Solution

Week 80 (3/22/04)

Nine divisible by 9

First, consider the following simpler problem:

Problem: Given any five integers, show that there is at least one subset of three integers whose sum is divisible by 3.

Solution: Let us try to find a set of five integers that contains no subset of three integers whose sum is divisible by 3, a task that we will show is impossible. Each of the five integers is, for our purposes, equal to 0, 1, or 2, because we are concerned only with divisions by 3. We cannot have one of each of these, because $0+1+2$ is divisible by 3. We must therefore have at most two of the types. But the pigeonhole principle then implies that we have at least three of one of the types. The sum of these three integers is divisible by 3. ■

Returning to the original problem, pick five integers to obtain a triplet whose sum is divisible by 3. Then pick another five integers to obtain another such triplet. We can continue to do this for a total of five times, given the seventeen integers.

We now have five triplets, each of whose sum is divisible by 3. As far as divisions by 9 are concerned, these sums are equal to 0, 3, or 6. We can now use the same reasoning as in our auxiliary problem above (but with everything scaled up by a factor of 3) to show that we can find a set of three triplets that has a sum divisible by 9. In other words, we have found a set of nine integers whose sum is divisible by 9.

This result is a special case of the following theorem.

Theorem: Given any $2n-1$ integers, there is at least one subset of n integers whose sum is divisible by n.

We will prove this theorem by demonstrating two lemmas.

Lemma 1: If the theorem is true for integers n_1 and n_2, then it is also true for the product n_1n_2.

Proof: Consider a set of $2n_1n_2-1$ integers. Under the assumption that the theorem is true for n_1, we can certainly pick a subset of n_1 integers whose sum is divisible by n_1. From the remaining $2n_1n_2-1-n_1$ integers we can pick another such subset of n_1 integers, and so on. We can continue to do this until we have obtained $2n_2-1$ such subsets. This is true because after forming $2n_2-2$ such subsets, there are $[2n_1n_2-1]-[(2n_2-2)n_1] = 2n_1-1$ integers left over, from which we can pick one last such subset of n_1 integers.

Now consider these $2n_2-1$ sums divided by n_1. Assuming that the theorem holds for n_2, we can find n_2 of these sums (divided by n_1) that have a sum divisible by n_2. Bringing back in the factor of n_1, we see that we have found a set of n_1n_2 integers whose sum is divisible by n_1n_2. ■

In proving the general theorem, this first lemma shows that it is sufficient to prove the theorem for primes, p:

Lemma 2: If p is prime, then given $2p-1$ integers, there is at least one subset of p integers whose sum is divisible by p.

Proof: Consider all the possible $N \equiv \binom{2p-1}{p}$ subsets of p integers. Label the sums of these subsets as S_j, where $1 \le j \le N$ (these may be indexed in an arbitrary manner), and consider the sum

$$S = \sum_{j=1}^{N} S_j^{(p-1)}. \tag{1}$$

Remark: The following proof isn't mine (I'm not sure where it came from originally). At first glance, it might seem that adding up these $(p-1)$st powers is a little out of the blue, but it's actually a fairly reasonable thing to do. There are two types of sums: "good" ones that are divisible by p, and "bad" ones that aren't. It would be nice to label them all in a sort of binary way, say, with a "0" for good, and a "1" for bad. Fermat's Little Theorem (which states that if $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1 \pmod{p}$) provides the perfect way for doing this.

We will prove this second lemma by demonstrating two claims:

Claim 1: S is be divisible by p.

Proof: Let the $2p-1$ integers be a_i, where $1 \le i \le 2p-1$. Expand all of the $S_j^{(p-1)}$ powers and collect all the like terms in S. The terms will have the form of some coefficient times $a_{i_1}^{b_1} a_{i_2}^{b_2} \cdots a_{i_k}^{b_k}$. The number, k, of different a_i's involved may be any number from 1 to $p-1$, and the b_j's must of course add up to $(p-1)$.

We will now show that the coefficient of an arbitrary $a_{i_1}^{b_1} a_{i_2}^{b_2} \cdots a_{i_k}^{b_k}$ term is divisible by p. The coefficient will depend on the b_i, but it will happen to always be divisible by p. The coefficient may be viewed as the product of two factors.

- Firstly, there is a multinomial coefficient from each $S_j^{(p-1)}$ in which the given $a_{i_1}^{b_1} a_{i_2}^{b_2} \cdots a_{i_k}^{b_k}$ occurs. This multinomial coefficient is $\binom{p-1}{b_1, b_2, \ldots, b_k}$, but it will turn out not to be important.
- Secondly, we must count the number of different $S_j^{(p-1)}$ in which the given $a_{i_1}^{b_1} a_{i_2}^{b_2} \cdots a_{i_k}^{b_k}$ occurs. This number may be found as follows. We know that k of the p integers in S_j must be $a_1, a_2, \ldots, a_k$. The remaining $p-k$ integers can be any subset of the other $2p-1-k$ integers. There are $\binom{2p-1-k}{p-k}$ such subsets.

The coefficient of the $a_{i_1}^{b_1} a_{i_2}^{b_2} \cdots a_{i_k}^{b_k}$ term in S is therefore $\binom{p-1}{b_1, b_2, \ldots, b_k}\binom{2p-1-k}{p-k}$. Writing the second factor in this as

$$\binom{2p-1-k}{p-k} = \frac{(2p-1-k)(2p-2-k)\cdots p}{(p-k)!} \tag{2}$$

demonstrates that every coefficient is divisible by p, independent of the values of the b_i. Therefore, S is divisible by p. Q.E.D.

Claim 2: If none of the S_j are divisible by p, then S is not divisible by p.

Proof: Assume that none of the S_j are divisible by p. Then by Fermat's Little Theorem (which states that if $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1 \pmod{p}$), we have

$$S \equiv \left(\sum_{i=1}^{N} 1\right) \pmod{p} \equiv N \pmod{p}. \tag{3}$$

We now note that

$$N \equiv \binom{2p-1}{p} = \frac{(2p-1)(2p-2)\cdots(p+1)}{(p-1)!}\,, \tag{4}$$

which is not divisible by p. Therefore, S is not divisible by p. Q.E.D.

These two claims show that at least one of the S_j must be divisible by p. ■

Remark: For the case where n is a prime number, p, it is possible to say a bit more about exactly how many of the S_j are divisible by p. We claim that either 1, $p+1$, $2p+1$, …, of the S_j are divisible by p. The reasoning is as follows.

Fermat's Little Theorem implies that each S_j that is not divisible by p contributes 1 to S, while each S_j that is divisible by p contributes 0 to S. Under the (incorrect) assumption that none of the S_j are divisible by p, eq. (3) states that $S \equiv N \pmod{p}$. Using eq. (4), and noting that

$$(2p-1)(2p-2)\cdots(p+1) \equiv (p-1)! \pmod{p}, \tag{5}$$

we see that this assumption leads to the incorrect conclusion that $S \equiv 1 \pmod{p}$. But since we know from eq. (2) that S must actually be divisible by p, then either 1, $p+1$, $2p+1$, …, of the S_j must be divisible by p, because each S_j that is divisible by p will contribute 0, instead of 1, to S. Thus, for example, given five integers, there are either one, four, seven, or ten subsets of three integers whose sum is divisible by 3.

It is easy to construct a case where only one of the S_j is divisible by p. We may pick $p-1$ of the $2p-1$ integers to be congruent to each other modulo p, and then pick the remaining p integers to also be congruent to each other (but not to the other $p-1$ integers) modulo p. Then the subset consisting of these latter p integers is the only subset of p integers whose sum is divisible by p.