1 Show that the above division algorithm works for $\mathbb{Z}[i]$. *Hint*: Take $q' = a/b \in \mathbb{C}$ and let q be one of the closest gaussian integers to q'.

Solution We wish to show that given $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, there exist $q, r \in \mathbb{Z}[i]$ so that $a = bq + r$ and $N(r) < N(b)$.

Let $a, b \in \mathbb{Z}[i]$ with $b \neq 0$.

If $a = qb$ for some $q \in \mathbb{Z}[i]$, then $a = bq + 0$, and since $N(b) \neq 0$, we have $0 = N(r) < N(b)$. Assume from now on that $b \nmid a$ so that $N(r) \neq 0$.

Consider the following set:

$$S = \{N(n) \in \mathbb{Z}^+ \mid \exists q \in \mathbb{Z}[i] \text{ s.t. } n = a - bq\}.$$

This set is non-empty, indeed, given a, we can take $q = 0$ so that $n = a$, which means that $N(a) \in S$.

By well-ordering, S has a minimal element $N(r)$ for some $r \in \mathbb{Z}[i]$. By definition, we can write $a = bq + r$ for some $q \in \mathbb{Z}[i]$.

We claim that $N(r) < N(b)$.

Consider $q' = a/b$, which is not a Gaussian integer because $b \nmid a$. If we write $q' = \alpha + i\beta$, then we round α and β to the closest integers α' and β', respectively. Then

$$N\Big(\frac{a}{b} - c\Big) = (\alpha - \alpha')^2 + (\beta - \beta')^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

Thus,

$$a = bc + s \implies s = a - bc \in S.$$

Since r was the least element of S,

$$N(r) \leq N(s) = N(bc - a) \leq N(b)N\Big(c - \frac{a}{b}\Big) < N(b),$$

as desired.

---

2 Show that a gcd d of a, b exists and is a linear combination of a, b. *Hint*: Look for the $\mathbb{Z}[i]$ linear combination of a, b of the smallest norm.

Solution If a or b are 0, then there's nothing to prove, so assume that they are both non-zero from now on.

Consider the set $S = (N(na + mb) \in \mathbb{Z}^+ \mid n, m \in \mathbb{Z}[i] \text{ and } N(na + mb) > 0)$, which is clearly non-empty since a and b are non-empty.

By well-ordering, it contains a minimal element $N(na + mb)$ for some $n, m \in \mathbb{Z}[i]$. We'll call this element d and show that it is a gcd of a and b.

Assume that $d \nmid b$. Then $b = qd + r$, for some $q \in \mathbb{Z}[i]$ and $0 < N(r) < N(d)$. Then

$$b = q(na + mb) + r \implies r = (1 - qm)b - qna \implies N(r) \in S.$$

Since $N(d)$ was the minimal element, we have

$$N(r) \geq N(d),$$

which is a contradiction. Hence, $r = 0$ and $d \mid a$. By the same argument, $d \mid b$ also.

All that's left is to show that if we have $e \in \mathbb{Z}[i]$ with $e \mid a$ and $e \mid b$, then $e \mid d$.

$e \mid a \implies a = \alpha e$, $e \mid b \implies b = \beta e$, for some $\alpha, \beta \in \mathbb{Z}[i]$. Then

$$d = ma + nb = m\alpha e + n\beta e = (m\alpha + n\beta)e,$$

so $e \mid d$.

3** Show that if d is irreducible and $d \mid ab$, then $d \mid a$ or $d \mid b$.

Solution We first prove a lemma: If e is a gcd of a, b with $N(e) = 1$, then $1, -1, i, and - i$ are also gcd's of a and b.

Note that if $e = a + ib$, then $N(e) = a^2 + b^2 = 1 \implies a^2 = 1$ and $b^2 = 0$, or $a^2 = 0$ and $b^2 = 1$. It is easy to see that this implies that $a = 1, -1$ or $b = 1, -i$. Altogether, we get that $e \in \{1, -1, i, -i\} \subseteq \mathbb{Z}[i]$.

Thus, since $N(e) = 1$, $e \in \{1, -1, i, -i\}$. We can rotate between all the different units by multiplying by powers of i. Hence, since e is a gcd of a and b, there exist $n, m \in \mathbb{Z}[i]$ such that

$$e = na + mb \implies ei^k = i^k na + i^k mb$$

for any $k \in \mathbb{Z}^+$.

Moreover, $i^k e \mid e$ since we can multiply by i's until we get e again. Thus, the lemma is proved.

Since $d \mid ab$, there exists $k \in \mathbb{Z}[i]$ such that $ab = kd$.

Assume without loss of generality that $d \nmid a$.

