This summarizes some of the main definitions, results and algorithms from class leading up to and following from the fundamental theorem of arithmetic. This is in no way a comprehensive list of everything you need to know, but is intended to help you review and organize your knowledge. They are ordered according to when we covered them in lecture.

**Definitions**

**Definition 1.** Given integers \( a, b \), we say \( a \) divides \( b \), or that \( a \) is a divisor of \( b \), and write \( a \mid b \), if there exists an integer \( q \) such that \( b = q \cdot a \).

**Definition 2.** An integer \( a > 1 \) is prime if its only positive integer divisors are 1 and itself.

**Definition 3.** Given \( a, b \in \mathbb{Z} \) not both zero, the greatest common divisor of \( a \) and \( b \), written \( (a, b) \) or \( \gcd(a, b) \), is the greatest integer which divides both \( a \) and \( b \). By convention, we set \((0, 0) = 0\). We say that \( a \) and \( b \) are relatively prime if \((a, b) = 1\).

**Definition 4.** Given \( n \geq 2 \), and \( a_1, \ldots, a_n \in \mathbb{Z} \) not all zero, the greatest common divisor of \( a_1, \ldots, a_n \), denoted \((a_1, \ldots, a_n)\), is the greatest integer which divides all of the \( a_i \). By convention, we set \((0, \ldots, 0) = 0\). We say \( a_1, \ldots, a_n \) are mutually relatively prime if \((a_1, \ldots, a_n) = 1\).

**Results**

**Theorem 5.** There are infinitely many prime numbers.

**Proposition 6.** Every integer greater than 1 has a factorization as a product of primes.

**Theorem 7** (The division “algorithm”). Given \( a, b \in \mathbb{Z} \) with \( b \neq 0 \), there exist unique \( q, r \in \mathbb{Z} \) such that \( a = bq + r \), and \( 0 \leq r < |b| \).

**Theorem 8.** For any integers \( a, b \), if \( d = (a, b) \), then there exist \( x, y \in \mathbb{Z} \) such that \( d = ax + by \).

In particular, if \( d' \) is any common divisor of \( a \) and \( b \), then \( d' \) also divides \( d \).

**Corollary 9.** Given \( a, b, c \in \mathbb{Z} \), the equation \( ax + by = c \) has integer solutions if and only if \((a, b) \mid c\).

**Corollary 10.** If \( p \) is a prime number, then given \( n \in \mathbb{P} \) and \( a_1, \ldots, a_n \in \mathbb{Z} \), if \( p \mid (a_1 \cdots a_n) \), then \( p \mid a_i \) for some \( i \).

**Theorem 11** (Fundamental Theorem of Arithmetic). Let \( a > 1 \) be an integer. Then there is a factorization \( a = p_1 \cdots p_n \) of \( a \) as a product of primes (where the \( p_i \) are not necessarily distinct), and this factorization is unique up to reordering.

**Corollary 12.** Suppose that \( \alpha \) is a zero of a polynomial of the form \( x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0 \), where \( c_i \in \mathbb{Z} \) for all \( i \), and suppose also that \( \alpha \) is a rational number. Then \( \alpha \) is an integer.
Proposition 13. Given \(a, b, c \in \mathbb{Z}\), suppose that the equation
\[ax + by = c\]
has a solution with \(x, y \in \mathbb{Z}\). Then it has infinitely many such solutions. More specifically, if \(x_0, y_0\) is any fixed solution, then every solution can be written in the form \(x = x_0 + (b/d)q, y = y_0 - (a/d)q\), where \(d = (a, b)\), and \(q \in \mathbb{Z}\).

Corollary 14. Given \(a, b, c \in \mathbb{Z}\), suppose that the equation
\[ax + by = c\]
has a solution with \(x, y \in \mathbb{Z}\). If \(a, b > 0\), then there are at most finitely many solutions with \(x, y \geq 0\). If \(x_0, y_0\) is any fixed solution, then the nonnegative solutions are of the form \(x = x_0 + (b/d)q, y = y_0 - (a/d)q\), with \(d = (a, b)\), and
\[-(d/b)x_0 \leq q \leq (d/a)y_0.\]

Theorem 15. Given \(a_1, \ldots, a_n, b \in \mathbb{Z}\):
(i) the solutions to the equation
\[a_1x_1 + \cdots + a_nx_n = b\]
with all the \(x_i \in \mathbb{Z}\) are the same as the solutions to the two equations
\[a_1x_1 + \cdots + a_{n-2}x_{n-2} + (a_{n-1}, a_n)w = b\]
and
\[a_{n-1}x_{n-1} + a_nx_n = (a_{n-1}, a_n)w,\]
where \(w\) is also allowed to vary in \(\mathbb{Z}\);
(ii) the equation (1) has solutions if and only if
\[(a_1, \ldots, a_n)|b,\]
and in this case, it has infinitely many solutions;
(iii) if all the \(a_i\) and \(b\) are positive, then (1) has at most finitely many solutions with all the \(x_i\) nonnegative.

Algorithms

Algorithm 16 (Euclidean algorithm). Given nonzero integers \(a, b\), set \(r_0 = a, r_1 = b\) and for \(i \geq 2\), as long as \(r_{i-1} \neq 0\), let \(r_i\) be the remainder when dividing \(r_{i-2}\) by \(r_{i-1}\). Let \(n\) be maximal with \(r_n \neq 0\), and set \(d = r_n\). Then \(d = (a, b)\).

Algorithm 17 (Extended Euclidean algorithm). Given \(a, b\), let \(q_i\) be the quotient arising in the \(i\)th step of the algorithm, so that \(r_{i-1} = r_iq_i + r_{i+1}\). Then we can find \(x, y\) with
\[ax + by = d\]
as follows: let \(s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1\), and then for \(i > 1\) let
\[s_i = s_{i-2} - q_{i-1}s_{i-1}, \text{ and } t_i = t_{i-2} - q_{i-1}t_{i-1}.\]
Then
\[(a, b) = s_na + t_nb.\]

Algorithm 18 (Trial division). Given an integer \(a > 1\):
(I) Let \(S = \{p_1 < \cdots < p_n\}\) be the primes less than or equal to \(\sqrt{a}\).
(II) Let \(i = 1\), and \(b = a\).
(III) divide \(p_i\) into \(b\) as many times as possible, and let \(e_i\) be the largest integer such that \(p_i^{e_i}|b\)
(so that \(e_i > 0\) if and only if \(p_i|b\).
(IV) If $e_i > 0$, replace $b$ by $b/p_i^{e_i}$, update $S$ by removing any primes larger than the new value of $\sqrt{b}$.

(V) If $p_{i+1}$ is still in $S$, increase $i$ and return to step (III). Otherwise, stop.

If $n'$ is the final number of primes tested, the prime factorization of $a$ is
$$p_1^{e_1} \cdots p_{n'}^{e_{n'}} \cdot a/(p_1^{e_1} \cdots p_{n'}^{e_{n'}}).$$

Algorithm 19 (Sieve of Eratosthenes). Given an integer $a > 1$, to find all primes less than or equal to $a$:

(I) start by writing all integers greater than 1 and less than or equal to $a$.

(II) Let $b$ be the smallest number in the list (2, to start with).

(III) $b$ is prime. Go over the list, removing all multiples of $b$.

(IV) If the next entry on the list is not bigger than $\sqrt{a}$, replace $b$ by it, and return to step (III). Otherwise, stop. The remaining numbers are the primes.