MAS114 Solutions

Sheet 6 (Week 6)

1. Make a list of all primes between 1 and 100.

   (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?

   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?

   Solution The primes are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

   There are 25 of them.

   On division by three, one leaves remainder 0, 11 leave remainder 1, and 13 leave remainder 2.

   On division by four, one leaves remainder 2, 11 leave remainder 1, and 13 leave remainder 3.

   These counts seem fairly even among the remainders that can actually happen. There is a long story about what does happen, but "fairly even" is a good start.

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?

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

Solution

(i) We can do this one directly: let our odd number take the form $2k+1$; its square is then $(2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1$; hence the remainder upon division by 4 is 1.

(ii) Note that the number k^2+k is even for all k, since $k^2+k = k(k+1)$ and one of these two is always even. Hence $k^2+k = 2l$ for some l, and so $(2k+1)^2 = 8l+1$ as required.

(iii) Since the square of an odd number is of the form $8k+1$ (as seen in the previous question), it's either of the form $16l+1$ or $16l+9$. Both are possible (for example, 1^2 and 3^2 are of each of those forms).

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.

Solution

(i) The fraction $\frac{u}{v}$ is in lowest terms if and only if u and v have greatest common divisor 1: in other words, if they are coprime.

(ii) We use the methodology of Euclid's algorithm to show that $\gcd(14n+3, 21n+4) = 1$ for all n.

Indeed, we have

$$\begin{aligned}\gcd(14n+3, 21n+4) &= \gcd(14n+3, (21n+4)-(14n+3))\\ &= \gcd(14n+3, 7n+1)\\ &= \gcd((14n+3)-2(7n+1), 7n+1)\\ &= \gcd(1, 7n+1) = 1.\end{aligned}$$

Since they have no nontrivial factors, the fraction is in lowest terms.

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).

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

Solution Here is a table showing the best chains you can do (in many cases these are not unique), and what strategies (a) and (b) give you:

power	a shortest chain	optimal	strategy (a)	strategy (b)
x^2	x^2	1	1	1
x^3	x^2, x^3	2	2	2
x^4	x^2, x^4	2	2	2
x^5	x^2, x^3, x^5	3	3	3
x^6	x^2, x^3, x^6	3	3	3
x^7	x^2, x^3, x^5, x^7	4	4	4
x^8	x^2, x^4, x^8	3	3	3
x^9	x^2, x^4, x^8, x^9	4	4	4
x^{10}	x^2, x^4, x^5, x^{10}	4	4	4
x^{11}	$x^2, x^4, x^5, x^{10}, x^{11}$	5	5	5
x^{12}	x^2, x^3, x^6, x^{12}	4	4	4
x^{13}	$x^2, x^4, x^8, x^9, x^{13}$	5	5	5
x^{14}	$x^2, x^3, x^5, x^7, x^{14}$	5	5	5
x^{15}	$x^2, x^3, x^6, x^{12}, x^{15}$	5	6	5
x^{16}	x^2, x^4, x^8, x^{16}	4	4	4
x^{17}	$x^2, x^4, x^8, x^9, x^{17}$	5	5	5
x^{18}	$x^2, x^4, x^8, x^{16}, x^{18}$	5	5	5
x^{19}	$x^2, x^4, x^8, x^{16}, x^{18}, x^{19}$	6	6	6
x^{20}	$x^2, x^3, x^5, x^{10}, x^{20}$	5	5	5
x^{23}	$x^2, x^3, x^5, x^{10}, x^{20}, x^{23}$	6	7	7
x^{33}	$x^2, x^4, x^8, x^{16}, x^{32}, x^{33}$	6	6	7

As can be seen from x^{15} and x^{33}, it is possible for each strategy to give the optimal solution, but the other one not to. As can be seen from x^{23}, it is also possible that neither strategy gives the optimal solution!

There is quite a lot of weird behaviour: for example, it is known that $x^{375494703}$ requires 35 multiplications. One would expect that $x^{750989406} = (x^{375494703})^2$ would be harder, but in fact it's easier: it only needs 34 multiplications!