Chapter 11

Section 11.1

Question:
16. Let $a$ and $b$ be relatively prime integers. Prove that there are integers $m, n$ such that $a^m + b^n \equiv 1 \pmod{ab}$.

Answer:
Since $a, b$ are relatively prime we have that $\mathbb{Z}_{ab} \approx \mathbb{Z}_a \times \mathbb{Z}_b$ with $\varphi: \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ such that $\varphi(c) = (c \mod a, c \mod b)$ are an isomorphism. (You should check that indeed $\varphi$ is an isomorphism).

Since $\mathbb{Z}_a$ is a finite group $\exists j > \ell > 0$ such that $b^j \equiv b'^j \pmod{a}$, which implies that $b^j \equiv b^\ell \equiv 0 \pmod{a}$ and $b^j(1 - b^\ell) \equiv 0 \pmod{a}$. Since $a$ and $b$ are relatively prime, then $b^j$ has an inverse and $(1 - b^\ell) \equiv 0 \pmod{a}$, i.e. there exist an integer $n$ such that $b^n = 1 \pmod{a}$. Similarly, there exist an integer $m$ such that $a^m \equiv 1 \pmod{b}$. But
$$\varphi(a^m + b^n) = \varphi(a^m) + \varphi(b^n) = (b^n \mod a, b^n \mod b) = (0, 1) + (1, 0) = (1, 1).$$
Since $\varphi$ is an isomorphism, this means that $a^m + b^n \equiv 1 \pmod{ab}$.

Section 11.2

Question:
1. Prove the following.
   a.) The polynomial ring $\mathbb{R}[x, y]$ in two variables is a Euclidean domain.

Answer:
   a.) If $\mathbb{R}[x, y]$ was a Euclidean domain then $\mathbb{R}[x, y]$ would be a principal ideal domain. But if $\mathbb{R}[x, y]$ is a PID then the maximal ideals are the principal ideals generated by irreducible elements. The polynomial $x$ is irreducible, so $(x)$ would be a maximal ideal. On the other hand, the ideal $(x, y)$ is an ideal which is not all of $\mathbb{R}[x, y]$, since polynomials $p(x, y)$ such that $p(0, 0) \neq 0 \notin (x, y)$. But clearly $x \in (x, y)$, thus, $(x) < (x, y)$, contradicting the fact that $(x)$ was maximal.

   b) The ring $\mathbb{Z}[x]$ is a principal ideal domain.
Answer:

b.) A similar argument with \((2, x) \subset \mathbb{Z}[x]\) and \((2) \subset (2, x)\) yields that \(\mathbb{Z}[x]\) is not a PID.

Question:

2. Prove that the following rings are Euclidean domains.
   a) \(\mathbb{Z}[w] , w = e^{2\pi i/3}\)  
   b) \(\mathbb{Z} \left[ \sqrt{-f/2} \right]\).

Answer:

An integral domain \(\mathbb{R}\) with a size function \(\sigma: \mathbb{R} - \{0\} \to \{0, 1, 2, \ldots\}\) such that if \(a, b \in \mathbb{R}\) and \(a \neq 0\) then there exists elements \(q, r \in \mathbb{R}\) such that \(b = aq + r\) and either \(\sigma(r) = 0\) or \(\sigma(r) < \sigma(a)\), is a Euclidean domain.

a) Let \(w = e^{2\pi i/3} = \frac{-1}{2} + i \frac{\sqrt{3}}{2}\)
\[\begin{align*}
w^2 &= e^{4\pi i/3} = \frac{-1}{2} - i \frac{\sqrt{3}}{2} = -(1 + w) \\
w^3 &= 1
\end{align*}\]

Thus, \(\mathbb{Z}[w] = \{a + bw / a, b \in \mathbb{Z}\}\). It is easy to check that \(\mathbb{Z}[w]\) is an integral domain.
Define a size function \(\sigma: \mathbb{Z}[w] \to \{0, 1, 2, \ldots\}\)
by \(\sigma(a + bw) = a^2 + b^2 - ab\).

We must show that for any \(x, y \in \mathbb{Z}[w], y \neq 0 \exists q, r \in \mathbb{Z}[w]\) such that
\(x = yq + r\) with \(\sigma(r) < \sigma(y)\) or \(\sigma(r) = 0\).
First it is easy to show that we can always write \(x\) has a “multiple” of \(y\), i.e.:
\(x = zy\) where \(z = z_0 + z_1 w\) and \(z_0, z_1 \in \mathbb{R}\).

