I.B. Integers

We turn to some results of Euclid. A prime number \( p \in \mathbb{Z} \) is one not equal to 0, 1, \(-1\) and whose only divisors are \( \pm p, \pm 1 \).

I.B.1. Fundamental Theorem of Arithmetic. Any natural number \( n \in \mathbb{N}\setminus\{0,1\} \) has (up to order) a unique factorization

\[
n = p_1 p_2 \cdots p_s,
\]
where the \( \{p_i\} \) are (positive) primes, which are not necessarily distinct.

Proof. We use induction (\( n = 1 \) is clear). Assume the statement holds for all \( n < m \). Then \( m \) has a prime factorization: either it is itself prime, or factors into \( m_1 m_2 \) with \( m_1, m_2 < m \).

As for uniqueness: if \( m = p_1 \cdots p_s = q_1 \cdots q_t \) with \( p_1 = q_1 \), this follows from induction. If instead \( p_1 < q_1 \), then \( t > 1 \) (since \( q_1 \) is prime and \( m \) isn’t) and

\[
1 < n_0 := \underbrace{p_1(p_2 \cdots p_s - q_2 \cdots q_t)}_{m} = (q_1 - p_1)q_2 \cdots q_t < m.
\]
Factoring the parentheticals into primes, the inductive hypothesis says that the resulting factorizations of \( n_0 \) must be the same (up to order). So we either have

\[
p_1 \mid (q_1 - p_1) \implies p_1 \mid q_1 \implies p_1 = q_1,
\]
which is a contradiction, or \( p_1 \) is one of the \( q_2,\ldots,q_t \). Reordering puts us back in the \( p_1 = q_1 \) case. \( \square \)

I.B.2. Proposition. There are infinitely many primes.

Proof. Suppose \( p_1,\ldots,p_s \) is a complete list of positive primes; then none of them divide \( p_1 \cdots p_s + 1 \), contradicting I.B.1. \( \square \)

The FTA leads to the notion of the \( \text{gcd} \) (= greatest common divisor) of \( m, n \in \mathbb{Z} \), written \( (m,n) \) and well-defined up to sign. To find it, one traditionally employs the
I.B.3. DIVISION ALGORITHM. Given \( a, b \in \mathbb{Z}, \ b \neq 0 \), there exist \( q, r \in \mathbb{Z} \) such that

\[
0 \leq r < |b| \quad \text{and} \quad a = bq + r.
\]

PROOF. We may assume \( b > 0 \); then \( M := \{bn \mid n \in \mathbb{Z}, \ bn \leq a\} \) is nonempty and bounded above, hence\(^4\) has a largest element \( bq \). So \( a = bq + r \) (for some \( r \geq 0 \)) and \( b(q + 1) > a \), from which \( b > r \). \( \square \)

To find \((m, n)\), we write as in I.B.3

\[
\begin{align*}
n &= q_0m + r_0 \\
m &= q_1r_0 + r_1 \\
r_0 &= q_2r_1 + r_2 \\
r_1 &= q_3r_2 + r_3 \\
&\vdots
\end{align*}
\]

in which the gcd is the last nonzero remainder \( r_i \).\(^5\) This is best covered and proved later in a more general context (that of principal ideal domains). For now, we shall just show:

I.B.4. PROPOSITION. \((m, n) = mu + nv\) for some \( u, v \in \mathbb{Z} \).

PROOF. Let \( I := \{mx + ny \mid x, y \in \mathbb{Z}\} \), with least positive element \( d = mu + nv \in I \cap \mathbb{Z}_{>0} \). Writing \( m = dq + r \) (with \( 0 \leq r < d \)), one finds

\[
r = m - dq = m - (mu + nv)q = m(1 - uq) - n(vq) \in I.
\]

For this not to contradict leastness of \( d \), we must have \( r = 0 \) and thus \( d \mid m \). Similarly, \( d \mid n \). Moreover, any \( e \) dividing both \( m \) and \( n \) divides \( d \), which is therefore maximal among common divisors. \( \square \)

---

\(^4\)This is the well-ordering principle; it is equivalent to the principle of induction.

\(^5\)The idea: \((n, m) = (n - q_0m, m) = (r_0, m)\) and so on. You eventually reach \((r_{i-1}, r_i)\), with \( r_{i-1} = q_{i+1}r_i \).