Math 189H Joy of Numbers Activity Log

Tuesday, November 1, 2011

Werner Heisenberg: "An expert is someone who knows some of the worst mistakes that can be made in his/her subject, and how to avoid them."

Isaac Newton was a member of the British parliament. In all of their official records, he is recorded as speaking in chambers exactly once, to ask that a window be closed.

$n = 4,700,063,497$ is the smallest number so that $2^n \underset{n}{\equiv} 3$.

Class started with a question about induction, so we illustrated the ideas that go into an inductive proof with a specific example. Picking all (but one!) of the numbers at random, we looked at the sequence of integers $a_n = 11\cdot 12^n + 18\cdot 41^n$. For $n = 0$, this is 29; for $n = 1$ it is $11 \cdot 12 + 18 \cdot 41 = 870 = 29 \cdot 30$. In fact, every a_n is a multiple of 29, something that we can prove by induction! Either of the two computations above can serve as our base case, and to establish the result by induction, we also need to prove the *inductive step*: if $29|a_n$ (and $n \geq 1$) then it follows that $29|a_{n+1}$. The whole idea is that from the base case a_1, the inductive step assures us that $29|a_2$, and then the inductive step again shows that $29|a_3$, which implies $29|a_4$, and there is nothing to stop this process from continuing; the inductive step always allows us to move to the next number in sequence and know that it is a multiple of 29. This means, though, that the <u>only</u> thing we are allowed to use, in showing that $29|a_{n+1}$ is that ($n \geq 1$: we are only looking to the 'right' of 1, and) $29|a_n$. So we suppose that $a_n = 11 \cdot 12^n + 18 \cdot 41^n = 29K$ for some integer K, and look at $a_{n+1} = 11 \cdot 12^{n+1} + 18 \cdot 41^{n+1}$. A very useful principle for inductive arguments is to 'look for' the thing that the inductive hypothesis tells you that you know something about 'inside' of the thing that you are trying to understand; in this case $11 \cdot 12^{n+1} + 18 \cdot 41^{n+1}$ 'contains' both $11 \cdot 12^n$ (inside of $11 \cdot 12^{n+1} = (11 \cdot 12^n) \cdot 12$) and $18 \cdot 41^n$ (inside of $18 \cdot 41^{n+1} = (18 \cdot 41^n) \cdot 41$), but it contains different multiples of each! But in any event, it contains 12 of each of them, and considering what we are after (to show that something is a multiple of 29), we can, as we have before, set aside things we know are multiples of 29 in order to deal with what is left over. So we can write

$a_{n+1} = 11 \cdot 12^{n+1} + 18 \cdot 41^{n+1} = (11 \cdot 12^n) \cdot 12 + (18 \cdot 41^n) \cdot 41$
$= (11\cdot 12^n)\cdot 12 + (18\cdot 41^n)\cdot 12 + (18\cdot 41^n)\cdot(41-12) = (11\cdot 12^n + 18\cdot 41^n)\cdot 12 + (18\cdot 41^n)\cdot(29)$
$= 12a_n + 29 \cdot (18 \cdot 41^n)$

But since $a_n = 29K$, this means that $a_{n+1} = 12(29K) + 29\cdot(18\cdot 41^n) = 29(12K + 18\cdot 41^n)$ is also a multiple of 29 (!). This establishes our inductive hypothesis, finishing the argument. So a_n is always a multiple of 29.

We can craft many statements like this, that we could then prove by induction. Looking at the argument we built, what appeared to be important was that $41 - 12 = 29$, so what we split off from the piece we knew something about was a multiple of 29, so would not change what we were congruent to modulo 29. By a parallel kind of reasoning, for example, we could show that $b_n = 11 \cdot 12^n + 17 \cdot 41^n$ is <u>never</u> a multiple of 29, since we could show, as before, that $b_{n+1} = 12b_n + 29(17 \cdot 41^n)$, but now we would start with $b_0 = 11 + 17 = 28$, which is not a multiple of 29; in fact, it is relatively prime to 29, as is 12, and so $12b_n$

would actually be relatively prime to 29 (by our inductive hypothesis); adding a multiple of 29 won't change that, so b_{n+1} is also relatively prime to 29, and so isn't a multiple of 29, either! This established the inductive step: $29 \not| b_n$ implies $29 \not| b_{n+1}$. [What we really established was that $\gcd(b_n, 29) = 1$ implies that $\gcd(b_{n+1}, 29) = 1$, which, since 29 is prime, really amounts to the same thing!]

After this discussion, we returned to our discussion about 'fast exponentiation', as a way to speed up our 'compositivity test': If $\gcd(a, n) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n cannot be prime. We saw last time that to compute $a^k \bmod n$ more quickly, we could adopt a strategy of repeatedly dividing the exponent by 2 (with remainder 0 or 1); keeing track of the remainders and running the process backwards allows us to carry out exponentiation much more quickly. Looking at another example for inspiration, we found that

$373 = 2\cdot 186+1$, $186 = 2\cdot 93+0$, $93 = 2\cdot 46+1$, $46 = 2\cdot 23+0$,
$23 = 2\cdot 11+1$, $11 = 2\cdot 5+1$, $5 = 2\cdot 2+1$, $2 = 2\cdot 1+0$

This should feel kind of like the Euclidean algorithm?, except that the divisor never changes! Reassembling this from the bottom up, kind of as we did with the Euclidean algorithm, we find that

