Math 411 Individual Homework 2

Jack Madden

September 2023

Problem 1

a)

$$1001 = 6 \cdot 163 + 23$$

$$163 = 7 \cdot 23 + 2$$

$$23 = 11 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$gcd(163, 1001) = 1, 78 \cdot 1001 - 479 \cdot 163 = 1$$

b)

$$2023 = 3 \cdot 629 + 136$$

$$629 = 4 \cdot 136 + 85$$

$$136 = 1 \cdot 85 + 51$$

$$85 = 1 \cdot 51 + 34$$

$$51 = 1 \cdot 34 + 17$$

$$34 = 2 \cdot 17 + 0$$

$$gcd(2023, 629) = 17, 14 \cdot 2023 - 45 \cdot 629 = 17$$

Problem 2

a) False, $15 \mid 3 \cdot 5$ but $15 \nmid 3$ and $15 \nmid 5$.

b) True, if $a \mid b$, then $ak = b$ for some $k \in \mathbb{Z}$. So then $ak \mid c$, meaning that for some $m \in \mathbb{Z}$, $(ak)m = c$. We suggestively rewrite this as $a(km) = c$. Since $km \in \mathbb{Z}$, $a \mid c$.

c) *PrimeQ[314159265358979]* in Mathematica returned *False*.

d) If $a \mid b$ and $b \mid a$, $ak = b, b\ell = a$ for some $k, \ell \in \mathbb{Z}$. Then:

$$ak = b$$
$$(b\ell)k = b$$
$$b(\ell k) = b$$
$$\ell k = 1$$

Since $k, \ell \in \mathbb{Z}$, the only possible solutions to this equation are $k = 1, \ell = 1$ or $k = -1, \ell = -1$. Since $b\ell = a$ and ℓ can take on either -1 or 1, $a = \pm b$.

e) This is true. We will perform this proof using the Euclidean algorithm. For Fibonacci numbers F_n, F_{n-1}, we see that $F_n = 1 \cdot F_{n-1} + Fn - 2$. So we see that in this recursive way the Euclidean algorithm would reverse the Fibonacci sequence like this:

$$(F_n, F_{n-1}) \to (F_{n-1}, F_{n-2}) \to (F_{n-2}, F_{n-3}) \cdots \to (F_1, F_0)$$

, where $F_1 = 1, F_0 = 0$. At this point the algorithm would terminate and return 1 as the gcd. This makes any consecutive Fibonacci numbers F_n, F_{n-1} coprime.

Problem 3

a) First, we must prove reflexivity. We may represent a as $nk + r$ where $k \in \mathbb{Z}$ and r is $a\ mod\ n$. We see that a clearly has the same r as itself and is therefore congruent to itself.

b) Second, we must prove symmetry. We assume that $a \equiv b \mod n$. We may represent a as $nk_1 + r$ and b as $nk_2 + r$ where $k_1, k_2 \in \mathbb{Z}$. We can see that a also has the same remainder r as b, so congruence is symmetric.

c) Third, we must prove transitivity. We assume $a \equiv b \mod n$, and $b \equiv c \mod n$. Thus, $a = nk_1 + r, b = nk_2 + r, c = nk_3 + r, k_1, k_2, k_3 \in \mathbb{Z}$. We observe that a and c have the same remainder r. Thus, congruence is also transitive.

Problem 4

a)

*	1	5
1	1	5
5	5	1

b)

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

c)

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Problem 5

We construct an isomorphism $f : \mathbb{Z}_6 \to {\mathbb{Z}_7}^*$ as follows:

x	$f(x)$
0	1
1	3
2	2
3	6
4	4
5	5

We construct the table for ${\mathbb{Z}_7}^*$ such that the structural similarity can be seen

*	1	3	2	6	4	5
1	1	3	2	6	4	5
3	3	2	6	4	5	1
2	2	6	4	5	1	3
6	6	4	5	1	3	2
4	4	5	1	3	2	6
5	5	1	3	2	6	4

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Problem 6

First, we will prove that a group isomorphism $f : G \to G'$ must map the identity of G to the identity of G'. We will do this by contradiction. Assume $f(e) = a' \neq e'$. Then:

$$f(ee) = f(e)f(e)$$

$$f(e) = f(e)f(e)$$

$$a' = a' \cdot a'$$

$$a'^{-1} \cdot a' = a^{-1} \cdot a' \cdot a'$$

$$e' = e' \cdot a'$$

$$e' = a'$$

So we have a contradiction and have proven that the isomorphism must map the first group's identity to the other.

