

From this, we have that

$$242 \cdot \underset{x}{(31)} + 1870 \underset{y}{(-4)} = 22.$$

Thus, we have used Euclid's alg. to solve the
Bezout equation.

Now suppose we want a solution to

$$242x + 1870y = 44.$$

We know $\gcd(242, 1870) = 22$ and $22 \mid 44$.

Therefore,

$$242(62) + 1870(-8) = 44.$$

How do we get all possible solutions to
 $ax + by = c$?

Thm. Let $a, b, c \in \mathbb{N}$, and set $d = \gcd(a, b)$.
The equation

$$ax + by = c$$

has a solution if and only if $d \mid c$.

If (x_0, y_0) ~~are~~ is a solution, then every integer solution is of the form:

$$x = x_0 + \frac{b}{d} \cdot n, \quad y = y_0 + \frac{a}{d} \cdot n$$

for all (and any) integer n .

minus!

$$y = y_0 - \frac{a}{d} n$$

Let's verify that all $x = x_0 + \frac{b}{d}n$, $y = y_0 + \frac{a}{d}n$ are solutions.

$$a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 + \frac{a}{d}n\right)$$

$$= ax_0 + \frac{ab}{d}n + by_0 + \frac{ab}{d}n$$

$$= ax_0 + by_0 = c. \quad (\text{Because } (x_0, y_0) \text{ a sol.})$$

With this new theory, try the apples and oranges problem again.

Procedure to get non-negative solutions.

$$ax + by = c.$$

1. Compute $d = \gcd(a, b)$.
2. Check $d | c$. (Assume $d | c$)
3. Use back-sub to ~~get one solution~~
solve the Bezout equation

$$ax + by = d$$

4. Multiply by $\frac{c}{d}$ to get a solution to $ax + by = c$
5. Write $x = x_0 + \frac{b}{d}n$, $y = y_0 - \frac{a}{d}n$
6. Impose $x \geq 0$, $y \geq 0$. (21)

Modular Arithmetic

Def. Let $a, b, m \in \mathbb{Z}$, $m \geq 2$. We say that a is congruent to b modulo m , written as

$$a \equiv b \pmod{m},$$

← notation!

if $a - b$ is an integer multiple of m .

In symbols,

there exists an integer k such that

$$a - b = k \cdot m.$$

(22)

The integer m is called the modulus.

Ex: $a = 9, b = ? , m = 5.$

If

$$a \equiv b \pmod{5},$$

then

$$a - b = 5k \quad \text{for some } k \in \mathbb{Z}.$$

What values of b satisfy the congruence?

$$b = 4, 9, 14, 19, 24, \dots, \textcircled{+5}, -1, \boxed{-6}, -11, -16, \dots, \textcircled{-5}$$

$$9 \equiv -6 \pmod{5}$$

$$9 - (-6) = 15 = 5 \cdot 3 \quad \checkmark.$$

$\textcircled{23}$