(I.A) THE EUCLIDEAN ALGORITHM

We begin our discussion with the division algorithm:

**Proposition 1.** Given \( a, b \in \mathbb{N} \), there exist unique \( q, r \in \mathbb{Z} \) such that

\[ a = b \cdot q + r \quad \text{with} \quad 0 \leq r < b. \]

Of course, the “algorithm” isn’t in the formal statement, but in how we produce \( q \) and \( r \).

**Example 2.** Suppose \( a = 313 \) and \( b = 9 \). In grade school, you learned to write

\[
\begin{array}{c|c}
34 & \\
9 \overline{313} \\
27 & \\
43 & \\
36 & \\
7 & \\
\end{array}
\]

which yields

\[ 313 = 9 \cdot \underbrace{34}_{q} + \underbrace{7}_{r}. \]

The algorithm is simply long division with remainder.

**Proof of Proposition 1.** For the “existence” part, let

\[ S := \{ a - bk \mid k \in \mathbb{Z}, \ a - bk \geq 0 \} \subseteq \mathbb{N} \cup \{0\}. \]

Since \( a \in S \), \( S \neq \emptyset \). Let \( r \) be the least element of \( S \). Then \( r = a - bq \geq 0 \) for some \( q \in \mathbb{Z} \). If \( r \geq b \) then \( S \) contains \( r - b = a - b(q + 1) \), contradicting minimality of \( r \). So \( r < b \).

To see the uniqueness, write

\[ bq' + r' = a = bq + r, \]

with \( 0 \leq r, r' < b \). This yields

\[ r = b(q' - q) + r', \]
and if we had \( q' > q \), then \( q' \geq q + 1 \) would imply \( r \geq b + r' \geq b + 0 = b \), a contradiction. Symmetrically, one argues that \( q > q' \) is impossible. Therefore \( q = q' \) and then also \( r = r' \). □

Next, we turn to **divisibility** and the **GCD** (= greatest common divisor).

**Definition 3.** Let \( a, b \in \mathbb{Z} \), with \( b \neq 0 \). Then

\[
 b \mid a \iff \exists c \in \mathbb{Z} \text{ such that } a = bc. 
\]

(We say that “\( b \) divides \( a \”).)

Here are some basic examples:

- everything divides 0;
- \( 2 \mid a \iff a \) is even;
- \( b \mid a \iff r = 0 \) in the division algorithm.

and some basic properties:

(i) \( a \mid b \) and \( b \mid c \implies a \mid c \)

(ii) \( a \mid b, c \implies a \mid bx + cy \) for all \( x, y \in \mathbb{Z} \) (e.g. \( b + c, b - c \))

(iii) \( a \mid b \) and \( b \mid a \implies a = \pm b \).

**Proof of (iii).** Given \( b = ad, a = bc \) (and \( a, b \neq 0 \)), we have \( a = adc \)

\[
 \implies dc = 1 \implies d = \pm 1 = c. 
\]

For any \( a, b \in \mathbb{Z} \), not both 0, let

\[
 S(a, b) := \{ d \in \mathbb{N} \mid d \mid a, b \} .
\]

**Definition 4.** The **GCD of \( a \) and \( b \)** is

\[
 (a, b) := \text{the biggest element of } S(a, b). 
\]

(Of course, you need only check integers less than or equal to the smallest of \( |a| \) and \( |b| \).) We say that \( a \) and \( b \) are **relatively prime** if \( (a, b) = 1 \).

Again, here are some simple examples:

- \( (4, -6) = 2 \)
- \( (0, 7) = 7 \)
• (12, 7) = 1

and some properties:

(iv) \((0, b) = b = (b, b)\)
(v) \((a, b) = (b, a) = (a, -b)\)
(vi) \((b, a - mb) = (a, b)\) for every \(m \in \mathbb{Z}\).

