EMAT10001 Workshop Sheet 4 - outline solutions.

Conor Houghton 2013-10-17

1. No solution given.

2. If $r_1 = a \bmod c$ then $a = n_1c + r_1$, similarly if $r_2 = b \bmod c$ then $b = n_2c + r_2$ so the right hand side is $r_1 + r_2 \bmod c$ and the left hand side is $n_1c + r_1 + n_2c + r_2 \bmod c$ and we can loose the $(n_1+n_2)c$ since it's a multiple of c. For the second one the right hand side is $r_1r_2 \bmod c$ whereas the left hand side is $(r_1 + n_1c)(r_2 + n_2c) \bmod c = (r_1r_2 + \text{stuff} \cdot c) \bmod c = r_1r_2 \bmod c$.

3. $60 = 3 \cdot 4 \cdot 5$ has 12 factors; it is the smallest number with 12 factors, but 72, 84, 90 and 96 do as well. The idea is to quicky write out the table, but you can guess it is a number with all the low factors, so, for example, under 1000 the best is $840 = 3 \cdot 5 \cdot 7 \cdot 8$ with 32 factors.

4. Take an example first, $8 = 2^3$ and it is divided by 1, 2, 4 and 8. More generally $p^r/p^s = p(r - s)$ and the answer is $r + 1$, taking in to account $s = 0$.

5. The lemma about division.

   (a) If $a|b$ then $b = ma$ and if $x|y$ then $y = nx$ so $by = mnax$ and hence $ax|by$.

   (b) So if $a|b$ then $b = ma$ and if $b|c$ then $c = nb$ hence $c = mna$ and $a|c$.

   (c) Well if $a|b$ then $b = na$ and $n \neq 0$ if $b \neq 0$ so $b >= a$.

   (d) In the usual way $b = ma$ and $c = na$ so $bx + cy = xma + yna$ so $a|(bx + cy)$.

6. If one was a prime then the integers wouldn't be a unique factorization domain and lots of theorems would be harder to

7. The first 99 values are given at `http://oeis.org/A000010`.

8. If $d|p^n$ it must be in the form p^s, so if $d|a$ then $a = mp$ for some m. Now, to work out the possible values of m, divide p^n by p, giving p^{r-1}.

9. Any number that isn't p is coprime with p so $\phi(p) = p - 1$.

10. From our calculation above, there are p^{r-1} numbers which are co-prime with p^r so

$$\phi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right) \tag{1}$$

11. This follows from what we have done above

$$\phi(n) = n \prod \left(1 - \frac{1}{p_i}\right) \tag{2}$$

12. So if $d|a$ and $d|b$ then $d|(a-b)$, conversely, if $d|(a-b)$ and $d|b$ then $d|a$ so a and b and $a-b$ and b have the same common divisors, so the have the same greatest divisor. The important point is you need to argue both ways to show the set of common divisors are the same and not just that one is contained in the other.

13. So the answer if $(\phi(n)-2)/2$; basically, if you skip on to the $i+k$th star each time, if $(n,k) \neq 1$ you get back to where you started without visiting all the points, $k=1$ is explicitely excluded in the question and if $(n,k)=1$ then $(n-k,n)=1$ but that gives the same star, so you have to divide by two.

14. No answer given; you can check your answers at `http://gcd.awardspace.com/`, though of course, it is best to write your own.

15. The slowest convergence is when there is the least change each time; thus at each step we want
$$r = x + y \tag{3}$$
but if you write it out this amounts to $t_{n+1} = t_n + t_{n-1}$ then, depending how you define 'slowest' this gives the Fibonacci sequence.

16. Prove that
$$[a + b \bmod c] = [[a \bmod c] + [b \bmod c] \bmod c] \tag{4}$$
and
$$[ab \bmod c] = [[a \bmod c][b \bmod c] \bmod c] \tag{5}$$

17. Symmetry and reflexivity are obvious, for transitivity $a \equiv b \pmod ()n$ means $a-b = m_1 n$ for some m_1, similarly $b \equiv c \pmod ()n$ means $b - c = m_2 n$ for some m_2, so $a - c = a - b + (b - c) = (m_1 + m_2)n$ so $a \equiv c \pmod ()n$.