Math 145 (Jao: section 1) A2 Numerical

Simon Liu — 20765498

7 Numerical Problem 1

7.1 Finding -1 in $\mathbb{Z}_n$

Axiom $A4$ states that $a + (-a) = 0$.

$\mathbb{Z}_5$:

$$\begin{aligned} 1 + (-1) &= 0 \\ 1 + 4 &= 0 \\ \therefore -1 &= 4. \end{aligned}$$

In integer systems $\mathbb{Z}_6$, $\mathbb{Z}_7$, and $\mathbb{Z}_10$,

	$\mathbb{Z}_5$	$\mathbb{Z}_6$	$\mathbb{Z}_7$	$\mathbb{Z}_{10}$
-1	4	5	6	9

Theorem 7.1. *$-1 = n - 1$ in $\mathbb{Z}_n$.*

See proof for Theorem 7.2 with $a = 1$.

Theorem 7.2. *$-a = n - a$ in $\mathbb{Z}_n$.*

Proof. For all a and k in $\mathbb{Z}$,

$$\begin{aligned} a &\equiv kn + a \pmod{n} \\ -a &\equiv -kn - a \pmod{n} \end{aligned}$$

Letting $k = -1$,

$$-a \equiv n - a \pmod{n}$$

We know that

$$\forall m \in \mathbb{Z}, m \pmod{n} \in \mathbb{Z}_n$$

So,

$$-a \equiv n - a \pmod{n} \in \mathbb{Z}_n$$

$\square$

7.2 Finding $\frac{1}{2}$ in $\mathbb{Z}_n$

Definition 7.1. *$\frac{1}{a}$ is the element of $\mathbb{Z}_n$ satisfying $a \cdot \frac{1}{a} = 1, \forall a \in \mathbb{Z}_n$ if it exists.*

For $\frac{1}{2}$, $a = 2$ in Definition 7.1.

$\mathbb{Z}_5$:

$$2 \cdot \frac{1}{2} \equiv 1 \equiv 6 \pmod 5$$
$$\frac{1}{2} = 3 \in \mathbb{Z}_5$$

$\therefore \frac{1}{2}$ exists in $\mathbb{Z}_5$.

$\mathbb{Z}_6$:

$$2 \cdot \frac{1}{2} \equiv 7 \pmod 6$$

However, there is no integer b where $2 \cdot b = 7$, so we try larger products that are congruent to 1 (mod 6), only to observe that the product (R.S. of equation) is always odd. There is no such $a \in \mathbb{Z}_6$ that when multiplied by 2 results in an odd integer.

$\therefore \frac{1}{2}$ does not exist in $\mathbb{Z}_5$.

Working more examples,

	$\mathbb{Z}_5$	$\mathbb{Z}_6$	$\mathbb{Z}_7$	$\mathbb{Z}_8$	$\mathbb{Z}_9$	$\mathbb{Z}_{10}$
$\frac{1}{2}$	Exists	DNE	Exists	DNE	Exists	DNE

Theorem 7.3. *$\frac{1}{2}$ does not exist in $\mathbb{Z}_n$ when $\mathbb{Z}_n$ is even.*

See proof for Theorem 7.4 with $k = 2$.

7.3 Finding $\frac{1}{3}$ in $\mathbb{Z}_n$

$\mathbb{Z}_5$:

$$3 \cdot \frac{1}{3} \equiv 1 \equiv 6 \pmod 5$$
$$\frac{1}{3} = 2 \in \mathbb{Z}_5$$

$\therefore \frac{1}{3}$ exists in $\mathbb{Z}_5$.

$\mathbb{Z}_6$:

$$3 \cdot \frac{1}{3} \equiv 1 \equiv 7 \equiv 13 \pmod 6$$

Similar to how $\frac{1}{2} \notin \mathbb{Z}_6$ in Section 7.2, $\frac{1}{3}$ does not seem to exist in $\mathbb{Z}_6$ either.