Proof of (vi). Let \(d \mid a, b\). Then \(d \mid a - mb\). Conversely, if \(d \mid b, a - mb\), then \(d \mid mb + (a - mb) = a\). So \(S(a, b) = S(b, a - mb)\) and they have identical largest elements. □

Property (vi) has the key consequence:

**Lemma 5.** Say \(a = bq + r\) in the division algorithm. Then

\[(a, b) = (b, r)\]

Proof. Write \(r = a - bq\), and use (vi). □

**Example 6.** How do we use this to find a GCD, like \((345, 92)\)? By applying it in concert with the division algorithm: starting with \(a = 345\) and \(b = 92\), we have

\[
\begin{align*}
345 &= 92 \cdot 3 + 69 & (345, 92) &= (92, 69) \\
92 &= 69 \cdot 1 + 23 & (a, b) &= (b, r_1) \\
69 &= 23 \cdot 3 + 0 & (92, 69) &= (69, 23) \\
r_1 &= r_2 \cdot q_3 + r_3 & (b, r_1) &= (r_1, r_2) \\
r_1 &= r_2 \cdot q_3 + r_3 & (69, 23) &= (23, 0) = 23 \\
\end{align*}
\]

So \((345, 92) = 23\).

**Theorem 7 (Euclidean Algorithm).** Given \(a, b \in \mathbb{N}\), \((a, b)\) may be computed by repeated application of the Division Algorithm. That is, writing

\[
\begin{align*}
a &= bq_1 + r_1 \quad , \quad 0 \leq r_1 < b, \\
b &= r_1q_2 + r_2 \quad , \quad 0 \leq r_2 < r_1, \\
r_1 &= r_2q_3 + r_3 \quad , \quad 0 \leq r_3 < r_2, \\
&\vdots \\
\end{align*}
\]
we eventually reach

\[ \vdots \]
\[ r_{n-1} = r_nq_{n+1} + r_{n+1} \quad \text{with} \quad r_{n+1} = 0, \]

and then \((a, b) = r_n\).

Proof. There are two statements here: first, that the algorithm terminates after finitely many steps. But we have \(b > r_1 > r_2 > \cdots \geq 0\) (as a byproduct of Proposition 1), which clearly cannot continue indefinitely, so that indeed we must have \(r_{n+1} = 0\) for some \(n\).

Second, the theorem claims that \((a, b) = r_n\). To see this, we just use Lemma 5 to write

\[ (a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_n, r_{n+1}) = (r_n, 0) = r_n. \]

Now returning to Example 6, the first two equations yield the following “bonus”

\[
23 = 92 - 69 \cdot 1 \quad r_2 = b - r_1q_2 \\
= 92 - (345 - 92 \cdot 3) \cdot 1 \quad = b - (a - bq_1)q_2 \\
= 4 \cdot 92 + (-1) \cdot 345 \quad = (1 + q_1q_2)b + (-q_2)a
\]

expressing the GCD as an integer linear combination of \(a\) and \(b\). This is a general fact: let \(a, b\) be integers, not both zero.

**Theorem 8.** There exist \(x, y \in \mathbb{Z}\) such that \((a, b) = ax + by\).

Proof. In the Euclidean algorithm, \((a, b)\) appears as the last nonzero remainder \(r_n\). We show by induction that all the remainders are integer linear combinations of \(a\) and \(b\).

For \(n = 1\), we have \(r_1 = a + (-q_1)b\). Now assume that \(r_j = ax_j + by_j\) \((x_j, y_j \in \mathbb{Z})\) for \(j = 1, \ldots, k - 1\). To check that this is true for \(j = k\), write \(r_{k-2} = r_{k-1}q_k + r_k \implies\)

\[
r_k = r_{k-2} + (-q_k)r_{k-1} = (x_{k-2}a + y_{k-2}b) + (-q_k)(x_{k-1}a + y_{k-1}b) \\
= \underbrace{(x_{k-2} - q_kx_{k-1})}_{= : x_k} a + \underbrace{(y_{k-2} - qky_{k-1})}_{= : y_k} b.
\]
Corollary 9. \((a,b)\) is the least element of
\[ S := \{ ax + by \mid x, y \in \mathbb{Z}, ax + by > 0 \} . \]

