1 Amaze Your Friends

You want to trick your friends into thinking you can perform mental arithmetic with very large numbers. What are the last digits of the following numbers?

(a) $11^{2017}$

(b) $9^{10001}$

(c) $3^{987654321}$

2 Combining Moduli

Suppose we wish to work modulo $n = 40$. Note that $40 = 5 \times 8$, with $\gcd(5, 8) = 1$. We will show that in many ways working modulo 40 is the same as working modulo 5 and modulo 8, in the sense that instead of writing down $c \pmod{40}$, we can just write down $c \pmod{5}$ and $c \pmod{8}$.

(a) What is $8 \pmod{5}$ and $8 \pmod{8}$? Find a number $a \pmod{40}$ such that $a \equiv 1 \pmod{5}$ and $a \equiv 0 \pmod{8}$.

(b) Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod{5}$ and $b \equiv 1 \pmod{8}$. 
(c) Now suppose you wish to find a number \( c \) (mod 40) such that \( c \equiv 2 \) (mod 5) and \( c \equiv 5 \) (mod 8). Find \( c \) by expressing it in terms of \( a \) and \( b \).

(d) Repeat to find a number \( d \) (mod 40) such that \( d \equiv 3 \) (mod 5) and \( d \equiv 4 \) (mod 8).

(e) Compute \( c \times d \) (mod 40). Is it true that \( c \times d \equiv 2 \times 3 \) (mod 5), and \( c \times d \equiv 5 \times 4 \) (mod 8) for all integers \( c \) and \( d \)?

3 Baby Fermat

Assume that \( a \) does have a multiplicative inverse mod \( m \). Let us prove that its multiplicative inverse can be written as \( a^k \) (mod \( m \)) for some \( k \geq 0 \).

(a) Consider the sequence \( a, a^2, a^3, \ldots \) (mod \( m \)). Prove that this sequence has repetitions.

(b) Assuming that \( a^i \equiv a^j \) (mod \( m \)), where \( i > j \), what can you say about \( a^{i-j} \) (mod \( m \))?

(c) Prove that the multiplicative inverse can be written as \( a^k \) (mod \( m \)). What is \( k \) in terms of \( i \) and \( j \)?