GCD's w/ recursion.

for $a, b \in \mathbb{Z}$, $\gcd(a,b) =$

$$\max\{d \in \mathbb{Z} \mid d|a \neq d|b\}$$

$(d|a \iff \exists q \in \mathbb{Z} \text{ s.t. } a = dq)$

in C++: $a \,\%\, d == 0$

Observation: Let $r = a \,\%\, b$ (remainder of a/b)

$(d|a \neq d|b) \iff d|r$

So, {common divisors of a,b} =

{common divisors of b, r} ⊗

Recall the "division algorithm":

$\forall a, b \in \mathbb{Z}^+, \exists q, r \in \mathbb{Z}^+, r \lneq b$ s.t. $a = qb + r$

("for all" ↑, "there exists" ↑)

(in C++, $q = a/b$, $r = a \,\%\, b$)

(of observation)

Proof: suppose $d|a \neq d|b$.

$\exists q_a, q_b \in \mathbb{Z}$ s.t. $a = dq_a$, $b = dq_b$.

From division algo:

$a = qb + r$, $r \lneq b$.

$dq_a = qdq_b + r$

$d(q_a - q q_b) = r$. $\therefore$ $d \mid r$. ✓

Conversely, if $d \mid b$ & $d \mid r$, then $d \mid a$:

$b = dq_b$, $r = dq_r$ for some $q_b, q_r \in \mathbb{Z}$.

So, $a = qb + r = qdq_b + dq_r$

$= (qq_b + q_r)d$

$\therefore$ $d \mid a$. ✓

How to turn the observation into a program?

Note: $r < b$, & $\gcd(a,b) = \gcd(b,r)$

(getting smaller!)

What if $b = 0$? $\gcd(a,0) = a$.

Finally, a program:

```
int gcd(int a, int b)
{   if (b == 0) return a;
    return gcd(b, a%b);
}
```

Example traces:

$\gcd(12, 18) = \gcd(18, 12)$

$= \gcd(12, 6)$

$= \gcd(6, 0) = 6$ (base case)

Merge sort:

High level sketch:

```
void sort(int* A, int n)
{
    if (n < 2) return;
    int mid = n/2;
    sort(A, mid);
    sort(A+mid, n-mid);
    merge(A, mid, A+mid, n-mid);
}
```

think of the 2 decks of cards analogy...

Exercise: figure out how to write merge...