Abstract Algebra Homework 2

Joe Loser

February 1, 2016

This problem set includes problems from sections 2.3, 3.4, and two extra problems from lecture.

31) Using the fact that 2 is prime, show that there do not exist integers p and q such that $p^2 = 2q^2$.

Proof: We will prove the statement using contradiction. First, find the largest number $k \in \mathbb{N}$ such that 2^k divides divides both p and q. It should be easy to see that k will be 0 if either p or q is odd.

Now, let $a := \frac{p}{2^k}$ and $b := \frac{q}{2^k}$. Since we found the *largest* k, we are certain that either a or b is odd. Otherwise, we could have increased k. By our definitions of a and b, $p = a2^k$ and $q = b2^k$. Then,

$$\begin{aligned} p^2 &= 2q^2 \\ (a2^k)^2 &= 2(b2^k)^2 \\ a^2(2^k)^2 &= 2b^2(2^k)^2 \\ a^2 &= 2b^2 \end{aligned}$$

Thus, we see that a^2 is even. Using the given fact that 2 is prime, a must also be even. In fact, b must also be odd due to our previous work. Let $c := \frac{a}{2}$. So $a = 2c$. Then,

$$\begin{aligned} (2c)^2 &= 2b^2 \\ 4c^2 &= 2b^2 \\ 2c^2 &= b^2 \end{aligned}$$

But now we have shown that b^2 is even which implies that b is even since 2 is a prime. However, this contradicts how we constructed such an a and b. By contradiction, no such integers p and q can exist that satisfy the condition $p^2 = 2q^2$. It is well know that $\sqrt{2} \notin \mathbb{Q}$. $\square$

1b) Find all $x \in \mathbb{Z}$ such that $5x + 1 \equiv 13 \pmod{23}$.

Proof: We will begin with the definition of congruent mod m, find the least residue class, and then find the other solutions that satisfy the equation.

Let a and b be integers and m be a natural number. Then, a is congruent to b modulo m, i.e. $a \equiv b \pmod{m}$ if $m|(a-b)$ by definition. In our case, $a = 5x+1, b = 13$, and $m = 23$. So, we want to find all $x \in \mathbb{Z}$ such that $23|(5x-12)$. Beginning with $x = 0$ and going up to $x = 23$, we see that $x = 7$ is a solution and is indeed the least residue class. If $x = 7, 5x - 12 = 23$. We can keep on generating more x values that satisfy the equation by adding the modulus value $m = 23$ to our latest x value. So, all $x \in \mathbb{Z}$ that work are $x = 7 + 23n$ for $n \in \mathbb{Z}$. $\square$

Remark: I exploited the fact that 23 is prime which is what allows me to find the *unique* least residue class technically. While we have not proved this, it is perfectly acceptable and I did indeed brute force all the way from $x = 0$ to $x = 23$ to find all x that satisfy the equation initially before just adding $\bmod 23$ to generate more possible values x can take on. The alternative, more systematic approach is to use the Euclidean Algorithm rather than just working by inspection or brute force as this would not be ideal if m is large.

7) Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Proof: First, we will prove that the set S is indeed a group and then we will show that the group S is in fact abelian.

To show that the set S is a group with a binary operation $*$, it needs to satisfy the following conditions:

1. $*$ is associative, i.e. $(a * b) * c = a * (b * c)$ for $a, b, c \in S$.
2. S is closed under $*$.
3. There exists an element $e \in S$ such that for any element $a \in S, e * a = a * e = a$ (identity property)
4. For each element $a \in S$, there exists an inverse element in S which we denote a^{-1} such that $a * a^{-1} = a^{-1} * a = e$ (inverse property)
5. * is a binary operator

We show each of these conditions in order now.

1. We have to show $(a*b)*c = a*(b*c)$ for $a, b, c \in S$. By applying the definition

of our binary operation $*$ we have that

$$\begin{aligned}(a*b)*c &= (a+b+ab)*c\\ &= (a+b+ab)+c+(a+b+ab)c\\ &= a+b+ab+c+ac+bc+abc\\ &= a+b+c+bc+a(b+c+bc)\\ &= a+(b+c+bc)+a(b+c+bc)\\ &= a*(b*c)\end{aligned}$$

2. We need to show that S is closed under $*$, i.e. we need to make sure $a*b$ never equals -1. Note that if $a*b = a+b+ab = -1$, then $a+b+ab+1 = 0$. This is equivalent to $(b+1)+a(1+b) = 0$ by factoring out an a where we can. This is the same as $(b+1)(a+1) = 0$. Now, note that a and b cannot be -1 because the set $S = \mathbb{R} \setminus \{-1\}$ and a and $b \in S$. Since a and b are not -1, neither is $a+b+ab$. Therefore, S is closed under the binary operation $*$.

