \{0\}$ and so we must have $D(b) \subseteq D(0)$. Thus
  $$D(0, b) = D(0) \cap D(b) = D(b),$$
  a set with a maximal element $|b|$. Therefore
  $$\gcd(0, b) = \max D(0, b) = \max D(b) = |b|.$$
- If $a \neq 0$ and $b|a$ then $D(b) \subseteq D(a)$ since every divisor of b is a divisor of a. Thus
  $$D(a, b) = D(a) \cap D(b) = D(b).$$
  Also, $a \neq 0$ and $b|a$ imply that $b \neq 0$. Therefore
  $$\gcd(a, b) = \max D(a, b) = \max D(b) = |b|.$$

Theorem 2.1.11 *For all $a, b \in \mathbb{Z}$, at least one of which is non-zero, the* $\gcd(a, b)$ *exists.*

Proof p.140 but I give it here.

Assume without loss of generality, (w.l.o.g.) that a is non-zero.

If $f \in D(a)$ then by definition $f|a$ which means that $fq = a$ for some $q \in \mathbb{Z} \setminus \{0\}$.

Yet $q \in \mathbb{Z} \setminus \{0\}$ implies $|q| \geq 1$.

Thus
$$|a| = |fq| = |f|\,|q| \geq |f|\,.$$
Turn this around and look upon this as bound on $|f|$ to see that all elements $f \in D(a)$ are bounded in modulus by $|a|$. Hence $D(a)$ is a bounded set. Since $1 \in D(a)$ it is non-empty. Therefore $D(a)$ is a non-empty, bounded set of *integers* and is thus finite.

Since $D(a, b) = D(a) \cap D(b) \subseteq D(a)$, we have that $D(a, b)$ is also a finite set. Again, you can find the maximal element of a finite set in finite time so we have that $\max D(a, b)$ exists. Yet by definition $\gcd(a, b) = \max D(a, b)$ and so the gcd exists. ■

Note that $D(-a) = D(a)$ so $D(-a, b) = D(a, b)$ and thus
$$\gcd(-a, b) = \gcd(a, b)\,.$$
Similarly for $\gcd(a, -b)$ and $\gcd(-a, -b)$.

Question How do we *find* the greatest common divisor?

Theorem 2.1.12 *For $a, b \in \mathbb{Z}$, at least one of which is non-zero, write*
$$a = bq + r$$
for some $q, r \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(b, r)\,.$

Proof p.202 but I give the proof here. It suffices to show that $D(a, b) = D(b, r)$, for then
$$\gcd(a, b) = \max D(a, b) = \max D(b, r) = \gcd(b, r)\,.$$
To show set equality $D(a, b) = D(b, r)$ we need to show both
$$D(a, b) \subseteq D(b, r) \quad \text{and} \quad D(a, b) \supseteq D(b, r)\,.$$

Case 1. To show that $D(a,b) \subseteq D(b,r)$.

Assume that $s \in D(a,b)$ is given, so $s|a$ and $s|b$. This means that $a = ms$ and $b = ns$ for some m, $n \in \mathbb{Z}$. But then

$$r = a - bq = ms - nsq = (m - nq)\, s.$$

Yet $m - nq \in \mathbb{Z}$ and so $s|r$. Thus we have both $s|b$ and $s|r$, i.e. $s \in D(b,r)$. Hence $D(a,b) \subseteq D(b,r)$.

Case 2 To show that $D(a,b) \supseteq D(b,r)$. I leave this to the student.

Therefore $D(a,b) = D(b,r)$ as required. ■

Example 2.1.13 *Apply Theorem 2.1.12 to* 1561 *and* 217.

Solution $1561 = 7 \times 217 + 42$. Thus, by Theorem 2.1.12,

$$\gcd(1561, 217) = \gcd(217, 42).$$

■

Important observation The sizes of the numbers have been reduced. In particular the largest integer, a say, has been replaced by one *strictly* smaller than the other original integer, b.

Important idea A strictly decreasing sequence of non-negative numbers must reach 0 at some point. when the process terminates.

Conclusion If we repeatedly apply Theorem 2.1.12 the process will end.

Example 2.1.14 *2.1.13* ***continued****. Calculate* $\gcd(1561, 217)$.

Solution From $217 = 5 \times 42 + 7$ we deduce that

$$\gcd(217, 42) = \gcd(42, 7).$$

Continuing, $42 = 6 \times 7 + 0$, which is when the process terminates. We could then quote Theorem 2.1.12, that $\gcd(a, 0) = |a|$, which here gives

$$\gcd(42, 7) = \gcd(7, 0) = 7.$$

Alternatively, Theorem 2.1.12 also says that if $a \neq 0$ and $b|a$ then $\gcd(a,b) = |b|$. And since $7|42$ this immediately gives $\gcd(42, 7) = 7$. ■

Example 2.1.15 *Calculate* $\gcd(166363, 4043)$.

