Math 189H Joy of Numbers Activity Log

Thursday, October 13, 2011

(Douglas) Hofstadter's Law: "It always takes longer than you expect, even when you take into account Hofstadter's Law."

Albert Einstein: "Since the mathematicians have invaded the theory of relativity, I do not understand it myself anymore."

Every integer $n > 128$ can be written as a sum of distinct perfect squares: $n = a_1^2 + \cdots + a_k^2$ with $0 < a_1 < \cdots < a_k$. (Le Lionnais)

At the end of last time we had formulated a statement to the effect that factorizations of numbers into primes are essentially unique:

If $N = p_1 \cdots p_n$ and $N = q_1 \cdots q_m$ with $p_1 \leq p_2 \leq \ldots \leq p_n$ and $q_1 \leq q_2 \leq \ldots \leq q_m$, and all p_i, q_j prime, <u>then</u> $n = m$ and $p_i = q_i$ for <u>every</u> i .

Our idea came down to showing that p_1 must equal one of the primes in the list $q_1, \ldots q_m$. Then we could cross both numbers off of their list, effectively giving us two prime factorizations of the number N/p_1, which is smaller than N. Meaning that, by an inductive hypothesis, both of the lists for N/p_1 are the same (up to re-ordering the primes in the list). So our original lists for N were also the same!

And the fact that p_1 appears in the list of the q_j's we thought, in the end, we could establish by induction! The question was, how does knowing that p_1 is prime help us? And what exactly would the induction do? The thing that we could imagine changing was the number of prime factors in $N = q_1 \cdots q_m$. Making this shorter amounts to setting aside one of the prime factors, as $N = q_1(q_2 \cdots q_m)$. Which gets us started: p_1 being a prime factor of N means that $p_1 | N$, so $p_1 | q_1(q_2 \cdots q_m) = q_1 R$. So, in essence, we have $p | qR$ with p and q prime. If we think about p and q (with divisibility on our minds), we came to realize that there were only two possibilities: either p and q are the same or they are different! Put a bit differently, either $p = q$ or the only common factor of p and q is 1, i.e., $\gcd(p, q) = 1$. [In keeping with common usage, especially for any outside reading you might do for your group project, we introduced the commonly-used notation of (p, q) for the gcd of p and q. And then tried to avoid using it...] And what our inductively-phrased claim asserts, really, is that if p is prime, $p|N$ and $N = qR$ with p and q prime, then either $p = q$ or $p|R$ (and then our inductive assumption will allow us to identify p with one of the primes in a prime factorization of R).

But since q is prime, we realized that $p = q$ is the same as $p|q$, so we could rephrase our assertion as: if $p|N$ and $N = qR$, then either $p|q$ or $p|R$ (with the added assumption that q is prime...). And the point to having p prime, we saw, was that the only common factors that p and q can have are either p or 1 (since p is prime), and $\gcd(p, q) = p$ really means that $p|q$. What we will employ now is what is usually called *proof by contradiction*; it is a time-honored technique for getting extra information to help us reach our conclusion. We suppose that something we would like to be true is <u>false</u>, in the hopes of getting ourselves into trouble. In this case, we will suppose that p does not divide q; since p is prime this implies that p and q are relatively prime. We then use this extra information to find a way to show that p must in fact divide R. [A more 'traditional' proof by contradiction would 'deny' our entire conclusion, i.e., assert that p does not divide q and p does not divide R, and then get ourselves into trouble. For fun, you might try adapting the argument we eventually came up with, below, to show that these two assertions imply that p divides 1!]

How do we use that p and q are relatively prime? This means that their gcd is 1, and we eventually remembered that this meant that we can write 1 as a combination of p and q: $1 = px + qy$ for some integers x and y. So what we have then is that $N = pd$, $N = qR$ and (if we assume that p does not divide q) we have $1 = px + qy$. And what we want to show is that p must divide R.

