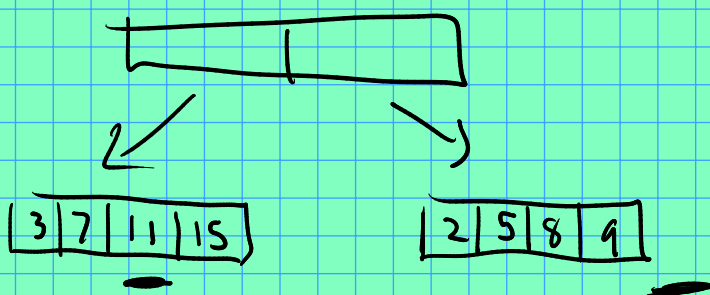


Question about merge (see lectures/18/)



2 3 5 7 8 9 11 15 ✓

more practice w/ recursion.

$\text{GCD}(a, b)$ = 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.
 $a = qb + r$
 $r \leq b$
 $r \neq b$

\mathbb{Z} = integers
 $\mathbb{Z}_{\geq 0}$ = non-negative integers.
 \forall = "for all"
 \exists = "there exists"

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

$$\begin{pmatrix} 8 = 2 \cdot 3 + 2 \\ a \quad q \quad b \quad r \end{pmatrix}$$

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 $A \overset{A \subseteq B}{B}$ are equal, a nice way is to show $A \subseteq B$ + $B \subseteq A$.)

$$\S \quad d|a \neq d|b. \quad \left(d|a \Leftrightarrow \exists k \in \mathbb{Z} \text{ s.t. } a = kd \right)$$

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

$$a = qb + r$$

$$kd = qdk_b + r$$

$$\text{so, } r = (ka - qk_b)d$$

$$\therefore d|r. \quad \checkmark$$

Now $\S \quad d|b \neq d|r$.

$$\begin{aligned} \text{Then } a &= qdk_b + dk_r \\ &= d(qk_b + k_r) \end{aligned}$$

$$\text{So } d|a. \quad \checkmark$$

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

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

Now for a recursive algorithm...

Recall the high level strategy:

- ① base case
- ② Assume the thing works for all smaller inputs, + build soln 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:

$(\underbrace{8, 12}_{\text{size}}) \rightarrow (\underbrace{12, 8}_{\text{size}}) \rightarrow (\underbrace{8, 4}_{\text{size}}) \rightarrow \text{return } 4. \checkmark$

Now the extended gcd:

Fact: $\gcd(a, b) = ua + vb$
 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 $u \neq v$?

$\text{int } \&\text{xgcd}(\text{int } a, \text{int } b, \text{int } \&u, \text{int } \&v);$

Diagram illustrating the inputs and outputs of the `xgcd` function:

- Inputs: `a` and `b` (pointed to by arrows from the label "inputs").
- Outputs: `u` and `v` (pointed to by arrows from the label "outputs").
- The return value is `&xgcd` (pointed to by an arrow from the label "return").