

MODULAR ARITHMETIC

5 minute review. Remind students what addition and multiplication mod m means and the notation they saw in Semester 1, e.g. $3 + 4 \equiv 2 \pmod{5}$ and $3 \times 3 \equiv 4 \pmod{5}$. Introduce $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ as the set of remainders mod m , and the bar notation for modular addition and arithmetic, e.g. writing $\bar{3} + \bar{4} = \bar{2}$ and $\bar{3} \times \bar{3} = \bar{4}$ in \mathbb{Z}_5 .

Class warm-up. Ask for suggestions as to why $\bar{2}, \bar{4}, \bar{1}, \bar{3}, \bar{0}, \bar{2}, \dots$ and $\bar{3}, \bar{1}, \bar{4}, \bar{2}, \bar{0}, \bar{3}, \dots$ are arithmetic progressions in \mathbb{Z}_5 . How do the arithmetic progressions in \mathbb{Z}_7 starting (i) $\bar{2}, \bar{4}, \dots$ and (ii) $\bar{4}, \bar{1}, \dots$ continue? The sequences $\bar{1}, \bar{2}, \bar{4}, \bar{3}, \bar{1}, \bar{2}, \bar{4}, \bar{3}, \dots$ and $\bar{1}, \bar{4}, \bar{1}, \bar{4}, \bar{1}, \bar{4}, \dots$ in \mathbb{Z}_5 are not APs. What structure do they have?

Problems. Choose from the below.

1. Geometric progressions.

- Compute the first 8 terms of the GPs beginning (i) $\bar{1}, \bar{2}$ in \mathbb{Z}_3 ; (ii) $\bar{1}, \bar{3}$ in \mathbb{Z}_5 ; (iii) $\bar{1}, \bar{3}$ in \mathbb{Z}_7 .
- What do you notice about how often the sequences above repeat themselves? Are you reminded of any theorem from Semester 1?
- Now compute the GPs starting (i) $\bar{1}, \bar{2}$ in \mathbb{Z}_7 ; (ii) $\bar{1}, \bar{6}$ in \mathbb{Z}_7 ; (iii) $\bar{1}, \bar{8}$ in \mathbb{Z}_{13} . Can you make these fit with your conjecture above?

2. Fibonacci sequences.

The Fibonacci sequence, $1, 1, 2, 3, 5, 8, 13, \dots$, is a recursive sequence defined by $F_1 = F_2 = 1$ and $F_i = F_{i-2} + F_{i-1}$ for $i > 2$.

- What does the Fibonacci sequence look like mod 2? And mod 3? Do these sequences repeat, and if so after how many terms?
- Where do you find $\bar{0}$ in the Fibonacci sequence mod 3? Complete the sentence “The Fibonacci number F_n is a multiple of 3 if and only if ...”.
- What can you say about the two terms after a $\bar{0}$ in a modular Fibonacci sequence?
- How frequently do the Fibonacci sequences mod 5, 7 and 11 repeat?

3. More on Fibonacci sequences.

- In the Fibonacci sequence mod 3, notice that $\overline{F_5} = \overline{F_6} = \bar{2}$, and so $\overline{F_7} = \bar{2} + \bar{2} = \bar{2} \times \bar{1} + \bar{2} \times \bar{1} = \bar{2} \times \overline{F_1} + \bar{2} \times \overline{F_2} = \bar{2} \times (\overline{F_1} + \overline{F_2}) = \bar{2} \times \overline{F_3}$.
Prove, by induction, that $\overline{F_{n+4}} = \bar{2} \times \overline{F_n}$ whenever $n \geq 1$.
- This means that the Fibonacci sequence mod 3 breaks into blocks of 4, each block obtained from the previous by multiplying by $\bar{2}$. Using results from earlier, can you see why the Fibonacci sequence mod 3 must repeat every 8 terms?
- Can you find similar formulas of the form $\overline{F_{n+c}} = \bar{d} \times \overline{F_n}$ for the Fibonacci sequences mod 5, 7 and 11? Can you fit these answers with how often the sequences repeat?
- For the Fibonacci sequence mod 13, find the first $\bar{0}$, and use this to determine how often the sequence repeats.

For the warm-up, (i) has common difference $\bar{2}$, so continues $\bar{2}, \bar{4}, \bar{6}, \bar{1}, \bar{3}, \bar{5}, \bar{0}, \bar{2}, \dots$; (ii) has common difference $\bar{5}$, so continues $\bar{4}, \bar{1}, \bar{5}, \bar{2}, \bar{6}, \bar{3}, \bar{0}, \bar{4}, \dots$. The final two sequences are geometric progressions, with common ratios $\bar{2}$ and $\bar{4}$ respectively.

Selected answers and hints.

1. (b) Working mod p , these repeat after $p - 1$ terms. Fermat's Little Theorem states $a^{p-1} \equiv 1 \pmod{p}$ if a is coprime to p ; that is, $\bar{a}^{p-1} = \bar{1}$ in \mathbb{Z}_p if $\bar{a} \neq \bar{0}$. Hence, in the sequence $\bar{a}, \bar{a}\bar{r}, \bar{a}\bar{r}^2, \dots$, the p th term is the same as the first, so the sequence must repeat in blocks of $p - 1$ terms.

