Math 561/661 **Fall 2021**
Homework 3 **Drew Armstrong**

---

1. Units and Associates. We say that $u \in R$ is a *unit* if there exists $v \in R$ with $uv = 1$. Let $R^\times$ be the set of units. We say that $a, b \in R$ are *associates* if there exists a unit $u \in R^\times$ such that $au = v$. We define the notation

$$a \sim b \iff \exists u \in R^\times, au = b.$$

(a) Prove that $\sim$ is an equivalence relation on the set R.
(b) Prove that $\mathbb{Z}^\times = \{\pm 1\}$. [Hint: Use absolute value.]
(c) Prove that $\mathbb{F}[x]^\times = \mathbb{F} \setminus \{0\}$. [Hint: Use degree.]

(a): **Reflexive.** Since 1 is a unit we have $a1 = a$ and hence $a \sim a$. **Symmetric.** If $a \sim b$ then we have $au = b$ for some unit $u \in R^\times$, which implies that $bu^{-1} = a$. Since u^{-1} is also a unit this implies that $b \sim a$. **Transitive.** If $a \sim b$ and $b \sim c$ then we have $au = b$ and $bv = c$ for some units $u, v \in R^\times$. But note that uv is also a unit with inverse $(uv)^{-1} = v^{-1}u^{-1}$.[1] Then since $c = bv = (au)v = a(uv)$ we have $a \sim c$.

(b): First we observe that 1 and -1 are units because $1 \cdot 1 = 1$ and $(-1)(-1) = 1$. Conversely, we want to show that any unit must be equal to 1 or -1. So let $u \in \mathbb{Z}$ be a unit. This means that $uv = 1$ for some integer $v \in \mathbb{Z}$. Since $u \neq 0$ we also have $v \neq 0$, hence $1 \leq |u|$ and $1 \leq |v|$. It follows that

$$\begin{aligned}
1 &\leq |v| & & \\
|u| &\leq |u||v| & & \text{multiply both sides by } |u| \\
|u| &\leq |uv| & & \\
|u| &\leq |1| & & \\
|u| &\leq 1. & &
\end{aligned}$$

Since $u \neq 0$ this implies that $u = 1$ or $u = -1$.

(c): First we observe that nonzero constant polynomials are units. Indeed, if $f(x) = a$ for some nonzero constant $a \in \mathbb{F}$ then since $\mathbb{F}$ is a field the inverse constant $a^{-1} \in \mathbb{F}$ exists and $f(x)^{-1} = a^{-1}$. Conversely, we want to show that any unit must be a nonzero constant. So let $f(x) \in \mathbb{F}[x]$ be a unit. This means that $f(x)g(x) = 1$ for some polynomial $g(x) \in \mathbb{F}[x]$, and taking degrees gives

$$\begin{aligned}
\deg(fg) &= \deg(1) \\
\deg(f) + \deg(g) &= 0.
\end{aligned}$$

Since $f(x)$ and $g(x)$ are nonzero we have $\deg(f) \geq 0$ and $\deg(g) \geq 0$, hence the above equation implies that $\deg(f) = 0$ and $\deg(g) = 0$. In other words, $f(x)$ and $g(x)$ are nonzero constants.

2. Lemmas for the Euclidean Algorithm.

---

[1] I could have said $(uv)^{-1} = u^{-1}v^{-1}$ but I chose to write $(uv)^{-1} = v^{-1}u^{-1}$ because this second identity also holds in cases where the multiplication is not commutative; for example, for matrix multiplication.

(a) For elements a, b, c, x in a ring R satisfying $a = bx + c$, prove that the following sets of common divisors are equal:

$$\text{Div}(a, b) = \text{Div}(b, c).$$

[Hint: You need to prove the inclusion in both directions.]

(b) Now let R be a Euclidean domain with size function $N : R \backslash \{0\} \to \mathbb{N}$. For any nonzero element $a \in R$, prove that

$$d \sim a \quad \Longleftrightarrow \quad d \text{ is a maximum-sized element of Div}(a).$$

[Hint: Every divisor $d|a$ satisfies $N(d) \leq N(a)$, so a itself is among the maximum-sized divisors of a. Use this to show that every associate of a is a maximum-sized divisor. Conversely, let $d|a$ be a maximum-sized divisor, i.e., with $N(d) = N(a)$. To prove $d \sim a$ you need to show $a|d$. Divide d by a and show that the remainder r is divisible by d. Then show that $r \neq 0$ leads to a contradiction.]

