MATH3044 Number Theory

Cheatsheet

2022/23

This document collects together the important definitions and results presented throughout the lecture notes. The numbering used throughout will be consistent with that in the lecture notes.

Contents

1 Prime Factorisation

Reminder: The set of natural numbers in this module is $\mathbb{N} := \{0, 1, 2, ..., \}$ (including zero). In contrast, the set of positive integers in this module is $\mathbb{Z}^+ := \{1, 2, 3, ...\}$ (excluding zero).

1.1 Greatest Common Divisors

Definition 1.1.1 Let $n, d \in \mathbb{Z}$. We say that d is a divisor (or factor) of n if there exists $q \in \mathbb{Z}$ such that $n = qd$. In this case, we write $d \mid n$. If d is **not** a divisor, we write $d \nmid n$.

Remark If $d \mid a$ and $d \mid b$, then we have $d \mid (ax + by)$ for any $x, y \in \mathbb{Z}$. Indeed, by assumption there exist $q_1, q_2 \in \mathbb{Z}$ with $a = q_1 d$ and $b = q_2 d$. Thus, $ax + by = (q_1 x + q_2 y)d =: qd$, which satisfies Definition 1.1.1 since $\mathbb{Z}$ is closed under addition and multiplication (it is a *ring*).

Note: Furthermore, if $a \mid b$ and $b \mid c$, then $a \mid c$. In words, this says divisors are transitive.

Definition 1.1.3 If $a, b \in \mathbb{Z}$ are **not both** zero, then their greatest common divisor (or highest common factor) is the largest $d \in \mathbb{Z}^+$ that is a factor of both a and b. We denote this by $\gcd(a, b)$ or $\mathrm{hcf}(a, b)$ or simply (a, b).

We extend Definition 1.1.3 by declaring $\gcd(0, 0) := 0$, so we now work with any pair of integers.

Definition If $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, then we call them coprime (or relatively prime).

Lemma 1.1.5 (Division Algorithm) *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then, there exist some $q, r \in \mathbb{Z}$ (called the quotient and remainder, respectively) with $0 \leq r < |b|$ such that $a = qb + r$.*

Proof: Suppose first that $b > 0$ and let $q \in \mathbb{Z}$ be the largest integer where $qb \leq a$. By this assumption, we must have that $a < (q + 1)b$. We now define $r := a - qb$ and claim this satisfies the inequality. Indeed, what we have so far is $qb \leq a < (q + 1)b = qb + b$, and subtracting qb from everything yields $0 \leq a - qb < b$, the middle being precisely r.

Next, if $b < 0$, we know that $-b > 0$ so we can find $q', r \in \mathbb{R}$ from the argument above such that $a = q'(-b) + r$. If we then absorb the minus into the q' and relabel (setting $q := -q'$), then this is $a = qb + r$. The fact that $0 \leq r < |b|$ is again a consequence of the case above. □

Theorem 1.1.7 (Bézout's Lemma) *For every $a, b \in \mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that*

$$\gcd(a, b) = sa + tb.$$

Moreover, if $a, b > 0$, we can always find s and t where they satisfy $s > 0$ and $t < 0$.

Proof: If $a = b = 0$, then $s = t = 0$ satisfies the result. Now, suppose at least one of $a, b \neq 0$; this means there exist **positive** integers expressible in the form $sa + tb$ (e.g. $|a|$ if $a \neq 0$). So let $h \in \mathbb{Z}$ be the smallest such of these integers. We aim to prove that $h = \gcd(a, b)$.

Since $h > 0$, we can apply the Division Algorithm to write $a = qh + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < h$. But now, the remainder is nothing more than

$$r = a - qh = a - q(sa + tb) = (1 - qs)a + tb.$$

This is a linear combination of a and b, so by the minimality of h, the only option is to have $r = 0$ (since $r < h$ when we apply the Division Algorithm). Therefore, $h \mid a$ and $h \mid b$, showing that $h \leq \gcd(a, b)$. Conversely, $\gcd(a, b)$ divides both a and b, so it divides any linear combination. In particular, $\gcd(a, b) \mid h$ which means $\gcd(a, b) \leq h$. Combining these gives us equality. Finally, if $a, b > 0$, then we can find a sufficiently large $k \in \mathbb{Z}$ ensuring the following inequalities are true:

$$s' \coloneqq s + kb > 0 \qquad \text{and} \qquad t' \coloneqq t - ka < 0.$$

But clearly $s'a + t'b = sa + kba + tb - kba = sa + tb = \gcd(a, b)$, so we are done. □

> **Note:** We haven't yet found a concrete process for computing greatest common divisors or the integers s and t in Bézout's Lemma. But don't fear; we do this in the next section.

1.2 Euclid's Algorithm

Theorem 1.2.1 (Euclid's Algorithm) *Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and we obtain the following:*

$$\begin{aligned}
a &= q_1 b + r_1, && \text{for } 0 \leq r_1 < |b_1|, \\
b &= q_2 r_1 + r_2, && \text{for } 0 \leq r_2 < r_1, \\
r_1 &= q_3 r_2 + r_3, && \text{for } 0 \leq r_3 < r_2, \\
&\vdots && \vdots \\
r_{k-2} &= q_k r_{k-1} + r_k, && \text{for } 0 \leq r_k < r_{k-1}.
\end{aligned}$$

The algorithm terminates when $r_k = 0$ for some $k \in \mathbb{Z}^+$. Consequently, $\gcd(a, b) = r_{k-1}$.

Proof: First, the algorithm terminates because $|b| > r_1 > r_2 > \cdots \geq 0$ so there will certainly be some k such that $r_k = 0$. We now just need to show that $\gcd(a, b) = r_{k-1}$. Indeed, the last few steps of the algorithm are as follows:

$$\begin{aligned}
r_{k-4} &= q_{k-2} r_{k-3} + r_{k-2}, && \text{for } 0 \leq r_{k-2} < r_{k-3}, \\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}, && \text{for } 0 \leq r_{k-1} < r_{k-2}, \\
r_{k-2} &= q_k r_{k-1} + r_k, && \text{for } 0 \leq r_k < r_{k-1}.
\end{aligned}$$

Because $r_k = 0$, the final line tells us that $r_{k-1} \mid r_{k-2}$. But by using the second-to-last line, we therefore conclude that $r_{k-1} \mid r_{k-2}$. Proceeding like this up the whole ladder of equalities, we

conclude that $r_{k-1} \mid r_j$ for every j, ending with $r_{k-1} \mid b$ and $r_{k-1} \mid a$. This means it is at least a common divisor, so $r_{k-1} \leq \gcd(a, b)$. On the other hand, we can again work backwards to obtain

$$\begin{aligned} r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2} \\ &= r_{k-3} - q_{k-1}(r_{k-4} - q_{k-2} r_{k-3}) && \text{(substituting for } r_{k-2}\text{)} \\ &= (1 - q_{k-1} q_{k-2}) r_{k-3} - q_{k-1} r_{k-4} \\ &= (1 - q_{k-1} q_{k-2})(r_{k-5} - q_{k-3} r_{k-4}) - q_{k-1} r_{k-4} && \text{(substituting for } r_{k-3}\text{)} \\ &\vdots \\ &= ma + nb, \end{aligned}$$

for some $m, n \in \mathbb{Z}$ given in terms of the quotients and remainders . What this establishes is that r_{k-1} is a linear combination of a and b, which means that $\gcd(a, b) \mid r_{k-1}$, so $\gcd(a, b) \leq r_{k-1}$. Combining both inequalities gives us an equality. □

Corollary 1.2.3 *Let $a, b, n \in \mathbb{Z}$. Then, we have the following:*

(i) *If $n \mid a$ and $n \mid b$, then $n \mid \gcd(a, b)$.*
(ii) *If $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.*
(iii) *If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.*
(iv) *If $\gcd(a, b) = 1$ with $a \mid n$ and $b \mid n$, then $ab \mid n$.*

Proof: (i) If $n \mid a$ and $n \mid b$, then we see that $n \mid (sa + tb)$ for any $s, t \in \mathbb{Z}$. But by Bézout's Lemma, we can find s and t such that $sa + tb = \gcd(a, b)$; this gives the result.

(ii) Using Bézout's Lemma, there exist $s, t \in \mathbb{Z}$ such that $\gcd(a, n) = sa + tn = 1$. Multiplying by b tells us that $sab + tnb = b$. Combined with the fact $n \mid ab$ and $n \mid n$, we see that n divides the entire of the left-hand side, so $n \mid b$.

(iii) Suppose $d \mid ab$ and $d \mid n$ is an arbitrary common divisor. We note that $\gcd(a, n) = 1$ implies $\gcd(a, d) = 1$, so $d \mid b$ by part (ii) above (substitute $n = d$ into the statement). Therefore, d is a divisor of both n and b, so we must have $d \leq \gcd(b, n) = 1$. We thus must have $d = 1$.

(iv) Using Bézout's Lemma, there exist $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb = 1$. Multiplying by n tells us that $san + tbn = n$. Because $a \mid n$ and $b \mid n$, we know there exist $q_1, q_2 \in \mathbb{Z}$ such that $n = q_1 a$ and $n = q_1 b$. Substituting these into the multiplied equation tells us that $n = sa(q_2 b) + tb(q_1 a) = (sq_2 + tq_1)ab$, so $ab \mid n$ as required. □

1.3 Prime Numbers

Definition 1.3.1 An integer $p > 1$ is prime if its only positive factors are one and itself. If an integer is **not** prime, it is called a composite.

Note: Another neat definition is this: a prime is a positive integer with exactly two **distinct** positive factors. Of course, one and itself always satisfy this, so "exactly two" ensures the usual notion of a prime and "distinct" ensures that 1 is **not** classed as a prime number.

Lemma 1.3.2 *Let p be prime and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof: Suppose $p \nmid a$. Then, $\gcd(a, p) = 1$ and Corollary 1.2.3(ii) implies that $p \mid b$. □

Note: We extend Lemma 1.3.2 inductively: if $p \mid (a_1 \cdots a_n)$, then $p \mid a_i$ for at least one i.

Theorem 1.3.3 *Every positive integer can be written as a product of primes.*

Proof: Let $n \in \mathbb{Z}^+$. For ease, we consider $n > 1$ (note that $n = 1$ can be considered as the "empty product" of primes, so it satisfies the theorem vacuously). Suppose to the contrary that n is the least integer that can **not** be written as a product of primes. Then, n itself is not prime (otherwise it is the trivial product of one prime). We can therefore factorise it as $n = ab$ where $1 < a < n$ and $1 < b < n$. Because n is the smallest such where this property fails, we know that each of q and s are a product of primes, say $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$. But then we see that $n = p_1 \cdots p_r q_1 \cdots q_s$ is a product of primes, a contradiction. □

Theorem 1.3.4 (Euclid's Theorem) *There are infinitely-many primes.*

Proof: Suppose for a contradiction there are finitely-many primes, say $p_1, ..., p_r$. We consider the number $n \coloneqq p_1 \cdots p_r + 1$, that is multiply the finite list of primes and add one. If n is prime, this isn't on our list and we have a contradiction. If n is composite, we can write n as a product of primes, say $n = q_1 \cdots q_s$, by Theorem 1.3.3. But each $p_i \nmid n$ which means q_1 is a new prime number not on our list, another contradiction. □

Theorem 1.3.6 (Fundamental Theorem of Arithmetic) *Every $n > 1$ can be expressed as a unique product of primes up to order, that is if $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ where p_i, q_j are primes, then $r = s$ and the p_i and q_j can be paired-off so they are equal within pairs.*

Proof: Suppose this is not the case and let n be the smallest integer which can be written as a product of primes in **different** ways, say $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$. The first tells us that $p_1 \mid n$, so the second implies $p_1 \mid (q_1 \cdots q_s)$. By (the extension of) Lemma 1.3.2, we know that $p_1 \mid q_j$ for some j. Because q_j is also prime, we must have that $p_1 = q_j$. Cancelling p_1, we obtain $p_2 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s$. Repeating this with $p_2, ..., p_r$, we pair-off each p_i with some q_j, but then we have that $r = s$, a contradiction to distinct products. □

Remark 1.3.8 Using the Fundamental Theorem of Arithmetic to write two positive integers $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ as a product of prime powers, we obtain the following:

$$\gcd(n, m) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)},$$
$$\operatorname{lcm}(n, m) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}.$$

2 Modular Arithmetic

2.1 Congruences

Definition 2.1.1 Let $a, b, m \in \mathbb{Z}$ with $m > 1$. We say a and b are congruent modulo m if there exists $k \in \mathbb{Z}$ with $a = b + km$, meaning $m \mid (a - b)$. This is denoted $a \equiv b \pmod{m}$. Otherwise, we say that they are incongruent modulo m and write $a \not\equiv b \pmod{m}$.

Lemma *Let $a, b, m \in \mathbb{Z}$ with $m > 1$. Then, $a \equiv b \pmod{m}$ if and only if a and b have the same remainder on dividing by m. In particular, $a \equiv 0 \pmod{m}$ is equivalent to $m \mid a$.*

Proof: ($\Rightarrow$) Let $a \equiv b \pmod{m}$, meaning $a = b + km$ for some $k \in \mathbb{Z}$. If we apply the Division Algorithm to a on dividing by m, we can write$a = qm + r$. But then, $qm + r = b + km$ which is equivalent to $b = (q - k)m + r$, so the remainder on diving b by m is also r.

($\Leftarrow$) Let r be the common remainder upon dividing a and b each by m, meaning $a = pm + r$ and $b = qm + r$ for some $p, q \in \mathbb{Z}$. But then, we see that $a - pm = b - qm$ and this rearranges to $a = b + (p - q)m$ and thus Definition 2.1.1 is satisfied with $k = p - q$. □

Note: Each integer is congruent modulo m to exactly one of $0, 1, ..., m - 1$ (which we can shift by one to be $1, 2, ..., m$). We then call these the "complete set of residues modulo m"

Reminder: An equivalence relation on a set X is a relation $\sim$ satisfying these properties:

(i) For all $x \in X$, we have $x \sim x$. (**Reflexivity**)

(ii) For all $x, y \in X$, we have $x \sim y \Rightarrow y \sim x$. (**Symmetry**)

(iii) For all $x, y, z \in X$, we have $x \sim y$ and $y \sim z \Rightarrow x \sim z$. (**Transitivity**)

Proposition *Congruence modulo m is an equivalence relation.*

Proof: We need to verify the three properties in the above reminder for $a, b, c, m \in \mathbb{Z}$ with $m > 1$.

(i) We see that $a \equiv a \pmod{m}$ by virtue of taking $k = 0$ in Definition 2.1.1.

(ii) Let $a \equiv b \pmod{m}$, meaning $a = b + km$ for $k \in \mathbb{Z}$. We can re-write this as $b = a - km$; this satisfies Definition 2.1.1e, so $b \equiv a \pmod{m}$.

