# Welcome to Math 127

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please 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: 2.5–2.6.
- PS00 due today.
- PS01 outline due Wed Feb 03, full version due Mon Feb 08.
- First real problem session Fri Feb 05, 10:00–noon on Zoom.

# Recap: Common divisor, greatest common divisor

$d$ div $a$ means for $q \in \mathbb{Z}$ $a = dq$ ($q$: quot, $d$: 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

How do you know: Tried dividing, 1, 2, 3, 4, nothing else works afterwards.
(E.g., 6 divides 12, but not 8.)

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:

(±1)

gcd(8,12) = ±4

(output prob + 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 $\gcd(a, b)$.

gcd(8,12):

divs of 8: 1, 2, 4, 8

8 doesn't div 12 ✗

4 div 12 ✓

So 4 = gcd(8,12)

(Makes sense to start by listing the divisors of the smaller number, because it seems reasonable that the smaller number might have fewer divisors, or at least you have to check fewer numbers to get all of the divisors.)

# 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.

unit of time = # div w/ 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 $C$?

# digits of n

# 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*

q=quotient r=remainder

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

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

Key: Remainder r is STRICTLY smaller than divisor d.

# 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*

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

Remainder has size at most half the size of divisor.

**Proof by example:**

$a = 102 \quad d = 16$

$\frac{a}{d} = 6.375 \approx 6$

$q = 6 \quad r = a - dq = 6$

$6 \leq \frac{16}{2}$ ✓

$102 = 16(6) + 6$

rounded up to 7

$a=107 \quad d=16 \quad a/d=6.6875 \approx 7$

$q=7 \quad r=107-7(16)=-5$

$|-5| \leq \frac{16}{2}$

$107=7(16)-5$

allowing negative remainders lets you obtain a smaller remainder

# The Euclidean Algorithm

Suppose $a$ and $b$ are positive integers and $a > b$.

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,

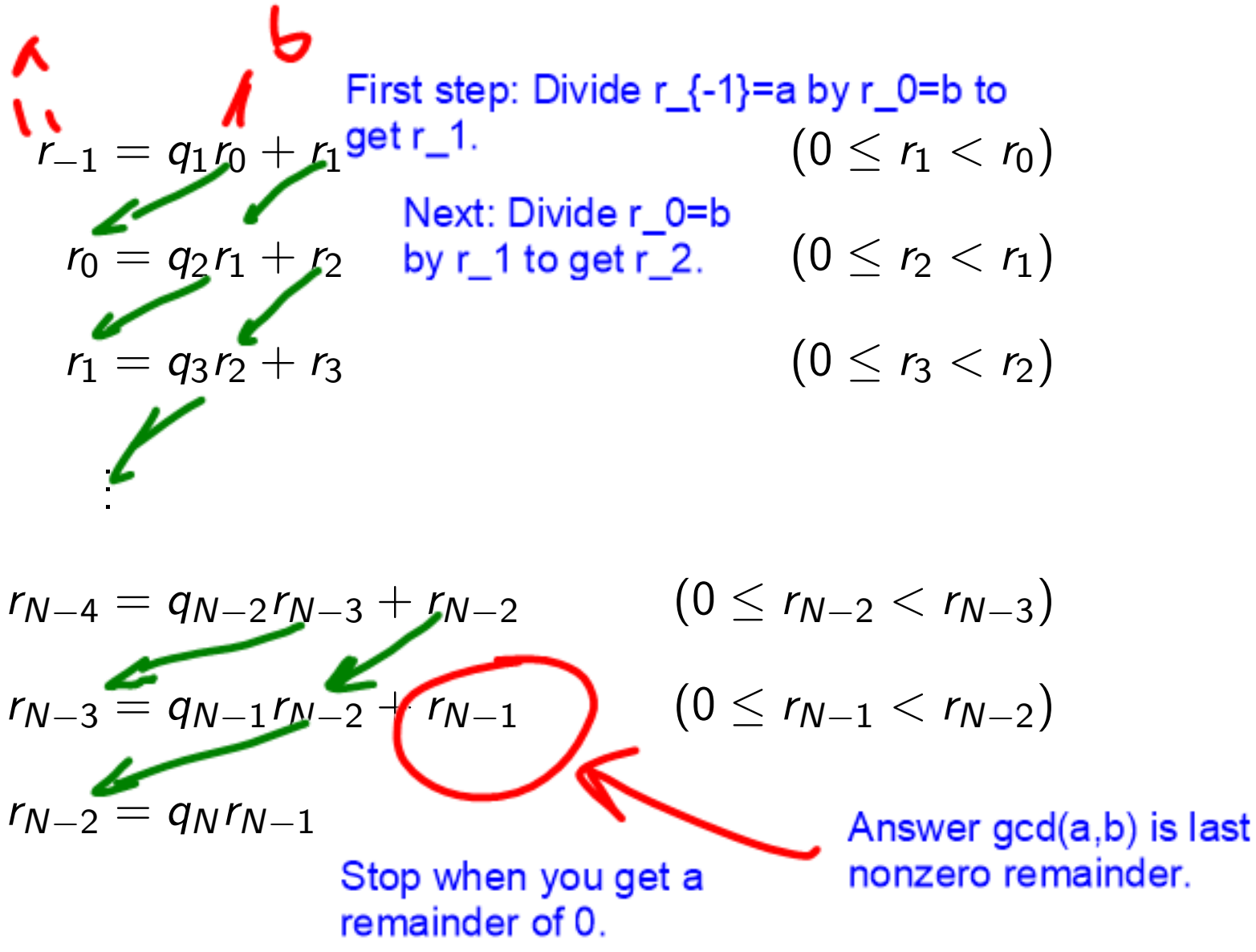
   Divide remainder 2 back by rem 1 back to get new rem.

