Objectives

Euclid's Algorithms

Dr. Mattox Beckman

University of Illinois at Urbana-Champaign Department of Computer Science

Your Objectives:

- ▶ Be able to calculate the GCD of two numbers using Euclid's algorithm.
- ▶ Use the extended Euclid's algorithm to solve Linear Diophantine equations.



4 D > 4 D > 4 E > 4 E > E 990

IntroductionEuclid's AlgorithmExtended Euclidean Algorithm
on one of the control of the

Calculating the GCD

- ▶ Let a > b > 0.
- ightharpoonup gcd(a,b) = gcd(b,mod(a,b))
- ► Why?

Calculating the GCD

- ▶ Let a > b > 0.
- ► Why
- Fact 1: if g|a and g|b then g|(a+b) and g|(a-b)
- ► So, we could use gcd(a,b) = gcd(a-b,b)





Introduction Euclid's Algorithm Extended Euclidean Algorithm Introduction Euclid's Algorithm Extended Euclidean Algorithm Occord

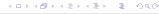
Calculating the GCD

- ▶ Let a > b > 0.
- ightharpoonup gcd(a,b) = gcd(b,mod(a,b))
- ► Why?
- Fact 1: if g|a and g|b then g|(a+b) and g|(a-b)
- ► So, we could use gcd(a,b) = gcd(a-b,b)
- ► That would be slow, so how about gcd(a,b) = gcd(b,a-nb), where n > 0 and a nb > 0 and minimal.

Calculating the GCD

- ▶ Let a > b > 0.
- ightharpoonup gcd(a,b) = gcd(b,mod(a,b))
- ► Why?
- Fact 1: if g|a and g|b then g|(a+b) and g|(a-b)
- ightharpoonup So, we could use gcd(a,b) = gcd(a-b,b)
- ► That would be slow, so how about gcd(a,b) = gcd(b,a-nb), where n > 0 and a nb > 0 and minimal.
- ightharpoonup Easy! Just let n = mod(a, b)





An example

$$\begin{aligned} \gcd(a,b) &= \gcd(b, mod(a,b)) = \gcd(90,25) \\ &= \gcd(25,15) \\ &= \gcd(15,10) \\ &= \gcd(10,5) \\ &= \gcd(5,0) \\ &= 5 \end{aligned}$$

Diophantine Equations

- ▶ A *Diophantine Equation* is a polynomial equation where we are only interested in integer solutions.
- ▶ Linear Diophantine equation: ax + by = 1,
- ► It doesn't have to be 1....
- ▶ Running example: Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?





How to do it

▶ We want: ax + by = g, where g = gcd(a, b). We know a, b, and we calculate g. How can we get x and y?

How to do it

- We want: ax + by = g, where g = gcd(a, b). We know a, b, and we calculate g. How can we get x and y?
- Suppose we had:

$$bx_1 + (a \mod b)y_1 = q$$





IntroductionEuclid's AlgorithmExtended Euclidean AlgorithmIntroductionEuclid's AlgorithmExtended Euclidean Algorithm○○○○○○

How to do it

- We want: ax + by = g, where g = gcd(a, b). We know a, b, and we calculate g. How can we get x and y?
- ► Suppose we had:

$$bx_1 + (a \mod b)y_1 = g$$

► Then take $a \mod b = a - \left| \frac{a}{b} \right| * b$ This gives:

$$bx_1 + (a - \left\lfloor \frac{a}{b} \right\rfloor * b)y_1 = g$$

How to do it

- We want: ax + by = g, where g = gcd(a, b). We know a, b, and we calculate g. How can we get x and y?
- ► Suppose we had:

$$bx_1 + (a \mod b)y_1 = g$$

▶ Then take $a \mod b = a - \lfloor \frac{a}{b} \rfloor * b$ This gives:

$$bx_1 + (a - \left\lfloor \frac{a}{b} \right\rfloor * b)y_1 = g$$

► Rearrange a bit..

$$bx_1 + ay_1 - \left\lfloor \frac{a}{b} \right\rfloor by_1 = g \quad \Rightarrow \quad ay_1 + b(x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1) = g$$





How to do it

- We want: ax + by = g, where g = gcd(a, b). We know a, b, and we calculate g. How can we get x and y?
- ► Suppose we had:

$$bx_1 + (a \mod b)y_1 = q$$

▶ Then take $a \mod b = a - \left| \frac{a}{b} \right| * b$ This gives:

$$bx_1 + (a - \left| \frac{a}{b} \right| * b)y_1 = g$$

► Rearrange a bit..

