Welcome to Math 127

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, you may turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 2.3–2.4.
- Reading for Wed Feb 02: 2.5–2.6.
- COVID Safety HW and PS00 due today.
- PS01 outline due Wed Feb 02, full version due Mon Feb 07.
- First problem session Fri Feb 04, 10:00–noon on Zoom.

No noon-1pm office hour today; two of you please stay afterwards and I'll talk with you for 5 min

Another reason definitions are important

Precise definitions make it possible to prove theorems. (See 1.3.1–1.3.4.)

Defn: To say that an integer d divides an integer n means that n=qd where q is an integer.

Theorem

Let k, n be integers. If 5 divides n and 5 divides k, then 5 divides $n + k$.

Proof:

DIRECT PROOF

(A) 5 div n, 5 div k k, n ∈ ℤ

By defn, n = q5, k = t5 (q, t ∈ ℤ)

So n+k = q5 + t5 = 5(q+t) Let v = q+t

So n+k = v5 (v ∈ ℤ)

(C) 5 div n+k

outline of a direct pf

Common divisors and greatest common divisor

Definition

For integers d, a, and b, to say that d is a **common divisor** of a and b means that d divides a and d divides b.

Definition

For integers a and b, at least one of which is not 0, the **greatest common divisor**, or **GCD**, of a and b is exactly what it sounds like: the greatest integer d that is a common divisor of a and b. We denote the greatest common divisor of a and b by the symbol $\gcd(a, b)$.

An example

Example: What is $\gcd(8, 12)$? How do you know?

$\gcd(8,12) = 4$

* Had to be even b/c both 8 and 12 div by 2 (b/c GCD is a multiple of every CD)
* Implied algorithm (that we will later call "naive" alg)
  - Find all divisors of 8
  - See which ones divide 12

Well, actually: If we use "greatest" to mean biggest in terms of absolute value, then gcd is determined exactly up to associates. So we can say:

$\gcd(8,12) = \pm 4$

Motivating problem for Ch. 2

Motivating Problem

Given nonzero integers a and b, how can we efficiently compute $\gcd(a, b)$?

Here's a **naive** algorithm for finding $\gcd(a, b)$. (Naive doesn't necessarily mean bad!)
Let a and b be positive integers.

1. Make an ordered list of positive divisors of a.
2. Check which of those divisors of a also divides b, starting from the largest divisor and going downwards.

The first common divisor found in step 2 will be $\gcd(a, b)$.

How fast or slow is the naive algorithm?

Suppose $a, b \leq n$. (I.e., we fix a maximum size n of integers that we'll consider.)

1. One way to find all positive divisors of a is to consider all d from 1 to a and divide a by d with remainder. This could take up to n divisions.
2. Then for each d in the list of divisors of a, we divide b by d and see if there's a remainder. There are no more than n divisors of a, so again we have no more than n divisions.

So worst-case scenario is $2n$ steps. One step = one division with remainder

Can we beat that speed by an exponential factor?

Motivating Problem

Suppose a, b are positive integers $\leq n$. Can we find an algorithm for computing $\gcd(a, b)$ that is guaranteed to take fewer than $C \log n$ steps, for some constant C?

