1 Reading
1. Read Chapter 9 of Dummit and Foote

2 Problems
1. 9.1.13

Solution: We already know that if $R$ is any commutative ring, then $R[x]/(x-r) \cong R$ for any $r \in R$. In the present situation we let $R = F[y]$, then

$$F[x, y]/(y^2 - x) = F[x, y]/(x - y^2) = R[x]/(x - y^2) \cong R = F[y].$$

This shows that $F[x, y]/(x - y^2)$ in an integral domain. The ring $F[x, y]/(y^2 - x^2)$, on the other hand, has zero divisors. In this ring,

$$0 = \bar{y}^2 - \bar{x}^2 = (\bar{y} - \bar{x})(\bar{y} + \bar{x}),$$

and neither $\bar{y} - \bar{x}$ nor $\bar{y} + \bar{x}$ are zero in this ring. This shows that $F[x, y]/(y^2 - x^2)$ and $F[x, y]/(y^2 - x)$ cannot be isomorphic.

2. 9.1.14

Solution: Consider the map $\varphi: R[x, y] \to R[t]$ given by

$$x \mapsto t^j$$
$$y \mapsto t^i$$

where $i, j$ are relatively prime positive integers. Then

$$\varphi(x^i - y^j) = (t^j)^i - (t^i)^j = 0$$

showing that $x^i - y^j \in \ker(\varphi)$. The purpose of this problem is to show that $\ker(\varphi) = (x^i - y^j)$ since then the first isomorphism theorem would yield that $R[x, y]/(x^i - y^j)$ is isomorphic to a subring of $R[t]$, and hence is an integral domain and thus $(x^i - y^j)$ is prime.

To achieve this, let $f(x, y) \in \ker(\varphi)$. The polynomial $x^i - y^j$ is monic in $y$ and hence if we view $R[x, y]$ as $(R[x])[y]$ then the results of 7.4.14 tell us that there exists $p(x, y) \in R[x, y]$ having $y$ degree less than $j$ with

$$f(x, y) \equiv p(x, y) \pmod{x^i - y^j}.$$ 

Thus we may write

$$p(x, y) = \sum_{r=0}^{n} \sum_{s=0}^{j-1} a_{rs} x^r y^s$$

for some $n \geq 0$ and $a_{rs} \in R$.

Since both $f(x, y)$ and $x^i - y^j$ are contained in $\ker(\varphi)$, it follows that $p(x, y) \in \ker(\varphi)$ as well. Thus

$$0 = \varphi(p(x, y)) = \sum_{r=0}^{n} \sum_{s=0}^{j-1} a_{rs} \varphi(x^r y^s)$$

$$= \sum_{r=0}^{n} \sum_{s=0}^{j-1} a_{rs} t^{r+s}.$$
I claim that the exponents showing up on the right hand side of the above equation are distinct integers. To prove this, assume there exist non-negative integers \( r \) and \( r' \), and integers \( 0 \leq s, s' < j \) with

\[
jr + is = jr' + is'.
\]

Rewrite this equation as

\[
j(r - r') = i(s' - s).
\]

Then \( j \mid i(s - s') \), but \( \gcd(i, j) = 1 \) implies that \( j \mid s - s' \). Since \( 0 \leq s, s' < j \) this forces \( s = s' \). Thus \( jr = jr' \) and by cancellation (R is an integral domain) we get \( r = r' \) as well. Therefore, since

\[
0 = \sum_{r=0}^{n} \sum_{s=0}^{j-1} a_{rs} t^{jr+is}
\]

yet all the degrees of terms on the right hand side are distinct integers, we must have all \( a_{rs} = 0 \). This proves that \( p(x, y) = 0 \) and hence

\[
f(x, y) \equiv 0 \pmod{x^i - y^j}.
\]

We have just proved that \( \ker(\varphi) \subseteq (x^i - y^j) \) which by our above remarks proves equality, and therefore the ideal \( (x^i - y^j) \) is prime.

