Last time:

Let $a, b \in \mathbb{Z}$. We say that b divides a if a is a multiple of b, i.e.

$$a = bk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } b|a.$$

If b does not divide a, then we write $b \nmid a$. LaTeX: \nmid

The divisors as the integers that divide a.

Examples:

$$-15|60 \quad \text{since} \quad 60 = (-15) * (-4);$$

$$15 \nmid 25 \quad \text{since there is no } k \in \mathbb{Z} \text{ such that } 25 = 15 \cdot k.$$

In general, for any non-zero $a \in \mathbb{Z}$,

$$\pm a|a, \quad \pm 1|a, \quad a|0 \quad \text{and } 0 \nmid a.$$

For two numbers $a, b \in \mathbb{Z}_{>0}$, a common divisor d is a divisor common to both numbers, i.e. $d|a$ and $d|b$.

For example,

3 is a divisor of 30, but not 40;
4 is a divisor of 40, but not 30;
1, 2, 5, and 10 are all common divisors of 30 and 40.

The greatest common divisor of a and b, denoted $\gcd(a, b)$ is largest integer that divides both a and b. Ex: $\gcd(30, 40) = 10$.

Claims:

1. $\gcd(a, b) = \gcd(b, a)$.
2. If $b|a$, then $\gcd(a, b) = b$.

If $\gcd(a, b) = 1$, we say that a and b are relatively prime.

Example: The divisors of 25 are $\pm 1, \pm 5$, and ± 25; the divisors of 12 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$, and ± 12; so 25 and 12 are relatively prime (even though neither is prime).

To compute the GCD of a and b...

Method 1: Compute all the divisors of a and b, and compare.

(VERY inefficient)

Method 2:

Compute the prime factorizations, and take their "intersection".

Example:

$$19500 = 2^2 * 3 * 5^3 * 13 \quad \text{and} \quad 440 = 2^3 * 5 * 11,$$

$$\text{so} \quad \gcd(19500, 400) = 2^2 * 5 = \boxed{20}$$

(i.e. $\gcd(a, b)$ is the product of primes p to the highest power n s.t. $p^n|a$ and $p^n|b$).

Not *computationally* efficient either, since prime factorization is computationally difficult/not possible without a list of primes.

Method 3: The Euclidean algorithm.

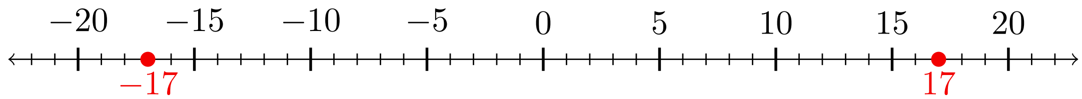
First, we'll need the division algorithm (book: division lemma), which says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."

Ex: if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

Ex: if $a = -17, b = 5$, then $q = -4$ and $r = 3$ since $-17 = 5 * (-4) + 2$.



Proof: (sketch)

Case 1: If a and b are the same sign, subtract b from a until the result is between 0 and $|b| - 1$. The result is r and the number of subtractions is q.

Case 2: If they're different signs, add b to a until the result is between 0 and $|b| - 1$. The result is r and the number of additions is $-q$.

We have

if $a = 17, b = 5$, then $q = 3$ and $r = 2$ since $17 = 5 * 3 + 2$.

If $a_2 = 5, b_2 = 2$, then $q_2 = 2$ and $r_2 = 1$ since $5 = 2 * 2 + 1$.

And if $a_3 = 2, b_3 = 1$, then $q_3 = 2$ and $r_3 = 0$ since $2 = 2 * 1 + 0$.

Notice: $\gcd(17, 5) = 1$.

Play this game again with new a and b:

1. Start with $a_1 = a$ and $b_1 = b$.
2. Compute the quotient q_i and remainder r_i in dividing a_i by b_i.
3. Repeat the division algorithm using $a_i = b_{i-1}$ and $b_i = r_{i-1}$.
4. Iterate until you get $r_n = 0$.
   Then compare $\gcd(a, b)$ with r_{n-1}.

For practice: Do this process with $a = 30$, $b = 12$, and then with $a = 84$, $b = 30$.

