Topics: Bad Proofs, Modular Arithmetic

1 Bad Proofs

Consider polynomials of the form

$$f(x) = A_n x^n + A_{n-1} x^{n-1} + \cdots + A_1 x + A_0,$$

where each A_i is an integer. Such a polynomial is *mystical* if $\forall x \in \mathbf{N}.\ x \geq 1 \implies f(x)$ is prime. For example, $f(x) = x + 1$ is not mystical since $f(3) = 4$ is not prime.

Now a Stanford professor claims that any polynomial $f(x)$ where $f(0) = 3$ cannot be mystical. He gives the following proof:

Claim: $f(0) = 3 \implies f(x)$ is not mystical.
Proof: Consider $f(3)$. Note that $f(3)$ is an integer, since $f(x)$ has integer coefficients. Since f is a polynomial, we may write it as $f(x) = A_n * x^n + \cdots + A_1 * x + A_0$. Then $f(0) = A_n * 0^n + \cdots + A_1 * 0 + A_0$, so if $f(0) = 3$, we must have $A_0 = 3$. Moreover, we may calculate

$$\begin{aligned} f(3) &= A_n * 3^n + ... + A_1 * 3 + 3 \\ &\equiv A_n * 0^n + ... + A_1 * 0 + 0 \ (mod\ 3) \\ &\equiv 0 + ... + 0 \ (mod\ 3) \\ &\equiv 0 \ (mod\ 3) \end{aligned}$$

which means that 3 is a divisor of $f(3)$. Consequently, $f(3)$ cannot be prime, which implies that f is not mystical.

Is there anything wrong with this proof[1]?

Before we look at his proof, let's first decide whether or not his claim is true. Is it true that $f(0) = 3$ means that $f(x)$ is not mystical? No, it doesn't, since $f(x) = 3$ satisfies $f(0) = 3$ and is mystical. Since the professor's claim is false, and his proof purports to prove it, there must be an error in his proof.

A close examination of the proof reveals that the Stanford professor used the justification $\exists p \in \mathbf{N}.\ p \mid n \implies n$ is not prime (here, the $\mid$ symbol means *evenly divides*). But consider the case where the only such p is $p = n$. Does this mean n is not prime? Of course not, since primes are always divisible by themselves. The attempt to use this false justification is the error in the proof.

2 Modular Arithmetic

The building blocks of modular arithmetic are *congruency* relations, just like equality relations for normal arithmetic. Congruency can be defined in multiple equivalent ways. One definition is

$$a \equiv b \ (mod\ m) \iff m \mid (|a - b|),$$

where $a \equiv b \ (mod\ m)$ means *a is congruent to b modulo m*. The second definition is

$$a \equiv b \ (mod\ m) \iff a \ \% \ m = b \ \% \ m,$$

where % is the remainder operation.

Just like with equations, there are certain identities that hold for congruencies. The most important ones are as follows:

[1] This question was taken from a midterm from Fall 2001. Infer from that what you will.

1. $a \equiv b \ (mod\ m) \implies a + c \equiv b + c \ (mod\ m)$
2. $a \equiv b \ (mod\ m) \implies a \cdot c \equiv b \cdot c \ (mod\ m)$
3. $a \equiv b \ (mod\ m) \wedge b \equiv c \ (mod\ m) \implies a \equiv c \ (mod\ m)$

Note that there is no rule for division that holds for congruencies.

These rules mean that it is possible to reduce each term in a congruency individually, modulo the base. Consider the equation $7x + 10^{2003} \equiv 0 \ (mod\ m)$. Since $7 \equiv 1 \ (mod\ m)$, we can replace the 7 with 1. And since $10 \equiv 1 \ (mod\ m)$, we can replace the 10 with 1 in the congruency. Thus

$$7x + 10^{2003} \equiv 2 \ (mod\ m) \longrightarrow x + 1^{2003} \equiv 2 \ (mod\ m) \longrightarrow x + 1 \equiv 2 \ (mod\ m) \longrightarrow x \equiv 1 \ (mod\ m).$$

Note that it is not legal to reduce the exponent 2003. It is legal to reduce the base, since $10^{2003} = 10 \cdot 10 \cdot \cdots 10$, and we can reduce each 10 individually by applying rule 3 from above. But no application of the above rules can be used to reduce exponents.

As with equations, we can solve systems of congruencies. Consider the set of congruencies

1. $10x + 2y \equiv 3 \ (mod\ 11)$
2. $x + y \equiv 5 \ (mod\ 11)$.

We use many of the same techniques of solving equations with congruencies, keeping in mind that we can't divide a congruency by any number. Multiplying equation[2] #2 by -2, we get $-2x - 2y \equiv -10 \ (mod\ 11)$. Then adding this to equation 1, we get $12x \equiv -7 \ (mod\ 11)$. Now we can reduce 12 to 1, and -7 to 4, to get $x \equiv 4 \ (mod\ 11)$. Substituting into equation #2 and subtracting 4 from each side, we get $y \equiv 1 \ (mod\ 11)$. Thus the solution to the system is $x \equiv 4 \ (mod\ 11)$ and $y \equiv 1 \ (mod\ 11)$.

