MAS114 Solutions

Sheet 8 (Week 9)

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 $3^2 \equiv 3^7 \pmod 5$?

   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?

   Solution

   (i) Yes, $2 \cdot 2 \cdot 2 \equiv 7 \cdot 7 \cdot 7 \pmod 5$.

   (ii) No, it's not true. $3^2 = 9 \equiv 4 \pmod 5$, but $3^7 = 2187 \equiv 2 \pmod 5$. So exponentiation doesn't work like that.

2. The function $\varphi(n)$ is the number of numbers from 1 to n which are coprime to n. So, for example, $\varphi(6) = 2$, as only 1 and 5 are coprime to 6. Also, $\varphi(7) = 6$, as 1, 2, 3, 4, 5, and 6 are all coprime to 7.

   (i) How many numbers from 1 to 5000 are even?

   (ii) How many numbers from 1 to 5000 are multiples of five?

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

   (iv) How many numbers from 1 to 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?

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

Solution There are 2500 even numbers, 1000 multiples of five, 500 which are both, 3000 which are one or the other, and so $\varphi(5000) = 2000$.

In general, $\varphi(p^a q^b) = (p-1)p^{a-1}(q-1)q^{b-1}$.

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?

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

Solution

(i) We can check that 2^n starts 1 modulo 10 and then cycles $2, 4, 8, 6, 2, \ldots$. So

$$2^{2016} = 2^{4\times 504} \equiv 6 \pmod{10}.$$

(ii) For this one, we can use Fermat's Little Theorem, which says that $2^{10} \equiv 1 \pmod{11}$. That means that

$$2^{2016} = 2^{201\times 10+6} \equiv 2^6 \equiv 64 \equiv 9 \pmod{11}.$$

(iii) All values $2^2, 2^3, \ldots$ will be $0 \pmod 4$ and hence 0, 4 or 8 modulo 12. This is determined by what they are modulo 3, but it can easily be checked (by Fermat's Little Theorem or pattern-spotting) that $2^{2016} \equiv 1 \pmod 3$ and hence $2^{2016} \equiv 4 \pmod{12}$.

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?

   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!

Solution Modulo 7, we have $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$ and $6^2 \equiv 1$. So the squares are 0, 1, 2 and 4.

Modulo 11, the squares are 0, 1, 3, 4, 5, and 9.

Modulo 13, they are 0, 1, 3, 4, 9, 10 and 12.

Modulo 17, they are 0, 1, 2, 4, 8, 9, 13, 15 and 16.

In general, for an (odd) prime p, there are $(p+1)/2$ squares modulo p.

Modulo 7, cubes are 0, 1 and 6. Modulo 13, they are 0, 1, 5, 8 and 12. Modulo 11 and 17, everything is a cube. In fact, for primes of the form $3n+2$, everything is a cube, and for primes of the form $3n+1$, there are $n+1$ cubes.