Modular Arithmetic

Previously, we defined

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

$$a = dq + r.$$

Def (GCD).

Def (Prime numbers).

GCD is a linear combination

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)

Def. a and b are *relative 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

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

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_j \qquad (p_1 \leq p_2 \leq \ldots \leq p_j)$$

This product is called prime factorization.

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

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:

$$22 \equiv 15 \pmod{7}$$

$$29 \equiv 15 \pmod{7}$$

$$36 \equiv 15 \pmod{7}$$

because

$$7 \mid (\underbrace{22 - 15}_{=7}),\ 7 \mid (\underbrace{29 - 15}_{=14}),\ 7 \mid (\underbrace{36 - 15}_{=21}).$$

Congruence

Example:

$$22 \equiv 15 \pmod 7$$

$$29 \equiv 15 \pmod 7$$

$$36 \equiv 15 \pmod 7$$

because

$$7 \mid (\underbrace{22-15}_{=7}),\ 7 \mid (\underbrace{29-15}_{=14}),\ 7 \mid (\underbrace{36-15}_{=21}).$$

14 *15* 16 17 18 19 20 21 *22* 23 24 25 26 27 28 *29* 30

The distance between 15, 22, 29, 36, etc. is a multiple of 7.

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

Congruence

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

Lemma.

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

Proof:
By the division algorithm,

$$a = q_1 n + r_1, \qquad b = q_2 n + r_2.$$

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

"$\Rightarrow$": 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 $a \equiv b \pmod{n}$. $\square$

Congruence

x	9	10	11	12	13	14	15	16	17
x **rem** 3	*0*	*1*	*2*	*0*	*1*	*2*	*0*	*1*	*2*
x **rem** $3 = 0$	9			12			15		
x **rem** $3 = 1$		10			13			16	
x **rem** $3 = 2$			11			14			17

Integers are divided into 3 congruence classes:

$\ldots, 9, 12, 15, 18, 21, \ldots$ are congruent modulo 3.

$\ldots, 10, 13, 16, 19, 22, \ldots$ are congruent modulo 3.

$\ldots, 11, 14, 17, 20, 23, \ldots$ are congruent modulo 3.

Congruence classes

Modulo 3:

$\{\ldots, 0, 3, 6, 9, 12, \ldots\}$ is the congruence class of 0 modulo 3.

$\{\ldots, 1, 4, 7, 10, 13, \ldots\}$ is the congruence class of 1 modulo 3.

$\{\ldots, 2, 5, 8, 11, 14, \ldots\}$ is the congruence class of 2 modulo 3.

Theorem.

$$a \mathbin{\textbf{rem}} n \equiv a \pmod{n}.$$

Modulo 7:

Similarly, the days of the week:
Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday define congruence classes modulo 7.

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

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, $a^{-1} = s$. $\square$

Multiplicative inverse

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

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

They are relative primes:

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

By Bezout's theorem:

$$101 \cdot s + 4620 \cdot t = 1$$

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

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

Extended Euclid's Algorithm

$$101 \cdot s + 4620 \cdot t = 1$$

Run Euclid's algorithm:

$$a_0 = 4620 = 45 \cdot 101 + 75$$
$$a_1 = 101 = 1 \cdot 75 + 26$$
$$a_2 = 75 = 2 \cdot 26 + 23$$
$$a_3 = 26 = 1 \cdot 23 + 3$$
$$a_4 = 23 = 7 \cdot 3 + 2$$
$$a_5 = 3 = 1 \cdot 2 + 1$$
$$a_6 = 2 = 2 \cdot 1$$
$$a_7 = 1$$

Work backwards, to express GCD in terms of $a_1 = 101$ and $a_0 = 4620$:

$$1 = 3 - 1 \cdot 2$$

Extended Euclid's Algorithm

$$101 \cdot s + 4620 \cdot t = 1$$

Run Euclid's algorithm:

$$\begin{aligned}
a_0 &= 4620 = 45 \cdot 101 + 75 \\
a_1 &= 101 = 1 \cdot 75 + 26 \\
a_2 &= 75 = 2 \cdot 26 + 23 \\
a_3 &= 26 = 1 \cdot 23 + 3 \\
a_4 &= 23 = 7 \cdot 3 + 2 \\
a_5 &= 3 = 1 \cdot 2 + 1 \\
a_6 &= 2 = 2 \cdot 1 \\
a_7 &= 1
\end{aligned}$$

