Math 189H Joy of Numbers Activity Log

Tuesday, October 11, 2011

Hugo Rossi: "In the fall of 1972 President Nixon announced that the rate of increase of inflation was decreasing. This was the first time a sitting president used the third derivative to advance his case for re-election."

Thomas Edison: "I have not failed. I've just found 10,000 ways that won't work."

The only Fibonacci numbers that are perfect squares are 1 and 144.

We started by looking for some more patterns that we could try to prove using induction. Picking some numbers more or less at random (and then shrinking a few once we realized that Maple 15 wasn't going to fare very well at factoring the resulting numbers), we looked at the numbers $A_n = 27 \cdot 3^n + 59 \cdot 7^n$ and their factorizations (courtesy of Maple):

$n = 1, A_n = 494 = 2 \cdot 13 \cdot 19$
$n = 2, A_n = 3134 = 2 \cdot 1567$
$n = 3, A_n = 20966 = 2 \cdot 11 \cdot 953$
$n = 4, A_n = 143846 = 2 \cdot 71 \cdot 1013$
$n = 5, A_n = 998174 = 2 \cdot 389 \cdot 1283$
$n = 6, A_n = 6960974 = 2 \cdot 3480487$
$n = 7, A_n = 48648086 = 2 \cdot 12959 \cdot 1877$
$n = 8, A_n = 340300406 = 2 \cdot 911 \cdot 186773$
$n = 9, A_n = 2381394254 = 2 \cdot 223 \cdot 1063 \cdot 5023$
$n = 10, A_n = 16667634014 = 2 \cdot 193 \cdot 1999 \cdot 21601$
$n = 11, A_n = 116667060806 = 2 \cdot 58333530403$
$n = 12, A_n = 816650293766 = 2 \cdot 15998321 \cdot 25523$
$n = 13, A_n = 5716494660734 = 2 \cdot 11 \cdot 13 \cdot 787 \cdot 7793 \cdot 3259$
$n = 14, A_n = 40015290438254 = 2 \cdot 20007645219127$
$n = 15, A_n = 280106516507126 = 2 \cdot 23 \cdot 53 \cdot 269 \cdot 427107533$
$n = 16, A_n = 1960744065867926 = 2 \cdot 980372032933963$
$n = 17, A_n = 13725203812029614 = 2 \cdot 6862601906014807$
$n = 18, A_n = 96076412737069694 = 2 \cdot 71 \cdot 173 \cdot 118337941 \cdot 33049$
$n = 19, A_n = 672534847318075046 = 2 \cdot 19 \cdot 139 \cdot 199 \cdot 273314017 \cdot 2341$
$n = 20, A_n = 4707743805702286886 = 2 \cdot 5449 \cdot 8093 \cdot 135431 \cdot 394129$
$n = 21, A_n = 32954206263343292894 = 2 \cdot 43 \cdot 251 \cdot 1526647190926679$
$n = 22, A_n = 230679442713684904334 = 2 \cdot 1505131361418257 \cdot 76631$
$n = 23, A_n = 1614756095606639892566 = 2 \cdot 11 \cdot 1117231681 \cdot 65696314913$
$n = 24, A_n = 11303292659079015934646 = 2 \cdot 5651646329539507967323$
$n = 25, A_n = 79123048583050721602574 = 2 \cdot 13 \cdot 409 \cdot 7440572558120248411$
$n = 26, A_n = 553861339989847881398174 = 2 \cdot 773 \cdot 7182910580359 \cdot 49875941$
$n = 27, A_n = 3877029379654413660327686 = 2 \cdot 1309921398437571133 \cdot 1479871$
$n = 28, A_n = 27139205656757331093915206 = 2 \cdot 13697937829 \cdot 990631071463207$
$n = 29, A_n = 189974439594830624072270654 = 2 \cdot 34492586951327683 \cdot 74717 \cdot 36857$
$n = 30, A_n = 1329821077156402287750487214 = 2 \cdot 67 \cdot 577 \cdot 17199372425003262988573$
$n = 31, A_n = 9308747540072579771987188406 = 2 \cdot 6033691043 \cdot 771397431003046121$

$n = 32, A_n = 6516123278044134967711652566 = 2 \cdot 71 \cdot 45888192098902358927543 4173$
$n = 33, A_n = 2 \cdot 11 \cdot 151 \cdot 317 \cdot 4331401491850423821 68191$
$n = 34, A_n = 2 \cdot 1620559043 \cdot 493301519231830537 \cdot 1997$
$n = 35, A_n = 2 \cdot 1073147985038338615182 4141 \cdot 1041343$
$n = 36, A_n = 2 \cdot 1201 \cdot 6513410487332373330146 3529763$
$n = 37, A_n = 2 \cdot 13 \cdot 19^2 \cdot 23^2 \cdot 19682785284732653 \cdot 281923 \cdot 39749$
$n = 38, A_n = 2 \cdot 11230814350102980749940717 50219 \cdot 3413$
$n = 39, A_n = 2 \cdot 137 \cdot 16565912325343 \cdot 11822508933100111853$
$n = 40, A_n = 2 \cdot 784875762418790178469937 45873651 \cdot 2393$
$n = 41, A_n = 2 \cdot 919 \cdot 585479946493475727234 9101263 \cdot 244351$
$n = 42, A_n = 2 \cdot 43 \cdot 617223422227463 \cdot 346759879055344599563$
$n = 43, A_n = 2 \cdot 11 \cdot 229 \cdot 281 \cdot 15884941 \cdot 6903276176602709 0861 \cdot 82997$
$n = 44, A_n = 2 \cdot 1619 \cdot 1663 \cdot 150799577 \cdot 1110699446167970961936967$
$n = 45, A_n = 2 \cdot 131927613379 \cdot 154318580600649732647 \cdot 155052899$

Looking at the prime factors, we could recognize several patterns. First, we noted that every one is even! But we realized that this follows from the fact that our A_n's are the sum of two odd numbers, since the product of a bunch of odd numbers is odd (which we could establish for an arbirarily long product, by induction!). Other patterns that we found were that it appears that:

$13 | A_n$ for $n = 13, 25, 37$, which we conjectured meant whenever $n = 12k + 1$, i.e., $n \equiv 1 \mod 12$.