(iii) Let $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, meaning $a = b + km$ and $b = c + lm$ for $k, l \in \mathbb{Z}$. Substituting gives $a = c + (k + l)m$; this satisfies Definition 2.1.1, so $a \equiv c \pmod{m}$. □

Lemma 2.1.3 (Arithmetic of Congruences) *Congruence modulo m is compatible with addition, subtraction, multiplication and powers. In other words, for $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then, we have the following:*

(i) $a + c \equiv b + d \pmod{m}$.
(ii) $a - c \equiv b - d \pmod{m}$.
(iii) $ac \equiv bd \pmod{m}$.
(iv) $a^n \equiv b^n \pmod{m}$.

Proof: Throughout, we are assuming that $a = b + km$ and $c = d + lm$ for some $k, l \in \mathbb{Z}$.

(i) Here, $a + c = (b + d) + (k + l)m$, which shows $a + c \equiv b + d \pmod{m}$.

(ii) Next, $a - c = (b - d) + (k - l)m$, which shows $a - c \equiv b - d \pmod{m}$.

(iii) Now, $ac = (b + km)(d + lm) = bd + (bl + dk + kl)m$, implying $ac \equiv bd \pmod{m}$.

(iv) Finally, $a^n = (b + km)^n = b^n + \Big(\sum_{i=1}^{n} \binom{n}{i} b^{n-i} k^i m^{i-1} \Big) m$, implying $a^n \equiv b^n \pmod{m}$. □

Lemma 2.1.4 (Cancellation) *Let $a, m \in \mathbb{Z}$ with $m > 1$. If $\gcd(a, m) = 1$, then there exists some $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$.*

Proof: By Bézout's Lemma, we can write $\gcd(a, m) = sa + tm = 1$ for some $s, t \in \mathbb{Z}$. Applying congruence modulo m, we see that $sa \equiv 1 \pmod{m}$ and thus $b = s$ is the desired integer. □

Note: We see Lemma 2.1.4 implies these **only when** $\gcd(a, m) = 1$ and $ab \equiv 1 \pmod{m}$:
- If $ax \equiv c \pmod{m}$, then $abx \equiv bc \pmod{m}$, meaning $x \equiv bc \pmod{m}$.
- If $ax \equiv ay \pmod{m}$, then $abx \equiv aby \pmod{m}$, meaning $x \equiv y \pmod{m}$.

Remark The condition that $\gcd(a, m) = 1$ is absolutely necessary for Lemma 2.1.4 and the above note to hold true. For example, $8 \equiv 12 \pmod{4}$ but dividing by two fails since $4 \not\equiv 6 \pmod{4}$.

2.2 Fermat's Little Theorem

Reminder: The factorial of a positive integer $n \in \mathbb{Z}^+$ is the product $n! := n \cdot (n-1) \cdots 2 \cdot 1$.

Theorem 2.2.3 (Fermat's Little Theorem 1) *Let p be prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider the numbers $a, 2a, ..., (p-1)a$ and note that **none** are congruent to zero modulo p. This is because $p \nmid a$ and, since it is prime, it also doesn't divide any of the coefficients $1, 2, ..., p-1$. Furthermore, $\gcd(a, p) = 1$ by primality and so Lemma 2.1.4 tells us that $ra \equiv sa \pmod{p}$

implies $r \equiv s \pmod{p}$. Therefore, $a, 2a, ..., (p-1)a$ are congruent in some order to $1, 2, ..., p-1$. If we multiply these numbers together, we obtain $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$. Since $(p-1)!$ is coprime to p, we simply cancel to obtain the intended $a^{p-1} \equiv 1 \pmod{p}$. □

Corollary 2.2.4 (Fermat's Little Theorem 2) *If p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.*

Proof: If $p \mid a$, then $a \equiv 0 \pmod{p}$ and therefore $a^p \equiv 0 \pmod{p}$ so the result holds. Otherwise, $p \nmid a$ and we use Theorem 2.2.3 to conclude $a^{p-1} \equiv 1 \pmod{p}$; then just multiplying by a. □

Definition A Mersenne prime is a prime number of the form $2^r - 1$ where $r \in \mathbb{Z}$.

Remark 2.2.5 It turns out if the number $2^r - 1$ is prime, then r is prime (proved in an exercise sheet). The converse is **not** true, e.g. $r = 11$ is prime but $2^{11} - 1 = 2047 = 23 \cdot 89$ is composite.

Theorem 2.2.6 *Let $r > 2$ be prime. Every prime factor of $2^r - 1$ is of the form $2kr + 1$.*

Proof: Let p be a prime factor of $2^r - 1$, meaning that $p \mid (2^r - 1)$ and therefore $2^r \equiv 1 \pmod{p}$. But we know by Fermat's Little Theorem that $2^{p-1} \equiv 1 \pmod{p}$. We aim to show that $2r \mid (p-1)$ since this is equivalent to $p - 1 = 2kr$ which rearranges to the form we wish to prove. Of course, $2 \mid (p-1)$ since $p > 2$ is a prime (because $2^r - 1$ is odd so it has no even factors) and thus one less is even. Since $\gcd(r, 2) = 1$, it suffices to show that $r \mid (p-1)$. Therefore, suppose to the contrary that $r \nmid (p-1)$. Because r is prime, we have $\gcd(r, p-1) = 1$. Applying Bézout's Lemma tells us $sr + t(p-1) = 1$ for some $s, t \in \mathbb{Z}$ with $s > 0$ and $t < 0$. If we define $m := -t$, we can write $sr = 1 + m(p-1)$. Exponentiating, we see that $2^{sr} = 2^{1+m(p-1)}$. However, we have

$$2^{sr} \equiv (2^r)^s \equiv 1^s = 1 \pmod{p} \qquad \text{and} \qquad 2^{1+m(p-1)} = 2(2^{p-1})^m \equiv 2(1)^m = 2 \pmod{p}.$$

Therefore, $1 \equiv 2 \pmod{p}$ which is false; this is the contradiction we were after. □

Method – Mersenne Numbers: Suppose we want to determine if $2^r - 1$ is prime.
(i) Check that r is prime.
(ii) Use Theorem 2.2.6 to look for factors of the form $2kr + 1$.
(iii) Reduce 2^r modulo $2kr + 1$; if you reach 1, then $2^r - 1$ is composite.

2.3 Wilson's Theorem

Theorem 2.3.1 (Wilson's Theorem) *For p prime, we have $(p-1)! \equiv -1 \pmod{p}$.*

Proof: For $p = 2, 3$ it is clear, so suppose $p > 3$ is prime. We will show that $2, 3, ..., p-2$ can be paired-off such that the products within each pair are congruent to one modulo p. Indeed, let $a \in \{1, 2, ..., p-1\}$. Since $\gcd(a, p) = 1$, we know there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{p}$ by

Lemma 2.1.4. We can replace b by its remainder modulo p (which is clearly non-zero) so we can always assume that $b \in \{1, 2, ..., p\}$. Furthermore, we get uniqueness by applying cancellation.

However, the situation $b = a$ occurs if and only $a^2 \equiv 1 \pmod{p}$; this is equivalent to $p \mid (a^2 - 1)$. Since we can factorise $a^2 - 1 = (a-1)(a+1)$, Lemma 1.3.2 implies that $p \mid (a-1)$ ir $p \mid (a+1)$. Since $a \in \{1, 2, ..., p-1\}$, this means either $a = 1$ or $a = p - 1$. Therefore, we pair-off the remaining integers $2, 3, ..., p-2$ with a being matched to its corresponding b. Consequently,

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p} \qquad \Leftrightarrow \qquad (p-2)! \equiv 1 \pmod{p}.$$

As a result, we see that $(p-1)! = (p-1) \cdot (p-2)! \equiv p - 1 \equiv -1 \pmod{p}$. □

Corollary 2.3.3 *Let p be prime. Then, the congruence equation $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p = 2$ or $p \equiv 1 \pmod{4}$, that is $p = 4k + 1$ for some $k \in \mathbb{Z}$.*

Proof: The $p = 2$ case is trivial; take $x = 1$. We assume $p > 2$, in particular that $p - 1$ is even.

($\Rightarrow$) Let $x = a$ be a solution, so $a^2 \equiv -1 \pmod{p}$. Applying Fermat's Little Theorem yields

$$1 \equiv a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

This tells us that $\frac{p-1}{2}$ is even and therefore $4 \mid (p-1)$; this is equivalent to $p \equiv 1 \pmod{4}$.

($\Leftarrow$) Suppose $p \equiv 1 \pmod{4}$ and notice $p - k \equiv -k \pmod{p}$ for every $1 \leq k \leq \frac{p-1}{2}$. Then,

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2) \cdot (p-1) \\
&= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdots (-2) \cdot (-1) \\
&= \left(\frac{p-1}{2}\right)! \cdot (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \\
&= (-1)^{\frac{p-1}{2}} \cdot \left(\left(\frac{p-1}{2}\right)!\right)^2.
\end{aligned}$$

By Wilson's Theorem, the left-hand side is congruent to -1 modulo p. Given that $p \equiv 1 \pmod{4}$, this tells us that $\frac{p-1}{2}$ is even, in particular the final line above is positive. Hence, we can take

$$x = \left(\frac{p-1}{2}\right)!.$$

□

2.4 Chinese Remainder Theorem

Theorem 2.4.1 (Chinese Remainder Theorem) *Let $a_1, ..., a_k \in \mathbb{Z}$ and suppose $m_1, ..., m_k > 1$ are pairwise coprime. Then, the following simultaneous congruences has a solution $x \in \mathbb{Z}$:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

Moreover, the solution is unique up to congruence modulo $m_1 m_2 \cdots m_k$.

Proof: We prove this for $k = 2$ (the general case follows by induction). Bézout's Lemma tells us there exist $s, t \in \mathbb{Z}$ with $sm_1 + tm_2 = 1$ by the fact the m_i are pairwise coprime. We claim that $x = sm_1a_2 + tm_2a_1$ is a solution. Justifying this amounts to showing the congresses are satisfied:

$$\begin{aligned} x &= sm_1a_2 + (1 - sm_1)a_1 \equiv a_1 \pmod{m_1}, \\ x &= (1 - tm_2)a_1 + tm_1a_2 \equiv a_2 \pmod{m_2}. \end{aligned}$$

As for uniqueness up to congruence, suppose $y \in \mathbb{Z}$ is another solution, meaning that $y \equiv a_i \pmod{m_i}$, which is equivalent to $y \equiv x \pmod{m_i}$ and therefore $m_i \mid (y - x)$. Consequently, y is a solution if and only if **both** m_1 and m_2 divide $y - x$. Since the m_i are coprime, it is equivalent to their product dividing $y - x$, meaning $y \equiv x \pmod{m_1 m_2}$. □

Note: Denote the residues modulo m by $\mathbb{Z}_m$ and let $M \coloneqq m_1 m_2 \cdots m_k$. In this notation, a *non-constructive* proof of the Chinese Remainder Theorem is to show that this is bijective:

$$f : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}, \qquad f(a + M\mathbb{Z}) = (a + m_1\mathbb{Z}, ..., a + m_k\mathbb{Z}).$$

Remark 2.4.2 The idea to take $x = sm_2a_1 + tm_1a_2$ in the proof of the Chinese Remainder Theorem seems to come at random, so we will justify this here. Indeed, if we solve the first congruence $x \equiv a_1 \pmod{m_1}$, then we get $x = a_1 + km_1$ for some $k \in \mathbb{Z}$ (this is immediate from Definition 2.1.1). Substituting this into the second equation gives us

$$km_1 \equiv a_2 - a_1 \pmod{m_2}.$$

Using Lemma 2.1.4, there exists $s \in \mathbb{Z}$ such that $sm_1 \equiv 1 \pmod{m_2}$. Furthermore, we can take the same s as in Bézout's Lemma because $sm_1 + tm_2 = 1$ implies that $sm_1 \equiv 1 \pmod{m_2}$ by reducing modulo m_2. Multiplying both sides of the above stand-alone equation by s gives

$$ksm_1 \equiv s(a_2 - a_1) \pmod{m_2} \qquad \Rightarrow \qquad k \equiv s(a_2 - a_1) \pmod{m_2}.$$

Therefore, we can simply take $k = s(a_2 - a_1)$ and substituting this into the first solution for x produces exactly what we expect, namely $x = sm_2a_1 + tm_1a_2$.

3 Euler's Totient Function

3.1 Euler's Totient Function

Definition 3.1.1 For $n \in \mathbb{Z}^+$, the totient of n is the number of integers k with $1 \leq k \leq n$ which are coprime to n, that is $\gcd(n, k) = 1$. The totient is a function denoted $\phi(n)$.

Remark 3.1.3 The integers from 1 to n that are coprime to n are a group under multiplication modulo n, denoted $\mathbb{Z}_n$ since its elements are residues modulo n. The group's order is just $\phi(n)$.

Note: We have always that $\phi(1) = 1$ and $\phi(p) = p - 1$, where p is a prime number.

Notation We can work with either $\{1, 2, ..., n\}$ or with $\{0, 1, ..., n-1\}$; it really doesn't matter.

Lemma 3.1.4 *If $m, n \in \mathbb{Z}^+$ are coprime, then $\phi(m)\phi(n) = \phi(mn)$.*

Proof: Let $f : \{0, 1, ..., m-1\} \to \{0, 1, ..., m-1\} \times \{0, 1, ..., m-1\}$ given by $f(x) = (a, b)$ where $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, that is it sends an element to the pair of remainders upon division by each of m and n. By the Chinese Remainder Theorem, this map is a bijection. Note that x is coprime to mn is equivalent to x being coprime with each of m and n separately by Corollary 1.2.3(iii), but this is equivalent to $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$. By definition, there are $\phi(m)$ possibilities for a and $\phi(n)$ possibilities for b, so there are $\phi(m)\phi(n)$ possibilities for the pair (a, b). In other words, there are $\phi(m)\phi(n)$ possible x which are coprime to mn, but this is just $\phi(mn)$ by Definition 3.1.1. □

Definition We say f is multiplicative if $f(1) = 1$ and $f(ab) = f(a)f(b)$ for **coprime** $a, b \in \mathbb{Z}$. We say f is completely multiplicative if $f(1) = 1$ and $f(ab) = f(a)f(b)$ for **every** $a, b \in \mathbb{Z}$.

We have therefore established in Lemma 3.1.4 that the totient function ϕ is multiplicative.

Remark 3.1.5 There are many important multiplicative functions in number theory such as these:

- The function $d(n)$, which outputs the number of positive factors of n.
- The function $\sigma(n)$, which outputs the sum of positive factors of n.
- The function $\sigma_k(n)$, which outputs the sum of the k^{th} powers of the positive factors of n.

  Note: We have $\sigma_0(n) = d(n)$ and $\sigma_1(n) = \sigma(n)$, so this covers the first two examples.

