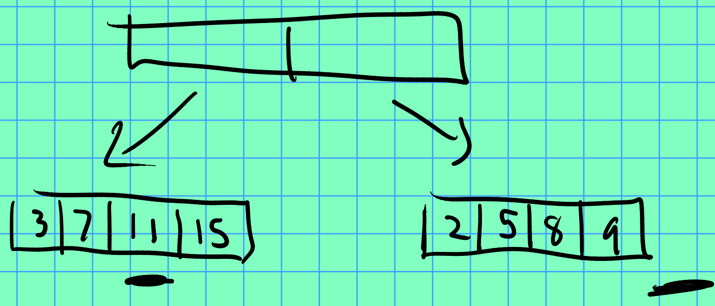
Question about merge (see lectures/18/)



2 3 5 7 8 9 11 15 ✓

More practice w/ recursion.

GCD(a,b) = greatest common divisor of a + b.

Division algorithm: $\forall\ a, b \in \mathbb{Z}_{\geq 0}$ $\exists\ q, r \in \mathbb{Z}_{\geq 0}$

s.t. $a = qb + r$

+ $r \lneq b$.

$\mathbb{Z}$ = integers

$\mathbb{Z}_{\geq 0}$ = non-negative integers.

$\forall$: "for all"

$\exists$: "there exists"

E.g. $a = 8,\ b = 3 \Longrightarrow q = 2,\ r = 2$

$$\left(\underset{a}{8} = \underset{q}{2} \cdot \underset{b}{3} + \underset{r}{2}.\right)$$

in C++: what is q? a/b.

what is r? a%b.

Claim: common divisors of $\{a, b\}$

= common divisors of $\{b, r\}$.

Proof: (Aside: to prove two sets ^{A,B} are equal, a nice way is to show $A \subseteq B$ & $B \subseteq A$.)

$\Rightarrow$ $d \mid a$ & $d \mid b$. ($d \mid a \Leftrightarrow \exists k \in \mathbb{Z}$ s.t. $a = kd$)

from the div. algo, $\exists q, r$ (w/ $r \lneq b$) s.t.

$$a = qb + r$$

$$k_a d = q d k_b + r$$

So, $r = (k_a - q k_b) d$

$\therefore$ $d \mid r$. ✓

Now $\Leftarrow$ $d \mid b$ & $d \mid r$.

Then $a = q d k_b + d k_r$

$= d(q k_b + k_r)$

So $d \mid a$. ✓

Therefore, common divisors of $\{a, b\}$ are the same as common divisors of $\{b, r\}$.

In particular, $\underline{\gcd(a,b) = \gcd(b,r)}$.

Now for a recursive algorithm...

Recall the high level strategy:

1. base case
2. Assume the thing works for all smaller inputs, & build sol'n to the input you're given.

```
int gcd(int a, int b) {
    if (a%b == 0) return b;
    // note: size of input ≡ second # (b)
    return gcd(b, a%b);
}
```

Example trace:

$$(8, \underline{12}) \longrightarrow (12, \underline{8}) \longrightarrow (8, \underline{4}) \longrightarrow \text{return } 4. \checkmark$$

size   size   size

Now the <u>extended</u> gcd:

<u>Fact</u>: $\gcd(a,b) = ua + vb$
where $u, v \in \mathbb{Z}$

Example: $a=8$, $b=12$. Then
$$\gcd(8,12) = 4 = -1\cdot 8 + 1\cdot 12$$

Question: how to find u & v?

```
int xgcd(int a, int b, int& u, int& v);
```

inputs

outputs