We can use these results to give a fast algorithm for finding $\gcd(a,b)$.

Idea:
- first assume $a \geq b$ (by swapping a and b if necessary).
- if $b \mid a$, then $\gcd(a,b) = b$.
- if $b \nmid a$, then divide a by b and let r be the remainder. Then $\gcd(a,b) = \gcd(b,r)$. We replace a, b with b, r, and repeat.

Example 1: What is $\gcd(68, 20)$?

- $68 = \underset{\substack{\uparrow \\ q}}{3} \times 20 + \underset{\substack{\uparrow \\ r}}{8}$, so $\gcd(68,20) = \gcd(20,8)$.
- $20 = 2 \times 8 + 4$, so $\gcd(20,8) = \gcd(8,4)$.
- $4 \mid 8$, so $\gcd(8,4) = 4$.

Example 2: What is $\gcd(76, 33)$?
- $76 = 2 \times 33 + 10$, so $\gcd(76,33) = \gcd(33,10)$.
- $33 = 3 \times 10 + 3$, so $\gcd(33,10) = \gcd(10,3)$.
- $10 = 3 \times 3 + 1$, so $\gcd(10,3) = \gcd(3,1)$.
- $1 \mid 3$, so $\gcd(3,1) = 1$.

Example 3: What is $\gcd(2904, 1001)$?
- $2904 = 2 \times 1001 + 902$, so $\gcd(2904, 1001) = \gcd(1001, 902)$.
- $1001 = 1 \times 902 + 99$, so $\gcd(1001, 902) = \gcd(902, 99)$.
- $902 = 9 \times 99 + 11$, so $\gcd(902, 99) = \gcd(99, 11)$.
- $11 \mid 99$, so $\gcd(99, 11) = 11$.

Now we give a precise algorithm:

> Euclid's algorithm for finding $\gcd(a,b)$:
>
> input: $a, b \in \mathbb{N}$ with $a \geq b$.
> - if $b \mid a$, then output b and stop.
> - if $b \nmid a$, then find $q, r \in \mathbb{Z}$ such that $0 < r < b$ and $a = qb + r$.
>
>   Replace a, b with b, r, and repeat.

4.4 Lowest common multiple

Defn: Suppose $a, b \in \mathbb{N}$. The <u>lowest common multiple</u> of a and b is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

We write $\mathrm{lcm}(a,b)$ for the lowest common multiple.

e.g.

- $\mathrm{lcm}(5,9) = 45$.
- $\mathrm{lcm}(40,60) = 120$.
- $\mathrm{lcm}(4000,6000) = 12000$
- $\mathrm{lcm}(10,12) = 60$.
- $\mathrm{lcm}(a,1) = a$ for every a
- $\mathrm{lcm}(a,a) = a$ for every a.
- if $b \mid a$, then $\mathrm{lcm}(a,b) = a$.

How do we find $\mathrm{lcm}(a,b)$? Our aim is to find a relationship between $\mathrm{lcm}(a,b)$ and $\gcd(a,b)$.

Let $m = \mathrm{lcm}(a,b)$. Then

$m, 2m, 3m, 4m, \ldots$

are all multiples of a and b. In fact, these are the only common multiples of a and b:

Lemma 4.7: Suppose $a, b \in \mathbb{N}$, and let $m = \mathrm{lcm}(a,b)$. If $n \in \mathbb{N}$ such that $a \mid n$ and $b \mid n$, then $m \mid n$.

Pf: By Lemma 4.5, we can find q, r such that

$$n = qm + r \quad \text{and} \quad 0 \le r < m.$$

We need to show that $r = 0$. Suppose for a contradiction that $r > 0$.

We know $a \mid m$ and $a \mid n$, so there are $k, l \in \mathbb{N}$ such that $m = ak$, and $n = al$. So

$r = n - qm = a(l - qk)$, so

$a \mid r$. Similarly $b \mid r$. So r is a common multiple of a and b, and $r < m$. But m is the smallest common multiple of a and b. $\lightning$. So $r = 0$.

$\square$

e.g. Suppose $a = 8$, $b = 12$.

multiples of 8: $8, 16, 24, 32, 40, 48, 56, 64, 72, \ldots$

multiples of 12: $12, 24, 36, 48, 60, 72, \ldots$

The lcm of 8 and 12 is 24.

The common multiples of 8 and 12 are

$24, 48, 72, \ldots$,

i.e. <u>the multiples of 24.</u>

Theorem 4.8: Suppose $a, b \in \mathbb{N}$. Then

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}.$$