Work backwards, to express GCD in terms of $a_1 = 101$ and $a_0 = 4620$:

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3
\end{aligned}$$

Extended Euclid's Algorithm

$$101 \cdot s + 4620 \cdot t = 1$$

Run Euclid's algorithm:

$$\begin{aligned} a_0 &= 4620 = 45 \cdot 101 + 75 \\ a_1 &= 101 = 1 \cdot 75 + 26 \\ a_2 &= 75 = 2 \cdot 26 + 23 \\ a_3 &= 26 = 1 \cdot 23 + 3 \\ a_4 &= 23 = 7 \cdot 3 + 2 \\ a_5 &= 3 = 1 \cdot 2 + 1 \\ a_6 &= 2 = 2 \cdot 1 \\ a_7 &= 1 \end{aligned}$$

Work backwards, to express GCD in terms of $a_1 = 101$ and $a_0 = 4620$:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\ &= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \end{aligned}$$

Extended Euclid's Algorithm

$$101 \cdot s + 4620 \cdot t = 1$$

Run Euclid's algorithm:

$$\begin{aligned}
a_0 &= 4620 = 45 \cdot 101 + 75 \\
a_1 &= 101 = 1 \cdot 75 + 26 \\
a_2 &= 75 = 2 \cdot 26 + 23 \\
a_3 &= 26 = 1 \cdot 23 + 3 \\
a_4 &= 23 = 7 \cdot 3 + 2 \\
a_5 &= 3 = 1 \cdot 2 + 1 \\
a_6 &= 2 = 2 \cdot 1 \\
a_7 &= 1
\end{aligned}$$

Work backwards, to express GCD in terms of $a_1 = 101$ and $a_0 = 4620$:

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\
&= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\
&= 8 \cdot 26 - 9(75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26
\end{aligned}$$

Extended Euclid's Algorithm

$$101 \cdot s + 4620 \cdot t = 1$$

Run Euclid's algorithm:

$$\begin{aligned}
a_0 &= 4620 = 45 \cdot 101 + 75 \\
a_1 &= 101 = 1 \cdot 75 + 26 \\
a_2 &= 75 = 2 \cdot 26 + 23 \\
a_3 &= 26 = 1 \cdot 23 + 3 \\
a_4 &= 23 = 7 \cdot 3 + 2 \\
a_5 &= 3 = 1 \cdot 2 + 1 \\
a_6 &= 2 = 2 \cdot 1 \\
a_7 &= 1
\end{aligned}$$

Work backwards, to express GCD in terms of $a_1 = 101$ and $a_0 = 4620$:

$$\begin{aligned}
\mathit{1} &= \mathit{3} - 1 \cdot \mathit{2} \\
&= \mathit{3} - 1 \cdot (\mathit{23} - 7 \cdot \mathit{3}) = -1 \cdot \mathit{23} + 8 \cdot \mathit{3} \\
&= -1 \cdot \mathit{23} + 8 \cdot (\mathit{26} - 1 \cdot \mathit{23}) = 8 \cdot \mathit{26} - 9 \cdot \mathit{23} \\
&= 8 \cdot \mathit{26} - 9(\mathit{75} - 2 \cdot \mathit{26}) = -9 \cdot \mathit{75} + 26 \cdot \mathit{26} \\
&= -9 \cdot \mathit{75} + 26 \cdot (\mathit{101} - 1 \cdot \mathit{75}) = 26 \cdot \mathit{101} - 35 \cdot \mathit{75}
\end{aligned}$$

Extended Euclid's Algorithm

$$101 \cdot s + 4620 \cdot t = 1$$

Run Euclid's algorithm:

$$\begin{aligned}
a_0 &= 4620 = 45 \cdot 101 + 75 \\
a_1 &= 101 = 1 \cdot 75 + 26 \\
a_2 &= 75 = 2 \cdot 26 + 23 \\
a_3 &= 26 = 1 \cdot 23 + 3 \\
a_4 &= 23 = 7 \cdot 3 + 2 \\
a_5 &= 3 = 1 \cdot 2 + 1 \\
a_6 &= 2 = 2 \cdot 1 \\
a_7 &= 1
\end{aligned}$$