$11 | A_n$ for $n = 3, 13, 23, 33, 43$, which we conjectured meant whenever $n = 10k + 3$, i.e., $n \equiv 3 \mod 10$.

$71 | A_n$ for $n = 18, 32$, and (we checked!) 46 and 60, which we conjectured meant whenever $n \equiv 4 \mod 14$.

and still more could be extracted from the list, if we kept looking. [Look, for example, for multiples of 43, or note what is missing: 37, for example, never appears as a factor.] We then verified one of these by induction! To show that $13 | A_n$ when $n \equiv 1 \mod 12$, for example, what we want to show is that $27 \cdot 3^{12k+1} + 59 \cdot 7^{12k+1}$ is always a multiple of 13, for any $k \geq 0$ (or wherever we decide to start...). The list above establishes the base case $k = 0$, and to show the inductive case, we can, in fact, adopt a reductio ad absurdum approach, by showing that $27 \cdot 3^{12(k+1)+1} + 59 \cdot 7^{12(k+1)+1}$ and $27 \cdot 3^{12k+1} + 59 \cdot 7^{12k+1}$ leave the exact same remainder on division by 13. [The idea here is that we are showing that if $27 \cdot 3^{12k+1} + 59 \cdot 7^{12k+1}$ is not a multiple of 13, then the same is true for some smaller value of k...] But saying that the two numbers have the same remainder is the same as saying that their difference is a multiple of 13. Actually, even more is true:

$27 \cdot 3^{n+12} + 59 \cdot 7^{n+12} \equiv 27 \cdot 3^n + 59 \cdot 7^n \mod 13$, for all values of n .

(We came across this insight by asking Maple to list the values of A_n mod 13 for a large range of n, and noticing that the pattern of remainders repeated itself.) This fact we could demonstrate by showing that

$(27 \cdot 3^{n+12} + 59 \cdot 7^{n+12}) - (27 \cdot 3^n + 59 \cdot 7^n) = 27 \cdot 3^n(3^{12} - 1) + 59 \cdot 7^n(7^{12} - 1)$

and realizing that this number is a multiple of 13 provided $3^{12}-1$ and $7^{12}-1$ are both multiples of 13. Which, we found by asking a calculator, they are! This actually proved even more, once we looked closer: since A_n and A_{n+12} are congruent, modulo 13, we can repeatedly subtract 12 from the subscript without changing whether or not the number is a multiple of 13, allowing us, in a reductio ad absurdum kind of way, to determine precisely which numbers A_n are a muliple of 13 by looking only at A_1 through A_{12}. Since only A_1 is a multiple of 13, the multiples of 13 are precisely the numbers A_{12k+1} (!). In fact, this line of reasoning confirms our experimental observation that the remainders, on division by 13, of the A_n repeat themselves every 12 times. A similar liine of reasoning (using the fact that $3^{10} \equiv 1$ and $7^{10} \equiv 1 \bmod 11$) will establish that $11|A_n$ precisely when $n \equiv 3 \bmod 10$, as our observations had indicated.

The facts that we used in these proofs - that $3^{12} \equiv 1$ and $7^{12} \equiv 1 \bmod 13$, and $3^{10} \equiv 1$ and $7^{10} \equiv 1 \bmod 11$ - sounded strangely familiar to our ears. These are the same kinds of observations we were using in finding tests for divisibility by 13 and 11. It wold appear that our conjecture, that if p is a prime not dividing 10 then $10^{p-1} \equiv 1 \bmod p$, might hold in even greater generality! and in fact, maybe the remainders, on division by p, of higher and higher powers always cycle around? We tested this by randomly trying $B_n = 18 \cdot 22^n + 11 \cdot 7^n$, looking at these numbers modulo 149; to the limits of our observations (to around $n = 600$) it did appear to repeat itself every 148 values!

Before we can make a stab at verifying this kind of pattern, we need to back up (again) to develop some more useful tools. Induction proved to be the needed tool to show that every integer $n \geq 2$ can be expressed as a product of primes. One thing we didn't address at that time (probably because we are used to thinking that it is true!) is: can a number be written as a product of primes in more than one way? After thinking about it, we concluded that the answer is 'yes', at least in a minor way: if it is the product of more than one prime, we can write the prime factors in a different order. But we couldn't see any other way that might work, and ended up conjecturing that, except for the order in which we write them, the factors of two different prime factorizations of the same number n should all be the same. One way to impose a 'canonical' order on factors is to list them in increasing order (which (look at our list above, cut directly out of Maple) Maple apparently does not do!). This led us to conjecsture:

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, then $n = m$ and $p_i = q_i$ for every i .

The question is, how to prove this?! The answer which immediately occured to us was 'By induction!', and in the course of thinking about it we decided that if we could show that $p_1 = q_1$, then we could remove them from each list, ending up with prime factorizations of a smaller number $M = N/p_1$; then an inductive argument would allow us to conclude that the remaining prime factors are all the same! We will pursue this line of reasoning next time.