### 3. 9.2.2

**Solution:** Let \( F \) be a finite field of order \( q \), and let \( f(x) \in F[x] \) be a polynomial of degree \( n \). Since \( (f(x)) = (cf(x)) \) for any \( c \in F^\times \), we may assume WLOG that \( f(x) \) is monic. By 7.4.14, we know that every \( g(x) \in F[x] \) is congruent modulo \( f(x) \) to a unique polynomial

\[
a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0
\]

where \( a_i \in F \). Since there are \( q \) possibilities for each \( a_i \), and there are \( n \) coefficients, we see that there are \( q^n \) elements in \( F[x]/(f(x)) \).

### 4. 9.2.3

**Solution:** Let \( f(x) \in F[x] \). The ring \( F[x] \) is a PID, hence \( f(x) \) is irreducible if and only if the ideal \( (f(x)) \) is prime if and only if the ideal \( (f(x)) \) is maximal. Thus \( f(x) \) is irreducible if and only if \( F[x]/(f(x)) \) is a field.

### 5. 9.2.5

**Solution:** By the fourth isomorphism theorem, ideals in \( F[x]/(p(x)) \) are in one-to-one correspondence with ideals in \( F[x] \) containing \( (p(x)) \). The ring \( F[x] \) is a PID, so every ideal containing \( (p(x)) \) is generated by some element \( f(x) \in F[x] \). Of course \( (f(x)) \subseteq (p(x)) \) if and only if \( p(x) \) divides \( f(x) \), so we see that the ideals containing \( f(x) \) are precisely those generated by divisors of \( f(x) \). To deal with the fact that associate elements generate the same ideal, we can just stick to monic divisors of \( p(x) \). Thus the ideals in \( F[x]/(p(x)) \) are precisely the principal ideals \( (f(x)) \) where \( f(x) \) is a monic divisor of \( p(x) \).
6. 9.3.1

Solution: We prove this by proving the contrapositive. Let $R$ be a UFD and let $p(x) \in R[x]$ be a monic polynomial. Assume that $p(x) = a(x)b(x)$ where $a(x), b(x) \in F[x]$ are monic polynomials. By Proposition 5, there exist $\alpha, \beta \in F$ with

$$p(x) = A(x)B(x)$$

where $A(x) = \alpha a(x) \in R[x]$ and $B(x) = \beta b(x) \in R[x]$. Since $a(x)$ and $b(x)$ are monic, the leading coefficient of $A(x)$ is $\alpha$ and the leading coefficient of $B(x)$ is $\beta$, implying that $\alpha, \beta \in R$. Moreover, the leading coefficient of $A(x)B(x)$ is $\alpha \beta$ and the leading coefficient of $p(x)$ is 1, so in fact $\alpha \beta = 1$. Thus

$$a(x) = \beta A(x)$$
$$b(x) = \alpha B(x)$$

show that both $a(x), b(x) \in R[x]$.

Now, by definition we have $\sqrt{2} \notin \mathbb{Z}[2\sqrt{2}]$, yet $\sqrt{2} = \frac{2\sqrt{2}}{2}$ showing that $\sqrt{2}$ is an element of the fraction field of $\mathbb{Z}[2\sqrt{2}]$. We have

$$(x - \sqrt{2})(x + \sqrt{2}) = x^2 - 2 \in \mathbb{Z}[2\sqrt{2}][x]$$

proving that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

7. 9.3.2

Solution: Let $f(x), g(x) \in \mathbb{Q}[x]$ have the property that $f(x)g(x) \in \mathbb{Z}[x]$. Extracting a lowest common denominator, following by factoring out common factors from the remaining coefficients, we may write

$$f(x) = \frac{a}{b} \cdot \tilde{f}(x)$$
$$g(x) = \frac{c}{d} \cdot \tilde{g}(x)$$

where $\tilde{f}(x), \tilde{g}(x) \in \mathbb{Z}[x]$ both have content 1 and $\gcd(a, b) = \gcd(c, d) = 1$. Gauss’s Lemma implies that $\operatorname{ct}(f(x)\mathbb{Z}[x]) = 1$ as well, and since

$$f(x)g(x) = \frac{ac}{bd} \cdot \tilde{f}(x)\tilde{g}(x)$$

has integer coefficients, we must have $bd \mid ac$. Any coefficient of $f(x)$ is of the form $\frac{a}{b} \cdot m$ where $m \in \mathbb{Z}$ and similarly any coefficient of $g(x)$ is of the form $\frac{c}{d} \cdot n$ where $n \in \mathbb{Z}$. Their product equals $\frac{ac}{bd} \cdot mn$ which is an integer since $bd \mid ac$.