Because d is irreducible, e with $|e| = 1$ is a gcd of d and a. By the lemma, 1 is also a gcd of d and a, so

$$1 = nd + ma \implies b = ndm + mab \implies b = ndm + mkd = (nm + mk)d,$$

so $d \mid b$. In the other case, $d \mid a$, so we're done.

---

4 Suppose $p \in \mathbb{Z}$ is a prime. Show p is not irreducible in the Gaussian integers if and only if there are $a, b \in \mathbb{Z}$ so the $p = a^2 + b^2$.

Solution "$\implies$"

Since p is not prime, there exist $a, b, \alpha, \beta \in \mathbb{Z}$ such that $p = (a + bi)(\alpha + \beta i)$.

By multiplicity of the norm,

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

But $N(a + bi)$ and $N(\alpha + \beta i)$ are integers and p is prime, so this implies that exactly one of the factors must be 1. Assume without loss of generality that $N(\alpha + \beta i) = 1$. Then

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

as desired.

"$\impliedby$"

We can write $p = (a + bi)(a - bi)$. If $p = N(p)$ were prime, then this implies that either $N(a + bi) = 1$ or $N(a - bi) = 1$. Either way, it implies that $p = a^2 + b^2 = 1$, which is a contradiction, since 1 is not prime. Hence, p is not prime.

5** Define a relation on $\mathbb{Z}^+ \times \mathbb{Z}^+$:

$$(a, b) \sim (c, d)$$

if

$$a + d = b + c.$$

Show $\sim$ is an equivalence relation and identify the equivalence classes with a familiar object.

Solution Let $(a, b), (c, d), (e, f) \in \mathbb{Z}^+ \times \mathbb{Z}^+$.

$a + b = b + a$, by commutativity of addition on $\mathbb{Z}^+$, so $(a, b) \sim (a, b)$, which means reflexivity holds.

Assume $(a, b) \sim (c, d)$. Then $a + d = b + c \implies b + c = a + d$, by symmetry of $=$, so $(c, d) \sim (a, b)$, which means symmetry holds.

Assume $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. By definition,

$$\begin{aligned} (a, b) \sim (c, d) &\iff a + d = b + c \implies a = b + c - d \\ (c, d) \sim (e, f) &\iff c + f = d + e \end{aligned}$$

Then

$$a + f = (b + c - d) + f = b - d + (c + f) = b - d + d + e = b + e \iff (a, b) \sim (e, f),$$

which means transitivity holds.

Thus, $\sim$ defines an equivalence relation.

Consider the map $(a, b) \mapsto a - b$, which we'll call f. We'll first show that f is well-defined.

Let $(a, b), (a', b')$ such that $(a, b) \sim (a', b')$. Then by definition,

$$a + b' = b + a' \iff a - b = a' - b'.$$

Thus,

$$\begin{aligned} f((a, b)) &= a - b \\ f((a', b')) &= a' - b' = a - b = f((a, b)), \end{aligned}$$

so f is well-defined.

Note that this is one-to-one, by definition of the equivalence relation. It is also onto; given $x \in \mathbb{R}$, $(x, 0) \mapsto x$, so this is a bijection. Hence, we can identify the set of equivalence classes with $\mathbb{R}$.

6 Let $\mathbb{R}[x]$ be the set of real-valued polynomials in one variable. Define an equivalence relation of $\mathbb{R}[x]$ by $P(x) \sim Q(x)$ if x^2+1 divides $P(x) - Q(x)$. Show $\sim$ is an equivalence relation. If $[P(x)]$ is the equivalence class of $P(x)$, show that the function

$$H([P(x)]) = P(i) \in \mathbb{C}$$

is well-defined, where $i^2 = -1$. Identify the equivalence classes of $\sim$ with a familiar object. You can use the properties of polynomial division, e.g., the division algorithm for polynomials.

Solution Note that by the division algorithm, for any $P(x) \in \mathbb{R}[x]$, there exists $q(x), r(x) \in \mathbb{R}[x]$ such that $P(x) = q(x)(x^2+1) + r(x)$.

Let $P(x), Q(x), R(x) \in \mathbb{R}[x]$.

$P(x) - P(x) = 0 = 0(x^2+1) \implies P(x) \sim P(x)$, so reflexivity holds.

Let $P(x) \sim Q(x)$. Then for some $r(x) \in \mathbb{R}[x]$, $P(x) - Q(x) = r(x)(x^2+1) \implies Q(x) - P(x) = -r(x)(x^2+1)$, so $(x^2+1) \mid Q(x) - P(x) \implies Q(x) \sim P(x)$, which means symmetry holds.