- The Möbius function $\mu(n)$ which is defined as follows:

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^k, & \text{if } n \text{ is a product of } k \text{ distinct primes} \\ 0, & \text{otherwise} \end{cases}.$$

3.2 Euler's Theorem

Theorem 3.2.1 *Let p be prime. Then, for a prime power p^α with $\alpha \in \mathbb{Z}^+$, we have*

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

In general, writing $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ as a product of powers of distinct primes, we obtain

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Proof: If p is prime, then $\phi(p^\alpha)$ is the number of integers in $1, 2, ..., p^\alpha$ that are coprime to p^α, by definition. But the numbers in this range that have a common divisor with p^α are the multiplies of p since it is prime, namely $p, 2p, ..., p^\alpha$ and there are $p^{\alpha-1}$ of them. Therefore, we see that

$$\phi(p) = p^\alpha - p^{\alpha-1},$$

which factorises in the necessary way. Lemma 3.1.4 implies ϕ is multiplicative, so the result for any $n \in \mathbb{Z}$ written as a product of powers of distinct primes follows immediately. □

Note: For $n > 2$, the totient $\phi(n)$ is even. Indeed, $\phi(n)$ counts the number of k such that $\gcd(n, k) = 1$, but $\gcd(n, n-k) = \gcd(n, k)$ so each k gives rise to two coprime integers: k itself and $n - k$. The degenerate situation $k = n - k$ has $\gcd(n, k) \neq 1$ so it doesn't count.

Theorem 3.2.3 (Euler's Theorem) *If $a, n \in \mathbb{Z}$ are coprime, then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof: Let $r_1, ..., r_{\phi(n)}$ be the numbers amongst $0, 1, ..., n-1$ that are coprime to n. Note that the numbers $ar_1, ..., ar_{\phi(n)}$ are pairwise incongruent modulo n. Indeed, if $ar_i \equiv ar_j \pmod{n}$, then $r_i \equiv r_j \pmod{n}$ by cancellation, so the only option here is $r_i = r_j$. This establishes that $ar_1, ..., ar_{\phi(n)}$ are congruent modulo n to $r_1, ..., r_{\phi(n)}$ in some order. So taking products yields

$$(ar_1) \cdots (ar_{\phi(n)}) \equiv r_1 \cdots r_{\phi(n)} \pmod{n}.$$

Because $\gcd(n, r_i) = 1$ for each i, we can cancel them all to obtain $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Remark 3.2.4 It turns out Euler's Theorem is a generalisation of Fermat's Little Theorem. Indeed, notice that Theorem 2.2.3 is a special case with n being prime, wherein $\phi(n) = n - 1$.

Method – Finding the Last Digits: Suppose we wish to find the last n digits of k. The objective is to reduce k using congruence modulo 10^n; we can speed it up slightly.

(i) Apply Euler's Theorem to see that $x^{\phi(10^n)} \equiv 1 \pmod{10^n}$.
(ii) Write k as a product involving a power of $\phi(10^n)$.
(iii) Use Step (i) to eliminate a factor in Step (ii).
(iv) Continue to reduce modulo 10^n until the result is less than 10^n.

3.3 Gauss' Theorem

Theorem 3.3.1 (Gauss' Theorem) *Let $n \in \mathbb{Z}^+$. Then, the sum of divisors $\sum_{d|n} \phi(d) = n$.*

Proof: For each positive $d \mid n$, define the set $S_d \coloneqq \{m \in \mathbb{Z} : 1 \leq m \leq n \text{ and } \gcd(m,n) = d\}$. Thus, $m \in S_d$ if and only if $d \mid m$ and $\gcd(m/d, n/d) = 1$. The size of this set is $|S_d| = \phi(n/d)$. Furthermore, each m lies in exactly **one** of these sets, namely with $d = \gcd(m,n)$. As a result,

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right).$$

But d is a factor of n if and only if n/d is a factor of n. This allows us to re-order the sum on the right-hand side above and replace n/d with d, giving the result. □

Note: The S_d partition the set $\{1, 2, ..., n\}$, meaning we can write this set as a union of the S_d such that no two different S_d's contains a common element. This implies $n = \sum_{d|n} |S_d|$.

4 Primitive Roots

4.1 Orders and Primitive Roots

Definition 4.1.1 Let $a, n \in \mathbb{Z}$ be coprime. The order of a modulo n is the smallest $d > 0$ satisfying the congruence $a^d \equiv 1 \pmod{n}$.

Remark The order modulo n always exists as a result of Euler's Theorem; we know that $\phi(n)$ satisfies the condition. However, it may be there is a smaller integer which is congruent to one. Similar reasoning tells us that the order of an element modulo n is at most $\phi(n)$.

Proposition 4.1.2 *Let $n > 1$ with $\gcd(n, 10) = 1$. Then, the decimal expansion of $1/n$ recurs with period d, where d is the order of 10 modulo n*

Proof: The period of $1/n$ is the least integer $d > 0$ such that the following is an integer:

$$10^d \cdot \left(\frac{1}{n}\right) - \frac{1}{n}.$$

We can rearrange this to say that $10^d - 1 = kn$ for some $k \in \mathbb{Z}$. Therefore, we are looking for the smallest $d > 0$ such that $n \mid (10^d - 1)$, but this is precisely to say $10^d \equiv 1 \pmod{n}$, that is d is the order of 10 modulo n. □

Lemma 4.1.3 *Let $a, n \in \mathbb{Z}$ be coprime and suppose that a has order d modulo n. Then, $a^m \equiv 1 \pmod{n}$ if and only if $d \mid m$. In particular, we conclude that $d \mid \phi(n)$.*

Proof: ($\Leftarrow$) If $d \mid m$, we have $m = kd$ for some $k \in \mathbb{Z}$. Therefore, $a^m = (a^d)^k \equiv 1^k = 1 \pmod{n}$.

($\Rightarrow$) If $a^m \equiv 1 \pmod{n}$, then the Division Algorithm allows us to write $m = qd + r$ for some $0 \leq r < d$. We aim to show that $r = 0$. Indeed, we see that $a^m = (a^d)^q a^r \equiv a^r \pmod{n}$ by definition of order. However, we assume that this is congruent to one, so $a^r \equiv 1 \pmod{n}$. But because d is the order, it is the **least** integer satisfying this; the fact $r < d$ tells us we must have $r = 0$. This establishes that $m = qd$ which is equivalent to $d \mid m$. □

Note: The fact $d \mid \phi(n)$ in Lemma 4.1.3 is now a direct consequence of Euler's Theorem.

Definition 4.1.5 Let $a, n \in \mathbb{Z}$ be coprime. We say that a is a primitive root modulo n (or simply a primitive root **of** n) if the order of a is maximal, that is its order is exactly $\phi(n)$.

4.2 A Theorem of Lagrange

Theorem 4.2.1 (Lagrange's Theorem) *If p is prime and $f(x)$ is a polynomial of degree n with integer coefficients and leading coefficient (in front of x^n)* **not** *divisible by p, then the equation $f(x) \equiv 0 \pmod{p}$ has at most n pairwise incongruent solutions modulo p.*

Proof: We proceed by induction on n. The base case $n = 1$ and $f(x) = ax + b$ for $a, b \in \mathbb{Z}$ is clear: any two solutions x and y satisfy $ax + b \equiv ay + b \pmod{p}$ which means $ax \equiv ay \pmod{p}$, so $x \equiv y \pmod{p}$ by cancellation. We now assume the result holds for $n = k$. Suppose now that $f(x)$ has degree $k+1$. If there are no solutions modulo p, then the result is vacuously true. Otherwise, suppose $x = c$ is a solution. Polynomial division allows us to write

$$f(x) = q(x)(x - c) + r,$$

where $q(x)$ is a polynomial and $r \in \mathbb{Z}$. Since $f(c) \equiv 0 \pmod{p}$, we have $r \equiv 0 \pmod{p}$. Thus,

$$f(x) \equiv 0 \pmod{p} \qquad \Leftrightarrow \qquad x \equiv c \pmod{p} \text{ or } q(x) \equiv 0 \pmod{p}.$$

Because $x - c$ is linear and $f(x)$ has degree $n+1$, it means that $q(x)$ has degree n. Therefore, the inductive hypothesis tells us there are at most n incongruent solutions to $q(x) \equiv 0 \pmod{p}$. If we add to this the solution $x \equiv c \pmod{p}$, this gives us a total of $n+1$ incongruent solutions. □

Note: This means there are at most n solutions in any complete set of residues modulo p.

Corollary 4.2.2 *If p is prime and $d \mid (p-1)$, then the equation $x^d - 1 \equiv \pmod{p}$ has exactly d solutions up to congruence modulo p.*

Proof: By Fermat's Little Theorem, $x^{p-1} - 1 \equiv \pmod{p}$ has exactly $p - 1$ solutions modulo p, namely $1, 2, ..., p - 1$. Under the divisibility assumption, we write $p - 1 = kd$ for some $k \in \mathbb{Z}$, so

$$x^{p-1} - 1 = x^{kd} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1).$$

By the fact that p is prime, any solution to $x^{p-1} - 1 \equiv 0 \pmod{p}$ must also be a solution to

$$x^d - 1 \equiv 0 \pmod{p} \qquad \text{or} \qquad x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1 \equiv 0 \pmod{p}.$$

By Lagrange's Theorem, the second has at most $d(k-1)$ solutions modulo p, so the first must have at least $(p-1) - d(k-1) = kd - d(k-1) = d$ solutions modulo p. But Lagrange's Theorem says it has at most d solutions modulo p; it has exactly d incongruent solutions. □

Lemma 4.2.3 *Let $a \in \mathbb{Z}$ have order d modulo p, where p is some prime.*
(i) *The $a, a^2, ..., a^d$ are* **all** *incongruent solutions to $x^d - 1 \equiv 0 \pmod{p}$.*
(ii) *The a^k with $1 \leq k \leq d$ and $\gcd(k, d) = 1$ are* **all** *incongruent elements of order d.*

Proof: (i) We first show that the powers are pairwise incongruent. Indeed, if $a^i \equiv a^j \pmod{p}$ where $1 \leq i < j \leq d$ without loss of generality, then $a^{i-j} \equiv 1 \pmod{p}$, a contradiction to the fact that d is minimal (since it is the order of a). Moreover, these a^k are all solutions because

$$(a^k)^d - 1 = (a^d)^k - 1 \equiv 1^k - 1 = 0 \pmod{p}.$$

Therefore, Corollary 4.2.2 guarantees any solution is congruent to some a^k for $1 \leq k \leq d$.

(ii) If x be an element of order d, then it is a solution to $x^d - 1 \equiv \pmod{0}$; we aim to show that $\gcd(k, d) = 1$. To that end, we know $x \equiv a^k \pmod{p}$ for some $1 \leq k \leq 1$. So if c is a non-trivial common divisor of k and d, then $x^{d/c} \equiv (a^k)^{d/c} = (a^d)^{k/c} \equiv 1 \pmod{p}$, but this contradicts the fact that d is minimal (again because it is the order of a). Thus, $c = 1$ and we get $\gcd(k, d) = 1$. Conversely, let $\gcd(k, d) = 1$ and assume its order of a^k is e; we aim to show that $e = d$. Indeed, we can use Lemma 4.1.3 to determine that

$$e \mid m \qquad \Leftrightarrow \qquad (a^k)^m \equiv 1 \pmod{p} \qquad \Leftrightarrow \qquad d \mid km,$$

where $m \in \mathbb{Z}$ is some integer. But because $\gcd(k, d) = 1$, we know that $d \mid km$ implies $d \mid m$ by Corollary 1.2.3(ii). Since m is arbitrary, this is true for **every** m. This says that e is a divisor if and only if d is a divisor, which means $e = d$. □

4.3 Results about Existence of Primitive Roots

Theorem 4.3.1 *If p is prime, then it has $\phi(p-1)$ primitive roots modulo p.*

Proof: Suppose $d \mid (p-1)$ and let $\psi(d)$ denote the number of integers in the range $1, 2, ..., p-1$ that have order d modulo p. Then, every m in this range has order dividing $\phi(p) = p - 1$, and

$$p - 1 = \sum_{d|(p-1)} \psi(d).$$

Note that $\psi(d) \leq \phi(d)$. Indeed, either $\psi(d) = 0$ or $\psi(d) > 0$ in which case there exists an element of order d and then we have $\psi(d) = \phi(d)$ by Lemma 4.2.3. Applying this inequality above gives

$$p - 1 = \sum_{d|(p-1)} \psi(d) \leq \sum_{d|(p-1)} \phi(d) = p - 1,$$

with the last equality via Gauss' Theorem. But clearly this means that $\psi(d) = \phi(d)$ for all d. In particular, the number of primitive roots, namely $\phi(p-1)$, is precisely the same as $\psi(p-1)$. □

Note: This implies the existence of primitive roots modulo some prime. However, this is **not** true for composite numbers, e.g. there are **no** primitive roots modulo 8 since $\phi(8) = 4$ and its totatives (elements less than 8 coprime to it: $1, 3, 5, 7$) have orders $1 \neq 4$ or $2 \neq 4$.

Proposition 4.3.3 *Let $n = uv \in \mathbb{Z}$ with $u, v > 2$ coprime. Then, n has* **no** *primitive roots.*

Proof: Recall that $\phi(k)$ is even for $k > 2$. Using Lemma 3.1.4, we know that $\phi(n) = \phi(u)\phi(v)$ with each of $\phi(u)$ and $\phi(v)$ being even. Furthermore, for some $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, we have

$$a^{\phi(u)} \equiv \pmod{u} \qquad \text{and} \qquad a^{\phi(v)} \equiv 1 \pmod{v}.$$

We claim that $m = \frac{1}{2}\phi(n) = \frac{1}{2}\phi(u)\phi(v)$ is a solution to $a^m \equiv 1 \pmod{n}$. Indeed, we see that $\phi(u) \mid m$ and $\phi(v) \mid m$, which tells us that $a^m \equiv 1 \pmod{u}$ and $a^m \equiv 1 \pmod{v}$, respectively. Combining these and using the fact $n = uv$ implies the claim. Finally, since $m < \phi(n)$, it means that its order is strictly less than $\phi(n)$, so a is **not** a primitive root modulo n. □

Theorem 4.3.4 (Classification of Primitive Roots) *Let $n > 1$ be an integer. Then, n has a primitive root if and only if $n \in \{2, 4, p^k, 2p^k\}$ for some positive $k \in \mathbb{Z}^+$ and prime p.*

Proof: (**Non-examinable**) Omitted. □

5 Detecting Primality

5.1 Detecting Primality using Powers

Definition A **composite** $n \in \mathbb{Z}$ is a Carmichael number if $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$.

Remark The smallest Carmichael number is $531 = 3 \cdot 11 \cdot 17$. To verify that $a^{531} \equiv a \pmod{531}$, we can re-write this as $a^{530} \equiv 1 \pmod{531}$ and use the fact that 530 is divisible by 2, 10 and 16.

Note: Consequently, we cannot use Fermat's Little Theorem as a test for primality. This is because Carmichael numbers will pass the so-called test without actually being prime!

Proposition 5.1.3 *Let $n > 1$ and $p_1, ..., p_k$ be the distinct prime factors of $n - 1$. If*

$$\begin{cases} a^{n-1} \equiv 1 \pmod{n} \\ a^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n} \end{cases} \qquad (*)$$

for some $a \in \mathbb{Z}$ and every $i \in \{1, ..., k\}$, then n is prime.