Proof. Given any \(\mu = ax_0 + by_0 \in S\), \(g := (a,b) \in S \) by Theorem 8. Then \(g|a,b \implies g|\mu \implies \frac{\mu}{g} \in \mathbb{N} \implies g \leq \mu. \)

Corollary 10.
(i) \((ma,mb) = m(a,b)\) for any \(m \in \mathbb{N}\)
(ii) \(\left(\frac{a}{d},\frac{b}{d}\right) = \frac{1}{d}(a,b)\) if \(d|a,b\) and \(d \in \mathbb{N}\).

Proof. (ii) follows from (i), and (i) follows from the observation that the least positive number of the form \(max + mby\) is \(m\) times the least positive number of the form \(ax + by\).

By part (ii), writing \(g := (a,b), \left(\frac{a}{g},\frac{b}{g}\right) = 1.\)

Corollary 11.
(i) If \(a, b\) are relatively prime to \(m\), then so is \(ab\).
(ii) If \((b,m) = 1\) and \(m|ab\), then \(m|a.\)

Proof. For (i), observe that there exist \(x,y,z,w \in \mathbb{Z}\) such that \(bz + mw = 1 = ax + my.\) Hence
\[
1 = (ax + my)(bz + mw) = ab(xz) + m(ybz + axw + myw),
\]
and we are done by Corollary 9.

To see (ii), write \(a = a \cdot 1 = a(b, m) = (ab, am) = m\left(\frac{ab}{m},a\right). \)

Definition 12. The LCM (= least common multiple) \([a,b]\) is the least element of \(S' := \{ n \in \mathbb{N} \mid a, b|n \} .\)

Corollary 13. We have \([a,b](a,b) = ab.\)

Proof. Set \(g := (a,b).\) Clearly \(\frac{ab}{g} = a\left(\frac{b}{g}\right) = b\left(\frac{a}{g}\right) \in S'.\) But is this number “least” among elements of \(S'\)?

If \(a, b|N\) (i.e. \(N \in S'\)) then \(N = Ma\) and \(\frac{b}{g}|N \implies M\frac{a}{g}.\) By Corollary 11(ii), \(\left(\frac{a}{g},\frac{b}{g}\right) = 1 \implies \frac{b}{g}|M \implies \frac{ab}{g}|Ma = N \implies N \geq \frac{ab}{g}. \)
As useful as Theorem 8 is, the method indicated in its proof yields awful formulas that require remembering all the \( \{q_i\} \): for example, if \( r_3 = (a, b) \), then
\[
x = 1 + q_2q_3 \quad \text{and} \quad y = -(q_1 + q_3 + q_1q_2q_3).
\]

A better approach is to perform the Division Algorithm on equations: start with
\[
\begin{align*}
345 & = 345 \cdot 1 + 92 \cdot 0 & \mathbf{E}_{-1}(=i) \\
92 & = 345 \cdot 0 + 92 \cdot 1 & \mathbf{E}_0
\end{align*}
\]

Now perform the Division Algorithm: subtract \( 3 \cdot \mathbf{E}_0 \) from \( \mathbf{E}_{-1} \) to get
\[
69 = 345 \cdot 1 + 92 \cdot (-3) \quad \mathbf{E}_1,
\]
them \( 1 \cdot \mathbf{E}_1 \) from \( \mathbf{E}_0 \) to get
\[
23 = 345 \cdot (-1) + 92 \cdot 4 \quad \mathbf{E}_2.
\]
(We stop here because \( \mathbf{E}_3 \) would have 0 on the left-hand side.) The point is that we have
\[
r_{i+1} = r_{i-1} - q_{i+1}r_i
\]
as before, but also
\[
\begin{align*}
x_{i+1} &= x_{i-1} - q_{i+1}x_i \\
y_{i+1} &= y_{i-1} - q_{i+1}y_i
\end{align*}
\]
by virtue of carrying the operations through to the whole equation. The result is the following, which uses almost no memory on a computer:

