Warmup

Compute the least residues of a^i mod n in each of the following examples.

1. $a = 2$, $n = 5$, $i = 1, 2, 3, 4, 5$.
2. $a = 2$, $n = 6$, $i = 1, 2, 3, 4, 5, 6$.
3. $a = 4$, $n = 5$, $i = 1, 2, 3, 4, 5$.
4. $a = 3$, $n = 4$, $i = 1, 2, 3, 4$.

Pro tip: For bigger and bigger i, instead of computing a^i and then reducing, instead take the reduced a^{i-1} and multiply it by a. For example, since

$$3^3 = 27 \equiv 7 \pmod{10},$$

you know

$$3^4 \equiv_{10} 3 * 7 \equiv_{10} 21 \equiv_{10} 1.$$

Last time

We solved congruences of the form

$$ax \equiv b \pmod{n}.$$

Namely, we had two cases: Calculate $d = \gcd(a, n)$.

1. If $d \nmid b$, then there are no solutions.
2. If $d|b$, then there are exactly d solutions (mod n).
   Find them as follows:
   (a) Find one solution, either by guessing...
   If $d = 1$ and you can find an a' satisfying $a'a \equiv 1 \pmod{n}$, then
   $x \equiv_n (a'a)x \equiv_n a'(ax) \equiv_n a'b$.
   ...or by using the Euclidean algorithm to calculate

   $$ua + vn = d, \qquad \text{so that} \qquad b = (b/d)d = (b/d)ua + (b/d)vn.$$

   Thus $x = (b/d)u$ is one solution.
   (b) For the rest, add n/d until you have a full set.

Nonlinear congruences

Theorem (Polynomial Roots Mod p Theorem)
Let p be prime in $\mathbb{Z}_{>0}$, and let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x],$$

with $n \geqslant 1$ and $p \nmid a_n$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most p incongruent solutions.

(See book for proof.)

Lemma

Let p be a prime number, and let $a \in \mathbb{Z}$. Then either

$$p|a, \qquad \text{so that } a^i \equiv 0 \pmod p \text{ for all } i,$$

or the list of the least residues of

$$a,\ 2a,\ 3a,\ \ldots,\ pa$$

is a rearrangement of the numbers

$$0, 1,\ 2,\ 3,\ \ldots,\ (p-1)$$

Example: let $n = 5$. The values of $ak \pmod 5$ are as follows:

$$\begin{array}{cc|ccccc} & & \multicolumn{5}{c}{\longleftarrow k \longrightarrow} \\ & & 1 & 2 & 3 & 4 & 5 \\ \hline & 1 & 1 & 2 & 3 & 4 & 0 \\ \uparrow & 2 & 2 & 4 & 1 & 3 & 0 \\ a & 3 & 3 & 1 & 4 & 2 & 0 \\ \downarrow & 4 & 4 & 3 & 2 & 1 & 0 \\ & 5 & 0 & 0 & 0 & 0 & 0 \end{array}$$

Theorem (Fermats Little Theorem)

Let p be a prime number, and let $a \in \mathbb{Z}$. Then either

$$p|a, \qquad \text{so that } a^i \equiv 0 \pmod p \text{ for all } i,$$

or

$$p \nmid a \qquad \text{and} \qquad a^{p-1} \equiv 1 \pmod p.$$

Proof. Consider the product $a(2a)(3a)\cdots((p-1)a)\dots$

Now what can we do with this?

Examples

1. Compute $2^{35} \pmod 7$.
2. Solve $x^{103} \equiv 4 \pmod{11}$.