We have seen earlier that $166361 = 41 \times 4043 + 598$ thus

$$\gcd(166361, 4043) = \gcd(4043, 598).$$

Continuing,

$$\begin{array}{ll} 4043 = 6 \times 598 + 455, & \text{so } \gcd(4043, 598) = \gcd(598, 455), \\ 598 = 455 + 143, & \text{so } \gcd(598, 455) = \gcd(455, 143), \\ 455 = 3 \times 143 + 26 & \text{so } \gcd(455, 143) = \gcd(143, 26), \\ 143 = 5 \times 26 + 13. & \text{Thus } \gcd(143, 26) = \gcd(26, 13). \end{array}$$

Finally, $\gcd(26, 13) = 13$ since $13|26$. Hence $\gcd(166363, 4043) = 13$. ■

The algorithm used in the above examples can be written in general as

Theorem 2.1.16 ***Euclid's Algorithm***. *Given integers a and $b > 0$, make repeated application of the Division Theorem to obtain a series of equations*

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b, \\ b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\ r_2 &= r_3 q_4 + r_4, \quad 0 < r_4 < r_3, \\ &\vdots \end{aligned}$$

Here we have a ***strictly*** *decreasing sequence of non-negative* ***integers*** $b > r_1 > r_2 > .... \geq 0$. *Thus one of these integers must be zero. Stop the applications of the Division Theorem when we reach the zero remainder and label this zero remainder* r_{j+1}. *Thus j is defined as the* ***label of the last non-zero remainder***. *So the last two lines look like*

$$\begin{aligned} &\vdots \\ r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_j q_{j+1}. \end{aligned}$$

Then $\gcd(a, b) = r_j$, *the last non-zero remainder.*

Aside an *algorithm* is a step-by-step procedure for calculations and according to Wikipedia 'a prototypical example of an algorithm is Euclid's algorithm'. An important aspect of an algorithm is that you know it will stop. A process that could go on forever looking for something is of no practical use.

Proof p.202 and p.206. Start by defining $r_0 = b$.

Let $P(i)$ be the statement

$$\text{“}\gcd(r_{i-1}, r_i) = \gcd(a, b)\text{”}.$$

We will prove by induction that $P(i)$ is true for all $1 \leq i \leq j$.

Base case $i = 1$. Consider

$$\begin{aligned} \gcd(r_0, r_1) &= \gcd(b, r_1) \quad \text{by definition of } r_0 = b, \\ &= \gcd(a, b) \end{aligned}$$

by previous Theorem, using $a = bq_1 + r_1$, the first line in Euclid's Algorithm. Hence $P(1)$ is true.

Inductive step Assume $P(k)$ is true for some $1 \leq k \leq j-1$, so $\gcd(r_{k-1}, r_k) = \gcd(a, b)$. We wish to show that $P(k+1)$ is true.

Consider

$$\begin{aligned} \gcd\left(r_{(k+1)-1}, r_{k+1}\right) &= \gcd(r_k, r_{k+1}) \\ &= \gcd(r_{k-1}, r_k) \end{aligned}$$

by previous Theorem, using $r_{k-1} = r_k q_{k+1} + r_{k+1}$, the $k+2$-th line in Euclid's Algorithm. Next use the inductive hypothesis that $P(k)$ is true, namely $\gcd(r_{k-1}, r_k) = \gcd(a, b)$. Use this in the last line above to get

$$\gcd\left(r_{(k+1)-1}, r_{k+1}\right) = \gcd(a, b),$$

and so $P(k+1)$ is true.

Thus, by induction, $P(i)$ is true for all $1 \leq i \leq j$. *End of induction*

Choose $i = j$, the last line in Euclid's Algorithm, when $P(j)$ says

$$\gcd(a, b) = \gcd(r_{j-1}, r_j) = r_j,$$

since $r_{j-1} = r_j q_{j+1}$, i.e. $r_j | r_{j-1}$. ■

Theorem 2.1.17 ***Bezout's Lemma***. *Let a and $b \in \mathbb{Z}$. Then there exist $m, n \in \mathbb{Z}$ such that*

$$\gcd(a, b) = ma + nb.$$

Proof p.207. *But I will give here a slightly different proof.*

Idea. Looking back at Euclid's Algorithm we see that a general step is of the form $r_{k-1} = r_k q_{k+1} + r_{k+1}$. This can be rewritten as

$$r_{k+1} = r_{k-1} - r_k q_{k+1}.$$

To use induction we need information on **both** r_{k-1} and r_k to say something about r_{k+1}. This is a form of *Strong Induction*, see p.48 PJE for more details. In particular, to say something about r_2 we need to know something of both r_0 and r_1. Thus we need *two* base cases. *End of idea.*

We will look separately at the cases $a, b > 0$ and then at least one of a or b non-positive.

