Lecture 7.1

Power Congruences

Pop quiz: what's $7^{327} \pmod{853}$?

I'll give you a hint: $\phi(853) = 852$.

Okay I admit that's not very helpful.

Here's a strategy: let's express 327 in binary, $327 = 256 + 64 + 4 + 2 + 1$, and compute $7^{2^k} \pmod{853}$ for k up to 8 ($2^8 = 256$).

Here's a table:

k	2^k	$7^{2^k} \pmod{853}$
1	2	49
2	4	$49^2 = 2401 \equiv 695$
3	8	$695^2 = 483025 \equiv 227$
4	16	$227^2 = 51529 \equiv 349$
5	32	$349^2 = 121801 \equiv 675$
6	64	$675^2 = 455625 \equiv 123$
7	128	$123^2 = 15129 \equiv 628$
8	256	$628^2 = 394384 \equiv 298$

Then $7^{327} = 7^{256+64+4+2+1}$

$$= 7^{256} \cdot 7^{64} \cdot 7^4 \cdot 7^2 \cdot 7$$

$$\equiv 298 \cdot 123 \cdot 695 \cdot 49 \cdot 7$$

$$\equiv 828 \cdot 695 \cdot 49 \cdot 7$$

$$\equiv -25 \cdot 695 \cdot 49 \cdot 7$$

$$\equiv 538 \cdot 49 \cdot 7$$

$$\equiv -81 \cdot 7 \equiv 286 \pmod{853}.$$

This method to compute $a^k \pmod{n}$ for large k is called "successive squaring".

In practice, this is more computationally efficient than evaluating a^k and then reducing mod

reducing mod n.

On the flip side, consider a congruence of the form

$$x^k \equiv a \pmod{n}.$$

In principle, we know this can be solved by testing $x = 0, 1, \ldots, n-1$ by hand, but as above, this is computationally expensive.

Ex Let's solve $x^{131} \equiv 758 \pmod{1073}$.

First, $1073 = 29 \cdot 37$ so

$$\phi(1073) = 28 \cdot 36 = 1008.$$

Now 131 and 1008 are coprime, so Euler's theorem for $a^{\phi(n)}$ doesn't help, BUT by expressing

$$1 = 131u + 1008v$$

we can cleverly rewrite x^{131}, which we'll do in a moment.

First, the gcd algorithm produces

$$1 = 131(731) - 1008(95).$$

Next, raise x^{131} to the 731st power and watch the magic:

$$(x^{131})^{731} = x^{1+1008\cdot 95}$$

$$= x \cdot (x^{1008})^{95}$$

$$\equiv x \cdot 1^{95} \equiv x \pmod{1073}.$$

So the congruence $x^{131} \equiv 758 \pmod{1073}$ becomes $x \equiv 758^{731} \pmod{1073}$ which we can compute by successive squaring:

$$731 = 512 + 128 + 64 + 16 + 8 + 2 + 1.$$

	k	2^k	$758^{2^k} \equiv 315^{2^k} \pmod{1073}$
—	1	2	$315^2 = 99225 \equiv 509$
	2	4	$509^2 = 259081 \equiv 488$
—	3	8	$488^2 = 238144 \equiv 1011 \equiv -62$
—	4	16	$62^2 = 3844 \equiv 625 \equiv -448$
	5	32	$448^2 = 200704 \equiv 53$
—	6	64	$53^2 = 2809 \equiv 663 \equiv -410$
—	7	128	$410^2 = 168100 \equiv 712 \equiv -361$
	8	256	$361^2 = 130321 \equiv 488$
—	9	512	$488^2 \equiv -62$

Then $758^{731} \equiv (-315)^{731}$

$$\equiv 315^{512} \cdot 315^{128} \cdot 315^{64} \cdot 315^{16} \cdot 315^{8} \cdot 315^{2} \cdot (-315)$$

$$\equiv -62 \cdot (-361) \cdot (-410) \cdot (-448) \cdot$$

$$\cdot (-62) \cdot 509 \cdot (-315)$$

$$\equiv 62^2 \cdot 361 \cdot 410 \cdot 448 \cdot 509 \cdot 315$$

$$\equiv 448 \cdot 361 \cdot 410 \cdot 448 \cdot 509 \cdot 315$$

$$\equiv (-295) \cdot 410 \cdot 448 \cdot 509 \cdot 315$$

$$\equiv 295 \cdot 410 \cdot 448 \cdot 509 \cdot 315$$

$$\equiv -299 \cdot 448 \cdot 509 \cdot 315$$

$$\equiv 173 \cdot 509 \cdot 315$$

$$\equiv 71 \cdot 315 \equiv 905 \pmod{1073}.$$

So $x = 905$ solves the congruence

$$x^{731} \equiv 758 \pmod{1073}.$$

Exercise 1: Solve the following congruences.

(a) $x^{731} \equiv 758 \pmod{29}$

(b) $x^{731} \equiv 758 \pmod{37}$

(c) $x^{7} \equiv 6 \pmod{101}$

Theorem If $\gcd(a,n) = 1$ and $\gcd(k, \phi(n)) = 1$,

then a solution to

$$x^k \equiv a \pmod{n}$$

exists and satisfies

$$x \equiv a^u \pmod{n}$$

where u is any solution to

$$ku - \phi(n)v = 1.$$

Exercise 2: Verify that $x = a^u$ is a solution to the congruence $x^k \equiv a \pmod{n}$.

(Or look at the proof in the textbook.)

Next time: cryptography.