So we started kicking things around! $1 = px+qy$ means that $qy = 1-px$, so $q = (1-px)/y$, so $R = N/q = pd/q = pdy/(1-px)$ is a multiple of p provided that $dy/(1-px)$ is an integer, meaning that $(1-px)|dy$. That sounds challenging to establish... $N = pd = qR$, so $R = pd/q = p(d/q)$, so $p|R$ so long as d/q is an integer, meaning that $q|d$. And, no, we don't know how to do that, either. Hm, and that didn't even try to use the fact that $1 = px + qy$.

Somewhere in here we also tried to see if a specific example might help us find a pattern we could exploit. Taking the number $N = 2^3 \cdot 3^2 \cdot 7 \cdot 23 \cdot 149$, whatever it is, and noting that we could write $N = 3R$ and $7|N$, we wanted to figure out that $7|R$ using only the fact that we could write 1 as a combination of 3 and 7 (which, we discovered, we could do in many ways!, as $4 \cdot 7 - 9 \cdot 3$, $1 \cdot 7 - 2 \cdot 3$, and $26 \cdot 3 - 11 \cdot 7$ for starters, settling on $1 \cdot 7 - 2 \cdot 3$ as being the simplest).We quickly decided, though, that this wasn't going to help much, and quietly stopped thinking in terms of specific numbers...

Eventually, though, we realized that our earlier experiences with gcds - and $p|R$ is really the same as $\gcd(p, R) = p$ - showed us that adding and subtracting multiples of p will not change the fact that the gcd is (or rather, will turn out to be) p. And $1 = px + qy$, written as $1 - px = qy$, sort of shows us that multiples of q have mutiples of p in them that we can ignore. The goal them becomes how to build multiples of q that have more multiples of p in them to ignore... And this is precisely what $pd = N = qR$ tells us: R q's have p's in them for us to ignore. From there it was a short walk to the realization that taking $1 = px + qy$ and multiplying the q by R, to create multiples of p, led us to (since we can't really control what happens when we multiply one term by R, we need to multiply all of the terms by R)

$$R = R \cdot 1 = R \cdot (px + qy) = Rpx + Rqy = p(Rx) + (qR)y = p(Rx) + (pd)y = p(Rx + dy)$$

is a multiple of p (!). Which is precisely what we wanted. So we have shown that:

If p is prime, $p|qR$, and $p \not| q$, then $p|R$.

Or, cast in a more positive light:

If p is prime and $p|qR$, then either $p|q$ or $p|R$

since if it doesn't divide the first factor, q, then it must divide the second factor, R. From this we can put together our inductive argument about uniqueness of factorizations: suppose that p is prime, $p|N = q_1 \cdots q_m$, but p does not appear in the list of the primes

q_i. We get ourselves into trouble by noting that $p \neq q_1$ means that $\gcd(p, q_1) = 1$, and so $p | q_2 \cdots q_m$. But this product is shorter! So, turning this around, if we construct a statement $Q(m)$ which says "In any product of m primes $N = q_1 \cdots q_m$ if $p|N$ then p equals one of the primes q_i", then we have essentially proved the inductive step: with $N = q_1 \cdots q_m$, if $p \neq q_1$, then $p | q_2 \cdots q_m$ and so, by the inductive hypothesis, p equals one of the remaining primes. Together with the initial step ("If $N = q_1$ and $p|N$ then $p = q_1$", which is true, because $N = q_1$ is prime, and the only prime that is divisible by the prime p is, well, p (!), so $p = q_1$) yields our result: if $p|N = q_1 \cdots q_n$ with the q_i all prime, then p equals one of the q_i. Our original inductive argument (divide by p and look again!) then shows that, except for reordering the terms, the factorization of N into primes can be done in only one way.

In the end, it is gratifying to be able to show that prime factorizations are unique; but the result that we learned along the way, that if a prime number p divides a product of two numbers then it must divide one of the two factors, will in the long run be far more helpful! It will take us a long way toward establishing the truth in general of the observation we keep making, about powers of a number modulo a prime.