Proof: The hypotheses imply that a has order $n - 1$ modulo n. Indeed, $\gcd(a, n) = 1$ is clear and its order d modulo n must satisfy $d \mid (n - 1)$ per Lemma 4.1.3. However, we also know that $d \mid \phi(n)$ by the same result and the incongruence assumptions imply that $d \nmid (n - 1)/p_i$, which means that $d = n - 1$. Therefore, $\phi(n) = n - 1$ and this is equivalent to n being prime. □

Method – Detecting Primes: Suppose we wish to verify n is prime via Proposition 5.1.3.
(i) Find $a \in \mathbb{Z}$ such that $a^{n-1} \equiv 1 \pmod{p}$ is satisfied.
(ii) Determine distinct prime factors $p_1, ..., p_k$ of $n - 1$.
(iii) Reduce the powers $a^{(n-1)/p_i}$ modulo n; they should not be congruent to one.

5.2 A Probabilistic Test

Proposition 5.2.1 *Let $n > 1$ and $p_1, ..., p_k$ be the distinct prime factors of $n - 1$. Consider N random integer values in $\{1, ..., n - 1\}$ and take $(*)$ from* Proposition 5.1.3.
(i) *If $(*)$ ever holds, then n is prime.*
(ii) *If $(*)$ always fails, then n is probably composite.*
Moreover, the probability a prime slips through the test is less than $(1 - \frac{1}{2^k})^N$.

Proof: If n is prime, $(*)$ holds for **any** primitive root. The proportion of primitive roots here is

$$\frac{\phi(n-1)}{n-1} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \geq \frac{1}{2^k}.$$

The probability N random numbers from $1, 2, ..., n-1$ are **not** primitive roots is as indicated. □

5.3 Detecting Primality using Powers

Proposition 5.3.1 *Let $n > 1$ where $n - 1 = 2^k m$ for some $k, m \in \mathbb{Z}$ with m odd. If*

$$\begin{cases} a^m \not\equiv 1 \pmod{n} \\ a^{2^r m} \not\equiv -1 \pmod{n} \end{cases} \tag{$\dagger$}$$

for some $a \in \mathbb{Z}$ and every $0 \leq r < k$, then n is composite.

Proof: We prove the contrapositive, so suppose that n is prime. By Fermat's Little Theorem, we have $a^{2^k m} \equiv 1 \pmod{n}$. Now let $0 \leq s \leq k$ be minimal with $a^{2^s m} \equiv 1 \pmod{n}$. If $s = 0$, then $(\dagger)$ fails, so suppose $s > 0$ and define $r := s - 1$ and $x := a^{2^r m}$. We can now see that

$$x^2 = a^{2^s m} \equiv 1 \pmod{n}.$$

Because n is prime, this implies that $x \equiv \pm 1 \pmod{n}$. Indeed, if n divides $x^2 - 1 = (x-1)(x+1)$ then it divides one of the factors by Corollary 1.2.3(iii). By minimality, we have $x \equiv -1 \pmod{n}$. Therefore, $a^{2^r m} \equiv -1 \pmod{n}$ and again $(\dagger)$ fails. □

5.4 The Miller-Rabin Test

Theorem 5.4.1 (Miller-Rabin Test) *Let $n \geq 5$ where $n - 1 = 2^k m$ for $k, m \in \mathbb{Z}$ with m odd. Consider N random integer values in $\{1, ..., n-1\}$ and take $(\dagger)$ from* Proposition 5.3.1.

(i) *If $(\dagger)$ ever holds, then n is composite.*

(ii) *If $(\dagger)$ always fails, then n is probably prime.*

Moreover, the probability that a composite slips through the test is less than $(\frac{1}{4})^N$.

Proof: (**Non-examinable**) Omitted. □

5.5 RSA Encryption

Definition The RSA public key encryption system is a type of encryption consisting of a pair $(n, e) \in \mathbb{Z}^2$ called the public key and a positive integer $s \in \mathbb{Z}^+$ called the private key.

Method – RSA Encryption: We will generate public and private keys for an RSA system.

(i) Choose two distinct large primes p and q and consider their product $n := pq$.

(ii) Use Lemma 3.1.4 to see that $\phi(n) = (p-1)(q-1)$.

(iii) Find $e \in \mathbb{Z}$ with $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.

(iv) Find $s \in \mathbb{Z}^+$ with $se \equiv 1 \pmod{\phi(n)}$ by using Euclid's Algorithm on $se - t\phi(n) = 1$.

Definition A message is an integer $0 \leq m < n$. In the context of RSA encryption, we say that an encrypted message is $r \equiv m^e \pmod{n}$ and a decrypted message is $r^s \equiv m \pmod{n}$.

6 Sums of Squares

6.1 Pythagorean Triples

Definition 6.1.1 A Pythagorean triple is a triple $x, y, z \in \mathbb{Z}^+$ such that $x^2 + y^2 = z^2$. In the case x, y, z has **no** common divisor, we say that (x, y, z) is a primitive Pythagorean triple.

Note: Let (x, y, z) be a Pythagorean triple and $d \coloneqq \gcd(x, y, z)$. Then, we can divide each integer by the greatest common divisor to obtain a primitive Pythagorean triple $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$.

Lemma 6.1.2 *Let (x, y, z) be a* **primitive** *Pythagorean triple. Then, x and y have opposite parity, that is one of them is odd and the other is even.*

Proof: If both x and y are even, then $2 \mid x$ and $2 \mid y$, in particular $2 \mid (x^2+y^2)$, that is $2 \mid z^2$, which means that $2 \mid z$, so (x, y, z) is not primitive, a contradiction. On the other hand, if both x and y are odd, this means $x \equiv \pm 1 \pmod 4$ and $y \equiv \pm 1 \pmod 4$. Thus, $z^2 = x^2 + y^2 \equiv 2 \pmod 4$. However, if $2 \mid z^2$, then we get $2 \mid z$ which means $4 \mid z^2$ and so $z^2 \equiv 0 \pmod 4$, a contradiction since zero and two are incongruent modulo four. □

Lemma 6.1.3 *Let $m, n \in \mathbb{Z}$ be coprime such that their product mn is a perfect square, which means $mn = a^2$ for some $a \in \mathbb{Z}$. Then, each of m and n are perfect squares.*

Proof: Let mn be a perfect square, meaning that its prime factorisation consists of only even powers. Assume to the contrary that m is **not** a perfect square. Then, its prime factorisation

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

has at least one α_i odd. Because m and n are coprime, the prime factors $p_i \neq q_j$ for any i, j where q_i are the prime factors of n (otherwise we would have a common factor). Thus, we have

$$mn = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})n.$$

Since at least one α_i is odd, it means that mn is **not** a perfect square, a contradiction. An identical argument works with n, so the result follows. □

Theorem 6.1.4 *Let $a, b \in \mathbb{Z}^+$ have opposite parity and be coprime with $a > b$. Then, (x, y, z) is a* **primitive** *Pythagorean triple if and only if $(x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2)$.*

Proof: ($\Leftarrow$) We verify that the stated formulae satisfy Definition 6.1.1. Indeed, we see that $(a^2 - b^2)^2 + (2ab)^2 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2)^2$. Now if it is **not** primitive, then $a^2 - b^2$ and $a^2 + b^2$ have a common prime divisor p. But adding/subtracting these, we see that $p \mid 2a^2$ and $p \mid 2b^2$. But opposite parity implies $a^2 - b^2$ is odd, so $p \neq 2$. Thus, $p \mid a$ and $p \mid b$, a contradiction.

($\Rightarrow$) On the other hand, let (x, y, z) be a primitive Pythagorean triple. By Lemma 6.1.2, x and y have opposite parity, so (exchanging them if necessary) we can assume that x is odd and y is even. Suppose $y = 2w$ for some $w \in \mathbb{Z}$. Because $z^2 = x^2 + y^2$, it follows that z is also odd, but that $z \pm x$ is even. Thus, we see that

$$y^2 = 4w^2 = z^2 - x^2 \qquad \Rightarrow \qquad w^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right).$$

The two numbers in this factorisation of w^2 are coprime. Indeed, if they were not and p is a common prime divisor, then p also divides their sum and difference, that is $p \mid z$ and $p \mid x$. This perpetuates to $p \mid (z^2 - x^2) \Leftrightarrow p \mid y^2$ and so $p \mid y$, a contradiction to primitivity of (x, y, z). Consequently, we have two numbers which are coprime whose product is a perfect square: Lemma 6.1.3 applies, telling us that there exist some $a, b \in \mathbb{Z}$ with

$$\frac{z+x}{2} = a^2 \qquad \text{and} \qquad \frac{z-x}{2} = b^2.$$

Clearly, $x = a^2 - b^2$ and $z = a^2 + b^2$. Last, $y = 2w = 2\sqrt{w^2} = 2\sqrt{a^2b^2} = 2ab$, so we are done. □

Corollary 6.1.5 *Let $a, b, s \in \mathbb{Z}^+$ be any positive integers with $a > b$. Then, (x, y, z) is a Pythagorean triple if and only if $(x, y, z) = \big(s(a^2 - b^2), s(2ab), s(a^2 + b^2)\big)$.*

Proof: ($\Leftarrow$) This is another algebra exercise in verifying the formulae satisfy Definition 6.1.1. Indeed, $(s(a^2 - b^2))^2 + (s(2ab))^2 = s^2a^4 + s^2(2a^2b^2) + s^2b^2 = (s(a^2 + b^2))^2$.

($\Rightarrow$) Suppose (x, y, z) is a Pythagorean triple and let $s := \gcd(x, y, z)$. As we noted above, we know $(\frac{x}{s}, \frac{y}{s}, \frac{z}{s}) =: (x', y', z')$ is a primitive Pythagorean triple. Indeed, if $h > 1$ is a common divisor of x', y', z', then $hs > s$ is a common divisor of x, y, z but this contradicts maximality of s. Thus, Theorem 6.1.4 implies $(x', y', z') = (a^2 - b^2, 2ab, a^2 + b^2)$, from which we conclude that

$$(x, y, z) = \Big(s(a^2 - b^2), s(2ab), s(a^2 + b^2)\Big).$$ □

Note: Geometrically, this classification comes from a stereographic projection of *rational points* (x, y), i.e. points where $x, y \in \mathbb{Q}$ are rational numbers, onto the circle $x^2 + y^2 = 1$.

6.2 Application to Fermat's Last Theorem

Theorem (Fermat's Last Theorem) *For $n > 2$, there are* **no** *non-trivial integer solutions to*

$$x^n + y^n = z^n.$$

Proof: (**Non-examinable**) This was a crowning achievement of 20th Century mathematics. □

Remark (Non-examinable) This theorem was conjecture for 358 years before Andrew Wiles was able to prove the then-known Modularity *Conjecture*; this relates elliptic curves over $\mathbb{Q}$ to so-called modular forms. The point is that **if** the equation $x^p+y^p = z^p$ where p is prime (which turns out to be sufficient; we don't need to consider composite powers) has a non-trivial solution, then the elliptic curve $v^2 = u(u-x^p)(u+y^p)$ in (u, v)-coordinates cannot be modular. The now-called Modularity *Theorem* would contradict this and so Fermat's Last Theorem is true!

Note: If we can prove Fermat's Last Theorem for $n = 4$ and for odd primes $p = 2k + 1$, then if we can solve $x^{ab} + y^{ab} = z^{ab}$, then we can get solutions for $n = a$ and $n = b$ too.

Theorem 6.2.1 *There are* **no** *non-trivial integer solutions to $x^4 + y^4 = z^2$, in particular there are no solutions where z is a perfect square (Fermat's Last Theorem with $n = 4$).*

Proof: Suppose $x^4 + y^4 = z^2$ does have a non-trivial solution, i.e. it is satisfied by some positive integers $x, y, z \in \mathbb{Z}$. We can choose z to be as small as possible. In particular, this means that any two of x, y, z are coprime. Indeed, if two of them had a common prime factor p, we must have $p \mid x$, $p \mid y$ and $p^2 \mid z$, so we can divide through by p^4 to reduce the size of z. Notice that this makes (x^2, y^2, z) a primitive Pythagorean triple, so Theorem 6.1.4 tells us that

$$x^2 = a^2 - b^2, \qquad y^2 = 2ab, \qquad z = a^2 + b^2$$

for some $a, b \in \mathbb{Z}$ (by swapping x and y if necessary). Note that x is odd since it its square is odd and thus the difference of two numbers of opposite parity, so $x \equiv 1 \pmod 4$. Therefore, it follows that a is odd and b is even; the other way would result in $x^2 \equiv -1 \not\equiv 1 \pmod 4$. Since it is even, we can write $b = 2k$ for some $k \in \mathbb{Z}$. Then, $y^2 = 2ab = 4ak$. We claim that a and k are perfect squares. Indeed, this is a direct result of the fact $\gcd(a, b) = 1$, which implies $\gcd(a, k) = 1$ and so Lemma 6.1.3 applies. Consequently, let $a = v^2$ and $k = w^2$. We can substitute these:

$$x^2 = v^4 - 4k^2 = v^4 - 4w^4 \qquad \Leftrightarrow \qquad x^2 + 4w^4 = v^4.$$

This shows that we have yet another primitive Pythagorean triple $(x, 2w^2, v^2)$ and we can repeat the argument: there exist $\alpha, \beta \in \mathbb{Z}$ via Theorem 6.1.4 such that

$$x = \alpha^2 - \beta^2, \qquad 2w^2 = 2\alpha\beta, \qquad v^2 = \alpha^2 + \beta^2,$$

where $\gcd(\alpha, \beta) = 1$ and they have opposite parity. Notice the second equation implies $\alpha\beta = w^2$, which means α and β are themselves perfect squares by Lemma 6.1.3, say $\alpha = s^2$ and $\beta = t^2$. Substituting these into the third equation produces

$$s^4 + t^4 = v^2,$$

which is another solution to the equation in question. However, $v = \sqrt{a} < a^2 + b^2 = z$ and this contradicts the minimality of z. Therefore, there is **no** solution to this equation after all. □

Note: Fermat first proved Theorem 6.2.1 (the margin wasn't too narrow for this, at least).

6.3 Representation of Integers as a Sum of Two Squares

Lemma 6.3.1 (Brahmagupta-Fibonacci Identity) *For any integers $a, b, c, d \in \mathbb{Z}$, we have*

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2.$$

In particular, if $n, m \in \mathbb{Z}$ are each the sum of two squares, so too is their product nm.