8. 9.4.8

Solution: To prove that both of these rings are fields, it suffices to show that $f(x) = x^2 + 1$ and $g(y) = y^2 + 2y + 2$ are irreducible in $\mathbb{F}_{11}[x]$ and $\mathbb{F}_{11}[y]$ respectively. Since these polynomials have
degree 2, we can just check to see that they do not have roots. We have

<table>
<thead>
<tr>
<th>a</th>
<th>f(a)</th>
<th>g(a)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

showing that \( f(x) \) and \( g(y) \) are irreducible. Both \( K_1 \) and \( K_2 \) are thus fields and have size 121 since \( f(x) \) and \( g(y) \) have degree 2. Now, consider the map

\[
\psi: \mathbb{F}_{11}[x] \to K_2
\]

given by \( p(x) \mapsto p(\bar{y} + 1) \). The evaluation map is a ring homomorphism, and

\[
\psi(x^2 + 1) = (\bar{y} + 1)^2 + 1 = \bar{y}^2 + 2\bar{y} + 2 = 0.
\]

Thus \( x^2 + 1 \in \ker(\psi) \) so \( \psi \) induces a ring homomorphism

\[
\mathbb{F}_{11}[x]/(x^2 + 1) \to \mathbb{F}_{11}[y]/(y^2 + 2y + 2).
\]

The map \( \psi \) is surjective since \( \psi(x-1) = \bar{y} \). Thus the induced map \( K_1 \to K_2 \) is surjective. Since both fields have the same cardinality, this map is necessarily injective and therefore is an isomorphism.

REMARK: By the quadratic formula, the polynomial \( x^2 + 1 \) has a root in \( \mathbb{F}_{11} \) if and only if \( \sqrt{-1} \in \mathbb{F}_{11} \), and \( y^2 + 2y + 2 \) has a root in \( \mathbb{F}_{11} \) if and only if \( \sqrt{-4} = \sqrt{7} \in \mathbb{F}_{11} \). Notice that both polynomials are irreducible if and only if \(-1\) is not a square in \( \mathbb{F}_{11} \) since \(-4\) is a square if and only if \(-1\) is a square. Of course \( 11 \equiv 3 \pmod{4} \) so we’ve previously proven that \(-1\) is not a square for such primes.

9. 9.4.11

**Solution:** To prove that \( x^2 + y^2 - 1 \) is irreducible in \( \mathbb{Q}[x,y] \), it suffices to prove that it is irreducible in \( (\mathbb{Q}[y])[x] \). Let \( R = \mathbb{Q}[y] \). The element \( y - 1 \in R[y] \) is irreducible hence prime since \( R \) is a UFD. Notice that

\[
y^2 - 1 = (y - 1)(y + 1)
\]

so \( y - 1 \) divides \( y^2 - 1 \) yet \( (y - 1)^2 \) does not divide \( y^2 - 1 \). Since \( x^2 + (y^2 - 1) \in R[x] \) is monic, Eisenstein tells us that \( x^2 + y^2 - 1 \) is irreducible.

10. 9.4.12

**Solution:** The book proves that

\[
f(x) = x^{n-1} + x^{n-2} + \ldots + x + 1
\]
is irreducible when \( n \) is prime. Thus we should prove that \( f(x) \) is reducible when \( n \) is composite. We have
\[
x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x + 1).
\]
By unique factorization in \( \mathbb{Z}[x] \), it thus suffices to prove that \( x^n - 1 \) has more than two irreducible factors. Since \( n \) is composite, we may write \( n = ab \) for integers \( a, b > 1 \). I claim that \( x^{a - 1} - 1 \) divides \( x^n - 1 \). To see this, we work modulo \( x^{a - 1} - 1 \) to get
\[
x^n - 1 = (x^{a - 1})^b - 1
\]
\[
\equiv 1^b - 1 \pmod{x^a - 1}
\]
\[
\equiv 0 \pmod{x^a - 1}.
\]
Thus there exists \( g(x) \in \mathbb{Z}[x] \) (this polynomial is easy to write down explicitly) with
\[
x^n - 1 = (x^{a - 1})g(x) = (x - 1)(x^{a - 1} + x^{a - 2} + \ldots + x + 1)g(x)
\]
showing that \( x^n - 1 \) has at least three irreducible factors.