$$bx_1 + ay_1 - \left| \frac{a}{b} \right| by_1 = g \quad \Rightarrow \quad ay_1 + b(x_1 - \left| \frac{a}{b} \right| y_1) = g$$

► This in turn gives us:

$$\begin{aligned}
 x &= y_1 \\
 y &= x_1 - \left| \frac{a}{b} \right| y_1
 \end{aligned}$$



The Code

$$x = y_1$$

$$y = x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1$$

o// Stolen from Competitive Programming 3

1// store x, y, and d as global variables

2 void extendedEuclid(int a, int b) {

3 if (b == 0) { x = 1; y = 0; d = a; return; }

4 extendedEuclid(b, a % b);

5 // similar as the original gcd

6 int x1 = y;

7 int y1 = x - (a / b) * y;

8 x = x1;

9 y = y1;

10}

◆□▶◆□▶◆■▶◆■▶ ■ 900

An Example

► Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?

а	b	X	y	$a \times x + b \times y = 3$
72	33			
33	6			
6	3			
3	0			

An Example

► Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?

а	b	x	y	$a \times x + b \times y = 3$
72	33			
33	6			
6	3			
3	0	1	0	$3 \times 1 + 0 \times 0 = 3$

An Example

► Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?

а	b	X	y	$a \times x + b \times y = 3$
72	33			
33	6			
6	3	0	1	$6 \times 0 + 3 \times 1 = 3$
3	0	1	0	$3 \times 1 + 0 \times 0 = 3$

An Example

► Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?

а	b	X	y	$a \times x + b \times y = 3$
72	33			
33	6	1	-5	$33 \times 1 + 6 \times -5 = 3$
6	3	0	1	$6 \times 0 + 3 \times 1 = 3$
3	0	1	0	$3 \times 1 + 0 \times 0 = 3$





Introduction	Euclid's Algorithm	Extended Euclidean Algorithm	Introduction	Euclid's Algorithm	Extended Euclidean Algorithn
0	00	00000	0	00	0000

An Example

▶ Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?

а	b	X	y	$a \times x + b \times y = 3$
72	33	-5	11	$72 \times -5 + 33 \times 11 = 3$
33	6	1	-5	$33 \times 1 + 6 \times -5 = 3$
6	3	0	1	$6 \times 0 + 3 \times 1 = 3$
3	0	1	0	$3 \times 1 + 0 \times 0 = 3$

An example, ctd.

- ► Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?
- ► Running the algorithm, we get...

$$72 \times -5 + 33 \times 11 = 3$$

lacktriangle We multiple both sides by 195 (since $585=3\times195$) This gives us...

$$72 \times -975 + 33 \times 2145 = 3$$

An example, ctd.

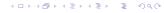
- ► Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?
- ► Running the algorithm, we get...

$$72 \times -5 + 33 \times 11 = 3$$

 \blacktriangleright We multiple both sides by 195 (since $585=3\times195$) This gives us...

$$72 \times -975 + 33 \times 2145 = 3$$

▶ We can add $72(\frac{33}{3})n$ to the 72 term and subtract $33(\frac{72}{3})n$ from the second term and still have a valid equation.



0

Introduction

Euclid's Algorithm

Extended Euclidean Algorithm 0000●

An example, ctd.

- ▶ Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?
- ► Running the algorithm, we get...

$$72 \times -5 + 33 \times 11 = 3$$

lacktriangle We multiple both sides by 195 (since $585=3\times195$) This gives us...

$$72 \times -975 + 33 \times 2145 = 3$$

- ▶ We can add $72(\frac{33}{3})n$ to the 72 term and subtract $33(\frac{72}{3})n$ from the second term and still have a valid equation.
- ► Solve -975 + 11n > 0, this reduces to n > 88.6. So take n = 89.
- ► This gives us the final equation

$$72 \times 4 + 33 \times 9 = 585$$



An example, ctd.

- ▶ Suppose you go to the store. You buy *x* apples at 72 cents each and *y* oranges at 33 cents each. You spend \$5.85. How many of each did you buy?
- ► Running the algorithm, we get...

$$72 \times -5 + 33 \times 11 = 3$$

 \blacktriangleright We multiple both sides by 195 (since $585=3\times195$) This gives us...

$$72 \times -975 + 33 \times 2145 = 3$$

- ▶ We can add $72(\frac{33}{3})n$ to the 72 term and subtract $33(\frac{72}{3})n$ from the second term and still have a valid equation.
- ► Solve -975 + 11n > 0, this reduces to n > 88.6. So take n = 89.

