DIS 3B

MODULAR ARITHMETIC

$x \equiv r \pmod{m} \iff x = mq + r, \quad q \in \mathbb{Z}$

↳ r is the remainder when dividing x by m

when working in mod m, we really only care about numbers $\{0, 1, \ldots, m-1\}$, since everything else is congruent to one of these.

USING OPERATIONS

if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

addition: $a + c \equiv b + d \pmod{m}$

subtraction: $a - c \equiv b - d \pmod{m}$

multiplication: $a \times c \equiv b \times d \pmod{m}$

exponentiation: $a^k \equiv b^k \pmod{m}$

note: $a^k \equiv (a \bmod m)^k \pmod{m}$
BUT $a^k \not\equiv a^{(k \bmod m)} \pmod{m}$

$\}$ can only reduce the base

MULTIPLICATIVE INVERSES

notice that there is no division in modular arithmetic. instead, we use multiplicative inverses.

in normal arithmetic:

the multiplicative inverse of 2 is $1/2$ $(2 \times 1/2 = 1)$

in modular arithmetic: (there are no fractions)

a is the inverse of x mod m $(a \equiv x^{-1} \bmod m)$

$\Updownarrow$ iff

$$ax \equiv 1 \pmod m$$

! the multiplicative inverse does not always exist

x has a multiplicative inverse mod m

$\Updownarrow$ iff

$$\gcd(m, x) = 1$$

(m and x are coprime)

MORE MULTIPLICATIVE INVERSES

ex. 4 and 6 are not coprime: $\gcd(4,6)=2$

what happens if we try to find $4^{-1} \pmod 6$

we want some x s.t. $4x \equiv 1 \pmod 6$

$x=0 \quad 4 \times 0 \equiv 0 \pmod 6$

$x=1 \quad 4 \times 1 \equiv 4 \pmod 6$

$x=2 \quad 4 \times 2 \equiv 2 \pmod 6$

$x=3 \quad 4 \times 3 \equiv 0 \pmod 6$

$x=4 \quad 4 \times 4 \equiv 4 \pmod 6$

$x=5 \quad 4 \times 5 \equiv 2 \pmod 6$

there is no such x!