

# Modular Arithmetic

# Previously, we defined

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

**Def (Divisibility).** We say that  $a$  *divides*  $b$  if there is an integer  $k$  such that

$$b = a \cdot k.$$

We write  $a \mid b$  if  $a$  divides  $b$ . Otherwise, we write  $a \nmid b$ .

**Theorem (The Division Algorithm).** Let  $a$  be an integer and  $d$  a positive integer. Then there are *unique* integers  $q$  and  $r$ , such that  $0 \leq r < d$  and

$$a = dq + r.$$

# GCD is a linear combination

GCD is a linear  
combination

Relative primes

Fundamental  
theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

**Def** (GCD).

**Theorem** (Bezout's Theorem). If  $a$  and  $b$  are positive integers, then there exist integers  $s$  and  $t$  such that

$$\gcd(a, b) = sa + tb.$$

Exmaple:  $\gcd(52, 44) = 4$

$$6 \cdot 52 + (-7) \cdot 44 = 4$$

So called Extended Euclid's algorithm constructs such  $s$  and  $t$ , and so proves the theorem. The algorithm is described in the last section of this lecture.

# Relative primes (co-primes)

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

**Def** (Prime numbers).

**Def** (Relative primes).  $a$  and  $b$  are *relative primes* (or co-primes) if

$$\gcd(a, b) = 1.$$

By Bezout's theorem,  $a$  and  $b$  are co-primes if and only if there exist  $s$  and  $t$  such that

$$sa + tb = 1$$

# Factorization of positive integers

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

**Theorem** (Fundamental theorem of arithmetic). Every positive integer  $n$  can be written in a unique way as a product of primes

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_j \quad (p_1 \leq p_2 \leq \dots \leq p_j)$$

This product is called prime factorization.

See Lehman and Leighton (p. 67) for the proof.

# Modular arithmetic

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

$\dots -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \dots$

What if instead of integers, we deal with  
a finite set of periodically repeating integers?

$\dots 5 \quad 6 \rightarrow 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \rightarrow 0 \quad 1 \dots$

# Modular arithmetic

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

$\dots -2 \quad -1 \quad \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad \quad 7 \quad 8 \dots$

What if instead of integers, we deal with  
a finite set of periodically repeating integers?

$\dots 5 \quad 6 \rightarrow 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \rightarrow 0 \quad 1 \dots$

For example, the days of the week behave in this way.

Mon, Tue, Wed, Thr, Fri, Sat, Sun,

are followed again by Mon, Tue, and so on.

# Modular arithmetic

...5 6  $\rightarrow$  0 1 2 3 4 5 6  $\rightarrow$  0 1...

We want to add, subtract, multiply, and, hopefully, divide such special “integers” ...

$$4 + 4 \text{ is } 1$$

$$2 - 3 \text{ is } 6$$

$$14 \cdot 5 \text{ is } 0$$

$$-7 \text{ is } 0 \text{ is } 7 \text{ is } 14 \text{ is } 21 \dots$$

First, we need to rigorously define, which integers can be called “equal” in such modular arithmetic. We will call them congruent.

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse



# Congruence

**Def.** For a positive integer  $n$ ,  $a$  is *congruent* to  $b$  modulo  $n$  if

$$n \mid (a - b).$$

This is denoted

$$a \equiv b \pmod{n}.$$

Example:

$$8 \equiv 1 \pmod{7}$$

$$15 \equiv 1 \pmod{7}$$

$$8 \equiv 15 \pmod{7}$$

because

$$7 \mid \underbrace{(8-1)}_{=7}, \quad 7 \mid \underbrace{(15-1)}_{=14}, \quad 7 \mid \underbrace{(15-8)}_{=7}.$$

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Congruence

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

**Lemma.** If  $a \equiv b \pmod{n}$ , then exists  $k \in \mathbb{Z}$  s.t.  $a = b + kn$ .

**Lemma.** Two numbers are congruent modulo  $n$  if and only if they have the same remainder when divided by  $n$ .

$$a \equiv b \pmod{n} \quad \text{if and only if} \quad a \bmod n = b \bmod n.$$

Proof: By the division algorithm,

$$a = q_1n + r_1, \quad b = q_2n + r_2.$$

$$a - b = (q_1 - q_2)n + (r_1 - r_2)$$

“ $\Rightarrow$ ”: If  $a \equiv b \pmod{n}$  then  $n \mid (a - b)$ . So  $r_1 - r_2 = 0$ , the remainders are equal.