(c) Here we find sequences repeating more frequently. However, from above, the period must be a factor of $p - 1$ in order to repeat a whole number of times in the block of length $p - 1$, which is what we see.
2. (a) Modulo 2, we get $\bar{1}, \bar{1}, \bar{0}, \bar{1}, \bar{1}, \bar{0}, \dots$ and the sequence repeats itself after three terms. Modulo 3, we have $\bar{1}, \bar{1}, \bar{2}, \bar{0}, \bar{2}, \bar{2}, \bar{1}, \bar{0}, \bar{1}, \bar{1}, \dots$ and the sequence repeats itself after 8 terms.

(b) We find $\bar{0}$ appearing every fourth term. (Is that a little vague?). The sentence could be finished as 'the Fibonacci number F_n is a multiple of 3 if and only if n is a multiple of 4'.

(c) They will be equal, and the same as the term directly preceding the $\bar{0}$.

(d) Mod 5, we get $\bar{1}, \bar{1}, \bar{2}, \bar{3}, \bar{0}, \bar{3}, \bar{3}, \bar{1}, \bar{4}, \bar{0}, \bar{4}, \bar{4}, \bar{3}, \bar{2}, \bar{0}, \bar{2}, \bar{2}, \bar{4}, \bar{1}, \bar{0}, \bar{1}, \bar{1}, \dots$, which repeats after 20 terms.
 Mod 7, $\bar{1}, \bar{1}, \bar{2}, \bar{3}, \bar{5}, \bar{1}, \bar{6}, \bar{0}, \bar{6}, \bar{6}, \bar{5}, \bar{4}, \bar{2}, \bar{6}, \bar{1}, \bar{0}, \bar{1}, \bar{1}, \dots$ repeats after 16 terms.
 Mod 11, $\bar{1}, \bar{1}, \bar{2}, \bar{3}, \bar{5}, \bar{8}, \bar{2}, \bar{10}, \bar{1}, \bar{0}, \bar{1}, \bar{1}, \dots$ repeats after 10 terms.
3. (a) We prove the formula $\overline{F_{n+4}} = \bar{2} \times \overline{F_n}$ by induction on n .

Initial step: Since $\overline{F_1} = \bar{1}$ and $\overline{F_2} = \bar{1}$, then $\overline{F_5} = \bar{2} = \bar{2} \times \overline{F_1}$ and $\overline{F_6} = \bar{2} = \bar{2} \times \overline{F_2}$, so the formula holds for $n = 1$ and $n = 2$.

Induction step: Let $k > 2$ and suppose that $\overline{F_{n+4}} = \bar{2} \times \overline{F_n}$ for all $n < k$. Then, by the induction hypothesis, $\overline{F_{k+3}} = \bar{2} \times \overline{F_{k-1}}$ and $\overline{F_{k+2}} = \bar{2} \times \overline{F_{k-2}}$ so

$$\overline{F_{k+4}} = \overline{F_{k+3}} + \overline{F_{k+2}} = \bar{2} \times \overline{F_{k-1}} + \bar{2} \times \overline{F_{k-2}} = \bar{2} \times (\overline{F_{k-1}} + \overline{F_{k-2}}) = \bar{2} \times \overline{F_k},$$

so the formula holds for $n = k$. By induction, the result holds for all n .

(b) Since $\bar{2}^2 = \bar{1}$ in \mathbb{Z}_3 , the third block (which is $\bar{2}$ times the second, so $\bar{2}^2$ times the first) will be the same as the first block.

(c) The Fibonacci sequence mod 5 starts $\bar{1}, \bar{1}, \bar{2}, \bar{3}, \bar{0}, \bar{3}, \bar{3}, \bar{1}, \bar{4}, \bar{0}, \bar{4}, \bar{4}, \bar{3}, \bar{2}, \bar{0}, \dots$, which appears to have blocks of length 5 obtained by multiplication by $\bar{3}$. That is, it seems that $\overline{F_{n+5}} = \bar{3} \times \overline{F_n}$, which can be proved as above. As $\bar{3}^4 = \bar{1}$ in \mathbb{Z}_5 , it follows that the sequence repeats after $4 \times 5 = 20$ terms.

In \mathbb{Z}_7 , the formula is $\overline{F_{n+8}} = \bar{6} \times \overline{F_n}$ and the sequence repeats after two blocks of length 8, since $\bar{6}^2 = \bar{1}$ in \mathbb{Z}_7 ; that is, it repeats after 16 terms.

In \mathbb{Z}_{11} , we get $\overline{F_{n+10}} = \overline{F_n}$, repeating after one block of length 10.

(d) In \mathbb{Z}_{13} , the first $\bar{0}$ is the 7th term, and we find $\overline{F_{n+7}} = \bar{8} \times \overline{F_n}$. The sequence repeats after 4 blocks of 7 since $\bar{7}^4 = \bar{1}$ in \mathbb{Z}_{13} .

For more details, start a thread on the discussion board.