Let $P(x) \sim Q(x)$ and $Q(x) \sim R(x)$. By definition, there exists $r(x), s(x) \in \mathbb{R}[x]$ such that

$$\begin{aligned} P(x) - Q(x) &= r(x)(x^2+1) \\ Q(x) - R(x) &= s(x)(x^2+1). \end{aligned}$$

Summing them, we get $P(x) - R(x) = (r(x) + s(x))(x^2+1)$, so $(x^2+1) \mid P(x) - R(x) \implies P(x)R(x)$, so transitivity holds.

Thus, $\sim$ is an equivalence relation.

We'll now show that H is well-defined.

Let $P(x), P'(x)$ be such that $P(x) \sim P'(x)$. Then

$$H(P(x)) - H(P'(x)) = P(i) - P'(i) = r(i)(i^2+1) = 0 \implies H(P(x)) = H(P'(x)),$$

so H is well-defined.

We can identify $R(x)/\sim$ with $\mathbb{C}$. Indeed, any polynomial in $\mathbb{R}[x]$ belongs to the equivalence class of a linear polynomial $a + bx$, since higher order terms will disappear. Moreover, if $a \neq a'$ or $b \neq b'$ the equivalence classes $[a+bx]$ and $[a'+b'x]$ are disjoint. Otherwise, $(a-a') + (b-b')x = r(x)(x^2+1) \equiv 0$, since the left-hand side contains no quadratic factors, which implies $[a+bx] = [a'+b'x]$.

We can map the equivalence classes of $\mathbb{R}[x]/\sim$ with $a+bi$, by replacing x with i. This is obviously a bijection, so we can identify the equivalence classes with $\mathbb{C}$.

4.17.11** Define $\sigma\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ by $\sigma(n) = \sum_{d|n} d$, the sum of the (positive) divisors of n. Show

a. If m and n are relatively prime (positive) integers, then $\sigma(mn) = \sigma(m)\sigma(n)$.

b. If p is a (positive) prime integer and n an integer, then $\sigma(p^n) = (p^{n+1} - 1)/(p - 1)$.

Solution a. Let m and n be relatively prime integers. Note that if $d_1 \mid m$ and $d_2 \mid n$, then $d_1 d_2 \mid mn$. Indeed, we can write $m = d_1 a$ and $n = d_2 b$ so that $mn = (d_1 d_2)ab$.

Consider the map
$$D \coloneqq \{(d_1, d_2) \mid d_1 \mid m \text{ and } d_2 \mid n\} \mapsto d_1 d_2,$$
which we claim is one-to-one. This implies that the representation of factors of mn as a product of a factor of m and a factor of n is unique.

Since m and n are relatively prime, if $(d_1, d_2) \in D$, then $(d_2, d_1) \notin D$, unless $(d_1, d_2) = (d_2, d_1) \implies d_1 = d_2 = 1$. Moreover, non-trivial factors of d_1 cannot be factors of n, and non-trivial factors of d_2 cannot be factors of m. Thus, if $(e_1 e_2, d_2) \in D$, then $(e_1, d_2 e_2) \notin D$ (or any other permutations of e_1, e_2, d_2. Thus, if $d_1 d_2 = e_1 e_2$, then $d_1 = e_1$ and $d_2 = e_2$.

We next show that any divisor of mn can be written as the product described.

Let $d \mid mn$, and reduce d to its prime factorization so that $d_1 d_2 \cdots d_n \mid mn$. In particular, $d_i \mid mn$ for all i, which means that for each d_i, either $d_i \mid m$ or $d_i \mid n$. So, we can separate the d_i so that $d = (d_{i_1} \cdots d_{i_k})(d_{j_1} \cdots d_{j_\ell})$, where the d_i are factors of m and d_j are factors of n.

Hence, all factors of mn are products of factors of m and factors of n, and the product representation is unique.

Finally, this gives us that
$$\sigma(mn) = \sum_{d|mn} d = \sum_{d_1|m, d_2|n} d_1 d_2 = \sum_{d_1|m} \sum_{d_2|n} d_1 d_2 = \sum_{d_1|m} \left[d_1 \left(\sum_{d_2|n} d_2 \right) \right] = \left(\sum_{d_1|m} d_1 \right) \left(\sum_{d_2|m} d_2 \right) = \sigma(m)\sigma(n).$$

b. Let p be prime. Then the unique prime factorization of p^n is itself, so the only divisors of p^n are $1, p, p^2, \ldots, p^n$. No other prime divides p^n, so no other numbers divide p^n. Thus,
$$\sigma(p^n) = \sum_{k=0}^{n} p^k = \frac{1 - p^{n+1}}{1 - p} = \frac{p^{n+1} - 1}{p - 1},$$
by geometric series.