“ $\Leftarrow$ ”: If  $r_1 = r_2$ , then  $n \mid (a - b)$ , so  $a \equiv b \pmod{n}$ . □

# Congruence

$x$	0	1	2	3	4	5	6	7	8
$x \bmod 3$	0	1	2	0	1	2	0	1	2
$x \bmod 3 = 0$	✓			✓			✓		
$x \bmod 3 = 1$		✓			✓			✓	
$x \bmod 3 = 2$			✓			✓			✓

Integers are divided into 3 congruence classes:

..., 0, 3, 6, 9, 12, ... are congruent modulo 3.

..., 1, 4, 7, 10, 13, ... are congruent modulo 3.

..., 2, 5, 8, 11, 14, ... are congruent modulo 3.

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Modular arithmetic

*Addition, subtraction, and multiplication preserve congruence.*

**Theorem.** if  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then

$$a + c \equiv b + d \pmod{n}.$$

**Theorem.** if  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then

$$ac \equiv bd \pmod{n}.$$

Proof.

Exist  $x, y \in \mathbb{Z}$  such that  $a - b = xn$  and  $c - d = yn$ .

$$ac - bd = (b + xn)(d + yn) - bd = n(xd + by + xny)$$

Thus  $ac \equiv bd \pmod{n}$ .



GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Multiplicative inverse

*What about division?*

**Theorem.** if  $a$  and  $n$  are relative primes, i.e.  $\gcd(a, n) = 1$ , then exists integer  $a^{-1}$  called *multiplicative inverse*, such that

$$aa^{-1} \equiv 1 \pmod{n}$$

Proof.

Exist  $s$  and  $t$ , such that  $sa + tn = 1$ . Therefore,

$$sa - 1 = tn$$

$$sa \equiv 1 \pmod{n}$$

Therefore,  $a^{-1} = s$ .



GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

*Multiplicative inverse*

# Multiplicative inverse

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

**Corollary.** If  $a$  and  $n$  are relative primes, then there exists a *unique* multiplicative inverse  $a^{-1} \in \{1, 2, \dots, n-1\}$  such that

$$aa^{-1} \equiv 1 \pmod{n}.$$

Ok, uniqueness is great, but we need a procedure for finding multiplicative inverses.

# Multiplicative inverse

Find inverse of 101 modulo 4620, that is  $x$  such that

$$101 \cdot x \equiv 1 \pmod{4620}$$

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Multiplicative inverse

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

Find inverse of 101 modulo 4620, that is  $x$  such that

$$101 \cdot x \equiv 1 \pmod{4620}$$

If 101 and 4620 are relative primes:

$$\gcd(101, 4620) = 1,$$

by Bezout's theorem: Exist  $s$  and  $t$  such that

$$101 \cdot s + 4620 \cdot t = \gcd(101, 4620) = 1$$

$$101 \cdot s \equiv 1 \pmod{4620}$$

We have to find Bezout coefficients  $s$  and  $t$ . Then  $s$  is the inverse.



# Recall Euclid's Algorithm

$$a_0 = 4620 = 45 \cdot 101 + 75$$

$$a_1 = 101 = 1 \cdot 75 + 26$$

$$a_2 = 75 = 2 \cdot 26 + 23$$

$$a_3 = 26 = 1 \cdot 23 + 3$$

$$a_4 = 23 = 7 \cdot 3 + 2$$

$$a_5 = 3 = 1 \cdot 2 + 1$$

$$a_6 = 2 = 2 \cdot 1$$

$$a_7 = 1$$

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Extended Euclid's Algorithm

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

The task:

Given two numbers  $a_0 \geq a_1$ , run Euclid's algorithm, computing

$$a_2 = \dots$$

$$a_3 = \dots$$

$\dots$

$$a_k = \gcd(a_0, a_1)$$

In addition, find the coefficients  $x_k$  and  $y_k$  such that

$$a_k = x_k a_0 + y_k a_1$$

We find a recurrent solution for  $x_k$  and  $y_k$ .