3. We need to show that S has an identity element. Notice that $a*0 = a+0+0 = a$, so S does indeed have an identity element and it is 0. One can also see that $a*0 = 0*a$ since S is abelian.

4. We need to show that every $a \in S$ has an inverse element. Choose any $a \in S$. We want to find an inverse for a, so we want to find a $b \neq -1$ such that $a*b = 0$. One can also see this is equal to $b*a$ since S is abelian.

$$\begin{aligned}a*b &= 0\\ ab+a+b &= 0\\ b(a+1) &= -a\\ b &= -\frac{a}{a+1}\end{aligned}$$

So, let $b = \frac{-a}{1+a}$. Now note that b cannot be -1, otherwise we would have that $-1 = \frac{-a}{1+a} \implies a = 1+a$ which is not possible. As a result, $b \in S$ and $a \neq -1$. Then,

$$\begin{aligned}a*b &= a+\frac{-a}{1+a}+a\frac{-a}{1+a}\\ &= \frac{a(1+a)}{1+a}+\frac{-a}{1+a}+\frac{-a^2}{1+a}\\ &= 0\end{aligned}$$

which is the identity.

5. Lastly, to show $*$ is a binary operation, if $a, b \neq -1$, we need to show $a*b \neq -1$. The only way $a*b = -1$ is if either a or b is -1. Thus $a*b \neq -1$ for all $a, b \in S$ and we have that $*$ is a binary operation.

So, we have shown that S is indeed a group. Now, in order for S to be an abelian group, S needs to also have the property that $a * b = b * a$ for all $a, b \in S$. Notice that $a * b = a + b + ab = b + a + ab = b * a$ for all $a, b \in S$. So, the binary operation $*$ is commutative.

Therefore, the set $S = \mathbb{R} \setminus \{-1\}$ is an abelian group. $\square$

E1) Let $a, b, g, s \in \mathbb{Z}$. If $b \neq 0$ and $a = bg + s$, show that $gcd(a, b) = gcd(b, s)$.

<u>Proof</u>: We will show that if $a = bg + s$ then there is an integer d that is a common divisor of a and b if and only if d is a common divisor of b and s.

Let d be a common divisor of a and b. By definition of common divisor, $d|a$ and $d|b$. Hence, by Corollary A6, $d|(a - bg)$ which means $d|s$ since $s = a - bg$. Thus d is a common divisor of b and s.

Now, suppose that d is a common divisor of b and s. By definition of common divisor, $d|b$ and $d|s$. Hence, by Corollary A6, $d|(bg + s)$ so $d|a$ since $a = bg + s$. Thus, d must be a common divisor of a and b.

Thus, the set of common divisors of a and b are the same as the set of common divisors of b and s. It follows that d is the *greatest* common divisor of a and b if and only if d is the greatest common divisor of b and s. $\square$

E2) Show that the set S formed in the proof of Theorem $A5$ consists precisely of all the positive multiples of $d = gcd(a, b)$.

To refresh ourselves, Theorem $A5$ is provided below for convenience. Let $a, b \in \mathbb{Z}$ with at least one of which is non-zero. Then,

1. $gcd(a, b)$ exists and is unique
2. There exists $r, s \in \mathbb{Z}$ such that $gcd(a, b) = ra + sb$.

In the proof of this theorem, we let $S := \{am + bn \mid m, n \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 1}$ and we also showed that $d = gcd(a, b)$ was the smallest element of S. We want to show that this set S contains all of the positive multiples of $d = gcd(a, b)$.

<u>Proof</u>: First, let $c \in S, d = gcd(a, b)$. Then, by our definition of the set S, there exist $m, n \in \mathbb{Z}$ such that $c = ma + nb$. Since $d = gcd(a, b)$, $d|a$ and $d|b$. So, there exist integers x and y such that $a = xd$ and $b = yd$. Then,

$$\begin{aligned} c &= ma + nb \\ &= mxd + nyd \\ &= (mx + ny)d \end{aligned}$$

Hence, $c = kd$ where $k = mx + ny$ and we conclude that $d|c$.

Showing the opposite direction now, again, let c be an integer and assume that $d|c$. Then there exist an integer x' such that $c = x'd$. By Theorem A5, then there exist integers r and s such that $d = ar + bs$. Substituting this value for d, we then have that

$$\begin{aligned} c &= x'd \\ &= x'(ar + bs) \\ &= x'ar + x'bs \\ &= a(rx') + b(sx') \end{aligned}$$

Hence, $c = am + bn$ where $m = rx'$ and $n = sx'$.

Therefore, the set S consists of all of the positive multiples of $gcd(a, b)$. $\square$