Math Circles - Pigeonhole Principle - Fall 2022

Week 2 (Nov 9)

This week, we'll be focusing on applying the pigeonhole principle to questions in number theory. Often, these questions involve proving that we can numbers from a given set which satisfy certain properties.

Before we jump into examples, there are a few concepts that come up frequently in these types of questions that would be helpful to know.

Modular Arithmetic

Like usual, let's start with an example.

Example. *Suppose we're telling time using a 12-hour clock (ignoring AM and PM), and that it is 7:00 right now.*

(a) What time will it be in 3 hours? How did you get this answer?

Solution. It will be 10:00, because $7 + 3 = 10$. ■

(b) What time will it be in 6 hours? How did you get this answer?

Solution. If will be 1:00. If we count 6 hours from 7:00, we would get 8:00, 9:00, 10:00, 11:00, 12:00, 1:00. ■

(c) What time will it be in 43 hours? How did you get this answer?

Solution. Well, I don't have enough fingers to count in the same way I did the last time, so I need a new strategy.

Every 12 hours, we end up back at the same time we started at. So, we only need to consider the remainder when $7+43 = 50$ is divided by 12. We have that $50 = 4(12)+2$, so the remainder is 2. So, in 43 hours it will be 2:00. ■

The key idea in the previous example is that we were grouping together all integers that have the same remainder when divided by 12, and treating them as equivalent, since they look the same on a basic clock. Since we were only asked what number the clock will be displaying at various times, we didn't need to distinguish between times that occurred in the morning or the afternoon, or even on different days. This doesn't mean that all the times are the same (asking someone to meet you at 1:00 Monday morning is not the same as asking someone to meet you at 1:00 on Tuesday afternoon), it just means that we can treat them the same in this context.

This is an example of *modular arithmetic*.

Formally, this is defined as follows:

Definition. *Let a, b, and n be integers. We say that $a \equiv b \mod n$ ("a is equivalent to b modulo n) if $n \mid b - a$.*

In other words, $a \equiv b \mod n$ if a and b both have the same remainder when divided by n.

When working with integers modulo n, we use the set of remainders under division by n. That is, we generally consider the integers $\{0, 1, \ldots, n-1\}$. We call these the *equivalence classes modulo n*. Informally, when we write $x \mod n$, we are referring to the equivalence class modulo n that x belongs to. In other words, we are referring to the value $a \in \{0, 1, \ldots, n-1\}$ such that $x \equiv a \mod n$.

Example. *We have the following modular equivalences:*

(a) $11 \equiv 1 \mod 5$

(b) $54 \equiv 4 \mod 10$

(c) $13 \equiv 1 \mod 3$

Addition, subtraction, multiplication, and division work the same with modular numbers as they do normally. We can add/subtract/multiply/divide the numbers first, and then take the result modulo n, or we can take the result modulo n during as many of the intermediate steps as we like, and then again at the very end.

Example. *We can compute* $5 + 6 + 7 \mod 4$ *in a few ways:*

- *We could do* $5 + 6 + 7 \equiv 18 \equiv 2 \mod 4$.
- *We could do* $5 \equiv 1 \mod 4$ *and* $6 \equiv 2 \mod 4$ *and* $7 \equiv 3 \mod 4$*, to get that* $5 + 6 + 7 \equiv 1 + 2 + 3 \equiv 6 \equiv 2 \mod 4$.
- *We could even do* $5 \equiv 1 \mod 4$ *and* $7 \equiv 3 \mod 4$ *to get that* $5 + 6 + 7 \equiv 1 + 6 + 3 \equiv 10 \equiv 2 \mod 4$.

What about negative numbers?

Negative numbers work exactly the same as positive numbers.

Example. *We have the following modular equivalences:*

(a) $-3 \equiv 7 \mod 10$ *since* $10 \mid 7 - (-3)$.

(b) $6 \equiv -24 \mod 10$ *since* $10 \mid -24 - 6$.

Modular arithmetic is a powerful tool that is used in many areas of math. This is just the very basics of it, but that should be enough to help you with the exercises. Although modular arithmetic is an extremely convenient tool, this language is not strictly necessary to answer any of the problems; you could phrase everything in terms of remainders during division by n if that is easier for you to understand. In both cases, you are doing the exact same thing, however, it is often easier to argue in terms of modular numbers than it is using remainders, because we have less things to keep track of.

Counting Subsets

Another thing that often comes up is counting the number of subsets of a set S containing k elements. Recall that, if S and S' are sets, the S' is a subset of S (written $S' \subseteq S$) if every element of S' is also an element of S.