Working more examples,

	$\mathbb{Z}_5$	$\mathbb{Z}_6$	$\mathbb{Z}_7$	$\mathbb{Z}_8$	$\mathbb{Z}_9$	$\mathbb{Z}_{10}$
$\frac{1}{2}$	Exists	DNE	Exists	Exists	DNE	Exists

	$\mathbb{Z}_6$	$\mathbb{Z}_9$	$\mathbb{Z}_{12}$	$\mathbb{Z}_{15}$	$\mathbb{Z}_{18}$	$\mathbb{Z}_{21}$
$\frac{1}{2}$	DNE	DNE	DNE	DNE	DNE	DNE

Generalizing Theorem 7.3,

Theorem 7.4. $\frac{1}{k}$ *does not exist in* $\mathbb{Z}_n$ *when* $k|n$

Proof. By Definition 7.1, letting $a = \frac{1}{k}$,

$$k \cdot a \equiv 1 \pmod n.$$

Suppose that $k|n$, ie. $n = k \cdot m, m \in \mathbb{Z}^+$. Then,

$$\begin{aligned} k \cdot a &\equiv 1 \pmod{mk} \\ k \cdot a &\equiv 1 \pmod k \\ k \pmod k \cdot a \pmod k &\equiv 1 \pmod k \\ 0 \cdot a \pmod k &\equiv 1 \pmod k \end{aligned}$$

This is not possible for the non-trivial values of $k > 1$, therefore a does not exist. □

7.4 Finding $\frac{1}{k}$ in $\mathbb{Z}_n$

After working through more examples on varying values of k and n, it seemed that k and n had to be coprime for $\frac{1}{k}$ to exist.

Here are some notable examples.

	$\mathbb{Z}_7$	$\mathbb{Z}_{10}$	$\mathbb{Z}_{12}$
1/1	1	1	1
1/2	4	DNE	DNE
1/3	5	7	DNE
1/4	2	DNE	DNE
1/5	3	DNE	5
1/6	6	DNE	DNE
1/7	DNE	3	7
1/8		DNE	DNE
1/9		9	DNE
1/10		DNE	DNE
1/11			11
1/12			DNE

Conjecture 7.5. $\frac{1}{k}$ *does not exist in* $\mathbb{Z}_n$ *when* $gcd(k, n) > 1$.

7.5 Finding $\sqrt{-1}$ in $\mathbb{Z}_n$

Definition 7.2. $\sqrt{a}$ *is an element of* $\mathbb{Z}_n$ *satisfying* $(\sqrt{a})^2 = a$ *if it exists.*

When looking for $\sqrt{-1}$, we need to look for a value a when squared results in $n - 1$ by Theorem 7.1.

I listed examples shown in the spreadsheet 'squares.ods' (uploaded to Learn) on Sheet 1. The second row is values of n representing integer systems $\mathbb{Z}_n$, and the first column is values of a to square. Entries in the table compute $a^2 \pmod{n}$.

If $\sqrt{-1}$ exists in any given $\mathbb{Z}_n$, then in its respective column there will exist a cell equal to $n - 1$. These values are highlighted in yellow.

Hoping to find a visual pattern for the existence of $\sqrt{-1}$, I did not reach any conclusions. I did however notice that for any given $\mathbb{Z}_n$, $a^2 \pmod{n}$ was symmetrical across a.

Theorem 7.6. $\forall a \in \mathbb{Z}_n, a^2 \equiv (n-a)^2 \pmod{n}$

Proof.

$$\begin{aligned} a^2 &\equiv (n-a)^2 \pmod{n} \\ a^2 &\equiv n^2 + a^2 - 2na \pmod{n} \\ a^2 \pmod{n} &\equiv n^2 \pmod{n} + a^2 \pmod{n} - 2na \pmod{n} \\ a^2 \pmod{n} &\equiv 0 + a^2 \pmod{n} - 0 \\ a^2 &= a^2 \pmod{n} \end{aligned}$$

$\square$

I did, however, have a list of $n \leq 100$ where $\sqrt{-1}$ exists in $\mathbb{Z}_n$. Call this sequence S_i.

$$S_i : \{1, 2, 5, 10, 13, 17, 25, 26, 29, 34, 37, 41, 50, 53, 58, 61, 65, 73, 74, 82, 85, 89, 97\}$$

In majority of the above number systems, there existed two values of $\sqrt{-1}$. Interestingly, $n = 65$ and $n = 85$ had four. There were some patterns I could recognize, however none of them described existence of $\sqrt{-1}$ completely.

