Math Club Notes: 2005 August 29

Solutions to two more of the 2005 IMO problems.

1 Coprime numbers

The problem (paraphrased):

> Find all positive integers relatively prime to $2^n + 3^n + 6^n - 1$ for all positive integers n.

The only such integer is 1. In what follows, let the variables n and k have type "positive integer", and the variable p have type "prime".

Lemma 1 $(\forall p : (\exists n : p \mid 2^n + 3^n + 6^n - 1))$

Proof Note that $p \mid 2^n + 3^n + 6^n - 1$ is equivalent to

$$2^n + 3^n + 6^n - 1 = 0\,,$$

when the arithmetic is done in the field $\mathbb{Z}_p$. We consider three cases:

1. $p = 2$: Any n will do in this case; for, calculating in $\mathbb{Z}_2$,

$$2^n + 3^n + 6^n - 1 = 0^n + 1^n + 0^n - 1 = 0 + 1 + 0 - 1 = 0\,.$$

2. $p = 3$: Any even n will do in this case; for, calculating in $\mathbb{Z}_3$,

$$2^{2k} + 3^{2k} + 6^{2k} - 1 = (-1)^{2k} + 0^{2k} + 0^{2k} - 1 = 1 + 0 + 0 - 1 = 0\,.$$

3. $p > 3$: Take $n = p - 2$ (which is a positive integer because $p > 3$). Note that in this case, p does not divide 2, 3, or 6, so these are all invertible in $\mathbb{Z}_p$; thus, in that field,

$$\begin{aligned}
& 2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \\
= \quad & \{\text{laws of exponents}\} \\
& \frac{2^{p-1}}{2} + \frac{3^{p-1}}{3} + \frac{6^{p-1}}{6} - 1 \\
= \quad & \{\text{Fermat's (little) theorem}\} \\
& \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \\
= \quad & \{\text{arithmetic}\} \\
& 0
\end{aligned}$$

□

(The third case might seem a little fishy. What needs to be proved?)
The rest of the solution is pretty simple; in formal terms it might look like...

Theorem 2 The only solution to $k\colon (\forall n\colon k \perp 2^n + 3^n + 6^n - 1)$ is $k = 1$.

Proof For any k,

$$
\begin{aligned}
& (\forall n\colon k \perp 2^n + 3^n + 6^n - 1) \\
\equiv \quad & \{\text{number theory: numbers are coprime iff no prime divides both}\} \\
& (\forall n\colon \neg(\exists p\colon p \mid k \text{ and } p \mid 2^n + 3^n + 6^n - 1)) \\
\equiv \quad & \{\text{logic: De Morgan's law}\} \\
& \neg(\exists n\colon (\exists p\colon p \mid k \text{ and } p \mid 2^n + 3^n + 6^n - 1)) \\
\equiv \quad & \{\text{logic: } \exists \text{ commutes with itself}\} \\
& \neg(\exists p\colon (\exists n\colon p \mid k \text{ and } p \mid 2^n + 3^n + 6^n - 1)) \\
\equiv \quad & \{\text{logic: and distributes over } \exists\} \\
& \neg(\exists p\colon p \mid k \text{ and } (\exists n\colon p \mid 2^n + 3^n + 6^n - 1)) \\
\equiv \quad & \{\text{the lemma}\} \\
& \neg(\exists p\colon p \mid k \text{ and true}) \\
\equiv \quad & \{\text{logic: true is the identity of and}\} \\
& \neg(\exists p\colon p \mid k) \\
\equiv \quad & \{\text{number theory: in } \mathbb{Z}^+, \text{ only 1 has no prime divisors}\} \\
& k = 1
\end{aligned}
$$

□

2 An enumeration of the integers

The problem:

> We are given an infinite sequence of integers $a_1, a_2, \ldots$. The sequence contains infinitely many positive values and infinitely many negative values. For every positive integer n, the first n elements of the sequence leave n different remainders on division by n. Show that every integer occurs exactly once in the sequence.

I haven't been able to make the following solution formal in a satisfactory way (undoubtedly on account of my inexperience with formal methods), so I'll just give the argument in informal terms.

First, it's easy to see that no integer occurs more than once: if two elements were equal, they would leave the same remainder on division by any n, contrary to hypothesis.

Next, we recall that leaving different remainders on division by n is equivalent to not differing by a multiple of n. That is, any two elements among the first n do not differ by a multiple of n. In particular, they do not differ by n. Furthermore, if two elements are among the first n, then they are also among the first m for any $m \geq n$; so they do not differ by any $m \geq n$ either. Therefore any two elements among the first n differ by less than n. Now, among the first n elements there occur a minimum and a maximum; they differ by less than n. Let the minimum be m; then the maximum is at most $m + n - 1$, and the first n elements lie between m and $m + n - 1$, inclusive. There are exactly n integers in that range; since the first n elements are distinct, every integer in this range must occur as an element in the sequence. That is, the first n elements of the sequence form a range of consecutive integers (not necessarily in order).

Now, since there are infinitely many positive values in the sequence, it is unbounded above. For if it were bounded, say by B (where wlog $B \geq 0$), the sequence could contain only finitely many positive values, namely $1, 2, \ldots, B$, each of which occurs at most once. Similarly, the sequence is unbounded below.

So, for any integer k, the sequence contains elements less than k and elements greater than k. Take n large enough to include such elements; then, since the first n elements of the sequence form a range of consecutive integers, which by construction spans k, we conclude that k occurs among the first n elements. That is, every integer occurs in the sequence at least once.