(a): Suppose that $a, b, c, x \in R$ satisfy $a = bx + c$. To see that $\text{Div}(b, c) \subseteq \text{Div}(a, b)$, let d be a common divisor of b and c, so that $dk = b$ and $d\ell = c$ for some $k, \ell \in R$. It follows that

$$a = bx + c = dkx + d\ell = d(kx + \ell),$$

so that d is also a divisor of a. Hence d is a common divisor of a and b. Conversely, to see that $\text{Div}(a, b) \subseteq \text{Div}(b, c)$, let d be a common divisor of a and b, so that $dk = a$ and $d\ell = b$ for some $k, \ell \in R$. It follows that

$$c = a - bx = dk - d\ell x = d(k - \ell x),$$

so that d is also divisor of c. Hence d is a common divisor of b and c.

(b): First we observe that $N(a)$ is the maximum size of a divisor of a. Indeed, since a divides itself there does exist a divisor with this size. Also, since $d|a$ implies $N(d) \leq N(a)$ we see that no divisor of a has size larger than $N(a)$.

If $d \sim a$ then we have $d|a$ and $a|d$. The first of these says that d is a divisor of a. We also have $N(d) \leq N(a)$ and $N(a) \leq N(d)$, so that $N(d) = N(a)$. It follows that d is a divisor of maximum size.

Conversely, suppose that d is a divisor of a with maximum size. That is, suppose that $d|a$ and $N(d) = N(a)$. If we can show that $a|d$ then we will be done because $d|a$ and $a|d$ imply $d \sim a$. So let us divide d by a to obtain

$$\begin{cases} d = aq + r, \\ r = 0 \text{ or } N(r) < N(a). \end{cases}$$

Our goal is to show that $r = 0$ so let us assume for contradiction that $r \neq 0$, so that $N(r) < N(a)$. Since $d|a$ we also have $dk = a$ for some $k \in R$, hence

$$r = d - aq = d - dkq = d(1 - kq).$$

This implies that $d|r$ and hence $N(a) = N(d) \leq N(r)$. Contradiction.

3. Roots are Irrational. Let $d \geq 1$ be a positive integer and let $\sqrt[n]{d} > 0$ be its unique positive nth root. We will prove the following:

$$\text{If } \sqrt[n]{d} \text{ is not an integer then } \sqrt[n]{d} \text{ is not a rational number.}$$

In the proof we will use the notation $\nu_p(a)$ for the *multiplicity* of the prime p in the unique prime factorization of the integer a.

(a) Show that $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ for all primes p and integers $a, b \in \mathbb{Z}$.

(b) Consider integers $d, n \geq 1$. Prove that d is the nth power of an integer if and only if $n|\nu_p(d)$ for all primes p.[2]

(c) If $d \in \mathbb{Z}$ is not the nth power of an integer, prove that d is not the nth power of a rational number. [Hint: Assume for contradiction that $d = (a/b)^n$. Multiply both sides by b^n. Then use parts (a) and (b).]

(a): By definition we have

$$\begin{aligned} a &= 2^{\nu_2(a)}3^{\nu_3(a)}5^{\nu_5(a)}7^{\nu_7(a)}\cdots, \\ b &= 2^{\nu_2(b)}3^{\nu_3(b)}5^{\nu_5(b)}7^{\nu_7(b)}\cdots, \end{aligned}$$

so that

$$ab = 2^{\nu_2(a)+\nu_2(b)}3^{\nu_3(a)+\nu_3(b)}5^{\nu_5(a)+\nu_5(b)}7^{\nu_7(a)+\nu_7(b)}\cdots.$$

But we also have

$$ab = 2^{\nu_2(ab)}3^{\nu_3(ab)}5^{\nu_5(ab)}7^{\nu_7(ab)}\cdots,$$

hence it follows from uniqueness that $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ for all p.[3]

(b): Suppose that $d = c^n$ for some $c \geq 1$. Then for any prime p, part (a) gives

$$\nu_p(d) = \nu_p(c^n) = \nu_p(c) + \nu_p(c) + \cdots + \nu_p(c) = n\nu_p(c),$$

and hence $n|\nu_p(d)$. Conversely, suppose that $n|\nu_p(d)$ for all primes p. In other words, suppose that $\nu_p(d) = ne_p$ for some integers e_p. Then we have

$$\begin{aligned} d &= 2^{\nu_2(d)}3^{\nu_3(d)}5^{\nu_5(d)}7^{\nu_7(d)}\cdots, \\ &= 2^{ne_2}3^{ne_3}5^{ne_5}7^{ne_7}\cdots, \\ &= (2^{e_2}3^{e_3}5^{e_5}7^{e_7}\cdots)^n, \end{aligned}$$

so that d is the nth power of an integer.

