Homework **30** Solutions

Problems

1. (a) **Find a generator for arithmetic mod 13.**

   Let's start by trying 2. We have

$$
\begin{aligned}
2^2 &\equiv 4 \\
2^3 &\equiv 8 \\
2^4 &\equiv 16 \equiv 3 \\
2^5 &\equiv 6 \\
2^6 &\equiv 12 \equiv -1
\end{aligned}
$$

   where all of these equivalences are $\pmod{13}$. At this point, we can conclude that $\boxed{2}$ is a generator since we know that the remaining numbers in the sequence are just the negatives of the numbers we've already computed (eg $2^{10} = 2^6 \times 2^4 = -2^4 = -3 \pmod{13}$). See part (c) for other possibilities.

   (b) **Find a square root of $-1 \pmod{13}$.**

   $2^6 = -1 \pmod{13}$ so that $2^3 = \boxed{8}$ is a square root of $-1 \pmod{13}$. The other square root is $-8 \equiv \boxed{5}$.

   (c) **Find all other generators for arithmetic mod 13. How many are there? (Does your answer agree with the general formula you learnt today?)**

   Every generator is of the form 2^r where r is relatively prime to 12, so the generators are $2^1 \equiv \boxed{2}, 2^5 \equiv \boxed{6}, 2^7 \equiv \boxed{11}, 2^{11} \equiv \boxed{7}$ where we are working $\pmod{13}$.

   (d) **For each non-zero number a mod 13, find its *period* (i.e., the smallest number $k > 0$ such that $a^k \equiv 1 \pmod{13}$).**

a	1	2	3	4	5	6	7	8	9	10	11	12
period	1	12	3	6	4	12	12	4	3	6	12	2

   We know that 1 has period 1 and $12 \equiv -1$ has period 2. Also, the four generators (2, 6, 7, and 11) have period 12. The two square roots of -1 (5 and 8) have period 4. We can see that $2^4 \equiv 3$ and $2^8 \equiv 9$ have period 3 (as 3 is the least k for which 12 divides $4k$ and for which 12 divides $8k$). Similarly, $2^2 \equiv 4$ and $2^{-2} \equiv 10$ have period 6.

   Congrats on completing the last homework, and good luck on the final!