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 $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ as the set of remainders mod m, and the bar notation for modular addition and arithmetic, e.g. writing $\overline{3}+\overline{4} = \overline{2}$ and $\overline{3} \times \overline{3} = \overline{4}$ in $\mathbb{Z}_5$.

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

Problems. Choose from the below.

1. **Geometric progressions**.
   (a) Compute the first 8 terms of the GPs beginning (i) $\overline{1}, \overline{2}$ in $\mathbb{Z}_3$; (ii) $\overline{1}, \overline{3}$ in $\mathbb{Z}_5$; (iii) $\overline{1}, \overline{3}$ in $\mathbb{Z}_7$.
   (b) What do you notice about how often the sequences above repeat themselves? Are you reminded of any theorem from Semester 1?
   (c) Now compute the GPs starting (i) $\overline{1}, \overline{2}$ in $\mathbb{Z}_7$; (ii) $\overline{1}, \overline{6}$ in $\mathbb{Z}_7$; (iii) $\overline{1}, \overline{8}$ in $\mathbb{Z}_{13}$. Can you make these fit with your conjecture above?
2. **Fibonacci sequences**. The Fibonacci sequence, $1, 1, 2, 3, 5, 8, 13, \ldots$, is a recursive sequence defined by $F_1 = F_2 = 1$ and $F_i = F_{i-2} + F_{i-1}$ for $i > 2$.
   (a) What does the Fibonacci sequence look like mod 2? And mod 3? Do these sequences repeat, and if so after how many terms?
   (b) Where do you find $\overline{0}$ in the Fibonacci sequence mod 3? Complete the sentence "The Fibonacci number F_n is a multiple of 3 if and only if ...".
   (c) What can you say about the two terms after a $\overline{0}$ in a modular Fibonacci sequence?
   (d) How frequently do the Fibonacci sequences mod 5, 7 and 11 repeat?
3. **More on Fibonacci sequences**.
   (a) In the Fibonacci sequence mod 3, notice that $\overline{F_5} = \overline{F_6} = \overline{2}$, and so
   $\overline{F_7} = \overline{2} + \overline{2} = \overline{2} \times \overline{1} + \overline{2} \times \overline{1} = \overline{2} \times \overline{F_1} + \overline{2} \times \overline{F_2} = \overline{2} \times (\overline{F_1} + \overline{F_2}) = \overline{2} \times \overline{F_3}$.
   Prove, by induction, that $\overline{F_{n+4}} = \overline{2} \times \overline{F_n}$ whenever $n \geq 1$.
   (b) This means that the Fibonacci sequence mod 3 breaks into blocks of 4, each block obtained from the previous by multiplying by $\overline{2}$. Using results from earlier, can you see why the Fibonacci sequence mod 3 must repeat every 8 terms?
   (c) Can you find similar formulas of the form $\overline{F_{n+c}} = \overline{d} \times \overline{F_n}$ for the Fibonacci sequences mod 5, 7 and 11? Can you fit these answers with how often the sequences repeat?
   (d) For the Fibonacci sequence mod 13, find the first $\overline{0}$, and use this to determine how often the sequence repeats.

For the warm-up, (i) has common difference $\overline{2}$, so continues $\overline{2}, \overline{4}, \overline{6}, \overline{1}, \overline{3}, \overline{5}, \overline{0}, \overline{2}, \ldots$; (ii) has common difference $\overline{5}$, so continues $\overline{4}, \overline{1}, \overline{5}, \overline{2}, \overline{6}, \overline{3}, \overline{0}, \overline{4}, \ldots$. The final two sequences are geometric progressions, with common ratios $\overline{2}$ and $\overline{4}$ 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, $\overline{a}^{p-1} = \overline{1}$ in $\mathbb{Z}_p$ if $\overline{a} \neq \overline{0}$. Hence, in the sequence $\overline{a}, \overline{a}.\overline{r}, \overline{a}.\overline{r}^2, \ldots$, the pth 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 $\overline{1}, \overline{1}, \overline{0}, \overline{1}, \overline{1}, \overline{0}, \ldots$ and the sequence repeats itself after three terms. Modulo 3, we have $\overline{1}, \overline{1}, \overline{2}, \overline{0}, \overline{2}, \overline{2}, \overline{1}, \overline{0}, \overline{1}, \overline{1}, \ldots$ and the sequence repeats itself after 8 terms.

   (b) We find $\overline{0}$ 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 $\overline{0}$.

   (d) Mod 5, we get $\overline{1}, \overline{1}, \overline{2}, \overline{3}, \overline{0}, \overline{3}, \overline{3}, \overline{1}, \overline{4}, \overline{0}, \overline{4}, \overline{4}, \overline{3}, \overline{2}, \overline{0}, \overline{2}, \overline{2}, \overline{4}, \overline{1}, \overline{0}, \overline{1}, \overline{1}, \ldots$, which repeats after 20 terms.

   Mod 7, $\overline{1}, \overline{1}, \overline{2}, \overline{3}, \overline{5}, \overline{1}, \overline{6}, \overline{0}, \overline{6}, \overline{6}, \overline{5}, \overline{4}, \overline{2}, \overline{6}, \overline{1}, \overline{0}, \overline{1}, \overline{1}, \ldots$ repeats after 16 terms.

   Mod 11, $\overline{1}, \overline{1}, \overline{2}, \overline{3}, \overline{5}, \overline{8}, \overline{2}, \overline{10}, \overline{1}, \overline{0}, \overline{1}, \overline{1}, \ldots$ repeats after 10 terms.

3. (a) We prove the formula $\overline{F_{n+4}} = \overline{2} \times \overline{F_n}$ by induction on n.

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

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

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

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

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

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

   In $\mathbb{Z}_7$, the formula is $\overline{F_{n+8}} = \overline{6} \times \overline{F_n}$ and the sequence repeats after two blocks of length 8, since $\overline{6}^2 = \overline{1}$ 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 $\overline{0}$ is the 7th term, and we find $\overline{F_{n+7}} = \overline{8} \times \overline{F_n}$. The sequence repeats after 4 blocks of 7 since $\overline{8}^4 = \overline{1}$ in $\mathbb{Z}_{13}$.

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