(c): We will prove the contrapositive statement. Suppose that $\sqrt[n]{d} = a/b$ for some integers a, b, so that

$$\begin{aligned} \sqrt[n]{d} &= a/b \\ d &= a^n/b^n \\ db^n &= a^n. \end{aligned}$$

Then for any prime p we have

$$\begin{aligned} \nu_p(db^n) &= \nu_p(a^n) \\ \nu_p(d) + n\nu_p(b) &= n\nu_p(a) \\ \nu_p(d) &= n\left(\nu_p(a) - \nu_p(b)\right), \end{aligned}$$

and hence $n|\nu_p(d)$.

4. Modular Arithmetic. Fix a positive integer $n \geq 1$. Following Gauss, we define the following notation for all $a, b \in \mathbb{Z}$, and we call this *congruence modulo n*:

$$a \equiv b \mod n \quad \Longleftrightarrow \quad n|(a-b).$$

(a) Prove that congruence mod n is an equivalence relation on the set $\mathbb{Z}$.

[2] The version of the homework I gave you only asked for one direction of this theorem. Unfortunately, it was the wrong direction; i.e., the direction that is not useful for part (c). Oops.

[3] There are cleaner ways to do this but I think that writing out the factorizations explicitly, even though it's ugly, is the easiest proof to understand.

(b) Prove that congruence mod n respects addition and multiplication. In other words, if $a \equiv a'$ and $b \equiv b'$ mod n, prove that $a+b \equiv a'+b'$ and $ab \equiv a'b'$ mod n. [Hint: For the second property, consider the identity $ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + (a-a')b'$.]

(c) Prove that for all $a \in \mathbb{Z}$ there exists a unique integer $r \in \mathbb{Z}$ satisfying $a \equiv r$ mod n and $0 \leq r \leq n-1$. [Hint: Let r be the remainder of a when divided by n. Suppose that $a \equiv r$ and $a \equiv r'$ mod n for some $0 \leq r, r' \leq n-1$. If $r \neq r'$ then it follows that $n|(r-r')$ and hence $|n| \leq |r-r'|$. Use this to obtain a contradiction.]

It follows that the finite set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ can be viewed as a ring.[4]

(a): **Reflexive.** For all $a \in \mathbb{Z}$ we have $n0 = (a-a)$, which implies that $n|(a-a)$ and hence $a \equiv a$ mod n. **Symmetric.** If $a \equiv b$ mod n then we have $n|(a-b)$, hence $nk = a-b$ for some $k \in \mathbb{Z}$. It follows that $n(-k) = b-a$, which implies that $n|(b-a)$ and hence $b \equiv a$ mod n. **Transitive.** If $a \equiv b$ and $b \equiv c$ mod n then by definition we have $nk = a-b$ and $n\ell = b-c$ for some $k, \ell \in \mathbb{Z}$. But then we also have

$$a - c = (a-b) + (b-c) = nk + n\ell = n(k+\ell),$$

which implies that $a \equiv c$ mod n.

(b): Suppose that $a \equiv a'$ and $b \equiv b'$ mod n, so that $nk = a - a'$ and $n\ell = b - b'$ for some $k, \ell \in \mathbb{Z}$. Then we have

$$\begin{aligned}(a+b) - (a'+b') &= (a-a) + (b-b') \\ &= nk + n\ell \\ &= n(k+\ell),\end{aligned}$$

which implies that $a+b \equiv a'+b'$ mod n. And we have

$$\begin{aligned}ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b-b') + (a-a')b' \\ &= an\ell + nkb' \\ &= n(a\ell + kb'),\end{aligned}$$

which implies that $ab \equiv a'b'$ mod n.