11. 9.4.13

**Solution:** The polynomial \( f(x) = x^3 + nx + 2 \in \mathbb{Z}[x] \) is monic and non-constant, hence is irreducible over \( \mathbb{Z} \) if and only if it is irreducible over \( \mathbb{Q} \). Since \( f(x) \) has degree 3, it is irreducible if and only if it has a root in \( \mathbb{Q} \). By the rational root theorem, the only possible roots are \( \pm 1, \pm 2 \). Evaluating we get
\[
f(0) = 1 \quad f(1) = n + 3 \\
f(-1) = 1 - n \\
f(2) = 2n + 10 \\
f(-2) = -6 - 2n.
\]
Setting each of these equal to 0 and solving for \( n \) shows that \( f(x) \) is reducible if and only if \( n = 1, -3, \) or \(-5\).

12. Prove that the polynomial \( f(x) = x^2 + x + 1 \in \mathbb{F}_5[x] \) is irreducible. Find an element in \( \mathbb{F}_5[x]/(x^2 + x + 1) \) which generates the group of units.

**Solution:** Since \( f(x) \) has degree 2, to check if \( f(x) \) is irreducible it suffices to show that \( f(x) \) has no roots in \( \mathbb{F}_5 \). We can compute
\[
f(0) = 1 \\
f(1) = 3 \\
f(2) = 2 \\
f(3) = 3 \\
f(4) = 1
\]
showing that \( f(x) \) is irreducible and hence \( \mathbb{F}_5[x]/(x^2 + x + 1) \) is a field of 25 elements. There are several ways to find a generator for the multiplicative group of units in this field. The most brute
force way is to just start taking powers of various elements and looking for elements with order 24. Here is an alternative way.

We know that \( x^3 - 1 = (x - 1)(x^2 + x + 1) \), so in \( \mathbb{F}_5[x]/(x^2 + x + 1) \) we have \( |\bar{x}| = 3 \) (for those of you who didn’t take 502, this is the notation we used for the order of an element in a group). It’s easy to check that \( |\bar{2}| = 4 \) (in particular, \( 2 \) generates the group of units in \( \mathbb{F}_5 \)) so since \( \gcd(3, 4) = 1 \) we get \( |2\bar{x}| = 12 \). Thus we will be done if we can find some \( \alpha \in \mathbb{F}_5[x]/(x^2 + x + 1) \) with \( \alpha^2 = 2\bar{x} \).

Write \( \alpha = a\bar{x} + b \), then

\[
\alpha^2 = a^2\bar{x}^2 + 2ab\bar{x} + b^2 = a^2(4\bar{x} + 4) + 2ab\bar{x} + b^2 = (4a^2 + 2ab)\bar{x} + (4a^2 + b^2).
\]

Thus we immediately get that

\[
0 = 4a^2 + b^2 = b^2 - a^2 = (b - a)(b + a)
\]

implying that \( b = \pm a \). Plugging into the leading coefficient gives

\[
2 = 4a^2 \pm a^2
\]

and since the right hand side better be non-zero we get

\[
2 = 3a^2.
\]

This equation has two solutions, one of them is \( a = 2 \) and thus \( b = -2 = 3 \). The generator we have found is \( \alpha = 2\bar{x} + 3 \). You may have found a different generator since there are \( \varphi(24) = 8 \) generators of this group. They are:

\[
\begin{align*}
\alpha &= 2\bar{x} + 3 \\
\alpha^5 &= 3\bar{x} + 1 \\
\alpha^7 &= 4\bar{x} + 1 \\
\alpha^{11} &= \bar{x} + 2 \\
\alpha^{13} &= 3\bar{x} + 2 \\
\alpha^{17} &= 2\bar{x} + 4 \\
\alpha^{19} &= \bar{x} + 4 \\
\alpha^{23} &= 4\bar{x} + 3.
\end{align*}
\]

\subsection{3 Challenge Problems}

Challenge Problems tend to be harder than the rest of the problems (and sometimes more interesting). You do not need to turn these in, but you should get something out of thinking about these.