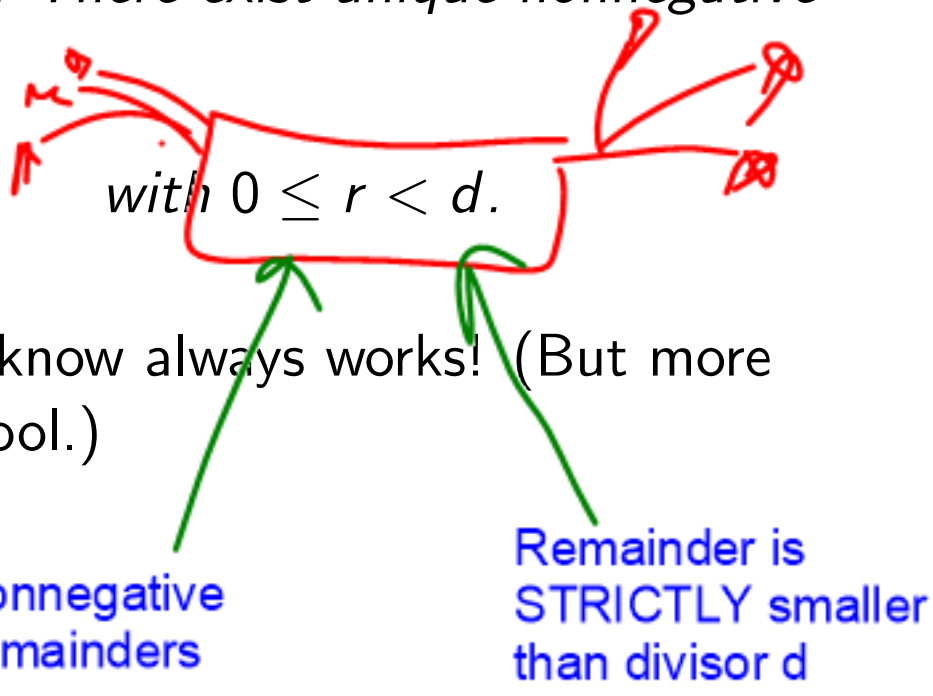
Division with remainder

Remember from elementary school:

Theorem (Division Theorem)

Let a and d be positive integers. There exist unique nonnegative integers q and r such that

$$a = dq + r, \qquad \text{with } 0 \leq r < d.$$



Just restating the fact that you know always works! (But more precisely than in elementary school.)

Signed division

Here's a kind of division with remainder that you probably didn't see in elementary school:

Theorem (Signed Division Theorem)

Let a and d be nonzero integers. There exist integers q and r such that

$$a = dq + r, \qquad \text{with } |r| \leq \frac{|d|}{2}.$$

Allow r<0; but we require that size of r is at most half the size of d.

Proof by example:

a = 215, d = 309. a/d = .696...., so round off to q=1.
Then choose r = a-qd = -94, whose size is less than half the size of d.
(Regular division with remainder would give r=215.)

a = 24, d = 5. a/d=4.8, so round off to q=5.
r = a-qd = 24 - 5(5) = -1, whose size is < |5|/2=2.5.
(Regular div w/ rem gives r=4.)

The Euclidean Algorithm

Suppose a and b are positive integers and $a > b$. To compute $\gcd(a, b)$:

1. *Initialize*. Let $r_{-1} = a$ and $r_0 = b$.
2. *Main loop*. For $i = 1, 2, \ldots,$ apply the Division Theorem to divide r_{i-2} by r_{i-1} with quotient q_i and remainder r_i, or in other words,

$$r_{i-2} = q_i r_{i-1} + r_i \qquad \text{with } 0 \leq r_i < r_{i-1}.$$

   Stop, after N divisions, as soon as you get a remainder $r_N = 0$.
3. *Claim*. The last nonzero remainder r_{N-1} is exactly $\gcd(a, b)$.