Proof: Simply expand both sides and compare. In fact, this can also be viewed as a sort-of corollary of the following fact for complex numbers: $|a \pm ib|^2|c \pm id|^2 = \big|(a \pm ib)(c \pm id)\big|^2$. □

Theorem 6.3.2 *Every prime p with $p \equiv 1 \pmod 4$ is expressible as a sum of two squares.*

Proof: By Corollary 2.3.3, we can solve $z^2 \equiv -1 \pmod p$ for $1 \leq z \leq p-1$. Hence, we have found some multiple of p which is a sum of two squares, say $np = z^2 + 1^2$. Now, suppose mp is the least positive multiple of p with this sum of two squares property, say $mp = x^2 + y^2$. Suppose for a contradiction that $m \geq 2$. Observe that $m < p$ because $m \leq n$ which means that

$$mp \leq np = z^2 + 1 \leq (p-1)^2 + 1 < p^2.$$

Now, let $-m/2 \leq u, v \leq m/2$ be integers such that $u \equiv x \pmod m$ and $v \equiv y \pmod m$. Thus,

$$u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod m \qquad \Rightarrow \qquad u^2 + v^2 = km$$

for some $k \in \mathbb{Z}$. If $k = 0$, then $u = v = 0$ and $x \equiv y \equiv 0 \pmod m$, meaning that $m \mid x$ and $m \mid y$; this implies that $m^2 \mid (x^2 + y^2) \Leftrightarrow m^2 \mid mp$. Since $m < m^2$, we conclude that $m \mid p$, but this is a contradiction since p is prime and $1 < m < p$. Therefore, this tells us that $k > 0$. Moreover, notice that

$$k = \frac{1}{m}(u^2 + v^2) \leq \frac{1}{m}\left(\frac{m^2}{4} + \frac{m^2}{4}\right) = \frac{m}{2} < m.$$

We can now apply the Brahmagupta-Fibonacci Identity in the following way:

$$m^2kp = (mk)(mp) = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2.$$

Looking at each of these summands modulo m, we conclude that

$$\begin{aligned} xu + yv &\equiv x^2 + y^2 \equiv 0 \pmod m \\ xv - yu &\equiv xy - yx \equiv 0 \pmod m. \end{aligned}$$

Therefore, each summand is divisible by m^2, so dividing through results in $kp = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Since $0 < k < m$, this contradicts the minimality of m. □

Method – Prime as a Sum of Two Squares: Suppose p is prime with $p \equiv 1 \pmod 4$. In order to express p as a sum of two squares, we just follow through the proof of Theorem 6.3.2 in the specific context that we are working in.

Theorem 6.3.4 (Fermat's Christmas Theorem) *An integer $n > 0$ is the sum of two squares if and only if each prime of the form $4k+3$ in its factorisation into distinct prime powers has an even power.*

Proof: ($\Leftarrow$) Note that $p = 2 = 1^2 + 1^2$ and Theorem 6.3.2 guarantees any prime of the form $p = 4k+1$ is a sum of two squares. The only other primes are of the form $p = 4k+3$. Since we assume these have even powers, it is unproblematic because $p^{2m} = p^{2m} + 0^m$ for any $m \in \mathbb{Z}$. Combining all this with the Brahmagupta-Fibonacci Identity, this guarantees that an integer $n > 0$ of the stated form is the sum of two squares.

($\Rightarrow$) Suppose $n = x^2 + y^2$ and let $p \mid n$ by a prime divisor of the form $p = 4k+3$; we will show that $p \mid x$ and $p \mid y$. Indeed, since p is prime, we know that $\gcd(y, p) \in \{1, p\}$, that is there are two options. If y and p are coprime, we know there exists $z \in \mathbb{Z}$ such that $yz \equiv 1 \pmod p$ by cancellation (Lemma 2.1.4). Therefore, the sum of two squares expression implies

$$nz^2 = x^2z^2 + y^2z^2 \equiv x^2z^2 + 1 \pmod p.$$

But because $p \mid n$, it follows that $p \mid nz^2$ and thus $x^2z^2 \equiv -1 \pmod p$, a contradiction to Corollary 2.3.3 since such things only have solutions modulo two or $p = 4k+1$. This means the only option we have is $\gcd(y, p) = p$ and thus $p \mid y$. An identical argument is true where we replace y with x instead, so $p \mid x$. This means that $p^2 \mid n$ as desired. It remains to mention therefore that

$$\left(\frac{n}{p^2}\right) = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$$

and we can repeat the same argument to conclude that having odd powers results in a contradiction. Indeed, all prime factors of the form $4k+3$ have even powers. □

6.4 Sums of Four Squares

The aim of this section is to prove that every integer is the sum of four squares.

Lemma 6.4.2 (Non-examinable) *For any $a, b, c, d \in \mathbb{Z}$, we have*

$$\begin{gathered}(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2) \\ \| \\ (a\alpha+b\beta+c\gamma+d\delta)^2 + (a\beta-b\alpha-c\delta+d\gamma)^2 \\ + (a\gamma+b\delta-c\alpha-d\beta)^2 + (a\delta-b\gamma+c\beta-d\alpha)^2.\end{gathered}$$

In particular, if $n, m \in \mathbb{Z}$ are each the sum of four squares, so too is their product nm.

Remark 6.4.3 How the Brahmagupta-Fibonacci Identity can be proved using complex numbers, Lemma 6.4.2 can be explained using the language of quaternions. This is how the strange-looking formula is obtained in the first place.

Lemma 6.4.4 *For p prime, there exists $m \in \mathbb{Z}$ with $0 < m < p$ where $mp = x^2 + y^2 + 1$.*

Proof: Finding m requires us to solve $x^2 + y^2 \equiv -1 \pmod{p}$. Note that $p = 2$ yields the trivial solution $(x, y) = (1, 0)$. Suppose therefore that p is odd (in fact, Corollary 2.3.3 establishes the result for $p \equiv 1 \pmod 4$ so we can be even more specific and assume only that $p \equiv 3 \pmod 4$, but we won't do this). Since p is odd, we can define the following sets:

$$S_1 := \left\{1 + x^2 : 0 \leq x \leq \frac{p-1}{2}\right\} \qquad \text{and} \qquad S_2 := \left\{-y^2 : 0 \leq y \leq \frac{p-1}{2}\right\}.$$

No two distinct elements of S_1 are congruent modulo p. Indeed, if $1 + x_1^2 \equiv 1 + x_2^2 \pmod p$, this implies that $p \mid (x_1^2 - x_2^2)$ and therefore $p \mid (x_1 + x_2)$ or $p \mid (x_1 - x_2)$ by Lemma 1.3.2. But because $x_1, x_2 \leq (p-1)/2$, the only way this can happen is if $x_1 = x_2$. An identical argument shoes that no two distinct elements of S_2 are congruent. This implies that the cardinalities are

$$|S_1| = \frac{p+1}{2} = |S_2| \qquad \Rightarrow \qquad |S_1 \cup S_2| = p + 1,$$

because each of x and y have $(p-1)/2 + 1 = (p+1)/2$ possibilities which lead to incongruent elements. But since there are at most p distinct remainders modulo p, this means that some element of S_1, say $1 + x^2$, is congruent to some element of S_2, say $-y^2$. Hence, we conclude that $1 + x^2 \equiv -y^2 \pmod p$, equivalent to saying there exists $m \in \mathbb{Z}$ with $mp = 1 + x^2 + y^2$. The final thing to show is the inequality $0 < m < p$, but this is clear from $x, y \leq (p-1)/2 < p/2$ and so

$$0 < mp = x^2 + y^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2. \qquad \square$$

Theorem 6.4.1 (Lagrange's Four-Square Theorem) *Every $n \in \mathbb{N}$ is the sum of four squares.*

Proof: (**Non-examinable**) By Lemma 6.4.2, it is sufficient to represent any prime number as the sum of four squares. We have already established in Theorem 6.3.2 that $p = 2$ and $p \equiv 1 \pmod 4$ require two squares (so they can be represented by four squares where two of them are 0^2). It remains to consider $p \equiv 3 \pmod 4$. We can interpret Lemma 6.4.4 as establishing that **some** multiples of p are expressible as a sum of three (and therefore four) squares; let mp be the least such multiple, say

$$mp = a^2 + b^2 + c^2 + d^2.$$

Suppose to the contrary that $m \geq 2$ (we know from Lemma 6.4.4 that $m < p$). We now follow the proof of Theorem 6.3.2 closely. Indeed, we can choose some integers $-m/2 \leq \alpha, \beta, \gamma, \delta \leq m/2$ such that $a \equiv \alpha, b \equiv \beta, c \equiv \gamma, d \equiv \delta \pmod m$. Thus,

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv 0 \pmod m \qquad \Rightarrow \qquad \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = km$$

for some $k \in \mathbb{Z}$. If $k = 0$, then $\alpha = \beta = \gamma = \delta = 0$ and $a \equiv b \equiv c \equiv d \pmod{m}$, meaning that $m \mid a$, $m \mid b$, $m \mid c$, $m \mid d$ and therein $m \mid (a^2 + b^2 + c^2 + d^2) \equiv m^2 \mid mp$. Since $m < m^2$ we conclude that $m \mid p$ but this is a contradiction since p is prime and $m < p$. Therefore, this tells us that $k > 0$. Moreover, notice that

$$k = \frac{1}{m}(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) \leq \frac{1}{m}\left(\frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4}\right) = m.$$

We will show $k < m$ (the inequality is strict). To do so would require $\alpha, \beta, \gamma, \delta \in \{\pm m/2\}$ and therefore $a \equiv b \equiv c \equiv d \equiv m/2 \pmod{m}$. Indeed, suppose $a = (s + \frac{1}{2})m$. Then we see that

$$a^2 = (s^2 + s + \frac{1}{4})m^2 \equiv \frac{m^2}{4} \pmod{m^2}.$$

The same holds for b, c, d also. Therefore,

$$mp = a^2 + b^2 + c^2 + d^2 \equiv \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} = m^2 \equiv 0 \pmod{m^2},$$

but this again says that $m^2 \mid mp$ which we saw was impossible. We can conclude that $0 < k < m$. We can now apply Lemma 6.4.2 in the following way:

$$m^2kp = (mk)(mp) = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)(a^2 + b^2 + c^2 + d^2) = w^2 + x^2 + y^2 + z^2$$

for the relevant $w, x, y, z \in \mathbb{Z}$ given in terms of the $a, b, c, d, \alpha, \beta, \gamma, \delta$. Importantly, we see that $m \mid w$, $m \mid x$, $m \mid y$ and $m \mid z$ from which we can divide out by m^2 to get kp as the sum of four squares.Since $0 < k < m$, this contradicts the minimality of m. □

6.5 Variations

Lemma 6.5.1 (Legendre's Three-Square Theorem) *Every $n \in \mathbb{N}$ is expressible as a sum of three squares if and only if n is* **not** *of the form $4^a(8b + 7)$ where $a, b \in \mathbb{Z}$.*

Proof: Omitted. □

Note: Let $g(n)$ be the number of n^{th} powers required to express every $n \in \mathbb{N}$ as a sum of them. Clearly, $g(1) = 1$ because every integer can be written as a sum of first powers using only one integer. We have also proven that $g(2) = 4$, that is there is a minimum of four square-powers required to express every integer. Waring's Problem about the existence of $g(n)$ for all $n \in \mathbb{N}$ was proven by Hilbert in 1909. What is still *conjecture* is this formula:

$$g(n) = 2^n + \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 2.$$

7 Quadratic Reciprocity

7.1 Quadratic Residues

Definition 7.1.1 Let $a, m \in \mathbb{Z}$ with $m \geq 2$. We say that a is a quadratic residue modulo m if there exists $x \in \mathbb{Z}$ with $x^2 \equiv a \pmod{m}$. If not, it is a quadratic non-residue modulo m.

Note: We can restrict to $1 \leq a \leq m-1$ (obviously $a = 0$ is always a quadratic residue)

Method – Quadratic Residues: To determine all quadratic residues modulo m, it amounts to computing the remainders modulo m of each of the powers 1^2, 2^2, ..., $(m-1)^2$.

Proposition 7.1.3 *If p is an odd prime, then half the numbers $1, ..., p-1$ are quadratic residues modulo p and half are quadratic non-residues modulo p.*

Proof: The quadratic residues are the remainders of 1^2,..., $(p-1)^2$ on division by p. Moreover, each remainder occurs exactly twice because $x^2 \equiv y^2 \pmod{p}$ is equivalent to $p \mid (x+y)(x-y)$, which means $p \mid (x+y)$ or $p \mid (x-y)$ by Lemma 1.3.2. For $x, y \in \{1, 2, ..., p\}$, this is equivalent to $x = y$ or $x = p - y$. Since p is odd, $p-1$ is even and this splits $1, ..., p-1$ exactly in half. □

7.2 The Legendre Symbol

Definition 7.2.1 For p an odd prime and $a \in \mathbb{Z}$ coprime with p, the Legendre symbol is

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a quadratic } \underline{\text{non}}\text{-residue modulo } p \end{cases}.$$

Lemma 7.2.3 *For p an odd prime and $a, b \in \mathbb{Z}$ not divisible by p, we have the following:*

(i) *If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(ii) $\left(\frac{a^2}{p}\right) = 1$.

(iii) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. (**Euler's Criterion**)

(iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof: (i) and (ii) These are immediate from Definition 7.2.1.

(iii) Let $y = a^{(p-1)/2}$, which means $y^2 = a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Hence, $p \mid (y^2 - 1)$ and again we know from Lemma 1.3.2 that $p \mid (y+1)$ or $p \mid (y-1)$. This tells us that $y \equiv \pm 1 \pmod{p}$, so the goal now is to prove that $y \equiv 1 \pmod{p}$ if and only if a is

a quadratic residue modulo p. Well, suppose first that a is a quadratic residue modulo p, say $a \equiv x^2 \pmod{p}$. Then we can apply Fermat's Little Theorem to see that

$$y = a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

On the other hand, suppose that $y = a^{(p-1)/2} \equiv 1 \pmod{p}$ and let r be a primitive root modulo p. Then, for some $1 \leq k \leq p-1$, we know that $a \equiv r^k \pmod{p}$ and we have by assumption that

$$y = a^{\frac{p-1}{2}} = r^{\frac{k(p-1)}{2}} \equiv 1 \pmod{p}.$$

That said, we clearly see that $(p-1) \mid k(p-1)/2$ which implies that $k/2 \in \mathbb{Z}$ and, consequently, k is even. But then, we see that a is a quadratic residue modulo p since we have the congruence

$$a \equiv r^k = (r^{\frac{k}{2}})^2 \pmod{p}.$$

(iv) The final property follows immediately from Euler's Criterion:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p},$$

but since each side is ± 1, it must be that the congruences are straight-up equalities. □

Note: Euler's Criterion allows us to compute Legendre symbols when a and p are small.

