Fermat's Little Theorem
Fall 2014

Some experiments

We've spent some time on the multiplication tables for an n hour clock – that's arithmetic (mod n). Now we will work on *exponentiation*: raising numbers to powers.

Finish filling out this (mod 7) table:

power:	0	1	2	3	4	5	6
1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1
3	1	3	2				
4							
5							
6							

Then pick another prime number (not 7) and build a similar table.

Make a *conjecture*.

Fast exponentiation

You just had some fun computing small clock powers of small numbers. But you need a new strategy to compute something like

$$3^{100} (\text{mod } 101)$$

Here's an algorithm.[1] Write the exponent 100 in *base 2*, by cutting it in half over and over again and keeping track of evens and odds. Keep track of the powers of 3 at the same time.

	step	bit	powers of 2	$3^{\text{powers of 2}}$
	100	0	$1 = 2^0$	$3^1 = 3$
100/2	50	0	$2 = 2^1$	$3^2 = 9$
50/2	25	1	$4 = 2^2$	$3^4 = (3^2)^2 = 81$
(25-1)/2	12	0	$8 = 2^3$	$3^8 = (3^4)^2 = 81^2 \equiv (-20)^2 = 400 \equiv -4$
12/2	6	0	$16 = 2^4$	$3^{16} \equiv (-4)^2 = 16$
6/2	3	1	$32 = 2^5$	$3^{32} \equiv 16^2 = 256 \equiv 54$
(3-1)/2	1	1	$64 = 2^6$	$3^{64} \equiv 54^2 = 2916 \equiv 88$

Check by adding up the powers that correspond to the odd bits to see that you have the base 2 expansion:

$$11001000_2 = 2^6 + 2^5 + 2^2 = 64 + 32 + 4 = 100.$$

Now you're ready for

$$3^{100} = 3^{64+32+4} = 3^{64}3^{32}3^4 \equiv 88 \times 54 \times 81 \equiv 1 (\text{mod } 101)$$

OK now practice. Pick some prime p and value a and compute $a^{p-1} (\text{mod } p)$.

[1] Do you know what an *algorithm* is?