Theorem 7.7. *$\sqrt{-1}$ exists in $\mathbb{Z}_n$ when $n = k^2 + 1, k \in \mathbb{Z}$.*

Proof.

$$\begin{aligned} \sqrt{-1} &= k \in \mathbb{Z}_{k^2+1} \\ \sqrt{-1} &\equiv k \pmod{k^2+1} \\ (\sqrt{-1})^2 &\equiv k^2 \pmod{k^2+1} \\ -1 &= k^2 \pmod{k^2+1} \end{aligned}$$

This is true by Theorem 7.1:

$$\begin{aligned} -1 &\equiv n - 1 \pmod{n} \\ 1 \equiv k^2 &\equiv (k^2+1) - 1 \pmod{n} \\ k^2 &\equiv k^2 \pmod{n} \end{aligned}$$

$\square$

With no additional insight, I entered the first few numbers of S_i into The On-Line Encyclopedia Of Integer Sequences (OEIS), finding sequence A008784 to be what I was looking for.

An interesting property of this sequence (other than that it represents n s.t. $\sqrt{-1}$ exists $\pmod{n}$) is that every element could be represented as a sum of squares. However, this did not mean that I could simply state that $\forall ab \in \mathbb{Z}, a^2 + b^2 \in S_i$.

This, in turn, meant that it was not as straightforward as I initially thought it would be to construct elements of S_i. I needed to recognize another pattern to do so.

By creating a table in Sheet 2 of 'squares.odt', I computed the sums of squares for $a, b \leq 10$. It seemed that a and b had to be coprime for the sum of their squares to belong in S_i.

Conjecture 7.8. *$\forall a, b \in \mathbb{Z}$, if $gcd(a, b) = 1$, then $\sqrt{-1}$ exists in $\mathbb{Z}_n$ where $n = a^2+b^2$.*

However, I could not explain the anomaly of there existing four or more values of $\sqrt{-1}$ in $\mathbb{Z}_{65}$ and $\mathbb{Z}_{85}$. Theorem 7.6 seemed to explain there existing two values of $\sqrt{-1}$ to some extent, but what caused four or more values?

I went to Prof. Jao's office hours, and he pointed out a particular property of modular arithmetic:

Definition 7.3. $a \equiv b \pmod{pq} \rightleftharpoons a \equiv b \pmod{p} \wedge a \equiv b \pmod{q}$.

Lending itself to:

Theorem 7.9. *If $\sqrt{-1}$ exists in $\mathbb{Z}_n$ and $\mathbb{Z}_m$, then it exists in $\mathbb{Z}_{nm}$.*

Now, with Conjecture 7.8 and Theorem 7.9, we can see that $65 = 4^2 + 7^2$, and is also the product of 5 and 13, both of which are values of n where $\sqrt{-1}$ exists in $\mathbb{Z}_n$. Similarly, $85 = 5^2 + 8^2$, and $85 = 5 * 17$.

8 Numerical Problem 2

8.1 Computation of $\left|\alpha - \frac{41}{24}\right|$

α	$\alpha - (41/24)$	$\lvert\alpha - (41/24)\rvert$
1/1	-17/24	17/24
2/1	7/24	7/24
5/3	-1/24	1/24
12/7	1/168	1/168
41/24	0	0

Notice that the sequence $\{\alpha - \frac{41}{24}\}$ seems to converge to 0, after having terms alternate between being positive and negative. $\{\left|\alpha - \frac{41}{24}\right|\}$ also converges to 0.

8.2 An attempt at defining a pattern

Let us define $S_A : \{0, 1, 3, 7, 17, 24, 41\}$, and $A = 7$ to be the size of S_A.
$a_n \in S_A$ where $a_1 = 0$, $a_2 = 1$, etc.

Similarly, we define $S_B : \{1, 1, 2, 2, 3\}$ with respective $B = 5$ and $b_n \in S_B$.
To express the general term a_n in terms of these two sets, we have:

$$a_n = a_{n-1} \cdot b_{B-n+3} + a_{n-2}$$

So, to construct members of S_A, the first two elements a_1 and a_2 must be given, as well as a full set S_B where $B = A - 2$.

8.3 Observations from the table

		1	1	2	2	3	b
0	1	1	2	5	12	41	c
1	0	1	1	3	7	24	a

From the patterns suggested in the assignment,

$$c = b \cdot 41 + 12$$

More generally, a term in the row containing c is the product of the term immediately above it with the term to the left, plus the term two to the left.

Furthermore, we can say that

$$a \cdot 41 - c \cdot 24 = 1$$