

Euclid's Algorithm.

Note Title

10/27/2014

Given integers $a, b > 0$ would like to find $\gcd(a, b)$ without having to factor a & b .

Euclid's algorithm for find \gcd dates back to 300 B.C.

Suppose $a > b$.

$$d \mid a \text{ and } d \mid b \iff d \mid b \text{ and } d \mid (a \bmod b).$$

The set of integers that divide both a & b

=

The set of integers that divide both $a \bmod b$ and b .

The largest integer that divides both a & b

=

The largest integer that divides $(a \bmod b)$ and b .

$$\underline{\gcd(a, b)} = \gcd(b, \underline{a \bmod b})$$

(smaller than b .
 $0 \dots b-1$)

\Rightarrow Recursion!

Base Case? If $\underline{b \mid a}$ then $\underline{\gcd(a, b)} = b$.

$$(\gcd(48, 12) = 12)$$

Rec GCD (a,b) // input pos ints a+b, a > b.

If (a mod b = 0)

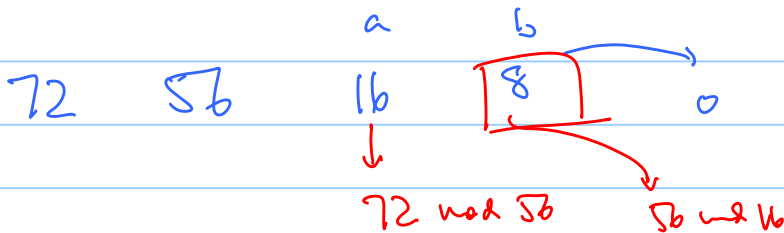
Return (b).

Else

Return (Rec GCD (b, a mod b))

End.

Find gcd (72, 56) = 8



$$s \cdot 259 + t \cdot 77 = 7$$

Find $\gcd(259, 77) = 7$

$$\begin{array}{cccccc} 259 & & 77 & & 28 & 21 & (7) & 0 \\ & & \cdot & & & & & \\ & & & & & & & \\ & & & & 259 & \leftarrow & 77 & \end{array}$$

Theorem Let a, b be two positive integers. Then there are two integers s and t such that

$$s \cdot a + t \cdot b = \gcd(a, b).$$

$$\gcd(72, 56)$$

$$n = d \cdot q + r \quad r = n - d \cdot \underline{q}$$

↓
(n div d)

$$\begin{array}{cccc} \underline{72} & \underline{56} & \underline{16} & \underline{8} \\ & & \downarrow & \downarrow \\ & & & \boxed{8} = 56 - 3 \cdot 16 \quad \textcircled{1} \\ & & & \\ & & \underline{16} = 72 - 56 \quad \textcircled{2} & \end{array}$$

$56 \text{ div } 16$
↓

$$\textcircled{1} \quad 8 = 56 - 3 \cdot \frac{16}{4}$$

$$56 = 3(72 - 56)$$

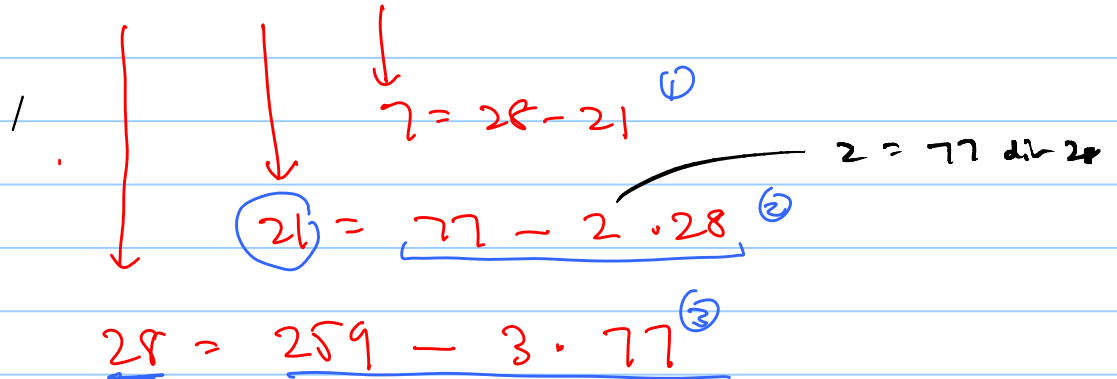
$$= 56 - 3 \cdot 72 + 3 \cdot 56$$

$$= \underbrace{(-3)}_s 72 + \underbrace{4}_t 56$$

Back to 259 and 77:

$$7 = 3 \cdot 259 + (-10) \cdot 77$$

259 77 28 21 7 0



$$\begin{aligned} 7 &= 28 - 21 \\ &= 28 - (77 - 2 \cdot 28) = 28 - 77 + 2 \cdot 28 \\ &= -77 + 3 \cdot 28 \\ &= -77 + 3(259 - 3 \cdot 77) \\ &= 3 \cdot 259 - 10 \cdot 77 \end{aligned}$$