1. Prove that every prime ideal of \( \mathbb{Z}[x] \) is of one of the following forms

   1. \((0)\)
   2. \((f(x)) \) where \( f(x) \in \mathbb{Z}[x] \) is an irreducible non-constant polynomial
   3. \((p) \) where \( p \in \mathbb{Z} \) is prime
   4. \((p, g(x)) \) where \( p \in \mathbb{Z} \) is prime, \( g(x) \in \mathbb{Z}[x] \) is non-constant, and \( \overline{g(x)} \in (\mathbb{Z}/p\mathbb{Z})[x] \) is irreducible.

Which of the above ideals are maximal?
Solution: Let $P \subseteq \mathbb{Z}[x]$ be a prime ideal. Then we know that $I = P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Therefore either $I = (0)$ or $I = (p)$ for some prime $p \in \mathbb{Z}$. In the latter case, we have

$$(p) \subseteq P$$

and so by the fourth isomorphism theorem we see that $P$ corresponds to a prime ideal in

$$\mathbb{Z}[x]/(p) \cong \mathbb{F}_p[x].$$

This ring is a PID and so ALL of its prime ideals are of the form $(0)$ or $\bar{g}(x)$ for some $g(x) \in \mathbb{Z}[x]$ in which $\bar{g}(x)$ is irreducible in $\mathbb{F}_p[x]$. Thus in this case we see that either $P = (p)$ or $P = (p, g(x))$ where $g(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{F}_p[x]$. Since the maximal ideals of $\mathbb{F}_p[x]$ are precisely the non-zero prime ideals, we see that $(p, g(x))$ is maximal yet $(p)$ is not.

Next, we consider the harder case of $I = (0)$, which is to say that $P$ contains no integers. We can obtain $\mathbb{Q}[x]$ from $\mathbb{Z}[x]$ via $\mathbb{Q}[x] = D^{-1}\mathbb{Z}[x]$ where $D = \mathbb{Z} - \{0\}$. In this case, we have that $P \cap D = \emptyset$, and so by homework 3 we know that $P$ corresponds to a prime ideal in $\mathbb{Q}[x]$. Given the natural embedding $\iota: \mathbb{Z}[x] \to \mathbb{Q}[x]$, we have that

$$P = \iota^{-1}(\bar{P})$$

for some prime ideal $\bar{P} \subseteq \mathbb{Q}[x]$. The prime ideals of $\mathbb{Q}[x]$ are precisely the ideals of the form $(0)$ and $(f(x))$ where $f(x)$ is an irreducible element in $\mathbb{Q}[x]$. One possibility in this case is that $P = \iota^{-1}((0)) = (0)$. Otherwise, we must have $P = \iota^{-1}((f(x)))$ for some irreducible polynomial $f(x) \in \mathbb{Q}[x]$. We can scale $f(x) \in \mathbb{Q}[x]$ by units to assume WLOG that $f(x) \in \mathbb{Z}[x]$ and that $\text{ct}(f(x)) = 1$. Because $f(x)$ is irreducible in $\mathbb{Q}[x]$, it follows that $f(x)$ is irreducible in $\mathbb{Z}[x]$ (because it has content 1) and hence it is prime since $\mathbb{Z}[x]$ is a UFD. Thus the ideal $(f(x))$ is prime in $\mathbb{Z}[x]$ and since $D^{-1}(f(x)) = (f(x))$ in $\mathbb{Q}[x]$, the correspondence of prime ideals proves that $P = (f(x))$ where $f(x) \in \mathbb{Z}[x]$ in an irreducible, non-constant polynomial.

Neither of these types of ideals are maximal, although we require an argument to show that $(f(x))$ is never maximal. Let $f(x) \in \mathbb{Z}[x]$ be any non-constant polynomial. By the infiniteness of $\mathbb{Z}$, there exists $n \in \mathbb{Z}$ with $f(n) \neq 0, \pm 1$. Thus $f(n)$ has some prime factor $p$. It’s clear that we have the ideal containment

$$(f(x)) \subseteq (p, f(x)).$$

We will be done proving that $(f(x))$ is non-maximal precisely when we’ve proven that $(p, f(x))$ is a proper ideal of $\mathbb{Z}[x]$. To do so, assume by way of contradiction that $(p, f(x)) = \mathbb{Z}[x]$. Then there exist polynomials $h(x), k(x) \in \mathbb{Z}[x]$ with

$$1 = p \cdot h(x) + f(x)k(x).$$

Plug in $n$ to both sides to obtain

$$1 = p \cdot h(n) + f(n)k(n).$$

This equation is absurd since $p$ divides both terms on the right hand side of the equality yet $p$ does not divide 1.