**Theorem 14** (Algorithm for computing \( x \) and \( y \)). Begin with the picture

<table>
<thead>
<tr>
<th>&quot;r&quot;</th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;x&quot;</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>&quot;y&quot;</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
and apply the Euclidean Algorithm to the top row, carrying operations through to the entire column at each stage:

\[
\begin{array}{ccccccc}
q_1 & q_2 & q_3 & \cdots & q_n & q_{n+1} \\
\hline
a & b & r_1 & r_2 & r_3 & \cdots & r_n & 0 \\
1 & 0 & x_1 & x_2 & x_3 & \cdots & x_b & - \\
0 & 1 & y_1 & y_2 & y_3 & \cdots & y_n & - \\
\end{array}
\]

--- that is, \( \text{col}_{i+1} = \text{col}_i - q_{i+1} \text{col}_i \). Then \( x_n a + y_n b = r_n = (a, b) \).

**Proof.** At each stage, we have \( r_k = x_k a + y_k b \), so the conclusion is clear. \( \square \)

For computer (or human\(^1\)) implementation of the Euclidean Algorithm, one problem remains: how large can \( n + 1 \) (the number of steps) be?

**Theorem 15.** Assume \( a \geq b \). We have \( n \leq 2 \log_2 (b) \).

**Lemma 16.** \( r_{i+2} < \frac{1}{2} r_i \) (\( \forall i \)).

**Proof of Lemma.** Without loss of generality, we may assume that

\[
(1) \quad r_{i+1} > \frac{1}{2} r_i.
\]

(Otherwise, \( r_{i+2} < r_{i+1} \leq \frac{1}{2} r_i \) and we’re done.) The Euclidean Algorithm gives \( r_i = r_{i+1} q_{i+2} + r_{i+2} \), whereupon (1) forces \( q_{i+2} = 1 \). So

\[
r_{i+2} = r_i - r_{i+1} > r_i - \frac{1}{2} r_i = \frac{1}{2} r_i.
\]

\( \square \)

**Proof of Theorem 15.** The Lemma gives

\[
(2) \quad (0 \leq ) \ r_k < \frac{1}{2} r_{k-2} < \frac{1}{4} r_{k-4} < \cdots < \frac{1}{2^{k-2}} r_2 < \frac{1}{2^k} b,
\]

since \( b \) is essentially “\( r_0 \)”.

\(^1\)Actually, before the 1940s, “computer” meant “a person who performs computations”!
Suppose that \( n > 2 \log_2(b) \). Then \( 2^n > \left(2^{\log_2 b}\right)^2 = b^2 \), and so 
\( b < 2^n \). If \( n \) is even, then (2) yields \( r_n < \frac{1}{2^n}b < 1 \implies r_n = 0 \); if \( n \) is odd, then \( r_{n+1} < \frac{1}{2^{n+1}}b < \frac{1}{\sqrt{2}} \implies r_{n+1} = 0 \). In either case \( r_{n+1} = 0 \), which is what we had to show.

\[ \square \]

Example 17. Consider the pair \( a = 85652, b = 16261 \). We apply Theorem 14, constructing the table

<table>
<thead>
<tr>
<th></th>
<th>5</th>
<th>3</th>
<th>1</th>
<th>2</th>
<th>1</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r )</td>
<td>85652</td>
<td>16261</td>
<td>4357</td>
<td>3220</td>
<td>1127</td>
<td>966</td>
</tr>
<tr>
<td>( x )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-3</td>
<td>4</td>
<td>-11</td>
</tr>
<tr>
<td>( y )</td>
<td>0</td>
<td>1</td>
<td>-5</td>
<td>16</td>
<td>-21</td>
<td>58</td>
</tr>
</tbody>
</table>

in which the top line denotes the values of \( q_i \) at each step. We conclude that

\[ 15a - 79b = 161 = (85652, 16261) \].

Note that \( 2 \log_2 16261 \) is close to 28, so we got somewhat lucky here.