Write \(z_0 = k + z'_0\) where \(|z_0| \leq \frac{1}{2}\) and \(z_1 = \ell + z'_1\) where \(|z'_1| \leq \frac{1}{2}\) and \(k, \ell \in \mathbb{Z}\). Let \(q = k + \ell w\) and \(r = x - qy\). Then clearly \(x = qy + r\) with \(q \in \mathbb{Z}[w]\) and \(r = x - (k + \ell w)y \in \mathbb{Z}[w]\). Thus, it remains to show that \(\sigma(r) < \sigma(y)\) which can be done by straightforward computation.

b) Let \(R = \mathbb{Z} \left[ \sqrt{-2} \right] = \{a + b \sqrt{-2} / a, b \in \mathbb{Z}\}\). It is easy to check that \(R\) is an integral domain. Again, given 2 elements \(k = a + b \sqrt{-2}, y = c + d \sqrt{-2}\) we can write \(x = yz\) where \(z = e + f \sqrt{-2}\) with \(e, f \in \mathbb{R}\). Let \(e = e_0 + r_1\) and \(f = f_0 + r_1\) with \(e_0, f_0 \in \mathbb{Z}\) and \(|r_i| \leq \frac{1}{2}\) for \(i = 1, 2\). Then
\[\begin{align*}
x &= y((e_0 + r_1) + (f_0 + r_1) \sqrt{-2}) \\
&= y(e_0 + f_0 \sqrt{-2}) + y(r_1 + r_2 \sqrt{-2}).
\end{align*}\]
Define $\sigma : \mathbb{Z}[\sqrt{-2}] \to \{0, 1, 2, \ldots\}$ by
\[
\sigma(a + b\sqrt{-2}) = a^2 + 2b^2
\]
It is a tedious but straightforward calculation to verify that $\sigma(r) = 0$ or $\sigma(r) < \sigma(y)$ where $r = y(r_1 + r_2\sqrt{-2})$. Hence, $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

**Question:**
3. Give an example showing that division with remainder need not be unique in a Euclidean domain.

**Answer:**
Let $\mathbb{Z}[i]$ be the Euclidean domain with $\sigma : \mathbb{Z}[i] \to \{0, 1, 2, \ldots\}$ given by
\[
\sigma(a + bi) = a^2 + b^2
\]
We can see that $(2 + 3i) = (2 + i)(2 + i) + (-1 - i)$
and $(2 + 3i) = (2 + i)(1 + i) + 1$
and $|1|^2 = 1 < 2^2 + 3^2$ and $1^2 + 1^2 = 2 < 13$. Hence factorization need not be unique in an Euclidean domain.

**Question:**
6. Prove Proposition (2.8), that a domain $R$, which has existence of factorizations is a unique factorization domain if and only if every irreducible element is prime.

**Answer:**
Assume every irreducible element of $R$ is prime. Let $a = p_1 \ldots p_m = q_1 \ldots q_n$ be two factorizations of $a$. Since $p_1$ is prime and $p_1 | q_1 \ldots q_n$, then $p_1$ divides some $q_i$. Reorder the $q_i$’s so that $q_i = q_1$. Since $q_i$ is irreducible and $p_1$ is not a unit, then $p_1$ is an associate of $q_1$. So we have that $p_1$ and $q_1$ are associates. Proceed in the same manner for $a' = p_2 \ldots p_m = q_2 \ldots q_n$ to obtain that $n = m$ and with a suitable ordering $p_i$ and $q_i$ are associates for $i = 1, \ldots, n$.

Suppose now that we have unique factorization domain. Let $p$ be an irreducible that divides $ab$, that is $\exists q \in R$ such that $pq = ab$. If either $a$ or $b$ is a unit, then $p$ divides the other one. Otherwise let $a = a_1 \ldots a_m$ and $b = b_1 \ldots b_n$ be their factorizations and let $q = q_1 \ldots q_k$. Then $ab = a_1 \ldots a_m b_1 \ldots b_n = pq_1 \ldots q_k$ are 2 factorizations of $ab$. Hence $p$ is an associate of one of the elements of $\{a_1, \ldots, a_m, b_1, \ldots, b_n\}$. Thus $p | a$ or $p | b$. 

Typeset by Georgeann Lorentz
Question:
8. Find the greatest common divisor of \((11 + 7i, 18 - i)\) in \(\mathbb{Z}[i]\).

Answer:
Using the “Euclidean” algorithm with \(\sigma = 11^2\) we have that

\[
\begin{align*}
18 - i &= (11 + 7i)(1 - i) + 3i \\
11 + 7i &= (3i)(2 - 4i) + (-1 + i) \\
3i &= (-1 + i)(1 - i) + 1 \\
(-1 + i) &= 1(-1 + i) + 0
\end{align*}
\]

So a \(\text{gcd}(11 + 7i, 18 - i) = 1\) in \(\mathbb{Z}[i]\). Note that \(-1, \pm i\) are also gcd of \(11 + 7i\) and \(18 - i\).