MAS114 Problems

Sheet 8 (Week 9)

Preamble

Themes from this week (ask your tutorial staff if you're stuck): 1. Inverses modulo n. 2. The Chinese Remainder Theorem. 3. Exponentiation in modular arithmetic. 4. Fermat's Little Theorem. 5. Euler's φ function. 6. The Fermat-Euler Theorem.

Work on these problems one at a time in small groups (of around four). For many problems there is designed to be a lot of work that's best shared; and for others discussion is vital to understanding.

1

Note that $2 \equiv 7 \pmod 5$.

(i) Is it true that $2^3 \equiv 7^3 \pmod 5$?

(ii) Is it true that $3^2 \equiv 3^7 \pmod 5$?

For discussion: Of course, this means you've got to be a little careful with exponentiation in modular arithmetic. Can you come up with a rule for what's permitted and what isn't?

2

(i) How many numbers between 1 and 5000 are even?

(ii) How many numbers between 1 and 5000 are multiples of five?

(iii) How many numbers between 1 and 5000 are even *and* multiples of five?

(iv) How many numbers between 1 and 5000 are even *or* multiples of five?

(v) What is $\varphi(5000)$?

(vi) Can you generalise these to find $\varphi(p^a q^b)$ where p, q are two different primes?

For discussion: Can you generalise this to find $\varphi(n)$, where the prime factorisation of n is $p_1^{a_1} \cdots p_r^{a_r}$?

3

(i) What is the remainder left upon dividing 2^{2016} by 10?

(ii) What is the remainder left upon dividing 2^{2016} by 11?

(iii) What is the remainder left upon dividing 2^{2016} by 12?

For discussion: I can think of at least two sensible ways of doing each of these. Can you?

4

Modulo 7, everything is congruent to 0, 1, 2, 3, 4, 5 or 6. Which of these seven residues can *squares* be congruent to?
What about squares modulo 11, 13 or 17 instead?
What about cubes?

For discussion: How many squares are there mod p in each case? Can you form a guess about how many there will be for any prime modulus p?
Try to guess which primes p have the property that -1 is a square modulo p: for example, -1 is not a square modulo 3, as the only squares are 0 and 1, and -1 is not congruent to either of these; however, -1 is a square modulo 5, since $2^2 \equiv -1$.
Note that this tells us something about which primes can occur as factors of numbers of the form $n^2 + 1$: for example, the prime 3 can't, but the prime 5 can. This could be useful!