The Euclidean Algorithm, written out in a table

$$r_{-1} = q_1 r_0 + r_1 \qquad (0 \le r_1 < r_0)$$

$$r_0 = q_2 r_1 + r_2 \qquad (0 \le r_2 < r_1)$$

$$r_1 = q_3 r_2 + r_3 \qquad (0 \le r_3 < r_2)$$

$$\vdots$$

$$r_{N-4} = q_{N-2} r_{N-3} + r_{N-2} \qquad (0 \le r_{N-2} < r_{N-3})$$

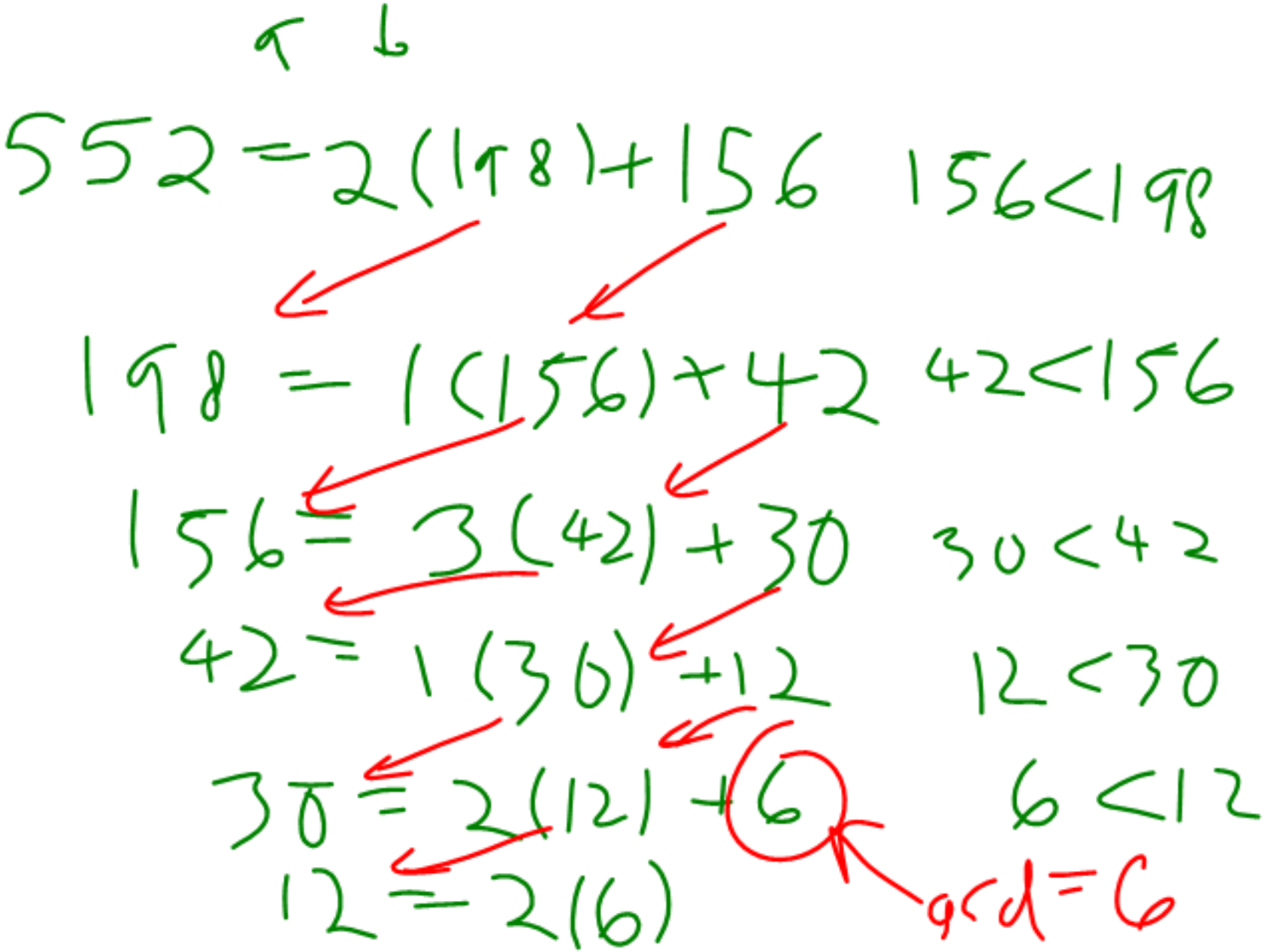
$$r_{N-3} = q_{N-1} r_{N-2} + r_{N-1} \qquad (0 \le r_{N-1} < r_{N-2})$$

$$r_{N-2} = q_N r_{N-1}$$

gcd(a,b)

zero rem

Example: gcd(552, 198)



