Session 1: Introduction to Modular Arithmetic

- Show students RSA challenge powerpoint. Explain that the system of internet encryption relies on use of modular arithmetic.

- Use familiar contexts (time, days of the week, Imperial Measures, days of the year) to introduce the concept of clock arithmetic to the students.

- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$. Students are to explore this relationship and then work on a proof of this relationship.

- Similarly, explore whether $ac \equiv bd \pmod{m}$

- By extension: If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$

Set students some questions relating to these rules to cement their understanding (IB Discrete textbook p.27).

Students to select some multiples of 9 and explore what happens using modular arithmetic:

Eq 369 = 300 + 60 + 9 and $300 + 60 + 9 \equiv 300 \pmod{9} + 60 \pmod{9} + 9 \pmod{9}$

$\equiv 3 \pmod{9} + 6 \pmod{9} + 9 \pmod{9}$

$\equiv 18 \pmod{9} \equiv 0 \pmod{9}$

Run through proof for test of divisibility by 9:

http://sites.google.com/site/mathematicsnotebook/divisibilityrules/divisibility3/alternate-proof

Extend argument to show that tests of divisibility can be carried out in this manner for any divisor by changing the number base such that it is one more than the divisor and then adding the digits up.