7.3 Gauss' Law of Reciprocity

Lemma 7.3.5 (Gauss' Lemma) *Let p be an odd prime with $a \in \mathbb{Z}$ coprime to p and define*

$$S = \left\{a, 2a, 3a, ..., \frac{p-1}{2}a\right\}.$$

If there are n elements of S whose remainder modulo p is strictly larger than $p/2$, then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Proof: Since $p \nmid a$ by coprimality, all the elements of S are incongruent to each other (and to zero) modulo p. Thus, we can re-order them so that $r_1, ..., r_m$ are their remainders less than $p/2$ and $s_1, ..., s_n$ are their remainders larger than $p/2$. Totalling up the number of elements, this means $m + n = (p-1)/2$. Note also that

$$1 \leq r_1, .., r_m < \frac{p}{2} \qquad \text{and} \qquad 1 \leq (p - s_1), ..., (p - s_n) < \frac{p}{2}.$$

We cannot have $p - s_i = r_j$ for any i or j. If we did, then $s_i \equiv va \pmod{p}$ and $r_j \equiv wa \pmod{p}$ for some integers $1 \leq v, w \leq (p-1)/2$. This would imply that $(v+w)a \equiv s_i + r_j = p \equiv 0 \pmod{p}$ and thus $p \mid (v+w)$, which is impossible by the fact $v, u, \leq (p-1)/2$. This establishes that

$$\{r_1, ..., r_m, s_1, ..., s_n\} = \left\{1, 2, ..., \frac{p-1}{2}\right\}$$

in some order. Multiplying the elements of the right-hand set and working modulo p yields

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= r_1 \cdots r_m \cdot (p-s_1)\cdots(p-s_n)\\ &\equiv r_1 \cdots r_m \cdot (-s_1)\cdots(-s_n)\\ &\equiv (-1)^n r_1 \cdots r_m \cdot s_1 \cdots s_n\\ &\equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a\\ &= (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!.\end{aligned}$$

Because $p \nmid \left(\frac{p-1}{2}\right)!$, we can cancel it to obtain $1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod{p}$, which is equivalent to $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. One need only apply Euler's Criterion to now conclude the result. □

Theorem 7.3.2 (Supplementary Laws) *For p an odd prime, we have the following:*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases} \qquad \text{and} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

Note: Equivalently, we can reformulate the statements of the Supplementary Laws as

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \text{and} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof: The first of the two laws is immediate from Corollary 2.3.3. As for the second, we can use Gauss' Lemma with $S = \{2, 4, 6, ..., p-1\}$. It turns out that reducing modulo p has no effect, so we just need to know how many elements are larger than $p/2$. There are four cases to analyse:

- If $p = 8k+1$, $S = \{2, 4, ..., 4k, 4k+2, ..., 8k\}$; there are $2k$ such elements.
- If $p = 8k+3$, $S = \{2, 4, ..., 4k, 4k+2, ..., 8k+2\}$; there are $2k+1$ such elements.
- If $p = 8k+5$, $S = \{2, 4, ..., 4k+2, 4k+4, ..., 8k+4\}$; there are $2k+1$ such elements.
- If $p = 8k+7$, $S = \{2, 4, ..., 4k+2, 4k+4, ..., 8k+6\}$; there are $2k+2$ such elements. □

Theorem 7.3.1 (Gauss' Law of Quadratic Reciprocity) *For p and q distinct odd primes,*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \qquad \text{if } \textbf{at most one } p, q \equiv 3 \pmod 4,$$

whereas

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \qquad \text{if } \textbf{both } p, q \equiv 3 \pmod 4.$$

Note: Equivalently, we can reformulate Gauss' Law of Quadratic Reciprocity as

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proof: (**Non-examinable**) Consider integer pairs $(x, y) \in \mathbb{Z}^2$ where $0 < x < p/2$ and $0 < y < q/2$; all our points lie within a rectangle on the plane. We then split this rectangle into four regions by way of the following three lines (and provide a sketch in Figure 1 below):

$$py = qx + \frac{p}{2}, \qquad py = qx, \qquad py = qx - \frac{q}{2}.$$

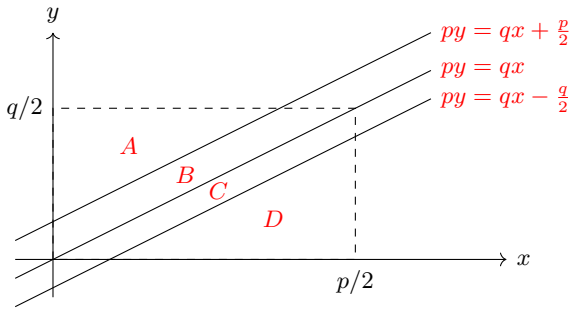

Figure 1: Four regions separated by the three equations above.

Note that there are no integer points on these lines. Indeed, if (x, y) was on $py = qx$, then it follows that $p \mid x$, but $0 < x < p/2$ disallows this. Similar contradictions work for the other lines. Now, every $x \in \mathbb{Z}$ admits **at most one** integer point (x, y) in the region labelled B in Figure 1. There is such a point if and only if the remainder of qx upon division by p is larger than $p/2$. We therefore conclude that (x, y) is in region B if and only if $qx < py < qx + p/2$, which is equivalent to $py - p/2 < qx < py$. Applying Gauss' Lemma tells us

$$\left(\frac{q}{p}\right) = (-1)^{|B|},$$

where there are $|B|$-man integer points in region B. By an identical argument, we have

$$\left(\frac{p}{q}\right) = (-1)^{|C|}.$$

Now, $|A| = |D|$ since the integer points in regions A and D are in 1-1 correspondence by the fact that we can apply the map $(x, y) \mapsto (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$ which associates to each point in one region a unique point in the other. Therefore, the total number of integer points in the rectangle is $2|A| + |B| + |C| = (p-1)(q-1)/4$. Noting that this total is even **except** when **both** $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, we obtain the reformulation of the statement of Gauss' Law of Quadratic Reciprocity noted above. Therefore,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{|B|+|C|} = (-1)^{2|A|+|B|+|C|} = (-1)^{\frac{(p-1)(q-1)}{4}}. \qquad \square$$

Method – Computing Legendre Symbols: Suppose we want to compute $\left(\frac{a}{p}\right)$.

(i) Write a as a product of powers of primes.

(ii) Use Step (i) and Lemma 7.2.3(iv) to write $\left(\frac{a}{p}\right) = \left(\frac{q_1^{\alpha_1}}{p}\right) \cdots = \left(\frac{q_k^{\alpha_k}}{p}\right)$.

(iii) Use previous results to handle the individual Legendre symbols: (a) use reciprocity and reduce modulo q_i, or (b) apply Lemma 7.2.3(ii), or (c) use Euler's Criterion.

7.4 Some Applications of Quadratic Reciprocity

Theorem 7.4.1 *If $p = 2k+1$ is prime and $p \equiv 1$ or $7 \pmod 8$, then $p \mid (2^k - 1)$.*

Proof: Note that $p \mid (2^k - 1) \Leftrightarrow p \mid (2^{(p-1)/2} - 1) \Leftrightarrow 2^{(p-1)/2} \equiv 1 \pmod p$ just by rearranging $p = 2k+1$ and interpreting divisors as congruences. But by Euler's Criterion, we know this occurs if and only if $\left(\frac{2}{p}\right) = 1$, which holds if $q \equiv 1$ or $7 \pmod 8$ as required. □

Note: Theorem 7.4.1 implies that $2^{11} - 1$ is **not** prime, since $2(11) + 1 = 23 \equiv 7 \pmod 8$.

Theorem 7.4.2 *There are infinitely-many primes of the form $p = 8k + 7$ for $k \in \mathbb{Z}$.*

Proof: Suppose that $p_1, ..., p_n$ is a complete list and define the number

$$N \coloneqq (p_1 \cdots p_n)^2 - 2.$$

Since each $p_i \equiv -1 \pmod 8$, it follows that their product $p_1 \cdots p_n \equiv \pm 1 \pmod 8$, and thus squaring implies $(p_1 \cdots p_n)^2 \equiv 1 \pmod 8$. In all, this means that $N \equiv 7 \pmod 8$. Note also that $p_i \nmid N$ since $N \equiv -2 \pmod{p_i}$ for each i. Therefore, if q is a prime such that $q \mid N$, then $q \neq 2$ since N is odd and

$$(p_1 \cdots p_n)^2 \equiv 2 \pmod q \qquad \Rightarrow \qquad \left(\frac{2}{q}\right) = 1.$$

We can now use the Supplementary Laws to conclude that $q \equiv 1$ or $7 \pmod 8$. But we have shown that $q \neq p_i$ for any i, which are all congruent to 7. Thus, we must have $q \equiv 1 \pmod 8$. Since this holds for all q, it means that $N \equiv 1 \pmod 8$, a contradiction. □

Theorem 7.4.3 *There are infinitely-many primes of the form $p = 3k + 1$ for $k \in \mathbb{Z}$.*

Proof: Suppose that $p_1, ..., p_n$ is a complete list and define the number

$$N \coloneqq 4(p_1 \cdots p_n)^2 + 3.$$

Since each $p_i \equiv 1 \pmod 3$, it follows that $N \equiv 1 \pmod 3$. Now, if N is prime then the contradiction is achieved immediately. We therefore assume that N is composite, i.e. there is a prime q such that $q \mid N$. Then, $(2p_1 \cdots p_n)^2 \equiv -3 \pmod q$ and Euler's Criterion tells us that

$$\left(\frac{-3}{q}\right) = 1.$$

Of course, note that $q \neq 3$ so we only consider $q \geq 5$. To determine for what q this Legendre equation is satisfied, note that it can be re-written as

$$\left(\frac{-1}{q}\right)\left(\frac{3}{q}\right) = 1.$$

Hence, this is true if and only if both factors are one or both factors are minus one. By the Supplementary Laws (the first one), we see that the first factor is one when $p = 4k+1$ and is minus one when $p = 4k+3$. By Gauss' Law of Quadratic Reciprocity, this means that

$$\left(\frac{3}{q}\right) = \left(\frac{q}{3}\right) = 1 \qquad \text{and} \qquad \left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) = -1,$$

respectively, which tells us that $q \equiv 1 \pmod 3$. Therefore, since $q = 3k+1$, it must be one of the p_i, but this is a contradiction to the fact that $p_i \nmid N$. $\square$

8 Gaussian Integers

8.1 Integral Domains

Reminder: A ring is a set R with an addition operation and a multiplication operation that satisfy a number of axioms. A subring is a subset $S \subseteq R$ containing the multiplicative identity of R which is closed under multiplication and subtraction.

Definition 8.1.1 The ring of Gaussian integers is $\mathbb{Z}[i] \coloneqq \{a + bi : a, b \in \mathbb{Z}\}$.

Lemma *The Gaussian integers form a subring of* $\mathbb{C}$.

Proof: It is clear that the multiplicative identity $1 = 1 + 0i \in \mathbb{Z}[i]$ since $0, 1 \in \mathbb{Z}$. As for closure under multiplication and subtraction, let $\alpha, \beta \in \mathbb{Z}[i]$ be of the form $\alpha = a + bi$ and $\beta = c + di$:

- For multiplication, we have $\alpha\beta = (a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$.
- For subtraction then, $\alpha - \beta = (a + bi) - (c + di) = (a - c) + (d - b)i \in \mathbb{Z}[i]$. □

Definition 8.1.2 An integral domain is a ring R satisfying the following conditions:
(i) R is commutative, that is $rs = sr$ for all $r, s \in R$.
(ii) R has **no** non-zero zero divisors, that is $rs = 0$ implies $r = 0$ or $s = 0$.

Remark Remark Most people simply call them *zero divisors*, omitting the "non-zero" for brevity.

Note: Any subring of $\mathbb{C}$ is automatically an integral domain, in particular $\mathbb{Z}[i]$ is such.

Definition 8.1.3 Let R be an integral domain and $\alpha, \beta \in R$. We say that β divides α if there exists $\gamma \in R$ such that $\alpha = \gamma\beta$. In this case, we write $\beta \mid \alpha$.

Remark In the case R is a subring of $\mathbb{C}$ and $\beta \neq 0$, we have that $\beta \mid \alpha$ if and only if $\alpha/\beta \in R$. Indeed, this is clear because Definition 8.1.3 say that we have the division if and only if $\alpha = \gamma\beta$ for some $\gamma \in R$, but we are in $\mathbb{C}$; we can rearrange this by dividing usually to obtain $\gamma = \alpha/\beta$.

Definition 8.1.4 Let R be an integral domain. We call $\alpha \in R$ a unit if $\alpha \mid 1$.

Lemma 8.1.5 *Let $\alpha, \beta \in R$ be elements of an integral domain. Then, $\alpha \mid \beta$ and $\beta \mid \alpha$ if and only if there exists a unit $u \in R$ such that $\alpha = u\beta$.*

Proof: ($\Rightarrow$) Let $\alpha \mid \beta$ and $\beta \mid \alpha$. Per Definition 8.1.3, there exist $\gamma, \delta \in R$ such that $\beta = \gamma\alpha$ and $\alpha = \delta\beta$. Therefore, we can substitute the first into the second to obtain $\alpha = \delta\gamma\alpha$, which is equivalent to $(1 - \delta\gamma)\alpha = 0$. Since R is an integral domain, either $\alpha = 0$ or $1 - \delta\gamma = 0$.

- If $\alpha = 0$, then $\beta = 0$ and the result holds trivially for **any** unit $u \in R$.
- If $1 - \delta\gamma = 0$, then $1 = \delta\gamma$, and so $\delta \mid 1$, that is δ is a unit; take $u = \delta$.

($\Leftarrow$) Let $\alpha = u\beta$ for a unit $u \in R$. This immediately implies that $\beta \mid \alpha$. On the other hand, we can rearrange to get $\beta = u^{-1}\alpha$ and thus $\alpha \mid \beta$. □

Note: A Gaussian integer $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $\frac{1}{\alpha} \in \mathbb{Z}[i]$. Its units are $\{\pm 1, \pm i\}$.

8.2 Norms

Definition 8.2.1 The norm of a Gaussian integer $\alpha = a + bi \in \mathbb{Z}[i]$ is defined as

$$N(\alpha) = a^2 + b^2.$$

For $\alpha \in \mathbb{Z}[i]$, it is clear that $N(a)$ is a non-negative integer. More generally, we can define $N(z) = a^2 + b^2$ for any complex number $z = a + bi \in \mathbb{C}$ and thus we can write $N(z) = |z|^2$.

Lemma 8.2.2 *For all $\alpha, \beta \in \mathbb{Z}[i]$, the norm satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Sketch of Proof: Let $\alpha = a + bi$ and $\beta = c + di$ and expand out both sides fully. □

Lemma 8.2.3 *Let $\alpha \in \mathbb{Z}[i]$.*
(i) *The norm $N(\alpha) = 0$ if and only if $\alpha = 0$.*
(ii) *The norm $N(\alpha) = 1$ if and only if α is a unit.*

Proof: (i) This is clear directly from Definition 8.2.1

(ii) If α is a unit, then $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[i]$. Therefore, applying the norm and using Lemma 8.2.2 tells us that $N(\alpha)N(\beta) = 1$. But since this is a product of non-negative integers, it must be that $N(\alpha) = 1$. Conversely, if $N(\alpha) = 1$, let $\alpha = a + bi$. Then, in $\mathbb{C}$, we have

$$\frac{1}{\alpha} = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a - bi}{N(\alpha)} = a - bi \in \mathbb{Z}[i].$$

We conclude that α is a unit since its reciprocal is a Gaussian integer (the above note). □

8.3 The Division Algorithm for Gaussian Integers

Proposition 8.3.1 (Division Algorithm for Gaussian Integers) *Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then, there exist $q, r \in \mathbb{Z}[i]$ with $0 \leq N(r) < N(\beta)$ such that $\alpha = q\beta + r$.*

Proof: The quotientα/β makes sense in $\mathbb{C}$ where we can write $\alpha/\beta = A + Bi$ for some $A, B \in \mathbb{R}$. Let $q \in \mathbb{Z}[i]$ be as close as possible to α/β in this sense: set $q := a + bi$ where $a, b \in \mathbb{Z}$ such that

$$|a - A| \leq \frac{1}{2} \qquad \text{and} \qquad |b - B| \leq \frac{1}{2}.$$

Let $r := \alpha - q\beta \in \mathbb{Z}[i]$. Then, we see that $\alpha = q\beta + r$ is satisfied. As for the inequality condition,

$$N\left(\frac{\alpha}{\beta} - q\right) = N\left((A - a) + (B - b)i\right) = (A - a)^2 + (B - b)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}.$$

This, in turn, implies precisely the inequality we desire (of course $0 \leq N(r)$ by default), namely

$$N(r) = N(\alpha - q\beta) = N\left(\frac{\alpha}{\beta} - q\right) N(\beta) \leq \frac{1}{2} N(\beta) < N(\beta). \qquad \square$$

Definition 8.3.3 Let R be an integral domain and $\alpha, \beta \in R$. A greatest common divisor (or highest common factor) is an element $\gamma \in R$ with the following properties:

(i) It is a common divisor, that is $\gamma \mid \alpha$ and $\gamma \mid \beta$.