Work backwards, to express GCD in terms of $a_1 = 101$ and $a_0 = 4620$:

$$\begin{aligned}
\mathit{1} &= \mathit{3} - 1 \cdot \mathit{2} \\
&= \mathit{3} - 1 \cdot (\mathit{23} - 7 \cdot \mathit{3}) = -1 \cdot \mathit{23} + 8 \cdot \mathit{3} \\
&= -1 \cdot \mathit{23} + 8 \cdot (\mathit{26} - 1 \cdot \mathit{23}) = 8 \cdot \mathit{26} - 9 \cdot \mathit{23} \\
&= 8 \cdot \mathit{26} - 9(\mathit{75} - 2 \cdot \mathit{26}) = -9 \cdot \mathit{75} + 26 \cdot \mathit{26} \\
&= -9 \cdot \mathit{75} + 26 \cdot (\mathit{101} - 1 \cdot \mathit{75}) = 26 \cdot \mathit{101} - 35 \cdot \mathit{75} \\
&= 26 \cdot \mathit{101} - 35 \cdot (\mathit{4620} - 45 \cdot \mathit{101}) \\
&= -35 \cdot \mathit{4620} + 1601 \cdot \mathit{101}
\end{aligned}$$

Extended Euclid's Algorithm

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

Bezout coefficients are $s = 1601$ and $t = -35$.

Therefore, $s = 1601$ is the multiplicative inverse:

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

It works, but it's confusing. Let's describe the extended Euclid's algorithm more systematically.

Extended Euclid's Algorithm

The task:

Given two numbers $a_0 \geq a_1$, compute $a_k = \gcd(a_0, a_1)$, and 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

Normally, when computing $\gcd(a_0, a_1)$, we produce the sequence of remainders

$$a_0,\ a_1,\ a_2,\ \ldots, a_k,$$

where the last $a_k = \gcd(a_0, a_1)$.

Our ultimate goal is to compute coefficients x_k and y_k such that

$$a_k = x_k \cdot a_0 + y_k \cdot a_1$$

Along the way, for every term a_i from the sequence, we compute x_i and y_i

$$a_i = x_i \cdot a_0 + y_i \cdot a_1$$

Extended Euclid's Algorithm

When computing $\gcd(a_0, a_1)$ with Euclid's algorithm, we produce the sequence of remainders.

$$a_0$$
$$a_1$$
$$\ldots$$
$$a_i$$
$$\ldots$$
$$a_k$$

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

Extended Euclid's Algorithm

When computing $\gcd(a_0, a_1)$ with Euclid's algorithm, we produce the sequence of remainders.

a_0
a_1
$\dots$
a_i
$\dots$
a_k $\quad$ x_k and y_k such that $\quad a_k = x_k a_0 + y_k a_1$

$a_k = gcd(a_0, a_1)$

Extended Euclid's Algorithm

When computing $\gcd(a_0, a_1)$ with Euclid's algorithm, we produce the sequence of remainders.

$$\begin{array}{l} a_0 \\ a_1 \\ \dots \\ a_i \\ \dots \\ a_k \quad x_k \text{ and } y_k \text{ such that} \quad a_k = x_k a_0 + y_k a_1 \quad x_k =? \quad y_k =? \end{array}$$

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

Extended Euclid's Algorithm

When computing $\gcd(a_0, a_1)$ with Euclid's algorithm, we produce the sequence of remainders.

$$
\begin{array}{lll}
a_0 & x_0 \text{ and } y_0 \text{ such that} & a_0 = x_0 a_0 + y_0 a_1 \\
a_1 & & \\
\ldots & & \\
a_i & & \\
\ldots & & \\
a_k & x_k \text{ and } y_k \text{ such that} & a_k = x_k a_0 + y_k a_1 \quad x_k = ? \quad y_k = ?
\end{array}
$$

$a_k = gcd(a_0, a_1)$

Extended Euclid's Algorithm

When computing $\gcd(a_0, a_1)$ with Euclid's algorithm, we produce the sequence of remainders.

$$
\begin{array}{lllll}
a_0 & x_0 \text{ and } y_0 \text{ such that} & a_0 = x_0 a_0 + y_0 a_1 & x_0 = 1 & y_0 = 0 \\
a_1 & & & & \\
\ldots & & & & \\
a_i & & & & \\
\ldots & & & & \\
a_k & x_k \text{ and } y_k \text{ such that} & a_k = x_k a_0 + y_k a_1 & x_k =? & y_k =?
\end{array}
$$