Claim: If n is the first time that $r_n = 0$, then $r_{n-1} = \gcd(a, b)$.
Note that if $r = 0$ in the first step, then $b|n$, so $\gcd(a, b) = b$.

Why does $r_{n-1} = \gcd(a, b)$?

In general, our process looks like

$$\begin{array}{rcrcll}
\overset{r_{-1}}{\cancel{a}} & = & \overset{r_0}{\cancel{b}} * q_1 & + & r_1 & \\
\overset{r_0}{\cancel{b}} & = & r_1 * q_2 & + & r_2 & \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
 & \vdots & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}$$

To make everything look the same, let $r_{-1} = a$ and $r_0 = b$. So every line comes in the form

$$r_{i-2} = r_{i-1} * q_i + r_i.$$

Why does $r_{n-1} = \gcd(a, b)$?

Let $r_{-1} = a$ and $r_0 = b$, so that the algorithm looks like

$$\begin{array}{rcrcll}
r_{-1} & = & r_0 * q_1 & + & r_1 & \\
r_0 & = & r_1 * q_2 & + & r_2 & \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
 & \vdots & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a, b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}$$

Last line: $r_{n-2} = r_{n-1} q_n$.

So

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} = (r_{n-1} q_n) q_{n-1} + r_{n-1} = r_{n-1}(q_n q_{n-1} + 1).$$

Then

$$\begin{aligned} r_{n-4} = r_{n-3} q_{n-2} + r_{n-2} &= r_{n-1}(q_n q_{n-1} + 1) q_{n-2} + r_{n-1} q_n \\ &= r_{n-1}(q_n q_{n-1} q_{n-2} + q_{n-2} + 1). \end{aligned}$$

And so on...

Why does $r_{n-1} = \gcd(a, b)$?

Example: We have

$$84 = 30 * 2 + 24$$
$$30 = 24 * 1 + 6$$
$$24 = 6 * 4 + 0. \qquad r_{n-1} = 6$$

So

$$30 = 24 * 1 + 6 = (6 * 4) * 1 + 6 = 6(4 * 1 + 1) = 6 * 5$$
$$84 = 30 * 2 + 24 = (6 * 5) * 2 + (6 * 4) = 6(5 * 2 + 4) = 6 * 24.$$

So 6 is a common divisor of 84 and 30.

For $a = 100$, $b = 36$:

$$100 = 36 * 2 + 28$$
$$36 = 28 * 1 + 8$$
$$28 = 8 * 3 + 4$$
$$8 = 4 * 2 + 0. \qquad r_{n-1} = 4$$

So

$$28 = 8 * 3 + 4 = (4 * 2) * 3 + 4 = 4(2 * 3 + 1) = 4 * 7$$
$$36 = 28 * 1 + 8 = (4 * 7) * 1 + (4 * 2) = 4(7 * 1 + 2) = 4 * 9$$
$$100 = 36 * 2 + 28 = (4 * 9) * 2 + (4 * 7) = 4(9 * 2 + 7) = 4 * 25.$$

So 4 is a common divisor of 100 and 36.

You try: use the following computations, working backwards, to show that 2 is a common divisor of 100 and 26:

$$100 = 26 * 3 + 22 \qquad 26 = 22 * 1 + 4$$
$$22 = 4 * 5 + 2 \qquad 4 = 2 * 2 + 0$$

Why does $r_{n-1} = \gcd(a,b)$?

Letting $r_{-1} = a$ and $r_0 = b$, and computing

$$\begin{array}{rcccll}
r_{-1} & = & r_0 * q_1 & + & r_1 & \\
r_0 & = & r_1 * q_2 & + & r_2 & \\
r_1 & = & r_2 * q_3 & + & r_3 & \\
 & \vdots & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow \gcd(a,b)? \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow r_n
\end{array}$$

we can reverse this process to show that r_{n-1} is, at the very least, a *common divisor* to $a = r_{-1}$ and $b = r_0$.

Wait! How do we know we ever get 0??

The division algorithm ensures that each remainder is strictly smaller than the last, and always non-negative:

$$b = r_0 > r_1 > r_2 > \cdots \geqslant 0.$$

So since the r_i's are all *integers*, this process ends at some point.

Why does $r_{n-1} = \gcd(a,b)$?

We have that r_{n-1} is a common divisor to a an b. Now why is it the *greatest* common divisor?