(ii) It is largest in the sense that if $\delta \in R$ with $\delta \mid \alpha$ and $\delta \mid \beta$, then $\delta \mid \gamma$.

Note: It may be that a greatest common divisor doesn't exist, and is **not** unique if it does!

Lemma 8.3.4 *Let R be an integral domain and $\alpha, \beta \in R$ have greatest common divisor γ. Then, ε is a greatest common divisor of α and β if and only if $\varepsilon = u\gamma$ for a unit $u \in R$.*

Proof: ($\Rightarrow$) Let ε be a greatest common divisor. In particular, this means that $\varepsilon \mid \delta$ for any $\delta \in R$ with $\delta \mid \alpha$ and $\delta \mid \beta$. Specifically, this is true for $\delta = \gamma$. We conclude that $\varepsilon \mid \gamma$. But because γ is also a greatest common divisor, this also works for $\delta = \varepsilon$, so $\gamma \mid \varepsilon$. Therefore, applying Lemma 8.1.5 tells us that there exists a unit $u \in R$ with $\varepsilon = u\gamma$.

($\Leftarrow$) Let $\varepsilon = u\gamma$. Because $u \mid 1$ by definition of a unit, we know that u divides **any** element of the integral domain (since any $\mu \in R$ can be written as $\mu = \mu \cdot 1$). In particular, $u \mid \alpha$ and $u \mid \beta$, which means that $\varepsilon \mid \alpha$ and $\varepsilon \mid \beta$ (since $\gamma \mid \alpha$ and $\gamma \mid \beta$ by the fact it is a greatest common divisor). Moreover, if $\delta \in R$ with $\delta \mid \alpha$ and $\delta \mid \beta$, then $\delta \mid \gamma$, so $\gamma = q\delta$ for some $q \in R$. However, this is equivalent to $\varepsilon = uq\delta$, so $\delta \mid \varepsilon$ also. Hence, Definition 8.3.3 is satisfied with ε. $\square$

Theorem 8.3.5 *Any two Gaussian integers $\alpha, \beta \in \mathbb{Z}[i]$ have a greatest common divisor γ. Moreover, there exist $s, t \in \mathbb{Z}[i]$ such that*

$$\gamma = s\alpha + t\beta.$$

Proof: If $\alpha = \beta = 0$, we can take $\gamma = 0$ and we are done. Now, suppose at least one of $\alpha \neq 0$ and $\beta \neq 0$. Amongst all non-zero elements $\gamma = s\alpha + t\beta$ for $s, t \in \mathbb{Z}[i]$, choose one with $N(\gamma)$ minimal. We will show that $\gamma \mid \alpha$. Indeed, by the Division Algorithm for Gaussian Integers, we can write

$$\alpha = q\gamma + r$$

where $0 \leq N(r) < N(\gamma)$. But then, we see that

$$r = \alpha - q\gamma = \alpha - q(s\alpha + t\beta) = (1 - qs)\alpha - qt\beta,$$

which contradicts the minimality of $N(\gamma)$ **unless** $r = 0$. Thus, we conclude that $\gamma \mid \alpha$. A near-identical argument means that $\gamma \mid \beta$, so we have at least that γ is a common divisor of α and β. Now, suppose that δ is another common divisor. Then, since it divides each of them, it divides any linear combination, i.e. $\delta \mid (s\alpha + t\beta) \Leftrightarrow \delta \mid \gamma$. □

Method – Greatest Common Divisor in $\mathbb{Z}[i]$: To find a greatest common divisor γ of two Gaussian integers, and to determine some elements $s, t \in \mathbb{Z}[i]$ such that γ has the form in Theorem 8.3.5, we simply adapt Euclid's Algorithm to the Gaussian integers by using the Division Algorithm for Gaussian Integers.

8.4 Primes and Irreducibles

Definition 8.4.1 Let R be an integral domain.

(i) We call $\alpha \in R$ is irreducible if $\alpha \neq 0$ and α is **not** a unit, and if this property is true:

$$\alpha = \beta\gamma \qquad \Rightarrow \qquad \beta \text{ is a unit or } \gamma \text{ is a unit.}$$

(ii) We call $\alpha \in R$ is prime if $\alpha \neq 0$ and α is **not** a unit, and if this property is true:

$$\alpha = \beta\gamma \qquad \Rightarrow \qquad \alpha \mid \beta \text{ or } \alpha \mid \gamma.$$

Theorem 8.4.2 *We have the following relationship between prime and irreducible elements:*

(i) *For any integral domain R, we have $\alpha \in R$ is prime implies $\alpha \in R$ is irreducible.*

(ii) *For the integral domain $\mathbb{Z}$, an element is prime if and only if it is irreducible.*

(iii) *For the integral domain $\mathbb{Z}[i]$, an element is prime if and only if it is irreducible.*

Proof: (i) Let $\alpha \in R$ be a prime and suppose that $\alpha = \beta\gamma$. We trivially have $\alpha \mid \beta\gamma$, but the fact it is prime means it divides one of the factors. Without loss of generality, suppose $\alpha \mid \beta$. Then, $\beta = q\alpha$ for some $q \in R$. Therefore, $\alpha = q\alpha\gamma$ which means that $q\gamma = 1$, so γ is a unit.

(ii) It follows from Definition 8.4.1 that the irreducible elements in $\mathbb{Z}$ are the numbers $\pm p$ where p is prime. Now, if $p \mid ab$, then $p \mid a$ or $p \mid b$ by Lemma 1.3.2. It follows that $\pm p$ are prime elements in $\mathbb{Z}$, so they are indeed the same.

(iii) Let $\alpha \in \mathbb{Z}[i]$ be irreducible with $\alpha = \beta\gamma$ such that $\alpha \nmid \beta$. In order to conclude that α is also prime, we must show that $\alpha \mid \gamma$. Well, we know from Theorem 8.3.5 that the greatest common divisor of α and β exists, namely δ. Moreover, since $\delta \mid \alpha$, we have $\alpha = q\delta$ for some $q \in \mathbb{Z}[i]$. But by irreducibility, q or δ is a unit. Note that q is **not** a unit since $\delta \mid \beta$ but $\alpha \nmid \beta$, so δ is the unit. Consequently, we know from Lemma 8.3.4 that 1 is a greatest common divisor, so we can write

$$s\alpha + t\beta = 1.$$

Multiplying gives us $\gamma = s\alpha\gamma + t\beta\gamma$ and both terms are divisible by α, so $\alpha \mid \gamma$. The converse (that prime implies irreducible) holds in general and thus we refer to part (i) above. □

Note: Traditionally, the irreducible/prime elements in $\mathbb{Z}[i]$ are known as Gaussian primes.

Theorem 8.4.4 (Fundamental Theorem of Arithmetic for Gaussian Integers) *Every non-zero and non-unit $\alpha \in \mathbb{Z}[i]$ can be expressed as a unique product of Gaussian primes up to order, that is if $\alpha = \pi_1 \cdots \pi_r$ and $\alpha = \sigma_1 \cdots \sigma_s$ where π_i, σ_j are primes, then $r = s$ and the π_i and σ_s can be paired-off so that $\pi_i = u\sigma_j$ for some unit $u \in \mathbb{Z}[i]$.*

Proof: We proceed inductively on k that any $\alpha \in \mathbb{Z}[i]$ with $1 \leq N(\alpha) \leq k$ can be written as a product of primes. Indeed, if $k = 1$, there is nothing to do and the result is vacuously true. Assume the result holds for k and let $N(\alpha) = k + 1$. If α is prime, there is again nothing to do. Otherwise, we can write it as $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathbb{Z}[i]$ **not** units. Therefore, $N(\beta) \neq 1$ and $N(\alpha) \neq 1$ and, by Lemma 8.2.2, we have that

$$N(\beta)N(\gamma) = N(\alpha) = k + 1.$$

It follows that $N(\beta), N(\gamma) \leq k$ so the inductive hypothesis means we can write β and γ each as a product of primes. Therefore, α can be written as a product of primes. For uniqueness, let

$$\pi_1 \cdots \pi_r = \sigma_1 \cdots \sigma_s.$$

Thus, $\pi_1 \mid \sigma_1 \cdots \sigma_s$ but because π_1 is prime, it divides some σ_j. Because σ_j is irreducible, we have $\pi_1 = u\sigma_j$ for a unit $u \in \mathbb{Z}[i]$. Thus, we can substitute this and cancel to obtain the following:

$$u\sigma_j\pi_2 \cdots \pi_n = \sigma_1 \cdots \sigma_s \qquad \Rightarrow \qquad v\pi_2\pi_3 \cdots \pi_r = \sigma_1 \cdots \sigma_{j-1}\sigma_{j+1} \cdots \sigma_s.$$

If we do this repeatedly, we pair-off each π_i with some σ_j, so we must have $r = s$ so that when we get down to one irreducible on the left, say, we also have one irreducible on the right. □

Theorem 8.4.6 *If $p \equiv 1 \pmod 4$ is prime in $\mathbb{Z}$, then p is* **not** *prime in $\mathbb{Z}[i]$ and there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.*

Note: We are using Gaussian integers to essentially re-prove Theorem 6.3.2 quickly.

Proof: Recall from the proof of Corollary 2.3.3 that $x^2 \equiv -1 \pmod{p}$ is solved by $x = \left(\frac{p-1}{2}\right)!$. In other words, $p \mid (x^2+1)$ in $\mathbb{Z}$, which means $p \mid (x^2+1)$ in $\mathbb{Z}[i]$. However, we can factorise $x^2+1 = (1+xi)(1-xi)$ in the Gaussian integers, but be aware that $\frac{1 \pm xi}{p} \notin \mathbb{Z}[i]$, so $p \nmid (1 \pm xi)$ in $\mathbb{Z}[i]$. Because p divides a product without dividing one of the factors, it means it is **not** prime in $\mathbb{Z}[i]$ and, hence, is not irreducible. Suppose $p = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[i]$ **not** units. Then,

$$p^2 = N(p) = N(\alpha)N(\beta).$$

Since p is prime in $\mathbb{Z}$ and $N(\alpha), N(\beta) \in \mathbb{Z}$, it must be that $N(\alpha) = N(\beta) = p$ (since $N(\alpha) \neq 1$ and $N(\beta) \neq 1$ by the fact they are not units). So if we write $\alpha = a + bi$, this tells us that

$$p = N(\alpha) = a^2 + b^2. \qquad \square$$

Theorem 8.4.8 *The Gaussian primes are precisely the following elements:*

- *Primes in $\mathbb{Z}$ of the form $4k+3$, multiplied by ± 1 or $\pm i$.*
- *Elements $a+bi$ where a^2+b^2 is either 2 or a prime of the form $4k+1$,*

Proof: It is straightforward to see that the listed elements are prime. indeed, if $p = 4k+3$ is prime in $\mathbb{Z}$ and it factorises $p = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[i]$ **not** units, then $p^2 = N(\alpha)N(\beta)$ and so $N(\alpha) = N(\beta) = p$. But $p = 4k+3$ cannot be written as a sum of two squares, so there are no elements of norm p. Now, any Gaussian integer $a+bi$ divides an ordinary integer, for instance

$$(a+bi)(a-bi) = a^2 + b^2.$$

This ordinary integer can be written as a product of primes in $\mathbb{Z}$ by the usual Fundamental Theorem of Arithmetic. But primes of the form $4k+3$ are prime in $\mathbb{Z}[i]$, and the other primes factorise as a product of irreducible elements of the form listed in the statement, namely

$$p = (a+bi)(a-bi).$$

Therefore, if $a+bi$ is prime, then it is (a unit multiplied by) one of the listed elements. $\square$

9 Some Other Rings of Integers

9.1 The Ring $\mathbb{Z}[\sqrt{d}]$

Definition 9.1.1 For $d \in \mathbb{Z}$ not a perfect square, the ring of square root-adjoined integers is

$$\mathbb{Z}[\sqrt{d}] \coloneqq \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

Note: Again, we can realise $\mathbb{Z}[\sqrt{d}]$ as a subring of $\mathbb{C}$. Moreover, it is an integral domain and therefore we still have the notions of units, divisors and greatest common divisors.

Definition 9.1.2 The norm of an element $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is defined as

$$N(\alpha) = \left|a^2 - db^2\right|.$$

Proposition *Let $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$. Then, we have the following:*
(i) *The norm $N(\alpha\beta) = N(\alpha)N(\beta)$.*
(ii) *The norm $N(\alpha) = 0$ if and only if $\alpha = 0$.*
(iii) *The norm $N(\alpha) = 1$ if and only if α is a unit.*

Proof: Omitted (pretty much the same as those for $\mathbb{Z}[i]$ from Lemmata 8.2.2 and 8.2.3). □

Theorem 9.1.3 (Division Algorithm for $\mathbb{Z}[\sqrt{d}]$) *If $d \in \{-2, -1, 2, 3\}$ and $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ with $\beta \neq 0$, there exist $q, r \in \mathbb{Z}[\sqrt{d}]$ with $0 \leq N(r) < N(\beta)$ such that $\alpha = q\beta + r$.*

Proof: ($d = -2$) First, we write $\alpha/\beta = A + B\sqrt{-2}$ for some $A, B \in \mathbb{R}$. Let $q \in \mathbb{Z}[\sqrt{-2}]$ be as close as possible to α/β in this sense: set $q \coloneqq a + b\sqrt{-2}$ where $a, b \in \mathbb{Z}$ such that

$$|a - A| \leq \frac{1}{2} \qquad \text{and} \qquad |b - B| \leq \frac{1}{2}.$$

Let $r \coloneqq \alpha - q\beta \in \mathbb{Z}[\sqrt{-2}]$. We see that $\alpha = q\beta + r$ is satisfied. As for the inequality condition,

$$N\left(\frac{\alpha}{\beta} - q\right) = N\left((A - a) + (B - b)\sqrt{d}\right) = \left|(A - a)^2 + 2(B - b)^2\right| \leq \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 = \frac{3}{4}.$$

This, in turn, implies precisely the inequality we desire (of course $0 \leq N(r)$ by default), namely

$$N(r) = N(\alpha - q\beta) = N\left(\frac{\alpha}{\beta} - q\right)N(\beta) \leq \frac{3}{4}N(\beta) < N(\beta).$$

($d = -1, 2, 3$) These arguments are similar in flavour to the one done above. □

Note: This proof fails for $d = -3$, say, because the inequality at the end doesn't work.

