CS 70 ## 2.11 LECTURE 7

For Gaussian Elimination, we need to be able to +, −, ×, ÷
We'd like a finite universe.

MODULAR ARITHMETIC

Think of how a clock wraps around 12. This is modular.
$x \bmod n$ is the remainder after dividing x by n.
↳ stand-in for $\{\dots, x-2n, x-n, x, x+n, x+2n, \dots\}$

NOTE congruence notation: $7+7 \equiv 2 \mod 12$ → comment, not action!

EXPONENTIATION

When we write a^b, we mean $a \cdot a \cdot a \cdot \dots \cdot a$ → b times.

± $(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

× $(ab) \bmod n = (a+k_1 n)(b+k_2 n) \bmod n = (ab + \overbrace{k_1 nb + k_2 na + k_1 k_2 nn}^{\text{multiple of } n}) \bmod n$

÷ times table mod 6 : $\{0,1,2,3,4,5\}$ ← in green cases, can find all

	0	1	2	3	4	5
1:	0	1	2	3	4	5
5:	0	5	4	3	2	1

	0	1	2	3	4	5
2:	0	2	4	0	2	4
3:	0	3	0	3	0	3

GCD x & 6

1:1	3:3	5:1
2:2	4:2	

THM Multiplicative inverses exist for $a \bmod m$ if $\gcd(a,m)=1$.
(or, prove everything's in a's times table mod m) & no repeats.

PROOF $ba \equiv ca \mod m \longrightarrow (b-c)a \equiv 0 \mod m \longrightarrow (b-c)a = km$
$\longrightarrow \exists\, l$ such that $(b-c) = lm \longrightarrow b \equiv c \mod m$ ▨
bc $\gcd(a,m)=1$