

Wednesday, 9/17 - (1)

Euclidean algorithm concluded:

Q: what to do if the algorithm gives you

$$ax - by = \gcd(a, b) \quad (*)$$

where  $x, y$  are not positive?

A: add any multiple of  $b$  - say  $nb$ , where  $n \in \mathbb{N}$  - to  $x$ , and add the same multiple  $na$  of  $a$  to  $y$ .

You get

$$a(x+nb) - b(y+na) = \gcd(a, b)$$

which is true whenever  $(*)$  is.

Example

Let  $k = 31$  and  $m = 55$ .

Show that  $\gcd(k, \varphi(m)) = 1$  and find  $x, y \in \mathbb{N}$  with

$$kx - \varphi(m)y = 1.$$

Solution.

$$\varphi(55) = \varphi(5 \cdot 11) = 4 \cdot 10 = 40.$$

We have

$$40 = 31 \cdot 1 + 9$$

$$31 = 9 \cdot 3 + 4$$

$$9 = 4 \cdot 2 + 1$$

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

So  $\gcd(k, \varphi(m)) = 1$ . Also:

②

$$\begin{aligned}1 &= 9 - 4 \cdot 2 \\ &= 9 - (31 - 9 \cdot 3) \cdot 2 \\ &= 9 \cdot 7 - 31 \cdot 2 \\ &= (40 - 31 \cdot 1) \cdot 7 - 31 \cdot 2 \\ &= 40 \cdot 7 - 31 \cdot 9.\end{aligned}$$

That is,

$$31(-9) - 40(-7) = 1.$$

So we add 40 to -9 and 31 to -7:

$$31(-9 + 40) - 40(-7 + 31) = 1$$

$$31 \cdot 31 - 40 \cdot 24 = 1.$$

(DIY: check this.)