Suppose d is a common divisor of a and b, i.e. $d|a$ and $d|b$. This means

$$a = d\alpha \quad \text{and } b = d\beta \quad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Back to our division calculation, and substitute these equations in:

$$\begin{array}{rcccll}
d\alpha & = & d\beta * q_1 & + & r_1 & \text{so } r_1 = d(\alpha - \beta q_1) = dm_1 \\
d\beta & = & dm_1 * q_2 & + & r_2 & \text{so } r_2 = d(\beta - m_1 q_2) = dm_2 \\
dm_1 & = & dm_2 * q_3 & + & r_3 & \text{so } r_3 = \cdots = dm_3 \\
 & \vdots & & & & \\
dm_{n-3} & = & dm_{n-2} * q_{n-1} & + & r_{n-1} & \text{so } \boxed{r_{n-1} = \cdots = dm_{n-1}} \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 &
\end{array}$$

So d is a divisor of r_{n-1}. In particular, since $r_{n-1} > 0$, we have

$$d | r_{n-1} \quad \textit{and} \quad d \leqslant r_{n-1}.$$

In other words, r_{n-1} is a common divisor to a and b, *and* any other common divisor is less than or equal to r_{n-1}.

Theorem (Euclidean algorithm). To compute $\gcd(a, b)$, let $r_{-1} = a$ and $r_0 = b$, and compute successive quotients and remainders

$$r_{i-2} = r_{i-1}q_i + r_i$$

for $i = 1, 2, 3, \ldots$, until some remainder r_n is 0. The last nonzero remainder r_{n-1} is then the greatest common divisor of a and b.

(This takes at most b steps (actually less), and is *much* more computationally efficient than the other methods.)

Proof technique: The definition of greatest common divisor is an "and" statement:

$$\gcd(a, b) = d \Leftrightarrow ((d|a \wedge d|b) \wedge (\delta|a \wedge \delta|b \Rightarrow \delta \leqslant d)).$$

So to show that $\gcd(a, b) = d$, you show that (1) d is a common divisor of a and b; and (2) if δ is a common divisor of a and b, then $\delta \leqslant d$.

Claim (on homework): For any non-zero $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$, i.e. $\gcd(a, b)$ is an integral combination of a and b.

Theorem. For any non-zero $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by.$$

Corollary (Euclid's Lemma). Suppose that n, a, and b are non-zero integers. If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.

You think: Analyze this theorem.

(Examples, non-examples, similar theorems, etc.)

Proof. Since $n|ab$, we have [ ].

Since $\gcd(n, a) = 1$, we have [ ].

...Conclusion: we have [ ]. □

Theorem. For any non-zero $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that
$$\gcd(a,b) = ax + by.$$

Corollary (Euclid's Lemma). Suppose that n, a, and b are non-zero integers. If $n|ab$ and $\gcd(n,a) = 1$, then $n|b$.

You think: Analyze this theorem.

(Examples, non-examples, similar theorems, etc.)

Proof. Since $n|ab$, we have $\boxed{ab = kn \text{ for some } k \in \mathbb{Z}}$.
Since $\gcd(n,a) = 1$, we have $\boxed{nx + ay = 1 \text{ for some } x, y \in \mathbb{Z}}$.
So

$$b = b \cdot 1 = b(nx + ay) = nbx + (ab)y = nbx + nky = n(bx + ky).$$

So since $bx + ky \in \mathbb{Z}$, we have $\boxed{b = \ell n \text{ for some } \ell \in \mathbb{Z}}$. □

You try: Let a and b be non-zero integers. Outline proofs of the following claims.

1. If δ is a common divisor of a and b, then $\delta | \gcd(a,b)$.
2. We call $\ell \in \mathbb{Z}$ a common multiple of a and b if $a|\ell$ and $b|\ell$. The smallest (positive) such ℓ is called the *least common multiple* of a and b, denoted $\operatorname{lcm}(a,b)$. For example, $\operatorname{lcm}(12, 66) = 132$.
   - (i) If $a|m$ and $b|m$, then $\operatorname{lcm}(a,b)|m$.
   - (ii) For any $r \in \mathbb{Z}$, $\operatorname{lcm}(ra, rb) = r \operatorname{lcm}(a,b)$.