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.

Euclids 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.

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

(smaller than b. $0 \ldots b-1$

$\Rightarrow$ Recursion!

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

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

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

    If ( a mod b = 0 )
          Return (b).
    Else
          Return ( RecGCD (b, a mod b) )
End.
```

Find $\gcd(72, 56) = 8$

		a	b	
72	56	16	$\boxed{8}$	0
		72 mod 56		56 mod 16

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

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

$259 \quad 77 \quad 28 \quad 21 \quad 7 \quad 0$

$259 \, -e \, 77$

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

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

$\gcd(72, 56)$

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

$\downarrow$

$(n \text{ div } d)$

$\underline{72} \quad \underline{56} \quad \underline{16} \quad \underline{8}$

56 div 16

$\boxed{8} = 56 - 3 \cdot 16$ ①

$\underline{16} = 72 - 56$ ②

① $8 = 56 - 3 \cdot 16$

$56 - 3(72 - 56)$

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

$= \underbrace{(-3)}_{s} 72 + \underbrace{4}_{t} (56)$

Back to 259 and 77:

$$\boxed{7 = \overset{3}{s} \cdot 259 + \overset{-10}{t} \cdot 77}$$

259 77 28 21 7 0

$7 = 28 - 21$ ①

$2 = 77 \text{ div } 28$

$21 = \underline{77 - 2 \cdot 28}$ ②

$\underline{28} = \underline{259 - 3 \cdot 77}$ ③

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