# Extended Euclid's Algorithm

Need to find the coefficients  $x_k$  and  $y_k$  such that

$$a_k = \gcd(a_0, a_1) = x_k a_0 + y_k a_1$$

But we compute more than that. We want to represent all  $a_i$  as a linear combination of  $a_0$  and  $a_1$

$$a_0 = x_0 a_0 + y_0 a_1$$

$$a_1 = x_1 a_0 + y_1 a_1$$

$$a_2 = x_2 a_0 + y_2 a_1$$

$$a_3 = x_3 a_0 + y_3 a_1$$

...

$$a_k = \gcd(a_0, a_1) = x_k a_0 + y_k a_1$$

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Extended Euclid's Algorithm

$$a_0 = x_0 a_0 + y_0 a_1$$

$$a_1 = x_1 a_0 + y_1 a_1$$

$$a_2 = x_2 a_0 + y_2 a_1$$

$$a_3 = x_3 a_0 + y_3 a_1$$

...

$$a_k = x_k a_0 + y_k a_1$$

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Extended Euclid's Algorithm

$$a_0 = x_0 a_0 + y_0 a_1$$

$$a_1 = x_1 a_0 + y_1 a_1$$

$$a_2 = x_2 a_0 + y_2 a_1$$

$$a_3 = x_3 a_0 + y_3 a_1$$

...

$$a_k = x_k a_0 + y_k a_1$$

$$a_0 = 1a_0 + 0a_1$$

$$a_1 = 0a_0 + 1a_1$$

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Extended Euclid's Algorithm

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

$$a_0 = x_0 a_0 + y_0 a_1$$

$$a_0 = 1a_0 + 0a_1$$

$$a_1 = x_1 a_0 + y_1 a_1$$

$$a_1 = 0a_0 + 1a_1$$

$$a_2 = x_2 a_0 + y_2 a_1$$

$$a_3 = x_3 a_0 + y_3 a_1$$

...

$$a_k = x_k a_0 + y_k a_1$$

The other  $x_i$  and  $y_i$  can be derived using the relations between  $a_i$ 's:

$$a_i = a_{i-2} - q_{i-1} \cdot a_{i-1}$$

# Extended Euclid's Algorithm

Euclid's algorithm computes the next remainder,  $a_i$ , this way:

$$a_i = a_{i-2} - q_{i-1} \cdot a_{i-1}$$

Two previous remainders are

$$a_{i-2} = x_{i-2}a_0 + y_{i-2}a_1 \quad \text{and} \quad a_{i-1} = x_{i-1}a_0 + y_{i-1}a_1$$

$$a_i = a_{i-2} - q_{i-1} \cdot a_{i-1}$$

$$= x_{i-2} \cdot a_0 + y_{i-2} \cdot a_1 - q_{i-1}(x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1)$$

$$= (x_{i-2} - q_{i-1}x_{i-1}) \cdot a_0 + (y_{i-2} - q_{i-1}y_{i-1}) \cdot a_1$$

$$= \underbrace{\left( x_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} x_{i-1} \right)}_{=x_i} \cdot a_0 + \underbrace{\left( y_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} y_{i-1} \right)}_{=y_i} \cdot a_1$$

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Extended Euclid's Algorithm

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

$$a_i = a_{i-2} - q_{i-1} \cdot a_{i-1}$$

This is how we compute all  $x_i$  and  $y_i$  up to  $x_k$  and  $y_k$ :

$$x_0 = 1$$

$$y_0 = 0$$

$$x_1 = 0$$

$$y_1 = 1$$

...

...

$$x_i = x_{i-2} - \underbrace{\frac{a_{i-2} - a_i}{a_{i-1}}}_{=q_{i-1}} x_{i-1}$$

$$y_i = y_{i-2} - \underbrace{\frac{a_{i-2} - a_i}{a_{i-1}}}_{=q_{i-1}} y_{i-1}$$

...

...

In the end, we get two numbers  $x_k$  and  $y_k$ , so we can express the GCD as a linear combination of  $a_0$  and  $a_1$ :

$$\gcd(a_0, a_1) = a_k = x_k \cdot a_0 + y_k \cdot a_1$$



# Extended Euclid's Algorithm

$$x_i = x_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} x_{i-1} \quad y_i = y_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} y_{i-1}$$

Run Euclid's algorithm:

$$a_0 = 4620 = 45 \cdot 101 + 75$$

$$a_1 = 101$$

$$a_2 = 75$$

Compute coefficients:

$$x_0 = 1$$

$$x_1 = 0$$

$$q = \frac{4620-75}{101} = 45$$

$$x_2 = 1 - 45 \cdot 0 = 1$$

$$y_0 = 0$$

$$y_1 = 1$$

$$y_2 = 0 - 45 \cdot 1 = -45$$

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

# Extended Euclid's Algorithm

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

$$x_i = x_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} x_{i-1} \quad y_i = y_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} y_{i-1}$$