Precise statement of results

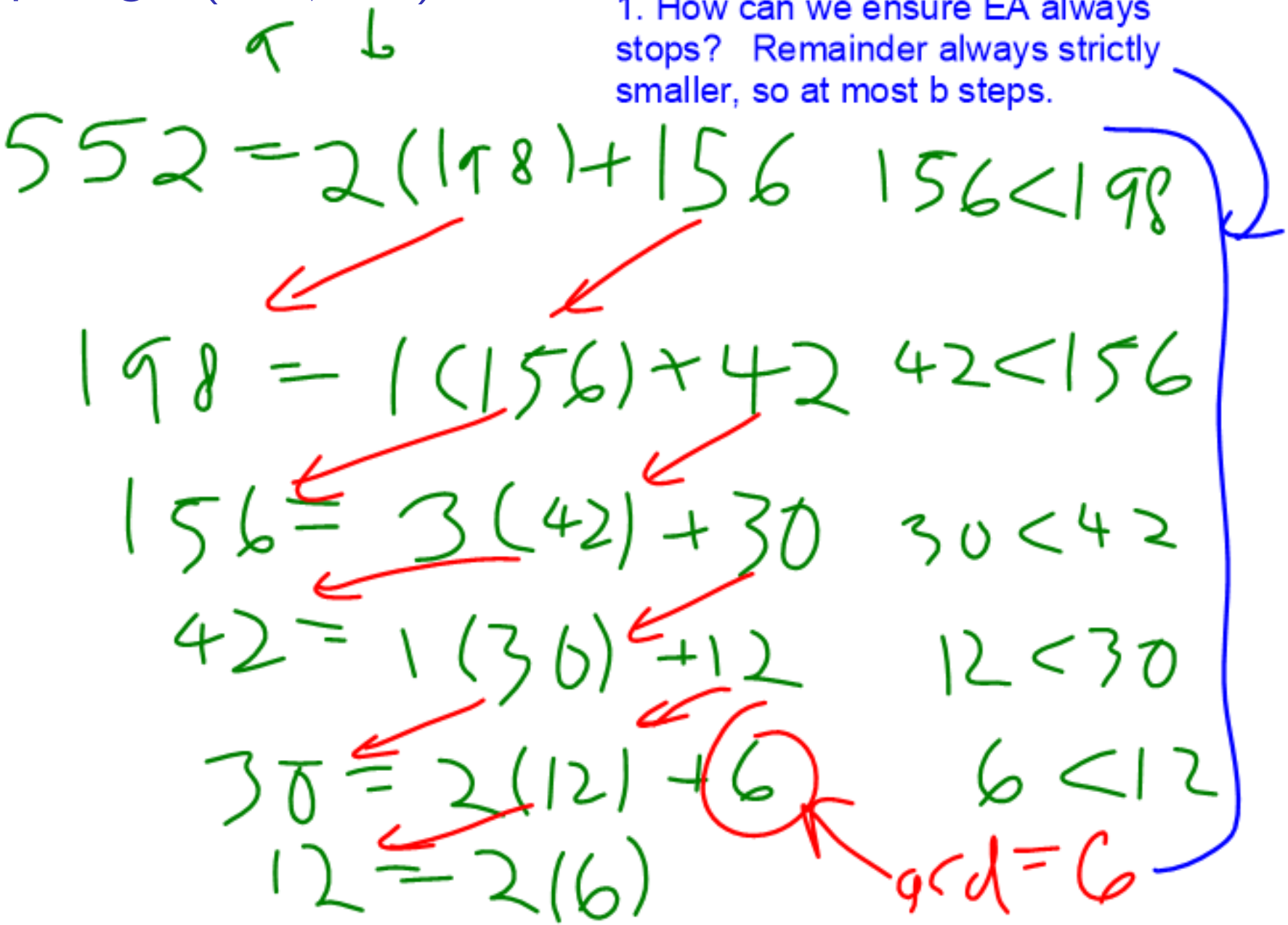
Thm: It is a fact that:

1. The Euclidean Algorithm terminates after finitely many steps, with some final nonzero remainder r_{N-1}.
2. Any common divisor of a and b divides r_{N-1}. (So r_{N-1} is at least as big as any common divisor of a and b.)
3. The last nonzero remainder r_{N-1} divides both a and b. (So r_{N-1} is, in fact, a common divisor of a and b, which means that r_{N-1} is the **greatest** common divisor of a and b.)

Super-non-obvious consequence: Every common divisor of a and b divides $\gcd(a, b)$.

Instead of proving in general, we look at why these facts are true in our specific example.

Example: gcd(552, 198)



Example: gcd(552, 198)