But now consider the set of congruencies

1. $5x + 2y \equiv 3 \ (mod\ 11)$
2. $x + y \equiv 5 \ (mod\ 11)$.

Eliminating y, we end up with the equation $3x \equiv 4 \ (mod\ 11)$. Now how do we eliminate the 3 on the left side? Notice that if we multiply 3 by 4, we get 12, which can be reduced to 1. So if we multiply $3x \equiv 4 \ (mod\ 11)$ by4, we get $12x \equiv 16 \ (mod\ 11)$, which reduces to $x \equiv 5 \ (mod\ 11)$. Solving for y, we get $y \equiv 0 \ (mod\ 11)$.

Since the product of 3 and 4 reduces to 1 modulo 11, 3 and 4 are *inverses* modulo 11. By multiplying an equation of the form $ax \equiv b \ (mod\ m)$ by the inverse of a, written as a^{-1}, we get $a^{-1}ax \equiv a^{-1}b \ (mod\ m)$, or $x \equiv a^{-1}b \ (mod\ m)$, a solution to the equation.

We saw in lecture that an inverse of a modulo m exists if $gcd(a, m) = 1$. Now we will see an informal proof that if $gcd(a, m) \neq 1$, a has no inverse modulo m. First we prove the following lemma:

Lemma 5.1: $a \equiv kp \ (mod\ m)$, where $p \mid a$, $p \mid m$, and $0 \leq kp < m$.
Proof: We know that p divides a and m, so $a = cp$ and $m = dp$ for some integer c and d. Thus $a \equiv cp \ (mod\ m)$. Now we can always subtract multiples of m from one side of a congruency, so $a \equiv cp - nm \ (mod\ m)$, where n is some integer, or $a \equiv (c - nd)p \ (mod\ m)$. Now in order for $0 \leq (c - nd)p < m$, it must be that $0 \leq c - nd < d$ for some n. Thus $c/d - 1 < n \leq c/d$. This is satisfied by $n = \lfloor c/d \rfloor$. Thus, if we choose this n, we have $a \equiv kp \ (mod\ m)$, where $k = (c - \lfloor c/d \rfloor p)$, and $0 \leq kp < m$.

Now we prove the following:

Theorem 5.2: $\forall b \in \mathbf{Z}.\ gcd(a, m) \neq 1 \implies ab \not\equiv 1 \ (mod\ m)$.
Proof: Let $gcd(a, m) = p$, $p \neq 1$. Consider an arbitrary b. Then $p \mid ab$. From lemma 5.1, $ab \equiv kp \ (mod\ m)$, where $0 \leq kp < m$. Now it is impossible for $kp = 1$ for any integer k. Thus $ab \not\equiv 1 \ (mod\ m)$ for any a.

[2]Notice my terminology getting sloppy here. Don't expect much of a distinction to be made between the terms *equation* and *congruency*.

As a final exercise, consider the following function[3]: $f(x) =$ *the sum of the cubes of each digit in* x. In other words, if $x = A_k A_{k-1} \cdots A_0$, where the A_i are the digits of x, $f(x) = A_k^3 + A_{k-1}^3 + \cdots + A_0^3$. Now prove that $f(x) \equiv x \ (mod\ 3)$ for all $x \in \mathbf{N}$.

Writing x in terms of its digits, we have $x = A_k \cdot 10^k + A_{k-1} \cdot 10^{k-1} + \cdots + A_1 \cdot 10 + A_0$. Working modulo 3, we can reduce each 10 to 1, to get $x \equiv A_k + A_{k-1} + \cdots A_0 \ (mod\ 3)$. Now in order for $f(x) \equiv x \ (mod\ 3)$, we require that $A_k^3 + A_{k-1}^3 + \cdots + A_0^3 \equiv A_k + A_{k-1} + \cdots A_0 \ (mod\ 3)$. This is satisfied if each $A_i^3 \equiv A_i \ (mod\ 3)$. So it suffices to prove that $n^3 \equiv n \ (mod\ 3)$ for all naturals n.

Now since any natural n can be reduced to either 0, 1, or 2, so it is sufficient to prove that $n^3 \equiv n \ (mod\ 3)$ for $n \in 0, 1, 2$. We can just enumerate all three cases. We have $0^3 = 0 \equiv 0 \ (mod\ 3)$, $1^3 = 1 \equiv 1 \ (mod\ 3)$, and $2^3 = 8 \equiv 1 \ (mod\ 3)$. Thus $n^3 \equiv n \ (mod\ 3)$ for all naturals n.

Thus, since each digit of a natural number is positive, we can reduce $A_k^3 + A_{k-1}^3 + \cdots + A_0^3$ modulo 3 term by term, using the fact that $n^3 \equiv n \ (mod\ 3)$, to get $A_k + A_{k-1} + \cdots A_0$, completing our proof.

[3]This was also taken from a midterm from Fall 2001.