Assume that a group isomorphism $f : {\mathbb{Z}_8}^* \to \mathbb{Z}_4$ exists. It is easily shown by looking at the multiplication table for ${\mathbb{Z}_8}^*$ that for any $a \in {\mathbb{Z}_8}^*$, $a \cdot a = 1$. Since f is an isomorphism and therefore a bijection, there must exist $x \in {\mathbb{Z}_8}^*$ such that $f(x) = 1$. So then:

$$f(xx) = f(x) +_4 f(x)$$

$$f(1) = f(x) +_4 f(x)$$

$$0 \neq 1 +_4 1 = 2$$

So this isomorphism f cannot exist and therefore the groups are not isomorphic.

Problem 7

We assume an isomorphism $f : \mathbb{Q} \to \mathbb{Z}$ We note that any odd $k \in \mathbb{Z}$ must be mapped to by f as an isomorphism is a bijection. Let $f(x) = k$ for some odd k. So then:

$$f\left(\frac{x}{2} + \frac{x}{2}\right) = f\left(\frac{x}{2}\right) + f\left(\frac{x}{2}\right) = 2 \cdot f\left(\frac{x}{2}\right) = k$$

Since k is odd, we observe that $f\left(\frac{x}{2}\right)$ is not an integer and thus f is not a valid map from $\mathbb{Q}$ to $\mathbb{Z}$. So no isomorphism may exist.

Problem 8

I'm bad at Mathematica but I wrote a program in C++ using backtracking that output the Latin squares and output the right number, 2, 12, and 576 for 2, 3, 4 respectively in C++ and output them in the Mathematica array format: https://pastebin.com/6UzmNJE9

Problem 9

We know that ${\mathbb{Z}_n}^* = \{k \in \mathbb{Z}_n | gcd(k, n) = 1\}$. So a group G such that ${\mathbb{Z}_n}^* \subset G \subset \mathbb{Z}_n$ would require that G contain at least one element m such that $gcd(m, n) > 1$. Let $gcd(m, n) = a > 1$. Then, for $c, d \in \mathbb{Z}, ac = m, ad = n$. We will show that the presence of m in G is problematic as it violates the group axiom requiring inverses for all elements.

It is clear that the identity element for any group ${\mathbb{Z}_n}^*$ is 1. Assume an inverse exists for m. This means that there exists $\gamma \in G$ such that $m\gamma \ mod \ n = 1$. We can write this equivalently as $m\gamma = n\sigma + 1$ for some $\sigma \in \mathbb{Z}$. Algebraically we rewrite this as:

$$m\gamma - n\sigma = 1$$

$$ac\gamma - ad\sigma = 1$$

$$a(c\gamma - d\sigma) = 1$$

$$c\gamma - d\sigma = \frac{1}{a}$$

. We know that $\frac{1}{a} \notin \mathbb{Z}$ as $a > 1$ and that $c\gamma - d\sigma \in \mathbb{Z}$. So here we have a contradiction and see that no inverse exists for a potential additional element m, and so no group G with the given constraints can exist.

Problem 10

a) First, we prove that L_a is injective. Assume that $c, d \in G$. We then assume $L_a(c) = a \cdot c = a \cdot d = L_a(d)$. Simple algebra gives $a^{-1} \cdot a \cdot c = a^{-1} \cdot a \cdot d$ and then $c = d$. Thus $L_a(c) = L_a(d)$ implies $c = d$ and L_a is injective.

Second, we prove that L_a is surjective. For any $y \in G$, we can construct an x such that $L_a(x) = a \cdot x = y$. This is $x = (a^{-1} \cdot y)$ as $a \cdot (a^{-1} \cdot y) = (a \cdot a^{-1}) \cdot y = e \cdot y = y$. So L_a is surjective.

Since L_a is surjective and injective it is a bijection.

b)

x	$L_3(x)$
1	3
2	6
3	9
4	1
5	4
6	7
7	10
8	2
9	5
10	8

c)

x	$L_2(x)$
1	2
2	1
3	5
4	6
5	3
6	4