**FM2** Assignment #38 Name: Maggie

1. An arithmetic sequence has first term 2 and common difference 4. Another arithmetic sequence has first term 7 and common difference 5. Find the set of numbers which are members of both sequences.

Let the first sequence be $\{a_n\}$ and the second $\{b_n\}$.

$\Rightarrow a_n = 4n-2$, $b_n = 5n+2$.

$\{a_n\} \cap \{b_n\} = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 4,\ x \equiv 2 \pmod 5 \text{ and } x \geqslant 7\}$

$= \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{20},\ x \geqslant 7\}$.

$= \{x \in \mathbb{Z} \mid x = 20k+2,\ k \in \mathbb{Z}^+\}$

2. What is the remainder when $314^{164}$ is divided by 165? Make sure to justify your answer.

$165 = 3 \times 5 \times 11$

By FLT.

$314^2 \equiv 1 \pmod 3 \Rightarrow 314^{160} \equiv 1 \pmod 3$

$314^4 \equiv 1 \pmod 5 \Rightarrow 314^{160} \equiv 1 \pmod 5 \Rightarrow 314^{160} \equiv 1 \pmod{3 \times 5 \times 11}$

$314^{10} \equiv 1 \pmod{11} \Rightarrow 314^{160} \equiv 1 \pmod{11}$

$314^4 \equiv (-16)^4 \equiv 91^2 \equiv 31 \pmod{165}$

Therefore, $314^{164} \equiv 31 \times 1 \equiv 31 \pmod{165}$

3. Show that every cyclic group of order greater than two has at least two generators.

Let $G$ be a cyclic group. $|G| > 2$

Let $\langle a \rangle = G$. Then $a^i = (a^{-1})^{-i}$ for any $a^i \in \langle a \rangle$.

$\Rightarrow \langle a^{-1} \rangle = G$. Therefore there must be at least two generators $a, a^{-1}$.

$\blacksquare$

4. (a) Show that $a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0 \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \pmod{11}$.

$10 \equiv -1 \pmod{11}$

So $\sum_{i=0}^{n} a_n \times 10^n \equiv \sum_{i=0}^{n} a_n \times (-1)^n$

$\equiv a_0 - a_1 + a_2 \cdots + (-1)^n a_n \pmod{11}$. $\square$

(b) Alice claims 27 182 818 284 590 452 is divisible by 11. Bob disagrees. Who is right? Explain.

By (a). The alternating sum of digits of the number in the question is

$2-5+4-\cdots-7+2=-22$.

Since $-22 \equiv 0 \pmod{11}$, it's divisible by 11.

Alice is right.

5. If $p$ and $q$ are distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

By FLT,

$$\begin{cases} p^{q-1} \equiv 1 \pmod{q}, \text{ and} \\ q^{p-1} \equiv 1 \pmod{p}. \end{cases}$$

Since $$\begin{cases} q^{p-1} \equiv 0 \pmod{q}, \\ p^{q-1} \equiv 0 \pmod{p} \end{cases}$$

$$\Rightarrow \begin{cases} p^{q-1} + q^{p-1} - 1 \equiv 0 \pmod{q} \\ q^{p-1} + p^{q-1} - 1 \equiv 0 \pmod{p} \end{cases}$$

$\Rightarrow$ both $p$ and $q$ is divisible by $(p^{q-1} + q^{p-1} - 1)$

$\Rightarrow p^{q-1} + q^{p-1} - 1 \equiv 0 \pmod{pq}$

$\Rightarrow p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

$\square$.