$2 = 2\cdot 1+0$, so
$5 = 2\cdot(2\cdot 1+0)+1$, so
$11 = 2\cdot(2\cdot(2\cdot 1+0)+1)+1$, so
$23 = 2\cdot(2\cdot(2\cdot(2\cdot 1+0)+1)+1)+1$
$46 = 2\cdot(2\cdot(2\cdot(2\cdot(2\cdot 1+0)+1)+1)+1)+0$
$93 = 2\cdot(2\cdot(2\cdot(2\cdot(2\cdot(2\cdot 1+0)+1)+1)+1)+0)+1$
$186 = 2\cdot(2\cdot(2\cdot(2\cdot(2\cdot(2\cdot(2\cdot 1+0)+1)+1)+1)+0)+1)+0$
$373 = 2\cdot(2\cdot(2\cdot(2\cdot(2\cdot(2\cdot(2\cdot(2\cdot 1+0)+1)+1)+1)+0)+1)+0)+1$

If you multiply this out without multiplying it out (that is, distribute all of the multiplcations across the sums), what you find is that this says that

$373 = 1+0\cdot 2+1\cdot 2^2+0\cdot 2^3+1\cdot 2^4+1\cdot 2^5+1\cdot 2^6+0\cdot 2^7+1\cdot 2^8 = 2^8+2^6+2^5+2^4+2^2+2^0$

(essentially, we are reading the remainders from right to left, pairing them with ever higher powers of 2. Or if you prefer, reading them from left to right, pairing them with ever lower powers of 2! [But then you need to figure out where to start...]). This is basically the *binary representation* of 373, writing it in base 2: $373 = 101110101_2$.

A different way to look at this is to think of writing 373 (to think in terms of a specific example) as a sum of distinct powers of 2; there is, in fact, only one way to do this. The process of division by 2 with remainders that we discovered is one way to do this. Note that, in essence, that process find the smallest power of two we need first; $373 = 2\cdot 186+1$ means we start with $2^0 = 1$, and then use the quotient, 186, to identify the next power of two ($186 = 2\cdot 93+0$ says that it won't be 2^1 (the 0 says skip that one), $93 = 2\cdot 46+1$ says that the next one is in fact 2^2)

Another way to reach the same answer is to work down from above; the largest power of 2 less than (or equal to) 373 is $256 = 2^8$, so $373 = 2^8+(373-256) = 2^8+117$. By continuing to remove the largest power of 2 that we can, we can revover the base 2 representation:

$373 = 2^8+117 = 2^8+2^6+(117-64) = 2^8+2^6+53 = 2^8+2^6+2^5+21 = 2^8+2^6+2^5+2^4+5 = 2^8+2^6+2^5+2^4+2^2+1 = 2^8+2^6+2^5+2^4+2^2+2^0 = 101110101_2$

[This representation is unique because of you skip a power of 2 that you could subtract off, the rest of the powers of 2 will never let you catch up: $1+2+2^2+\cdots+2^n = 2^{n+1}-1$ [which we can show by induction!], so all of them together can never add up to the number you are trying to represent.] We also demonstrated this with another, somewhat larger number, like 3059? [I could no longer remember the exact number]:

$3059 = 2048+1011 = 2048+512+499 = 2048+512+256+243$
$= 2048+512+256+128+115 = 2048+512+256+128+64+51$
$= 2048+512+256+128+64+32+19 = 2048+512+256+128+64+32+16+3$
$= 2048+512+256+128+64+32+16+2+1$
$= 2^{11}+2^9+2^8+2^7+2^6+2^5+2^4+2^1+2^0 = 101111110011_2$

The point to all of this, though, was to do exponentiation quickly! The basic idea is that if squaring a number, mod n, is our basic operation, then we can compute $a_1 = a \bmod n$, $a_2 = a^2 \bmod n$, $a_3 = a^4 \bmod n$, $\ldots$, $a_r = a^{2^r} \bmod n$ in r steps by repeated squaring, since $a^{2^{i+1}} = a^{2^i\cdot 2} = (a^{2^i})^2$. If we then know how to write k as a sum of powers of 2 (using either of the procedures above), we can then write $a^k \bmod n$ as the product, mod n, of the corresponding numbers a_i, since $a^{p+q} = a^p a^q$; exponentiation turns sums in to products. For a number k of any size, we can estimate how much work this will involve; if $2^N \le k < 2^{N+1}$, then the base 2 representation of k will have $N+1$ digits, so we will need N squarings to build the numbers a_i, and then, at worst, we will need to multiply all of them together to compute $a^k \bmod n$, which is another N multiplications. So all together, we will need at most $2N = 2\log_2(k)$ multiplications modulo n to compute $a^k \bmod n$. Which is a lot smaller than the $k-1$ multiplications that repeated multiplication by a would require!

Our process of division by 2 with remainders can also be used to compute $a^k \bmod n$ with essentially the same amount of work; at each step we either square the result of the previous step or square and then multiply by a, depending on whether the remainder is 0 or 1. To compute a^{373}, for example, we compute a, a^2, a^5, a^{11}, a^{23}, a^{46}, a^{93}, a^{186}, and a^{373} in turn, where each odd exponent encountered signifies that an additional a was multiplied to the square of the previous step.

This fact, that computing powers mod n is 'fast', enables us to have a fast way to determine that very large numbers are not prime, using Euler's Theorem. It is actually true that it can also be used as a fast way to show that numbers (of certain special forms, like 2^k+1 or 2^k-1) are prime; this is something that I hope we will have the time to explore shortly!