Problem 1. Let \( U \) be the group of units in \( \mathbb{Z}_{109} \) together with the usual multiplication.
(a) Show that \( U \) is an abelian group of order 108.
(b) Determine with justification whether the group \( U \) is isomorphic to the group \( \mathbb{Z}_6 \times \mathbb{Z}_{18} \).

Solution. a) In the first homework assignment, we proved that the collection of units in a ring is a group with the multiplication from the ring. As 109 is prime, \( \mathbb{Z}_{109} \setminus \{0\} \) is a field and every non-zero element is a unit. Thus \( U \) is an abelian group of order 108 where the abelian nature of \( U \) follows from multiplication in \( \mathbb{Z}_{109} \) being commutative.

b) Seeking a contradiction, suppose \( U \cong \mathbb{Z}_6 \times \mathbb{Z}_{18} \). Then, a standard result from Math 103A shows they necessarily have the same number of elements of order 2. (The group isomorphism \( \phi : U \rightarrow \mathbb{Z}_6 \times \mathbb{Z}_{18} \) preserves the order of elements.) As such, the groups should have the same number of solutions to \( x^2 = 1 \). In \( \mathbb{Z}_{109} \), it follows that \( \mathbb{Z}_{109} \) is an integral domain and hence there are two solutions in \( U \). In the additive group \( \mathbb{Z}_6 \times \mathbb{Z}_{18} \), \( x^2 = (0,0) \) implies that \( x \in \{(0,0), (3,0), (0,9), (3,9)\} \) and hence they have a different number of elements of order two.

Problem 2 (§18.52). Let \( r, s \) be positive integers so that \( (r, s) = 1 \). Use the isomorphism in Example §18.15 to show that for \( m, n \in \mathbb{Z} \), there exists an integer \( x \in \mathbb{Z} \) such that \( x \equiv m \pmod{r} \) and \( x \equiv n \pmod{s} \).

Solution. The isomorphism in Example §18.15 implies that since \( \gcd(r, s) = 1 \), \( \mathbb{Z}_r \times \mathbb{Z}_s \) is isomorphic to \( \mathbb{Z}_{rs} \). Letting the isomorphism be \( \phi : \mathbb{Z}_{rs} \rightarrow \mathbb{Z}_r \times \mathbb{Z}_s \), we have that letting \( m' \equiv m \pmod{r} \), \( n' \equiv n \pmod{s} \) with \( 0 \leq m' < r \) and \( 0 \leq n' < s \), there exists \( x \in \mathbb{Z}_{rs} \) such that \( \phi(x) = (m', n') \). In particular, we have that since this is a homomorphism, \( x \cdot \phi(1) = x \cdot (1,1) = (m', n') \), so \( x \equiv m' \equiv m \pmod{r} \) and \( x \equiv n' \equiv n \pmod{s} \). Thus, \( x \) is an integer satisfying the above.

Problem 3 (§20.13). Describe all solutions to \( 36x = 15 \pmod{24} \).

Solution. Seeking a contradiction, suppose there exists \( x \in \mathbb{Z}_{24} \) which satisfied the above equation. Then \( 36x = 24k + 15 \) for some \( k \in \mathbb{Z} \). This is a contradiction as the left hand side is even and the right hand side is odd.

\[ ^1 \text{technically this counts the number of elements of order at most 2} \]
The general theory here is that since $15 \nmid \gcd(12, 24)$, there are no solutions to the equation $36x = 15 \mod 24$ (cf. Theorem 20.12).

**Problem 4** ($§$20.15). Describe all solutions to $39x = 125 \mod 9$.

**Solution.** We first reduce the equation to $3x = 8 \mod 9$ and again appeal to Theorem 20.12 to get that there are no solutions since $8 \nmid \gcd(3, 9)$.

**Problem 5** ($§$20.19). Let $p$ be prime and use exercise 28 below to find the remainder of $(p - 2)!$ modulo $p$.

**Solution.** Exercise 28 involves proving Wilson’s theorem which says for a prime $p$, that $(p - 1)! = -1 \mod p$. We next note that $(p - 1)^{-1} = (p - 1)$ as

$$(p - 1)(p - 1) = (-1)(-1) = 1.$$  

Multiplying the result of Wilson’s theorem on both sides by $(p - 1)$, we recover

$$(p - 2)! = (p - 1)(p - 1)(p - 2)! = (p - 1)(p - 1)! = (p - 1)(-1) = 1.$$  

Another way to recover this result is by noting in a finite group, if we let $S_{\geq 3} \subset G$ be all the elements of order at least three, then

$$\prod_{a \in S_{\geq 3}} a = e$$

as for each $a \in S_{\geq 3}$, there exists a unique distinct $b \in S_{\geq 3}$ with $ab = e$. We then note that for $\mathbb{Z}_p$ ($p \geq 5$ prime) the element of order at least three are $\{2, 3, \ldots, p - 2\}$ and there are no such elements when $p \in \{2, 3\}$.

**Problem 6** ($§$21.1). Describe the field $F$ of quotients of the integral domain

$$D = \{n + mi : n, m \in \mathbb{Z}\}$$

of $\mathbb{C}$. That is, list the elements.

**Solution.** Let $F$ be the desired field of quotients. Then we claim

$$F = \mathbb{Q}(i) := \{a + ib : a, b \in \mathbb{Q}\}.$$  

First, we note that given any $n + mi, u + vi \in D$ where $u + vi \neq 0$ that

$$\frac{n + mi}{u + vi} = \frac{nu + mv}{u^2 + v^2} + \frac{mu - nv}{u^2 + v^2} \in \mathbb{Q}(i).$$  

Next, we observe that given any $\frac{a}{b} + i\frac{c}{d} \in \mathbb{Q}(i)$, that

$$\frac{a}{b} + i\frac{c}{d} = \frac{ad + icb}{bd} \in F$$

as both the numerator and denominator above are elements of the integral domain $D$.  

2
Problem 7 (§21.2). Describe the field of quotients of the integral domain $D = \{ n + m\sqrt{2} : \ n, m \in \mathbb{Z} \}$ of $\mathbb{R}$.

Solution. Let $F$ be the field of quotients for $D$. We claim that the field of quotients is $\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}$. First note that for any $n, m, p, q \in \mathbb{Z}$ with $p + q\sqrt{2} \neq 0$, then,

$$\frac{n + m\sqrt{2}}{p + q\sqrt{2}} = \frac{(n + m\sqrt{2})(p - q\sqrt{2})}{(p + q\sqrt{2})(p - q\sqrt{2})} = \frac{np - 2mq + (mp - nq)\sqrt{2}}{p^2 - 2q^2} = \frac{np - 2mq}{p^2 - 2q^2} + \frac{mp - nq}{p^2 - 2q^2} \sqrt{2}$$

where $\frac{np - 2mq}{p^2 - 2q^2}, \frac{mp - nq}{p^2 - 2q^2} \in \mathbb{Q}$. Thus, $F \subseteq \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}$. Conversely, for $a, b \in \mathbb{Q}$, we have that $a = \frac{m}{n}, \ b = \frac{p}{q}$ for $m, n, p, q \in \mathbb{Z}$. Then, note that $mq + pn\sqrt{2}, nq \in D$, so noting that $nq \neq 0$, we have that

$$a + b\sqrt{2} = \frac{mq}{nq} + \frac{pn}{nq} \sqrt{2} = \frac{mq + pn\sqrt{2}}{nq} \in F,$$

making this indeed the field of quotients.