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

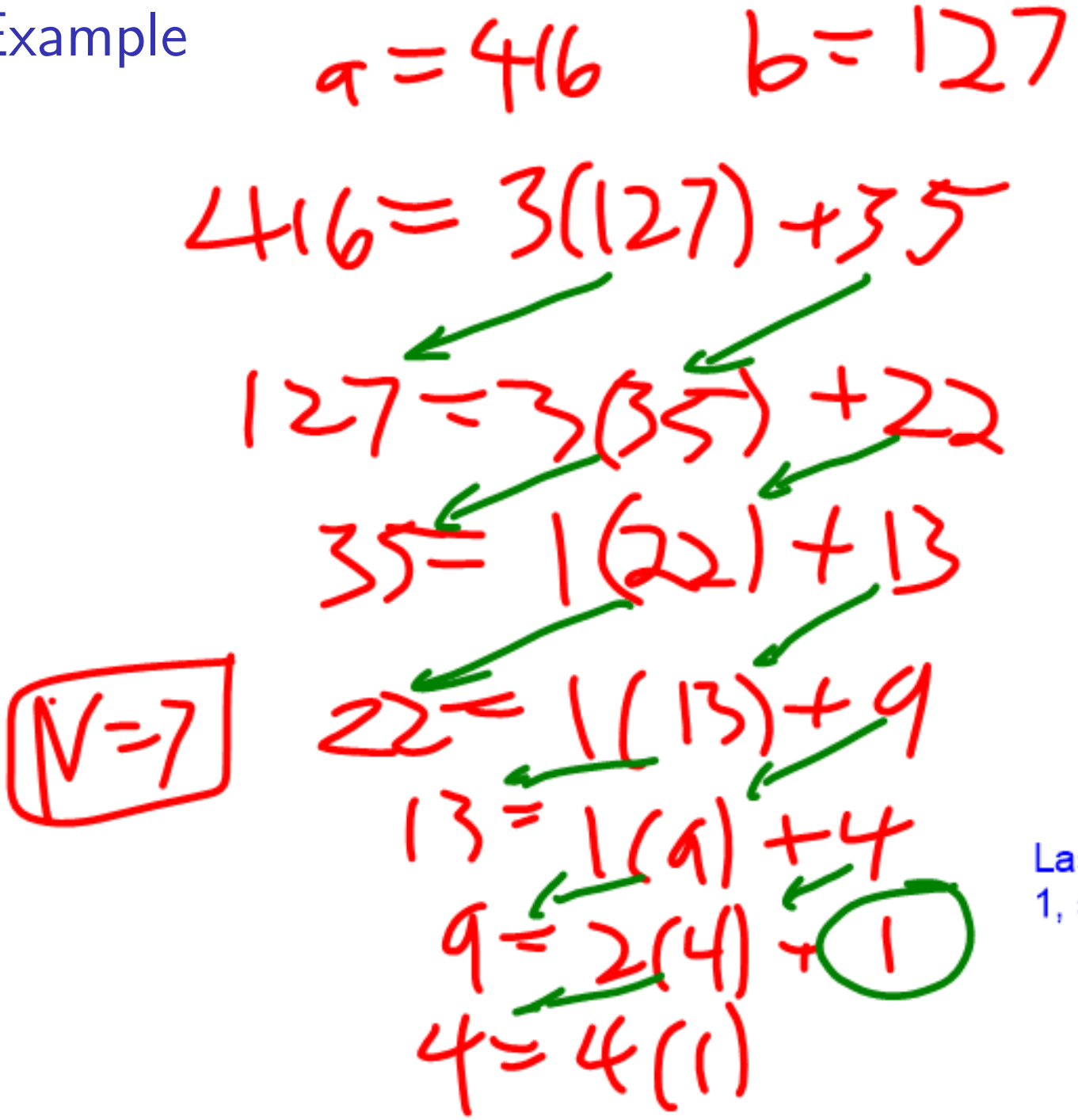
   each new rem smaller

   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



# Example




This is the UNsigned Euclidean algorithm, for which the quotients are always rounded down (like in grade school).

Last nonzero remainder is 1, so gcd(416,127)=1.

# 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 $\gcd(a, b)$.

# Proof that EA terminates

Remainders decrease by at least 1 in each step, so can't take more than r_0=b steps to finish.

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

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

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

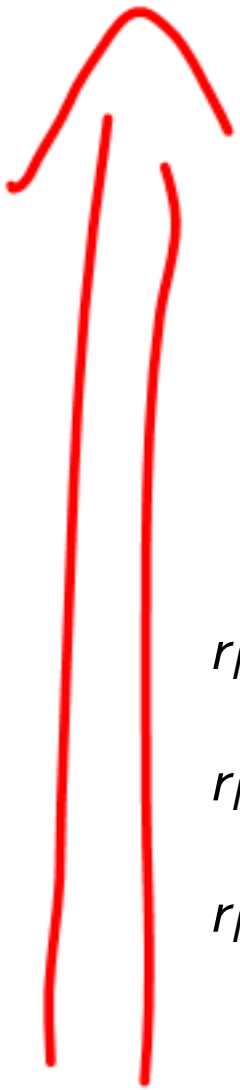
$$\vdots$$

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

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

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

# Proof that $r_{N-1}$ divides $a$ and $b$



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

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

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

$\vdots$

Then: Since r_{N-1} divides both terms on RHS, r_{N-1} divides r_{N-4}.

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

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

Next: Since r_{N-1} divides both terms on RHS, r_{N-1} divides r_{N-3}

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

Start: This shows that r_{N-1} divides r_{N-2}

# Proof that every common divisor divides $r_{N-1}$

Suppose $d$ is a common divisor of $a$ and $b$, i.e., $d$ divides both $a$ and $b$.

$$r_1 = r_{-1} - q_1 r_0$$

$$r_2 = r_0 - q_2 r_1$$

$$r_3 = r_1 - q_3 r_2$$

$$\vdots$$

$$r_{N-3} = r_{N-5} - q_{N-3} r_{N-4}$$

$$r_{N-2} = r_{N-4} - q_{N-2} r_{N-3}$$

$$r_{N-1} = r_{N-3} - q_{N-1} r_{N-2}$$