Math 189H Joy of Numbers Activity Log

Thursday, October 6, 2011

Herbert Wilf: "Induction makes you feel guilty for getting something out of nothing, and it is artificial, but it is one of the greatest ideas of civilization."

Warren Buffett: "The only time to buy these [stocks] is on a day with no 'y' in it"

We started by finishing our demonstration that $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$, by showing that $\Sigma = (1 + 2 + \cdots + n) = \frac{1}{2}(n^2 + n)$. We agreed that we could surely prove this by induction (and you were invited to do this for yourself!), but your instructor, being a lazy mathematician, pointed out that we could recover this fact from one of our previous ones: since $1 + 3 + \cdots + (2n-1) = n^2$ and we can go from our sum to this one by multiplying every term by 2 and subtracting 1 (from every term), in essence multiplying Σ by 2 and subtracting (n 1's, or) n, we can see that $2\Sigma - n = n^2$, so $2\Sigma = n^2 + n$ and $\Sigma = \frac{1}{2}(n^2 + n)$. So our inductive step is finished, and

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2 = \left(\frac{n(n+1)}{2}\right)^2 .$$

We decided to try our hands at one more of these: if we add together the odd squares, what do we get?

$1^2 = 1$
$1^2 + 3^2 = 1 + 9 = 10$
$1^2 + 3^2 + 5^2 = 10 + 25 = 35$
$1^2 + 3^2 + 5^2 + 7^2 = 35 + 49 = 84$
$1^2 + 3^2 + 5^2 + 7^2 + 9^2 = 84 + 81 = 165$
$1^2 + 3^2 + 5^2 + 7^2 + 9^2 + 11^2 = 165 + 121 = 286$
$1^2 + 3^2 + 5^2 + 7^2 + 9^2 + 11^2 + 13^2 = 286 + 169 = 455$
$1^2 + 3^2 + 5^2 + 7^2 + 9^2 + 11^2 + 13^2 + 15^2 = 455 + 225 = 680$
$1^2 + 3^2 + 5^2 + 7^2 + 9^2 + 11^2 + 13^2 + 15^2 + 17^2 = 680 + 289 = 969$
$1^2 + 3^2 + 5^2 + 7^2 + 9^2 + 11^2 + 13^2 + 15^2 + 17^2 + 19^2 = 969 + 361 = 1330$

What is the pattern in these sums? Initially, we had a hard time finding any. They do alternate even and odd, so every other number is divisible by 2. This eventually led us to start factoring the sums, after which we found:

sum through 1^2: 1
sum through 3^2: $2 \cdot 5$
sum through 5^2: $5 \cdot 7$
sum through 7^2: $2 \cdot 2 \cdot 3 \cdot 7$
sum through 9^2: $3 \cdot 5 \cdot 11$
sum through 11^2: $2 \cdot 11 \cdot 13$
sum through 13^2: $5 \cdot 7 \cdot 13$
sum through 15^2: $2 \cdot 2 \cdot 2 \cdot 5 \cdot 17$
sum through 17^2: $3 \cdot 17 \cdot 19$
sum through 19^2: $2 \cdot 5 \cdot 7 \cdot 19$

Staring at these for awhile, a kind of pattern did emerge! Most of the time, the sum through $2n-1$ was divisible by $2n-1$. In fact this was always true <u>except</u> when $2n-1$ was a multiple of 3. In those cases, though, the sum was divisible by $(1/3)(2n-1)$. More than that, the same was true for the previous sum! Or put a little differently, the sum through $(2n-1)$, when multiplied by 3, is a multiple of both $2n-1$ <u>and</u> $2n+1$. So, calling $1^2+3^2+\cdots+(2n-1)^2=\Sigma_n$, we conjectured that $3\Sigma_n=(2n-1)(2n+1)(\text{something})$. To figure out what the something is, we computed $3\Sigma_n/[(2n-1)(2n+1)]$ for $n=1$ through 6, and found that the answers were $1,2,3,4,5$ and 6 (!). So we conjectured:

$$1^2+3^2+\cdots+(2n-1)^2=\frac{1}{3}n(2n-1)(2n+1)$$

Once we had hit upon the right formula, it was all over but the shouting; verifying that this is true for $n=1$, and assuming that $\Sigma_n=1^2+3^2+\cdots+(2n-1)^2=\frac{1}{3}n(2n-1)(2n+1)$, showing that the same is true for Σ_{n+1} amounts to showing that