2. Let $R$ be the set of all functions from the positive integers to the complex numbers:

$$R = \{ f: \mathbb{Z}^+ \to \mathbb{C} \}.$$
Consider the operations of + and ∗ on \( \mathbb{R} \) where

\[
(f + g)(n) = f(n) + g(n)
\]

\[
(f ∗ g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)
\]

(a) Prove that \( \mathbb{R} \) is a commutative ring under + and ∗ with identity element \( \epsilon \) defined by

\[
\epsilon(n) = \begin{cases} 
1, & n = 1 \\
0, & n > 1 
\end{cases}
\]

**Solution:** That \( \mathbb{R} \) is an abelian group under + and that ∗ distributes over addition follows easily from the ring properties of \( \mathbb{C} \). The operation ∗ (called Dirichlet convolution) is commutative since

\[
(f ∗ g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b) = (g ∗ f)(n).
\]

The hard axiom to check is that ∗ is associative. To do so, let \( f, g, h \in \mathbb{R} \). Then for any \( n \in \mathbb{Z}^+ \) we have

\[
(f ∗ g) ∗ h(n) = \sum_{ab=n} (f ∗ g)(a)h(b) = \sum_{ab=n} \left( \sum_{cd=a} f(c)g(d) \right)h(b).
\]

We can rewrite this last sum as

\[
\sum_{cdab=n} f(c)g(d)h(b).
\]

This triple sum becomes

\[
\sum_{ce=n} f(c) \left( \sum_{db=e} g(d)h(c) \right) = \sum_{ce=n} f(c)(g ∗ h)(c) = f ∗ (g ∗ h)(n).
\]

Therefore \( f ∗ (g ∗ h) = (f ∗ g) ∗ h \) as claimed. Lastly we must check that \( \epsilon \) is an identity element for ∗. Of course for any \( n \geq 1 \) we have

\[
(\epsilon ∗ f)(n) = \sum_{d|n} \epsilon(d)f\left(\frac{n}{d}\right) = f(n)
\]

showing that \( \epsilon ∗ f = f \).

(b) Prove that the units in \( \mathbb{R} \) are precisely those functions with \( f(1) \neq 0 \).

**Solution:** One direction is easy. Assume that \( f \in \mathbb{R} \) has an inverse \( g \in \mathbb{R} \). Then \( \epsilon = f ∗ g \) so

\[
1 = \epsilon(1) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = f(1)g(1)
\]

showing that \( f(1) \neq 0 \).

To prove the converse, we will recursively define an inverse to \( f \in \mathbb{R} \). Assume that \( f(1) \neq 0 \). Let \( g \in \mathbb{R} \) be the function satisfying

\[
g(1) = \frac{1}{f(1)}
\]
and for \( n > 1 \),
\[
g(n) = \frac{-1}{f(1)} \cdot \sum_{\substack{ab=n \\ b<n}} f(a)g(b).
\]

Notice that this definition makes sense since the terms on the right hand side only use \( g(b) \) for \( b < n \). Let \( h = f \ast g \). Then
\[
h(1) = f(1)g(1) = 1
\]
and for \( n > 1 \),
\[
h(n) = \sum_{ab=n} f(a)g(b) = f(1)g(n) + \sum_{\substack{ab=n \\ b<n}} f(a)g(b) = 0
\]
by definition of \( g \). Therefore \( f \ast g(n) = \epsilon(n) \) for all \( n \in \mathbb{Z}^+ \) and so \( f \ast g = \epsilon \).

(c) A multiplicative function \( f : \mathbb{Z}^+ \to \mathbb{C} \) is a function satisfying \( f(ab) = f(a)f(b) \) whenever \( \gcd(a, b) = 1 \). Prove that if \( f, g \in R \) are both multiplicative then so is \( f \ast g \).