(c): Suppose that we have $a \equiv r$ and $a \equiv r'$ mod n for some integers $r, r' \in \mathbb{Z}$ satisfying $0 \leq r \leq n-1$ and $0 \leq r' \leq n-1$. We will show that $r = r'$.[5] By assumption we have $a - r = nk$ and $a - r' = n\ell$ for some k, ℓ, which implies that

$$\begin{aligned}nk + r &= n\ell + r' \\ r - r' &= n(\ell - k),\end{aligned}$$

and hence $|n| \leq |r - r'|$.[6] Now let's assume for contradiction that $r \neq r'$, so we may take $r' < r$ without loss of generality. It follows that

$$r < n = |n| \leq |r - r'| = r - r' \leq r,$$

which is a contradiction.

[4] I will explain the notation $\mathbb{Z}/n\mathbb{Z}$ later.

[5] This statement is equivalent to the uniqueness of quotients and remainders for integer division.

[6] Here's a reiminder: If $xy = z$ and $z \neq 0$ then we also have $x, y \neq 0$ and multiplying both sides of the inequality $|y| \geq 1$ by the positive number $|x|$ gives $|z| = |x||y| \geq |x|$.

5. Some Finite Fields. In class we proved that for all $a, b, p \in \mathbb{Z}$ with p prime we have

$$p|ab \implies p|a \text{ or } p|b.$$

(a) If p is prime, use this property to prove that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. Since this set is finite, it follows from the previous homework that $\mathbb{Z}/p\mathbb{Z}$ is a field.
(b) Since 23 is prime it follows from part (a) that the nonzero element $16 \in \mathbb{Z}/23\mathbb{Z}$ has a multiplicative inverse. Use the Vector Euclidean Algorithm to find this element. [Hint: Find some $x, y \in \mathbb{Z}$ such that $23x + 16y = 1$.]
(c) If $n \geq 1$ is not prime, prove that $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

(a): By definition of integral domain, we want to show that

$$ab \equiv 0 \mod p \implies a \equiv 0 \bmod p \quad \text{or} \quad b \equiv 0 \bmod p.$$

But this is just a direct translation of Euclid's lemma because $c \equiv 0 \bmod p$ if and only if $p|c$.

(b): We are looking for an integer y such that $16y \equiv 1 \bmod 23$. In other words, we are looking for an integer y such that $23|(1-16y)$. In other words, we are looking for integers x, y such that $23x = 1 - 16y$. And we know how to find such integers using the Vector Euclidean Algorithm. To do this we consider the set of triples (x, y, z) of integers such that $23x + 16y = z$. Then we combine the triples $(1, 0, 23)$ and $(0, 1, 16)$ to obtain a triple of the form $(x, y, 1)$:

x	y	z
1	0	23
0	1	16
1	-1	7
-2	3	2
7	-10	1

We conclude that $y = -10$ is one such integer. In other words:

$$16^{-1} \equiv -10 \equiv 13 \mod 23.$$

Check: Since $16 \cdot 13 = 208 = 23 \cdot 9 + 1$ we have $16 \cdot 13 \equiv 1 \bmod 23$.

Remark: There is also a slow method. We could multiply 16 by every element of $\mathbb{Z}/23\mathbb{Z}$ until we get 1:[7]

$$\begin{aligned} 16 \cdot 1 &\equiv 16 \not\equiv 1 \\ 16 \cdot 2 &\equiv 32 \equiv 9 \not\equiv 1 \\ 16 \cdot 3 &\equiv 48 \equiv 2 \not\equiv 1 \\ &\text{etc.} \end{aligned}$$

In general, to find the inverse of a mod p might take $p - 1$ steps using the slow method. But it takes approximately $\log_2(p)$ steps using the Euclidean Algorithm, which is much faster.

(c): We will ignore the case $n = 1$, since it is not important whether you want to call $\mathbb{Z}/1\mathbb{Z} = \{0\}$ a domain. If $n \geq 2$ is not prime then we can write $n = ab$ where $1 < a < n$ and $1 < b < n$, hence $a \not\equiv 0$ and $b \not\equiv 0 \bmod n$. If $\mathbb{Z}/n\mathbb{Z}$ were a domain this would imply $ab \not\equiv 0 \bmod n$. But we have

$$ab \equiv n \equiv 0 \mod n,$$

hence $\mathbb{Z}/n\mathbb{Z}$ is not a domain.

---

[7] All computations are mod 23.