Math 3200: Day 14

Modular Arithmetic

Previously, we've proved statements of the form "If ___ is even, then ___ is even", as well as statements about multiples of integers other than 2 (e.g. the exam problem).

Now, when we say a number is even, that means it's a multiple of 2, and likewise we can talk about multiples of 5 or 17 or 296. When we say a number is odd, what does that mean?

The simplest answer is "not even," & of course we could talk about a number not being a multiple of 5 or 296. But that would put 3 & 4 into the same category: "Not a multiple of 5." But we can do better:

More precisely, an integer n is odd if $n = 2m+1$ for some $m \in \mathbb{Z}$. Said another way, if you divide n by 2 you get a remainder of 1. This is the idea that generalizes.

Def: Suppose $a, n, m \in \mathbb{Z}$ with $m \geq 2$. We say that n is congruent to a modulo m, written $n \equiv a \pmod{m}$, if

$$n = cm + a$$

for some $c \in \mathbb{Z}$.

Ex: $7 \equiv 3 \pmod{2}$... and both are congruent to 1. As we already implicitly argued, all odd integers are congruent to 1 mod 2 and all even integers are congruent to 0.

Ex: $12 \equiv ? \pmod{7}$

Well, we can write $12 = 1 \cdot 7 + 5 = 2 \cdot 7 - 2 = 3 \cdot 7 - 9 = \dots$

so $12 \equiv 5 \equiv -2 \equiv -9 \dots \pmod{7}$.

We can then talk about modular arithmetic; i.e., doing arithmetic operations modulo n. This is actually something you're pretty well-known to do: **Q:** If it's currently 8:00, what time will it be in 37 hours?

A: In 36 hrs it'll be 8:00 again, so in 37 hrs it'll be 9:00.

Said differently, $8 + 37 \equiv 9 \pmod{12}$

(In more detail: $8+37=45=3\cdot 12+9$, so $45\equiv 9 \pmod{12}$)

Prop 1: Let $a,b,n\in\mathbb{Z}$. If $a\equiv b \pmod n$, then $a^2\equiv b^2 \pmod n$.

Pf: Suppose $a\equiv b \pmod n$. Then there exist $p,q,r\in\mathbb{Z}$ so that

$$a=pn+r \quad \& \quad b=qn+r.$$

Then $a^2=(pn+r)^2=p^2n^2+2prn+r^2=n(p^2n+2pr)+r^2$, so $a^2\equiv r^2 \pmod n$.

Likewise, $b^2=(qn+r)^2=q^2n^2+2qrn+r^2=n(q^2n+2qr)+r^2$, so $b^2\equiv r^2 \pmod n$ as well, completing the proof. ∎

Prop 2: Let $n\in\mathbb{Z}$. Then either $n^2\equiv 0 \pmod 4$ or $n^2\equiv 1 \pmod 4$.

Proof: If $n\in\mathbb{Z}$, then clearly $n\equiv 0,1,2,$ or $3 \pmod 4$. By Prop 1, then, we just have to determine $0^2, 1^2, 2^2$ & 3^2 mod 4:

- $0^2=0\equiv 0 \pmod 4$
- $1^2=1\equiv 1 \pmod 4$
- $2^2=4\equiv 0 \pmod 4$
- $3^2=9\equiv 1 \pmod 4$.

Therefore, $n^2\equiv 0$ or $1 \pmod 4$. ∎

Corollary: 1,000,000,002 is not a perfect square.

Pf: Clearly, $1,000,000,002\equiv 2 \pmod 4$, so the proposition tells us it can't be a perfect square. ∎

A more interesting corollary:

Corollary: If $a,b\in\mathbb{Z}$ are odd, then a^2+b^2 is not a perfect square.

Pf: Suppose $a,b\in\mathbb{Z}$ are odd. Then each is congruent to either 1 or 3 mod 4. As we saw in the proof of Prop 2, this means

$$a^2\equiv 1 \pmod 4 \quad \& \quad b^2\equiv 1 \pmod 4. \text{ Then}$$

$$a^2+b^2\equiv 1+1\equiv 2 \pmod 4$$

and so can't be a perfect square by Prop 2. ∎