$$\left[\frac{1}{3}n(2n-1)(2n+1)\right]+(2n+1)^2=\frac{1}{3}(n+1)(2n+1)(2n+3)$$

which, dividing everything by $2n+1$ and multiplying by 3 amounts to showing that $n(2n-1)+3(2n+1)=(n+1)(2n+3)$. Since the lefthand side of this is $2n^2+5n+3$ and $253=11\cdot 23$ (i.e., $2\cdot 10^2+5\cdot 10+3=(1\cdot 10+1)(2\cdot 10+3)$, one is led to suspect that $2n^2+5n+3$ factors as $(n+1)(2n+3)$, which it does!, and which is the result we want. This proves our inductive step; together with our initial step, PMI implies that our formula is true for all $n\geq 1$.

Mathematical induction is so useful throughout mathematics that many different versions, all amounting to the same thing, have been devised: one may be more pertinent to a particular problem than another, though. There is *complete induction*, where we show that $Q(n_0)$ is true and show that <u>if</u> $Q(k)$ is true for <u>all</u> $n_0\leq k<n$, <u>then</u> $Q(n)$ is true [i.e., we assume 'complete' knowledge of the truth of Q for every number below n in order to prove it true for n]; then we can conclude that $Q(n)$ is true for all $n\geq n_0$. There is also *reductio ad absurdum* ('reduce to absurdity'), where you show the $Q(n)$ is always true by supposing that there is some value n where $Q(n)$ is <u>false</u>; then by the Archimedean principle there is a smallest n where $Q(n)$ is false. Reductio ad absurdum proceeds by showing that whenever $Q(n)$ is false, there is a still smaller $m<n$ where $Q(m)$ is false. This violates the Archimdean principle, so there cannot be an n for which $Q(n)$ is false, so $Q(n)$ is always true!

As an example of a use for complete induction, we worked out a proof of something that we have implicitly used more than once already: every integer $n\geq 2$ can be written as a product of primes. Our base case is $n=2$, which is prime (and so a product of one prime(s)!). Assuming that every integer less than n can be written as a product of primes, now consider the integer n. If n is prime, we are done (it is a product of one prime(s)). Otherwise, n is composite, so $n=ab$ for some integers $a,b>1$. But then, as we learned before, a and b are both <u>smaller</u> than n, so by our (complete) induction hypothesis, we can write $a=p_1\cdots p_s$ and $b=q_1\cdots q_t$ [which reminded your instructor of the phrase 'on the qt' (meaning 'secretly'); 'qt', it turns out, stands for 'quiet' (thank you, Google)], where p_i and q_j are all prime. Then $n=ab=p_1\cdots p_s q_1\cdots q_t$, which is a product of primes. So our (complete) inductive step is proved, and so, by complete induction, our proposition is proved:

Every integer $n \geq 2$ can be written as a product of primes.

From this, we can establish an old result of Euclid:

There are infinitely many distinct prime numbers.

Put differently, given any number N, there is a prime number $p > N$. The key to showing that there is an infinite number of anything is to show that if you try to start listing them your list will never end. And one typically does this by supposing that your list does end (and proving that you were wrong!). [Attempts to turn this into a reductio ad absurdum argument didn't go very well...]

So we supposed that $p_1 < p_2 < \cdots < p_k$ was a list of all of the primes that there are. We want to prove that we are wrong! To do this, we hit upon the idea of building a number that is divisible by every prime in this list, since then if we add 1, the resulting number will not be divisible by any of them. The 'standard' way this is usually done is to take their product, $N = p_1 \cdots p_k$; this is divisible by all of the primes p_i, so $N+1$ isn't divisible by any of them. In the spirit of 'Name That Tune', we went for the version needing the fewest symbols; since we had been clever enough to list our primes in order, it turns out that $N = p_k!$ is divisible by every prime p_i, so $N + 1 = p_k! + 1$ leaves remainder 1 on division by each prime p_i, and so none of them are a factor of $N + 1$. But N has a prime factor (since it is a product of primes), and it cannot be on our list. So our list is not complete; there must be still more primes. So the list of primes cannot end; there are an infinite number of them.