5. The Fundamental Theorem of Arithmetic

Definition 5.1. *An integer $p > 1$ is called* **prime** *if its only positive divisors are 1 and p.*

Example 5.2. *(1) The integer 2 is prime, because assume that $n \mid 2$, where $n \geq 1$. Then $n \leq 2$, by Lemma 3.3(5). Hence $n \in \{1, 2\}$. Similarly we observe that if $n \mid 3$, then $n \in \{1, 2, 3\}$. As $3 = 1 \cdot 2 + 1$, it follows by the Division Algorithm that $2 \nmid 3$. In particular, 3 is prime. Next $4 = 2 \cdot 2$ is not prime. And so on...*

(2) (Sieve of Eratosthenes) Given $n \in \mathbb{N}$ let us find all primes in $S := \{2, \ldots, n\}$. Take $m \in S$. Either m is prime or $m = p \cdot r$, for some $p, r \in S$. We can choose p minimal in S by the Well-Ordering Principle. Then $p \leq r$. Now $p^2 \leq p \cdot r = m$ and so $p \leq \sqrt{m} \leq \sqrt{n}$. Overall m is prime or m is divisible by an integer p with $2 \leq p \leq \sqrt{n}$.

Let $n = 100$. Then $\sqrt{100} = 10$. Eliminating all proper multiples of $\{2, \ldots, 10\}$ in S gives all the primes in S. They are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

Lemma 5.3. *For integers a, b, let p is a prime divisor of ab. Then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$, there is nothing to prove. So assume that $p \nmid a$. Then $\gcd(p, a) = 1$. We deduce from Euclid's Lemma that $p \mid b$. □

Corollary 5.4. *Let $p, a_1, a_2, \ldots, a_k$ be integers, where p is prime. If $p \mid (a_1 a_2 \ldots a_k)$ then $p \mid a_i$, for some $i \in \{1, \ldots, k\}$.*

Corollary 5.5. *Let $p, q_1, q_2, \ldots, q_k$ be prime integers. If $p \mid (q_1 q_2 \ldots q_k)$ then $p = q_i$, for some $i \in \{1, \ldots, k\}$.*

Theorem 5.6 (Fundamental Theorem of Arithmetic)**.** *Given $n \in \mathbb{Z}$, non-zero, there exist $\epsilon \in \{\pm 1\}$ and primes $p_1, \ldots, p_k$ such that*

$$n = \epsilon \cdot p_1 p_2 \ldots p_k.$$

Moreover, this expression is unique up to a permutation of the factors $p_1, \ldots, p_k$.

Proof: W.l.o.g we assume $n \geq 1$. The statement holds for $n = 1$. Next assume the statement holds for $1, \ldots, n-1$. If n is prime, we are done. Otherwise, there is some positive divisor, say m, of n, such that $m \notin \{1, n\}$. Then $n = m \cdot r$, for some $r \in \mathbb{Z}$. Note that $1 < m, r < n$. By induction m and r are products of prime integers, and thus so is n. The uniqueness of this expression

can be shown using Corollary 5.5.

□

Example 5.7. *(1)* $-12 = (-1) \cdot 2^2 \cdot 3$
(2) $21780 = 2 \cdot 10890 = 2 \cdot 5445 = 2^2 \cdot 3 \cdot 1815 = 2^2 \cdot 3^2 \cdot 605 = 2^2 \cdot 3^2 \cdot 5 \cdot 121$
$= 2^2 \cdot 3^2 \cdot 5 \cdot 11^2$
(3) Let's find the prime factorisation of 2369. *Since* $\sqrt{2369} < 49$, *unless* 2369 *is prime, there must be a prime factor of* 2369 *that is* ≤ 48. *By checking* $2, 3, 5, 7, 11, 13, 17, 19, 23$ *we see that* $23 \mid 2369$, *as* $2369 = 23 \cdot 103$. *As* $\sqrt{103} < 11$, *and* $2, 3, 5, 7$ *do not divide* 103 *we conclude that* 103 *is prime. Therefore* $2369 = 23 \cdot 103$ *is the prime factorisation of* 2369.

Corollary 5.8. *There are an infinite number of prime integers.*

Proof: Suppose that $p_1, \ldots, p_n$ are all the prime integers. Then $p_1 p_2 \ldots p_n + 1$ is an integer which is not divisible by any of the p_i. Hence there must be further prime integers.

□

Remark 5.9. *Let* $a, b \in \mathbb{Z}$ *be non-zero and let* $p_1, \ldots, p_n$ *be a complete list of prime numbers dividing* a *and/or* b. *Furthermore let*

$$a = p_1^{r_1} \cdots p_n^{r_n}, \quad \text{and} \quad b = p_1^{s_1} \cdots p_n^{s_n},$$

be the respective prime factorisations of both a *and* b. *(Note that* $r_j, s_j \geq 0$, *for all* $j = 1, \ldots, n$, *but some might be zero.) Then*

$$\gcd(a, b) = p_1^{\min\{r_1, s_1\}} \cdots p_n^{\min\{r_n, s_n\}}$$

For instance we have $21780 = 2^2 \cdot 3^2 \cdot 5 \cdot 11^2$, *and* $15400 = 2^3 \cdot 5^2 \cdot 7 \cdot 11$. *Then*

$$\begin{aligned} \gcd(21780, 15400) &= 2^{\min\{2,3\}} \cdot 3^{\min\{2,0\}} \cdot 5^{\min\{1,2\}} \cdot 7^{\min\{0,1\}} \cdot 11^{\min\{2,1\}} \\ &= 2^2 \cdot 5 \cdot 11 = 220 \end{aligned}$$