Today we explore solving power congruences. We warm up with a bunch of examples:

1. $x^{18} \equiv 4 \pmod{17}$.
   Chris: By Fermat's Little Theorem, we have $x^{16} \equiv 1 \pmod{17}$ or $x \equiv 0$ (mod 1)7. The latter clearly can't be a solution to the given congruence, so we deduce that $x^{18} \equiv x^2 \equiv 4 \pmod{17}$, whence $x \equiv \pm 2 \pmod{17}$.

2. $x^3 \equiv 4 \pmod{17}$. We could just check every possible solution, or...
   Ben: $x^3 \equiv 4 \equiv -64 \pmod{17}$ so then $x \equiv -4 \pmod{17}$
   Akhil + Alex: From before, $(\pm 2)^{18} \equiv 4 \pmod{17}$. So then $((\pm 2)^6)^3 \equiv 4 \pmod{17}$, so $x = (\pm 2)^6 \equiv 13 \pmod{17}$.
   Max: $x^3 \equiv 4 \pmod{17} \implies x^6 \equiv 16 \pmod{17} \equiv -1 \pmod{17} \implies x^{18} \equiv (x^6)^3 \equiv (-1)^3 = -1 \equiv 16 \pmod{17}$ so $x \equiv \pm 4$. But then $+4$ doesn't work, so $x \equiv -4 \equiv 13 \pmod{17}$.

Question (Kimberly): Why isn't $x^{18} \equiv x^1 \pmod{17}$? Because we can't add/subtract 17 *in the exponent*, only in coefficients and constants. But in exponents, you *can* add/subtract by $\varphi(n)$.

We return to example 2 and point out there's yet another approach we can take. Max found that by raising both sides to the 6th, we obtain a congruence for x^2, which is easier to solve. But what we really want is x, not x^2. Is there some other power we can raise both sides of the congruence to to get x? Yes!

$$x \equiv x^{32} \cdot x \equiv x^{33} \equiv (x^3)^{11} \equiv 4^{11} \pmod{17}.$$

But notice that $4^2 \equiv -1 \pmod{17}$, so $4^{11} \equiv (-1)^5 4 \equiv -4 \pmod{17}$.

3. $x^5 \equiv 4 \pmod{17}$.
   Konnor+Oliver: Raise both sides to the 13th power:
   $$x^{5 \cdot 13} = x^{65} = x^{1+64} \equiv x \equiv 4^{13} \pmod{17}.$$
   And $4^{13} = (4^2)^6 \cdot 4 = (-1)^6 \cdot 4 \equiv 4 \pmod{17}$, thus $x \equiv 4 \pmod{17}$.

Question (Alex): Is there always a solution to $x^a \equiv b \pmod{p}$?

4. $x^2 \equiv 6 \pmod 7$
   Miranda: Cube both sides:
   $$1 \equiv (x^2)^3 \equiv 6^3 \equiv (-1)^3 = -1 \pmod 7.$$

Aaah! Contradiction! Right away this tells us there can't be a solution to this congruence. The issue with our approach is that 2 and $7-1=6$ are not relatively prime, so we cannot find a good exponent (i.e. one that produces just x).

5. $x^5 \equiv 11 \pmod{35}$.
Mia: $x^{\varphi(35)} \equiv 1 \pmod{35}$, and $\varphi(35) = \varphi(5 \cdot 7) = (5-1)(7-1) = 24$, so $x^{24} \equiv 1 \pmod{35}$.
Jeff: Raise both sides to the 5th:

$$(x^5)^5 = x^{1+24} \equiv x \equiv 11^5 \pmod{35}.$$

It therefore remains only to compute $11^5 \pmod{35}$:

$$11^5 \equiv 11 \cdot (11^2)^2 \equiv 11 \cdot (105+16)^2 \equiv 11 \cdot 16^2 \equiv 11 \cdot (245+11) \equiv 11^2 \equiv 16 \pmod{35}.$$

As a result, $x \equiv 16 \pmod{35}$.

Question (Kimberly): Okay, but how do you find the right exponent to raise both sides to? What is the formulaic/general approach?

The General Approach: Given $x^e \equiv y \pmod N$. Want to solve for x.
Step 0: Reduce e mod $\varphi(N)$.*

Step 1: Want to find an exponent, d, such that $de \equiv 1 \pmod{\varphi(N)}$.
(Miranda) If $\big(e, \varphi(N)\big) = 1$, by Bézout's Theorem there exists some k, d such that $ed + k\varphi(N) = 1$ so then $ed \equiv 1 \pmod{\varphi(N)}$. We can use the Euclidean Algorithm to solve for d.

Step 2: Then $x^{de} \equiv x^{1+k\varphi(N)} \equiv x \equiv y^d \pmod N$.

Step 3: Reduce $y^d \pmod N$. How do we do this efficiently? First compute, $y^2 \pmod N$. Then compute $y^4 = (y^2)^2 \pmod N$, by squaring the previous result. Square again to get y^8, etc. Now we can express d in binary (i.e. as a sum of distinct powers of 2), which means we can express y^d in terms of the powers of y we'd computed. Moreover, this process takes $\ll \log d$ computations.

Examples of binary notation: $13 = 8+4+1$. $168 = 128+32+8$. Can do this by always taking the largest power of 2 possible (greedy algorithm).

*Note that for this process to be *guaranteed* to work, we need $\big(e, \varphi(N)\big) = 1$. However, as Konnor pointed out, even when this doesn't happen (as in Example 1) the method still might lead to a solution!

Next time we will see how this is used to great effect in the RSA encryption algorithm.