MAS114 Problems

Sheet 6 (Week 6)

Preamble

Themes from this week (ask your tutorial staff if you're stuck): 1. Bezout's lemma. 2. If $p \mid ab$, then $p \mid a$ or $p \mid b$. 3. The fundamental theorem of arithmetic. 4. Solving linear diophantine equations in two variables. 5. Congruence modulo n.

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

Make a list of all primes between 1 and 200 (with appropriate groupwork, this shouldn't take too long; to help you check your working, there are 46 of them).

(i) How many leave each possible remainder (0, 1 or 2) upon division by 3?

(ii) How many leave each possible remainder (0, 1, 2 or 3) upon division by 4?

(iii) How many leave each possible remainder upon division by 5?

For discussion: Does there seem to be much of a pattern? Would you care to make any guesses about what would happen in the long term as we take more and more primes?

2

Recall that an *odd number* is one of the form $2k + 1$.

(i) Show that the square of an odd number leaves a remainder of 1 when divided by 4;

(ii) Show that the square of an odd number leaves a remainder of 1 when divided by 8;

(iii) Which remainders are possible when the square of an odd number is divided by 16?

For discussion: What techniques can you think of to deal with problems such as these? I can think of several.

3

(i) What is the relationship between a fraction being in lowest terms, and the greatest common divisor of two numbers?

(ii) Show by computing a greatest common divisor, that the fraction $\frac{14n+3}{21n+4}$ is in lowest terms, for all positive integers n.

4

Frequently we want to calculate x^n, given some input x (a real number, perhaps) and a positive integer n, and in this problem we seek to work out how to do it with as few multiplications as possible.
For example, if we want x^{10}, then the most naive strategy sees us calculate x^2 as $x \times x$, then x^3 as $x^2 \times x$, then x^4 as $x^3 \times x$, and so on. This would take nine multiplications. But we can do it with much fewer: calculate x^2, then x^4 as $x^2 \times x^2$, then x^5 as $x^4 \times x$, then x^{10} as $x^5 \times x^5$. This takes only four multiplications!

(i) Find the best ways you can for computing x^n for each $2 \leq n \leq 20$.

(ii) How well does each of the following recursive strategies perform in practice? Try them on a good range of numbers (certainly including $x^2, \ldots, x^{20}$ as above, but x^{23} and x^{33} are also particularly good to look at).

(a) If n is odd, we calculate x^{n-1} (using this strategy again) and multiply by x. If n is even, we calculate $x^{n/2}$ (using this strategy again) and multiply it by itself.

(b) If n is prime, we calculate x^{n-1} (using this strategy again) and multiply by x. If not, we write $n = ab$ and calculate x^n as $(x^a)^b$ (using this strategy again for both powers).

For discussion: How might one discover the best way of doing it? Can you think of any sensible strategies other than (a) and (b) above?