Assume first that $a, b > 0$**.** Let r_i, for $0 \leq i \leq j$, be the remainder terms occurring in Euclid's Algorithm (as before $r_0 = b$.)

Let $P(i)$ be the proposition,

$$\text{“}\exists m_i, n_i \in \mathbb{Z} \text{ such that } r_i = m_i a + n_i b.\text{”}$$

We will show by induction that $P(i)$ is true for all $0 \leq i \leq j$.

Base cases:

- When $i = 0$ recall $r_0 = b = 0 \times a + 1 \times b$ so choose $m_0 = 0$, $n_0 = 1$.
- When $i = 1$ then, from the first line of Euclid's Algorithm we have,

  $$r_1 = a - bq_1 = 1 \times a + (-q_1) b,$$

  so choose $m_1 = 1$ and $n_1 = -q_1$.

Thus both base cases $P(0)$ and $P(1)$ are true.

Inductive Step: Assume both $P(k-1)$ and $P(k)$ are true for some $1 \leq k \leq j-1$. This means $\exists m_{k-1}$, n_{k-1}, m_k, $n_k \in \mathbb{Z}$ for which

$$r_{k-1} = m_{k-1} a + n_{k-1} b \quad \text{and} \quad r_k = m_k a + n_k b. \tag{3}$$

We wish to show that $P(k+1)$ is true.

From Euclid's Algorithm we have $r_{k-1} = r_k q_{k+1} + r_{k+1}$ which can be rewritten as

$$r_{k+1} = r_{k-1} - r_k q_{k+1}.$$

Substitute in (3) from the inductive hypothesis to get

$$\begin{aligned} r_{k+1} &= (m_{k-1}a + n_{k-1}b) - (m_k a + n_k b)\, q_{k+1} \\ &= (m_{k-1} - m_k q_{k+1})\, a + (n_{k-1} - n_k q_{k+1})\, b. \end{aligned}$$

So if we choose $m_{k+1} = m_{k-1} - m_k q_{k+1}$ and $n_k = n_{k-1} - n_k q_{k+1}$ we see that $P(k+1)$ is true.

Hence by induction, $P(i)$ is true for all $0 \leq i \leq j$. (End of Induction.)

Choose $i = j$, the last line in Euclid's Algorithm, when $P(j)$ says that there exists $m, n \in \mathbb{Z}$ for which

$$ma + nb = r_j$$

Yet the conclusion of Euclid's Algorithm is that $r_j = \gcd(a, b)$. Hence $ma + nb = \gcd(a, b)$, when $a, b > 0$.

The proof continues....

Assume that at least one of a or b is non-positive.

1. If $a < 0$ and $b > 0$ then as seen earlier

   $$\gcd(a, b) = \gcd(-a, b).$$

   But $-a > 0$ and so, by the result just proven, $\gcd(-a, b) = m(-a) + nb$. Thus

   $$\gcd(a, b) = \gcd(-a, b) = m(-a) + nb = (-m)\, a + nb$$

   as required.

2. If $a > 0, b < 0$, then there exist $m, n \in \mathbb{Z}$ with

   $$\gcd(a, b) = \gcd(a, -b) = ma + n(-b) = ma + (-n)\, b.$$

3. If $a < 0, b < 0$, then there exist $m, n \in \mathbb{Z}$ with

   $$\gcd(a, b) = \gcd(-a, -b) = m(-a) + n(-b) = (-m)\, a + (-n)\, b.$$

4. Finally

   $$\gcd(a, 0) = |a| = \begin{cases} 1 \times a + 0 \times b & \text{if } a > 0, \\ -1 \times a + 0 \times b & \text{if } a < 0. \end{cases}$$

   Similarly for $\gcd(0, b)$, while $\gcd(0, 0) = 0 \times 0 + 0 \times 0$.

∎

Definition 2.1.18 *Given integers a and b, we say that an integer c is an* ***integral linear combination*** *of a and b if there exist $m, n \in \mathbb{Z}$ such that $c = ma + nb$.*

Question Bezout's Lemma states that for the greatest common divisor of a and b there exists $m, n \in \mathbb{Z}$ such that $\gcd(a, b) = ma + nb$. (An *existence* result). How can we find m and n?

Example 2.1.19 *2.1.13* ***revisited*** *Write* $\gcd(1561, 217)$ *as a linear combination of* 1561 *and* 217.