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

Extended Euclid's Algorithm

When computing $\gcd(a_0, a_1)$ with Euclid's algorithm, we produce the sequence of remainders.

$$\begin{array}{llll} a_0 & x_0 \text{ and } y_0 \text{ such that} & a_0 = x_0 a_0 + y_0 a_1 & x_0 = 1 \quad y_0 = 0 \\ a_1 & x_1 \text{ and } y_1 \text{ such that} & a_1 = x_1 a_0 + y_1 a_1 & \\ \dots & & & \\ a_i & & & \\ \dots & & & \\ a_k & x_k \text{ and } y_k \text{ such that} & a_k = x_k a_0 + y_k a_1 & x_k =? \quad y_k =? \end{array}$$

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

Extended Euclid's Algorithm

When computing $\gcd(a_0, a_1)$ with Euclid's algorithm, we produce the sequence of remainders.

$$
\begin{array}{lllll}
a_0 & x_0 \text{ and } y_0 \text{ such that} & a_0 = x_0 a_0 + y_0 a_1 & x_0 = 1 & y_0 = 0 \\
a_1 & x_1 \text{ and } y_1 \text{ such that} & a_1 = x_1 a_0 + y_1 a_1 & x_1 = 0 & y_1 = 1 \\
\ldots & & & & \\
a_i & & & & \\
\ldots & & & & \\
a_k & x_k \text{ and } y_k \text{ such that} & a_k = x_k a_0 + y_k a_1 & x_k = ? & y_k = ?
\end{array}
$$

$a_k = gcd(a_0, a_1)$

Extended Euclid's Algorithm

When computing $\gcd(a_0, a_1)$ with Euclid's algorithm, we produce the sequence of remainders.

$$
\begin{array}{lllll}
a_0 & x_0 \text{ and } y_0 \text{ such that} & a_0 = x_0 a_0 + y_0 a_1 & x_0 = 1 & y_0 = 0 \\
a_1 & x_1 \text{ and } y_1 \text{ such that} & a_1 = x_1 a_0 + y_1 a_1 & x_1 = 0 & y_1 = 1 \\
\ldots & & & & \\
a_i & x_i \text{ and } y_i \text{ such that} & a_i = x_i a_0 + y_i a_1 & x_i = ? & y_i = ? \\
\ldots & & & & \\
a_k & x_k \text{ and } y_k \text{ such that} & a_k = x_k a_0 + y_k a_1 & x_k = ? & y_k = ?
\end{array}
$$

$a_k = gcd(a_0, a_1)$

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

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

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

Extended Euclid's Algorithm

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

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

$$\begin{aligned}
x_0 &= 1 & y_0 &= 0 \\
x_1 &= 0 & y_1 &= 1 \\
&\ldots & &\ldots \\
x_i &= x_{i-2} - \underbrace{\frac{a_{i-2} - a_i}{a_{i-1}}}_{=q_{i-1}} x_{i-1} & y_i &= y_{i-2} - \underbrace{\frac{a_{i-2} - a_i}{a_{i-1}}}_{=q_{i-1}} y_{i-1} \\
&\ldots & &\ldots
\end{aligned}$$

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

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

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:

$x_0 = 1$ $\qquad$ $y_0 = 0$

$x_1 = 0$ $\qquad$ $y_1 = 1$

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

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

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

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

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

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

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

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

Extended Euclid's Algorithm

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

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:

$x_0 = 1 \qquad y_0 = 0$
$x_1 = 0 \qquad y_1 = 1$
$x_2 = 1 \qquad y_2 = -45$
$x_3 = -1 \qquad y_3 = 46$
$x_4 = 3 \qquad y_4 = -137$
$x_5 = -4 \qquad y_5 = 183$

$\frac{23-2}{3} = 7$
$x_6 = 31 \qquad y_6 = -1418$

$\frac{3-1}{2} = 1$
$x_7 = -35 \qquad y_7 = 1601$

Extended Euclid's Algorithm

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

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

By construction, they satisfy the equation

$$\gcd(a_0, a_1) = a_7 = x_7 \cdot a_0 + y_7 \cdot a_1$$

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

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 multuiplicative 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.