Example. *How many subsets do each of the following sets have?*

(a) $S = \emptyset$ *(recall that* $\emptyset$ *is the empty set – the set with no elements)*

Solution. $S = \emptyset$ has only one subset: $\emptyset$. Since $\emptyset$ has no elements, it is a subset of all sets, including itself. ■

(b) $S = \{1\}$

Solution. $S = \{1\}$ has two subsets: $\emptyset$ and $\{1\}$. ■

(c) $S = \{1, 2\}$

Solution. $S = \{1, 2\}$ has 4 subsets: $\emptyset$, $\{1\}$, $\{2\}$, and $\{1, 2\}$. ■

(d) $S = \{1, 2, 3\}$

Solution. $S = \{1, 2, 3\}$ has 8 subsets: $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, $\{1, 2, 3\}$. ■

Do you see a pattern?

Theorem. *Let S be a set containing k elements. Then S has 2^k subsets.*

Proof. Each element of S is either inside a given subset of S, or it isn't. So, there are two options for where to do with each element of S. Since each of these choices is independent, we get $2 \cdot 2 \cdot \cdots \cdot 2 = 2^k$ total different ways to form a subset. So, there are 2^k possible subsets. ■

Examples

Now that we have the theory, let's see how to apply the pigeonhole principle to number-theoretic questions.

Example. *Choose 101 distinct integers from the set $\{1, 2, \ldots, 200\}$. Prove that no matter how you choose these integers, two of them will be such that one divides the other.*

Solution. Recall that a divides b if every factor of a is also a factor of b. We can write each number that we choose as $2^k \cdot x$, where x is odd and $k \geq 0$. There are exactly 100 odd integers between 1 and 200, so two of the integers that we choose must have the same value for x; i.e., we must choose $a = 2^k \cdot x$ and $b = 2^{k'} \cdot x$ for some $k \neq k'$. Without loss of generality, suppose $k < k'$. Then 2^k divides $2^{k'}$. Since x divides itself, we must then have that $2^k \cdot x$ divides $2^{k'} \cdot x$, and hence that a divides b. ■

Example. *Let S be a set of six distinct integers between 1 and 14, inclusive. Show that there must be two distinct, non-empty[1] subsets of S (say, S_1 and S_2) such that the sum of the elements in S_1 is equal to the sum of the elements in S_2.*

Solution. Let S be a set of six distinct integers between 1 and 15, inclusive. For a given S, there are $2^6 - 1 = 63$ distinct, non-empty subsets of S. Now, we are interested in finding the number of possible sums of distinct subsets of S. Let x denote the smallest element of S. Then the smallest possible sum of a non-empty subset of S is x. The largest possible sum would be the sum of all the elements of S. So, for any given set S, the sum of each non-empty subset of S is between x and $x +$ (sum of all other elements of S). The largest that (sum of all other elements of S) could possibly be is $10 + 11 + 12 + 13 + 14 = 60$. So, the sum of every subset of S is between x and $x + 60$, therefore there are 60 different possible sums. But there are 63 different possible subsets of S. So, by letting the possible sums be our holes, and the subsets of S be our pigeons, then by the pigeonhole principle, at least two subsets of S have the same sum. ■

Example. *Let n be a positive integer. Prove that there exists a positive integer z such that z is a multiple of n and every digit of z is either a 1 or a 0.*

[1] A *non-empty* set (or subset) contains at least one element.

Solution. Consider the n integers $y_1 = 1, y_2 = 11, y_3 = 111, \ldots, y_n = 11 \cdots 1$. Notice that if we subtract y_i from y_j (where $i < j$), then we'll end up with an integer whose leading $j - i$ digits are all 1 and whose trailing i digits are all 0.
Consider the value of $y_i \mod n$ for each i. We have two cases to consider:
Case 1: If $y_i \equiv 0 \mod n$ for some i, then by definition of $\mod n$, we get that $n \mid y_i$, and since y_i consists of all 1-digits, this is exactly the multiple of n that we want.
Case 2: Otherwise, for each i, we have that y_i is equivalent to one of $\{1, 2, \ldots, n-1\}$ modulo n. If we take these $n - 1$ options to be our holes, and our values of $y_1, y_2, \ldots, y_n$ to be our pigeons, then by the pigeonhole principle, we get that for some i and j (without loss of generality, suppose $i < j$), $y_i \equiv y_j \mod n$. But by definition, this means that $n \mid y_j - y_i$. Since $y_j - y_i$ consists entirely of 0- and 1- digits, this is exactly the multiple of n that we want. ■