BMOC Mentoring Scheme

Advanced Level – Sheet 3

Possible Solutions

1. *Find counting arguments to prove the following identities (i.e. find something you can count in two different ways so that one way is the LHS and the other is the RHS)*

   (a) $\binom{n}{s} = \frac{n}{s}\binom{n-1}{s-1}$

   From a choice of n people we will pick s with one of them special. This can be done by picking all s people (in $\binom{n}{s}$ ways) and then picking the special person from these (in s ways). Or by first picking the special person (in n ways) and then picking the rest (in $\binom{n-1}{s-1}$ ways).

   (b) $\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$

   This is just a generalisation of the previous one: From a choice of n people we will pick r with k of them special.

   (c) $\sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i} = \binom{2n}{n} = \sum_{i=0}^{n}\binom{n}{i}^2$

   Imagine picking n people from a choice of n men and n women. We can either pick i men and $n-i$ women (and sum) which gives the LHS. Or we can pick i men and then pick i women who won't be in the group which gives the RHS. In total we are picking n people from a choice of $2n$ which is the middle term.

   (d) $\binom{n}{s} = \frac{n}{n-s}\binom{n-1}{s}$

   We choose a group of s people from a choice of n and then a special person from the unselected people. We do this by choosing the s people (in $\binom{n}{s}$ ways) and then the extra person (in $n-s$ ways). Or by picking the extra person first (in n ways) and then the group (in $\binom{n-1}{s}$) ways.

   (e) $\binom{n}{0} + \binom{n}{2} + \cdots = \binom{n}{1} + \binom{n}{3} + \cdots$

   The LHS is the number of even subsets of n elements and the RHS is the number of odd subsets of n elements. A bijection between them can be given as follows. If an even subset contains the element 1 then remove it, if not add it.

   (f) $\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+r}{r} = \binom{n+r+1}{r}$

   The RHS is the number of ways to choose r objects from $n+r+1$ objects. The LHS is the number of ways to do this if we assume 1 is not in the choice, 1 is in but 2 isn't, $1, 2$ are in but 3 isn't, ...

2. *The following game is played on the integer points (x, y) in the plane with x,$y \geq 0$. Initially, pieces are placed at $(0, 0)$, $(1, 0)$ and $(0, 1)$. The following move is allowed: if the square above and to the right of a piece are empty they*

can be filled with pieces and the original piece removed. Is it possible for the initially occupied squares to all be simultaneously unoccupied?

To the point (a, b) assign the weight 2^{-a-b}. Initially the weighted sum of the occupied squares is 2. It is easy to see that the allowed move does not change the sum. If the initial squares are unoccupied then, in order to get the sum to be 2 we need to occupy all the other squares. This is clearly impossible in a finite number of moves.

3. *Show that there are either infinitely many composite numbers in the sequence* $2^{2^n}+1$ *or infinitely many composite numbers in* $6^{2^n}+1$ *(or both).*

Suppose that there are infinitely many primes in the $2^{2^n}+1$ sequence. We need to show that there are lots of composites in the other sequence. Let $p = 2^{2^n}+1$ be a prime. The **order** of an element m modulo p is the smallest power to which m can be raised to get 1 modulo p. In other words

$$m^{\mathrm{ord}(m)} \equiv 1 \bmod p$$

By Fermat's little theorem we can see that the order of an element must divide $p-1$. In our case this means that the order of 6 modulo p must be a power of 2, say 2^m. Thus

$$6^{2^m} \equiv 1 \bmod p \quad \text{but} \quad 6^{2^{m-1}} \not\equiv 1 \bmod p$$

Thus, $6^{2^{m-1}} \equiv -1 \bmod p$ and so $6^{2^{m-1}}+1$ is divisible by p (and clearly not equal to p) and hence is not a prime. For larger and larger n this gives an infinite number of composites in the $6^{2^m}+1$ sequence.

Quadratic Reciprocity. There is a slightly easier way to do this question which uses a very beautiful theorem of number theory. As it is both very pretty and very useful I'll explain the basics here.

The **Legendre symbol** $\left(\frac{a}{p}\right)$ for p a prime and $(a,p)=1$ is defined to be 1 if $x^2 \equiv a \bmod p$ has a solution and -1 if it doesn't. In other words, the Legendre symbol answers the questions "does a have a square root?". There are two very basic properties the symbol has:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \text{and} \quad \left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$$

Less obvious are the following two properties

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p \text{ (for odd } p), \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$$

And finally, the law of quadratic reciprocity (for 203 different proofs go to `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \bmod 4 \end{cases}$$

This law is remarkably useful because it allows you to see if something has a square root quite easily (repeatedly use quadratic reciprocity and the multiplicative property). For example, can you use it to show that if $p = 2^{2^n} + 1$ then 6 does not have a square root (for $n \geq 1$)? If you can then we know

$$6^{(p-1)/2} \equiv -1 \bmod p$$

And so we can finish as in the first method. Notice that this way we know the exact value of m whereas we didn't with the first method.

4. *Find a simple formula for the sum* $\sum_{k=1}^{n} \binom{n}{k} k^2$.

   This represents picking a committee from n people with 2 special posts (which can be filled by the same person). So, we should try to count this in a different way (which doesn't involve summing). If the two posts are filled by the same person we could choose this person (in n ways) and then pick the rest of the committee (in 2^{n-1} ways — a person is either in or out). If the two posts are filled by different people we could choose them (in $n(n-1)$ ways) and then pick the rest of the committee (in 2^{n-2} ways). Adding these gives the answer $n(n+1)2^{n-2}$.

5. *Let $f(n)$ be a function defined on the set of positive integers which takes values in the positive integers. Prove that if*

   $$f(n+1) > f(f(n))$$

   for each positive integer n then $f(n) = n$.

   f has a unique minimum at $n = 1$ because, if $n > 1$ then we have $f(n) > f(f(n-1))$. Once we know this, the same equation then shows that the second smallest value is $f(2)$. By induction we get

   $$f(1) < f(2) < f(3) < \cdots$$

   As f takes values in the positive integers we already have $f(n) \geq n$. Suppose we have a k such that $f(k) \geq k+1$. Then $f(f(k)) \geq f(k+1)$ which contradicts the assumed inequality for f. So $f(n) = n$ for all n.

6. *Show that $n^7 - 77$ is never a Fibonacci number.*

   We want to look at this modulo p for some well chosen p. Because of the exponent being 7 a good idea would be to have $\phi(p)$ divisible by 7, so $p = 29$ is perhaps a good choice. We also want the Fibonacci sequence to not take on too many values modulo p. This also happens for $p = 29$:

   $$0, 1, 1, 2, 3, 5, 8, 13, -8, 5, -3, 2, -1, 1, 0, \ldots$$

   Modulo 29 the seventh powers are just $0, \pm 1, \pm 12$. So the values that $n^7 - 77$ takes are $-7, -2, 9, 10, 11$. None of these are in the Fibonacci sequence so we are done.