Run Euclid's algorithm:

$$a_0 = 4620 = 45 \cdot 101 + 75$$

$$a_1 = 101 = 1 \cdot 75 + 26$$

$$a_2 = 75 = 2 \cdot 26 + 23$$

$$a_3 = 26 = 1 \cdot 23 + 3$$

$$a_4 = 23$$

$$a_5 = 3$$

Compute coefficients:

$$x_0 = 1$$

$$y_0 = 0$$

$$x_1 = 0$$

$$y_1 = 1$$

$$q = \frac{4620-75}{101} = 45$$

$$x_2 = 1 - 45 \cdot 0 = 1 \quad y_2 = 0 - 45 \cdot 1 = -45$$

$$q = \frac{101-26}{75} = 1$$

$$x_3 = 0 - 1 \cdot 1 = -1 \quad y_3 = 1 - 1 \cdot (-45) = 46$$

$$q = \frac{75-23}{26} = 2$$

$$x_4 = 1 - 2 \cdot (-1) = 3 \quad y_4 = -45 - 2 \cdot 46 = -137$$

$$q = \frac{26-3}{23} = 1$$

$$x_5 = -1 - 1 \cdot 3 = -4 \quad y_5 = 46 - 1 \cdot (-137) = 183$$

# Extended Euclid's Algorithm

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

$$x_i = x_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} x_{i-1} \quad y_i = y_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} y_{i-1}$$

Run Euclid's algorithm:

$$a_0 = 4620 = 45 \cdot 101 + 75$$

$$a_1 = 101 = 1 \cdot 75 + 26$$

$$a_2 = 75 = 2 \cdot 26 + 23$$

$$a_3 = 26 = 1 \cdot 23 + 3$$

$$a_4 = 23 = 7 \cdot 3 + 2$$

$$a_5 = 3 = 1 \cdot 2 + 1$$

$$a_6 = 2 = 2 \cdot 1$$

$$a_7 = 1$$

Compute coefficients:

$$x_0 = 1 \quad y_0 = 0$$

$$x_1 = 0 \quad y_1 = 1$$

$$x_2 = 1 \quad y_2 = -45$$

$$x_3 = -1 \quad y_3 = 46$$

$$x_4 = 3 \quad y_4 = -137$$

$$x_5 = -4 \quad y_5 = 183$$

$$q = \frac{23-2}{3} = 7$$

$$x_6 = 31 \quad y_6 = -1418$$

$$q = \frac{3-1}{2} = 1$$

$$x_7 = -35 \quad y_7 = 1601$$

# Extended Euclid's Algorithm

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse

While computing the sequence of  $a_i$ 's with Euclid's algorithm, we eventually produced coefficients

$$x_7 = -35, \quad y_7 = 1601$$

By construction, they satisfy the equation

$$a_7 = x_7 \cdot a_0 + y_7 \cdot a_1$$

$$1 = \underbrace{-35}_{=x_7} \cdot \underbrace{4620}_{=a_0} + \underbrace{1601}_{=y_7} \cdot \underbrace{101}_{=a_1}$$

But from the last equation we can find the inverse of  $a_1$  modulo  $a_0$ , and the inverse of  $a_0$  modulo  $a_1$ .

# Finding a multiplicative inverse

Take this equation and find the multiplicative inverse of  $a_1 = 101$  modulo  $a_0 = 4620$ .

$$1 = \underbrace{-35}_{=x_7} \cdot \underbrace{4620}_{=a_0} + \underbrace{1601}_{=y_7} \cdot \underbrace{101}_{=a_1}$$

$$1601 \cdot 101 - 1 = 35 \cdot 4620$$

Therefore, by definition of congruence,

$$101 \cdot 1601 \equiv 1 \pmod{4620}.$$

So, 1601 is a multiplicative inverse of 101 modulo 4620.

We were able to find the inverse, because 101 and 4620 are relative primes, that is, their GCD is equal to 1.

GCD is a linear combination

Relative primes

Fundamental theorem of arithmetic

Modular arithmetic

Congruence

Modular arithmetic

Multiplicative inverse