**Solution:** Let \( f, g \in R \) be multiplicative functions and let \( h = f \ast g \). We want to prove that \( h(xy) = h(x)h(y) \) whenever \( x, y \in \mathbb{Z}^+ \) and \( \gcd(x, y) = 1 \). By definition of \( h \), we have
\[
h(x)h(y) = \left( \sum_{d \mid x} f(d)g \left( \frac{x}{d} \right) \right) \left( \sum_{e \mid y} f(e)g \left( \frac{y}{e} \right) \right).
\]
We can distribute this sum as
\[
h(x)h(y) = \sum_{d \mid x} \sum_{e \mid y} f(d)f(e)g \left( \frac{x}{d} \right)g \left( \frac{y}{e} \right).
\]
Since \( \gcd(x, y) = 1 \) we also have \( \gcd(d, e) = 1 \) for any \( d \mid x \) and \( e \mid y \). Thus we can use the multiplicativity of \( f \) and \( g \) so write
\[
h(x)h(y) = \sum_{d \mid x} \sum_{e \mid y} f(de)g \left( \frac{xy}{de} \right).
\]
Given \( d \mid x \) and \( e \mid y \) we clearly have \( de \mid xy \). Conversely, every \( k \) which divides \( xy \) can be written uniquely in the form \( k = ab \) where \( a \mid x \) and \( b \mid y \). You can prove this by showing that \( a = \gcd(k, x) \) and \( b = \gcd(k, y) \), which follows by unique factorization. This observation allows us to conclude that
\[
h(x)h(y) = \sum_{k \mid xy} f(k)g \left( \frac{xy}{k} \right) = h(xy).
\]

(d) Consider the function \( \mathbb{1} \in R \) defined by \( \mathbb{1}(n) = 1 \) for every \( n \geq 1 \) and let \( \mu \in R \) be the inverse of \( \mathbb{1} \). Then \( g = f \ast \mathbb{1} \) if and only if \( g \ast \mu = f \). Use this to prove that if \( \varphi(n) \) is the Euler phi function,
\[
\varphi(n) = \sum_{d \mid n} d \cdot \mu \left( \frac{n}{d} \right).
\]
(The function \( \mu \) can be used to prove that there are irreducible polynomials over \( \mathbb{F}_p \) of degree \( n \) for any \( n \geq 1 \). You can look at exercises 9.5.5 and 9.5.6 to see how already this is useful. This formula also gives an alternative proof that \( \varphi \) is multiplicative, which we’ve previously seen via the Chinese Remainder Theorem.)
Solution: I claim that
\[ n = \sum_{d|n} \varphi(d). \]

The easiest way to prove this is to use the fact that \( \varphi \) is multiplicative to prove this when \( n = p^m \), and then appeal to the previous problem to extend to all \( n \geq 1 \). Here is an alternative proof.

Consider the \( n \) fractions
\[ \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}. \]

Suppose we write each of these fractions in its lowest terms. Then the denominator of the resulting fraction will be a factor of \( n \). Let \( d \) be some positive divisor of \( n \), and let’s count how many fractions have denominator \( d \) in lowest terms. The fraction \( \frac{a}{n} \) has denominator \( d \) if and only if \( \gcd(a, n) = \frac{n}{d} \). Since \( 1 \leq a \leq n \), this occurs if and only if \( a = \frac{n}{d} \cdot i \) where \( 1 \leq i \leq d \) and
\[
\frac{n}{d} = \gcd(a, n) = \gcd\left(\frac{n}{d} \cdot i, \frac{n}{d} \cdot d\right) = \frac{n}{d} \gcd(i, d)
\]
which happens if and only if \( \gcd(i, d) = 1 \). Thus the number of such fractions is \( \varphi(d) \). Since there are \( n \) fractions in total, we get that
\[
n = \sum_{d|n} \varphi(d).
\]

This equation tells us that \( I = \varphi \ast \mathbb{1} \) where \( I \in \mathbb{R} \) is the function \( I(n) = n \). Convolving both sides with \( \mu \) gives
\[
I \ast \mu = \varphi \ast \mathbb{1} \ast \mu = \varphi \ast \epsilon = \varphi
\]
and hence
\[
\varphi(n) = \sum_{d|n} d \cdot \mu \left( \frac{n}{d} \right).
\]