Solution Recall

$$\begin{aligned} 1561 &= 7 \times 217 + 42 \\ 217 &= 5 \times 42 + 7 \\ 42 &= 6 \times 7, \end{aligned}$$

so $\gcd(1561, 217) = 7$. Working back up we see

$$\begin{aligned} 7 &= 217 - 5 \times 42 \\ &= 217 - 5 \times (1561 - 7 \times 217) \\ &= 36 \times 217 - 5 \times 1561. \end{aligned}$$

Hence

$$\gcd(1561, 217) = 36 \times 217 - 5 \times 1561.$$

∎

> **Aside** Be careful with *double negatives*. In this example, the final coefficient of 36 arose from $1 + (-5) \times (-7)$.

Example 2.1.20 *2.1.15* ***revisited*** *Write* $\gcd(166361, 4043)$ *as a linear combination of* 166361 *and* 4043.

Solution Recall

$$\begin{aligned} 166361 &= 41 \times 4043 + 598, \\ 4043 &= 6 \times 598 + 455, \\ 598 &= 1 \times 455 + 143, \\ 455 &= 3 \times 143 + 26, \\ 143 &= 5 \times 26 + 13, \\ 26 &= 2 \times 13, \end{aligned}$$

so $\gcd(166361, 4043) = 13$. Hence, working back up,

$$\begin{aligned}
13 &= 143 - 5 \times 26 \\
&= 143 - 5 \times (455 - 3 \times 143) = -5 \times 455 + 16 \times 143 \\
&= -5 \times 455 + 16 \times (598 - 1 \times 455) = 16 \times 598 - 21 \times 455 \\
&= 16 \times 598 - 21 \times (4043 - 6 \times 598) = -21 \times 4043 + 142 \times 598 \\
&= -21 \times 4043 + 142 \times (166361 - 41 \times 4043) \\
&= 142 \times 166361 - 5843 \times 4043.
\end{aligned}$$

Thus

$$\gcd(166361, 4043) = 142 \times 166361 - 5843 \times 4043.$$

■

Always, always check your answers by multiplying out your final answer.

> **Aside** In PJE, p.204, there is a discussion of a concise way of writing Euclid's Algorithm and on p.209 of finding the corresponding linear combination.

Definition 2.1.21 *Two integers a and b, not both zero, are **coprime** when*

$$\gcd(a, b) = 1.$$

Example 3 Let $a = 93$ and $b = 56$. Then

$$\begin{aligned}
93 &= 1 \times 56 + 37 \\
56 &= 1 \times 37 + 19 \\
37 &= 1 \times 19 + 18 \\
19 &= 1 \times 18 + 1 \\
18 &= 18 \times 1 + 0.
\end{aligned}$$

Hence $\gcd(93, 56) = 1$ and thus 93 and 56 are coprime.

Theorem 2.1.22 *Two integers a and b are coprime if, and only if, there exist $m, n \in \mathbb{Z}$ such that*

$$1 = ma + nb.$$

Proof ($\Rightarrow$) Assume a and b are coprime so $\gcd(a, b) = 1$. But from previous result there exist $m, n \in \mathbb{Z}$ such that $ma + nb = \gcd(a, b)$. Combine to get required result.

($\Leftarrow$) p.213, *but I will give here a slightly different proof.*

Assume there exist $m, n \in \mathbb{Z}$ such that $1 = ma + nb$.

First, trivially 1 divides both a and b, so 1 is *a* common divisor of both a and b.

Secondly, let c be *any* common divisor of both a and b. Then $\exists s, t \in \mathbb{Z}$ such that $a = cs$ and $b = ct$. Substitute to get

$$\begin{aligned} 1 &= ma + nb = mcs + nct \\ &= c\,(ms + nt)\,. \end{aligned}$$

Here $ms + nt \in \mathbb{Z}$ and thus $c|1$, which means $c = +1$ or -1. Hence $c \leq 1$ or, in other words, 1 is *greater* than any common divisor.

Thus we have **verified the definition** that 1 is the greatest of all common divisors of a and b, i.e. $1 = \gcd(a, b)$ as required. ■

Example 3 revisited Working back up the previous example we see that

$$\begin{aligned} 1 &= 19 - 1 \times 18 \\ &= 19 - 1 \times (37 - 1 \times 19) = 2 \times 19 - 1 \times 37 \\ &= 2 \times (56 - 1 \times 37) - 1 \times 37 = 2 \times 56 - 3 \times 37 \\ &= 2 \times 56 - 3 \times (93 - 1 \times 56)\,. \end{aligned}$$

Thus

$$1 = 5 \times 56 + (-3) \times 93.$$

We now give a simple result that has many applications both below and in our later study of prime numbers.

Corollary 2.1.23 *If a, b and c are integers with not both a and b zero, we have*

1. *If $a|bc$ and $\gcd(a, b) = 1$ then $a|c$.*
2. *If $d = \gcd(a, b)$ then*

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Proof p.214