

Does 403 have a mult. inverse

mod 2070? Only if it's rel.

prime to 2070.

$$n = q \cdot d + r$$
$$2070 = 5 \cdot \underline{403} + \underline{55}$$

$$403 = 7 \cdot \underline{55} + \underline{18}$$

$$55 = 3 \cdot \underline{18} + \boxed{\underline{1}}$$

$$18 = 18 \cdot 1 + 0$$

The gcd is the last non-zero remainder. Here, the gcd = 1. So the #s are rel. prime.

To find the gcd (greatest common divisor) of two numbers, divide the smaller into the larger, get a remainder, and then iterate with the smaller # and the remainder.

This means there is some # x , $0 \leq x \leq 2069$

Such that $403 \cdot x \pmod{2070} = 1$.

$$2070 = 5 \cdot 403 + 55$$

$$403 = 7 \cdot 55 + 18$$

$$55 = 3 \cdot 18 + 1$$

$$18 = 18 \cdot 1 + 0$$

So -113 is the inverse,
which is the same as

1957

~~negative~~
So 113 is the inverse!

$$= 22 \cdot 2070 - 113 \cdot 403$$

$$= 22(2070 - 5 \cdot 403) - 3 \cdot 403$$

$$= 22 \cdot 55 - 3 \cdot 403$$

$$= 55 - 3 \cdot (403 - 7 \cdot 55)$$

$$= 55 - 3 \cdot 18$$

Find the inverse of 17 mod 55.

Euclidean Algorithm

$$n = qd + r$$

$$55 = 3 \cdot \underline{17} + \underline{4} \quad \leftarrow$$

$$17 = 4 \cdot \underline{4} + \underline{1} \quad \leftarrow$$

$$4 = 4 \cdot 1 + 0$$

$$\text{gcd} = 1$$

So the inverse of 17 is 13

$$= 13 \cdot 17 - 4 \cdot 55$$

~~305~~

simplify

$$= 17 - 4 \cdot (55 - 3 \cdot 17) \quad \text{sub}$$

$$1 = 17 - 4 \cdot 4$$

So what about cryptography?

Suppose M is a message, and e is an encryption key. We might encrypt by multiplying M by e , reducing mod n for some n .

Encrypted message is $M \cdot e \% n$.

How would we decrypt it? Use $d = e$'s inverse.

To decrypt, take
 $(M \cdot e) \cdot d = M \cdot (e \cdot d) = M \cdot 1 = M$.