Theorem 9.1.4 *If $d \in \{-2, -1, 2, 3\}$, then any two $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ have a greatest common divisor γ. Moreover, there exist $s, t \in \mathbb{Z}[\sqrt{d}]$ such that*

$$\gamma = s\alpha + t\beta.$$

Proof: Omitted (similar to Theorem 8.3.5). □

Theorem 9.1.5 *If $d \in \{-2, -1, 2, 3\}$, then $\alpha \in \mathbb{Z}[\sqrt{d}]$ is prime if and only if it is irreducible.*

Proof: Omitted (similar to Theorem 8.4.2). □

Remark 9.1.6 It turns out this result is **not** true for $d = -3$. Indeed, $2 \in \mathbb{Z}[\sqrt{-3}]$ is irreducible. Indeed, if $2 = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$ are **not** units, then $4 = N(2) = N(\alpha)N(\beta)$. But $N(\alpha) \neq 1$ and $N(\beta) \neq 1$, which implies $N(\alpha) = N(\beta) = 2$. However, if $\alpha = a + b\sqrt{-3}$, then

$$2 = N(\alpha) = a^2 + 3b^2,$$

which has no solutions for $a, b \in \mathbb{Z}$. On the other hand, we can factorise $4 = (1+\sqrt{-3})(1-\sqrt{-3})$ and note that $2 \nmid (1 \pm \sqrt{-3})$ which means that 2 is **not** prime in $\mathbb{Z}[\sqrt{-3}]$.

Theorem 9.1.7 (Fundamental Theorem of Arithmetic) *If $d \in \{-2, -1, 2, 3\}$, then every non-zero and non-unit $\alpha \in \mathbb{Z}[\sqrt{d}]$ can be expressed as a unique product of primes up to order, that is if $\alpha = \pi_1 \cdots \pi_r$ and $\alpha = \sigma_1 \cdots \sigma_s$ where π_i, σ_j are primes, then $r = s$ and the π_i and σ_s can be paired-off so that $\pi_i = u\sigma_j$ for some unit $u \in \mathbb{Z}[\sqrt{d}]$.*

Proof: Omitted (similar to Theorem 8.4.4). □

9.2 Solving $a^2 + 2b^2 = n$

Theorem 9.2.1 *Any $n \in \mathbb{Z}^+$ can be written in the form $n = a^2 + 2b^2$ for $a, b \in \mathbb{Z}$ if and only if the primes of the form $8k + 5$ and $8k + 7$ have even exponent in the prime factorisation of n.*

Proof: ($\Leftarrow$) Saying $n = a^2 + 2b^2$ is the same as saying n is the norm of an element of $\mathbb{Z}[\sqrt{-2}]$. Thus, any product of two such n can also be written in the same form. Clearly, any square is of the form $a^2 + 2b^2$ with $a = 0$. Now, if p is a prime integer **not** of the form $p \equiv 5 \pmod 8$ or $p \equiv 7 \pmod 8$, then either $p = 2$ or we have $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$. Clearly, $p = 2$ can be written in the form $a^2 + 2b^2$ (take $a = 0$ and $b = 1$). Now, notice that

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = 1$$

by the Supplementary Laws (Theorem 7.3.2); this means that -2 is a quadratic residue modulo p, that is there exists a solution to $x^2 \equiv -2 \pmod{p}$. Thus,

$$p \mid (x^2+2) \qquad \Leftrightarrow \qquad p \mid (x+\sqrt{-2})(x-\sqrt{-2}).$$

However, $p \nmid (x^2 \pm \sqrt{-2})$ and so p is **not** prime in $\mathbb{Z}[\sqrt{-2}]$. In particular, it is **not** irreducible, so can be written as a product of non-units $p = \alpha\beta$. Then, if $\alpha = a + b\sqrt{-2}$, we have

$$p = N(\alpha) = a^2 + 2b^2.$$

($\Rightarrow$) Suppose $p \mid n$ where $n = a^2 + 2b^2$ and $p \equiv 5 \pmod{8}$ or $p \equiv 7 \pmod{8}$. We shall show that $p \mid a$ and $p \mid b$. Well, we now have

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = -1$$

by the Supplementary Laws; this means that -2 is a quadratic non-residue modulo p, that is there is no solution to $x^2 \equiv -2 \pmod{p}$. However, we do have a solution to $x^2 \equiv 2y^2 \pmod{p}$ in $x = a$ and $y = b$. If $p \nmid y$, then we can divide by y^2 and express -2 as a quadratic residue, a contradiction. So $p \mid y$. Similarly, $p \mid x$. Thus, $p^2 \mid n$ and n/p^2 can be written in the same form. Proceeding inductively, it must involve p to an even power. □

Definition A Diophantine equation is one for which only integer solutions are considered.

Theorem 9.2.3 *The only Diophantine solutions to $x^2 + 2 = y^3$ are $x = \pm 5$ and $y = 3$.*

Proof: We can re-write the equation as $(x+\sqrt{-2})(x-\sqrt{-2}) = y^3$ and we will now show that the two factors on the left-hand side are coprime in $\mathbb{Z}\sqrt{-2}$. Indeed, suppose $\alpha \in \mathbb{Z}[\sqrt{-2}]$ is irreducible and divides both of $x \pm \sqrt{-2}$. Then, by subtracting, we see that

$$\alpha \mid (-2\sqrt{-2}) \qquad \Leftrightarrow \qquad \alpha \mid (\sqrt{-2})^3.$$

Since α is irreducible, and therefore prime, we see that $\alpha \mid \sqrt{-2}$ and we must have $N(\alpha) = 2$. Consequently, $\alpha = \pm\sqrt{-2}$ and we then conclude that

$$\sqrt{-2} \mid (x+\sqrt{-2}) \text{ in } \mathbb{Z}[\sqrt{-2}] \qquad \Rightarrow \qquad \sqrt{-2} \mid x \text{ in } \mathbb{Z}[\sqrt{-2}] \qquad \Rightarrow \qquad 2 \mid x^2 \text{ in } \mathbb{Z}.$$

This tells us that x is even, so $4 \mid x^2$. It follows that y is also even, so $8 \mid y^3$. This means that $x^2 + 2 \equiv 0 \pmod{4}$ which is impossible. Therefore, no prime of $\mathbb{Z}[\sqrt{-2}]$ can divide both of $x \pm \sqrt{-2}$ and thus they are coprime. Now, by the Fundamental Theorem of Algebra (specifically, the uniqueness of the factorisation), it must be that $x + \sqrt{-2}$ and $x - \sqrt{-2}$ are both cubes in $\mathbb{Z}[\sqrt{-2}]$. Indeed, say

$$x + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}.$$

Comparing coefficients of $\sqrt{-2}$, we have $1 = 3a^2b - 2b^3 = b(2a^2 - 2b^2)$, from which it follows that $b = \pm 1$. Therefore, we have also that $3a^2 - 2 = \pm 1$ and we have two options: (i) $3a^2 = 1$ which has no integer solutions and (ii) $3a^2 = 3$ which has $a = \pm 1$ as the only solutions. Thus,

$$x = a^3 - 6ab^2 = \pm 5 \qquad \Rightarrow \qquad y = \sqrt[3]{x^2+2} = 3.$$ □

9.3 Eisenstein Integers

Definition 9.3.1 The ring of Eisenstein integers is $\mathbb{Z}[\omega] \coloneqq \{a + b\omega : a, b \in \mathbb{Z}\}$, where

$$\omega \coloneqq \frac{-1 + \sqrt{-3}}{2} = e^{2\pi i/3}.$$

Note: The complex number ω satisfies the following quadratic equation: $\omega^2 + \omega + 1 = 0$.

Definition The norm of an Eisenstein integer $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ is defined as

$$N(\alpha) = a^2 - ab + b^2 = |a + b\omega|^2 = (a + b\omega)(a + b\omega^2).$$

Proposition *Let $\alpha, \beta \in \mathbb{Z}[\omega]$. Then, we have the following:*
(i) *The norm $N(\alpha\beta) = N(\alpha)N(\beta)$.*
(ii) *The norm $N(\alpha) = 0$ if and only if $\alpha = 0$.*
(iii) *The norm $N(\alpha) = 1$ if and only if α is a unit.*

Proof: Omitted (pretty much the same as those for $\mathbb{Z}[i]$ from Lemmata 8.2.2 and 8.2.3). □

Lemma *The set of units in $\mathbb{Z}[\omega]$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$.*

Proof: Let $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ be a unit. Since $N(\alpha) = 1$, this is equivalent to $a^2 - ab + b^2 = 1$. Using the fact that $a^2 + b^2 \geq 2|ab|$, we see that either $ab = 0$ or $ab = \pm 1$. Since $a, b \in \mathbb{Z}$, we have

$$(a, b) = (\pm 1, 0) \qquad \text{or} \qquad (0, \pm 1) \qquad \text{or} \qquad (1, 1) \qquad \text{or} \qquad (-1, -1).$$

These imply that $\alpha \in \{\pm 1, \pm\omega, \pm(1 + \omega)\}$, but using the quadratic equation in the above note, we see that $\pm(1 + \omega) = \mp\omega^2$ so we have the result. □

Theorem 9.3.3 (Division Algorithm for $\mathbb{Z}[\omega]$) *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ with $\beta \neq 0$. Then, there exist $q, r \in \mathbb{Z}[\omega]$ with $0 \leq N(r) < N(\beta)$ such that $\alpha = q\beta + r$.*

Proof: First, we write $\alpha/\beta = A + B\omega$ for some $A, B \in \mathbb{R}$. Let $q \in \mathbb{Z}[\omega]$ be as close as possible to α/β in this sense: set $q \coloneqq a + b\omega$ where $a, b \in \mathbb{Z}$ such that

$$|a - A| \leq \frac{1}{2} \qquad \text{and} \qquad |b - B| \leq \frac{1}{2}.$$

Let $r \coloneqq \alpha - q\beta \in \mathbb{Z}[\omega]$. We see that $\alpha = q\beta + r$ is satisfied. As for the inequality condition,

$$N(r) = N(\alpha - q\beta) = N\left(\frac{\alpha}{\beta} - q\right) N(\beta) \leq \frac{3}{4} N(\beta) < N(\beta).$$ □

Theorem *Any two Eisenstein integers $\alpha, \beta \in \mathbb{Z}[\omega]$ have a greatest common divisor γ. Moreover, there exist $s, t \in \mathbb{Z}[\omega]$ such that*

$$\gamma = s\alpha + t\beta.$$

Proof: Omitted (similar to Theorem 8.3.5). □

Theorem 9.3.4 *There are* **no** *integer solutions to $x^3 + y^3 + z^3 = 0$ with $xyz \neq 0$, so there are no non-trivial integer solutions to $x^3 + y^3 = z^3$ (Fermat's Last Theorem with $n = 3$).*

Proof: (**Non-examinable**) Omitted. □

9.4 Units in $\mathbb{Z}[\sqrt{d}]$ and Pell's Equation

Definition Let $d \in \mathbb{Z}^+$ not be a perfect square. Then, Pell's equation is $x^2 - dy^2 = 1$.

We view this as a Diophantine equation, meaning we are interested in integer solutions $x, y \in \mathbb{Z}$.

Note: The units of $\mathbb{Z}[\sqrt{d}]$ are elements $a + b\sqrt{d}$ with $a^2 - db^2 = \pm 1$. Consequently, the set of elements where this equality is $+1$ correspond to solutions of Pell's equation.

Lemma *Given two solutions to Pell's equation, the product of the corresponding units in $\mathbb{Z}[\sqrt{d}]$ gives another solution to Pell's equation. Furthermore, taking powers of a unit produces solutions to Pell's equation.*

Proof: This essentially boils down to the fact units are closed under products and inverses. □

Definition Let $a_1, a_2, ..., a_n \in \mathbb{Z}^+$ be a collection of positive integers and $a_0 \in \mathbb{Z}$ possibly negative. The finite continued fraction they generate is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

Notation For shorthand, we denote the above finite continued fraction by $[a_0; a_1, a_2, ..., a_n]$.

Definition Let $a_1, a_2, a_3, ... \in \mathbb{Z}^+$ be a sequence of positive integers and $a_0 \in \mathbb{Z}$ possibly negative. The infinite continued fraction they generate is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}.$$

Notation For shorthand, we denote the above infinite continued fraction by $[a_0; a_1, a_2, a_3, ...]$.

Theorem *Consider a real number $x \in \mathbb{R}$.*
(i) *If $x \in \mathbb{Q}$, then it admits a finite continued fraction expression.*
(ii) *If $x \notin \mathbb{Q}$, then it admits a* **unique** *infinite continued fraction expression.*

Definition The k^{th} convergent to the infinite continued fraction $[a_0; a_1, a_2, ...]$ is the finite

$$C_k := [a_0; a_1, a_2, ..., a_k].$$

Proposition 9.4.1 *We have the formula $C_k = p_k/q_k$ for the k^{th} convergent, where we have the recurrence relations defining the p_k and q_k as follows for all $k \geq 0$:*

$$p_k = a_k p_{k-1} + p_{k-2}, \quad \text{where} \quad p_{-2} = 0 \quad \text{and} \quad p_{-1} = 1,$$
$$q_k = a_k q_{k-1} + q_{k-2}, \quad \text{where} \quad q_{-2} = 1 \quad \text{and} \quad q_{-1} = 0.$$

Reminder: The floor function $\lfloor x \rfloor$ gives us the integer value of $x \in \mathbb{R}$ (it rounds it down).

Method – Continued Fraction of $\sqrt{d}$: Suppose $d > 1$ is not a square. We use $a_i \in \mathbb{Z}$ to denote the continued fraction integers and we define the numbers $b_i \in \mathbb{R}$ via $a_i = \lfloor b_i \rfloor$.
(i) Set $a_0 = \left\lfloor \sqrt{d} \right\rfloor$, meaning that $b_0 = \sqrt{d}$.
(ii) Set $a_1 = \left\lfloor \frac{1}{\sqrt{d} - a_0} \right\rfloor$, meaning that $b_1 = \frac{1}{\sqrt{d} - a_0}$.
(iii) Set $a_2 = \left\lfloor \frac{1}{b_1 - a_1} \right\rfloor$, meaning that $b_2 = \frac{1}{\frac{1}{\sqrt{d} - a_0} - a_1}$.
(iv) Set $a_{k+1} = \left\lfloor \frac{1}{b_k - a_k} \right\rfloor$ for general $k \geq 0$.
(v) Continue this until entries start to repeat.

Note: The continued fraction $\sqrt{d} = [a_0; \overline{a_1, ..., a_m}]$ repeats itself after we reach $a_m = 2a_0$.

Theorem 9.4.2 *If $d > 1$ ia not a perfect square, there always exist solutions to Pell's equation with $x, y > 0$. Moreover, they all arise as $(x, y) = (p_k, q_k)$ for convergents to $\sqrt{d}$.*

Proof: Omitted. □

Method – Solving Pell's Equation: We wish to solve $x^2 - dy^2 = 1$ for $d > 1$ not a square.

(i) Find the continued fraction expression of $\sqrt{d}$ using the previous method.

(ii) Create a so-called *magic table* recording k, a_k, p_k, q_k and $p_k^2 - dq_k^2$.

(iii) Whenever $p_k^2 - dq_k^2 = 1$, we have a solution $(x, y) = (p_k, q_k)$.