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

$$a = dq + r.$$

Fundamental theorem of arithmetic

Def (Prime numbers). A number $p > 1$ with no positive divisors other than 1 and itself is called a *prime*.

Every other number greater than 1 is called *composite*.

The number 1 is considered neither prime nor composite.

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.

Divisibility by a prime

One more result about primes we are going to use in the future:

Theorem. Let p be a prime. If

$$p \mid a_1 a_2 \cdot \ldots \cdot a_n,$$

then p divides some a_i (at least one of them).

Example: If you know that $19 \mid 403 \cdot 629$, then you know that either $19 \mid 403$ or $19 \mid 629$, though you might not know which.

GCD is a linear combination

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)

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

$$sa + tb = 1$$

Modular arithmetic

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

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

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

Modular arithmetic

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

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

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

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

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

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

Modular arithmetic

$$\ldots 5 \quad 6 \quad \to \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad \to \quad 0 \quad 1 \ldots$$

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

$$\begin{array}{lll} 4+4 & \text{is} & 1 \\ 2-3 & \text{is} & 6 \\ 14 \cdot 5 & \text{is} & 0 \end{array}$$

$$-7 \quad \text{is} \quad 0 \quad \text{is} \quad 7 \quad \text{is} \quad 14 \quad \text{is} \quad 21 \ldots$$

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

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:

$$\begin{aligned} 8 &\equiv 1 \pmod{7} \\ 15 &\equiv 1 \pmod{7} \\ 8 &\equiv 15 \pmod{7} \end{aligned}$$

because

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

Congruence

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.

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

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	-3	-2	-1	0	1	2	3	4	5	6	7	8
x **rem** 3	*0*	*1*	*2*	*0*	*1*	*2*	*0*	*1*	*2*	*0*	*1*	*2*

Integers are divided into 3 congruence classes:

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

…, -2, 1, 4, 7, 10, 13, … are congruent modulo 3.

…, -1, 2, 5, 8, 11, 14, … are congruent modulo 3.

By the way, all Mondays, all Tuesdays, all Wednesdays, etc. are congruence classes too.

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

Modular arithmetic

Addition, subtraction, and multiplication preserve congruence. What does it mean practically?

If we have to find x such that

$$12^2 \cdot (-11) + 80 \equiv x \pmod 5$$

We know that

$$\begin{aligned} 12 &\equiv 2 \pmod 5, \\ -11 &\equiv -1 \pmod 5, \\ 80 &\equiv 0 \pmod 5) \end{aligned}$$

Therefore, we are free to substitute 12 with 2, -11 with -1, and 80 with 0:

$$12^2 \cdot (-11) + 80 \equiv 2^2 \cdot (-1) + 0 \equiv 2 \cdot 2 \cdot (-1) \equiv -4 \equiv 1 \pmod 5.$$

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, that is x such that

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

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

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

Let's adapt this algorithm for finding Bezout coefficients s and t:

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

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:

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

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

$$\mathit{1} = \mathit{3} - 1 \cdot \mathit{2}$$
$$= \mathit{3} - 1 \cdot (\mathit{23} - 7 \cdot \mathit{3}) = -1 \cdot \mathit{23} + 8 \cdot \mathit{3}$$

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 $a_0 = 4620$:

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

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

$$-35 \cdot \textcolor{orange}{\mathit{4620}} + 1601 \cdot \textcolor{orange}{\mathit{101}} = 1$$

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 easy to make a mistake using this method. Let's describe the extended Euclid's algorithm more systematically.

Extended Euclid's Algorithm (II)

The task:

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

$$\begin{aligned} a_2 &= \dots \\ a_3 &= \dots \\ &\dots \\ a_k &= \gcd(a_0, a_1) \end{aligned}$$

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 (II)

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

$$\begin{aligned}
a_0 &= x_0 a_0 + y_0 a_1 \\
a_1 &= x_1 a_0 + y_1 a_1 \\
a_2 &= x_2 a_0 + y_2 a_1 \\
a_3 &= x_3 a_0 + y_3 a_1 \\
&\dots \\
a_k &= \gcd(a_0, a_1) = x_k a_0 + y_k a_1
\end{aligned}$$

Extended Euclid's Algorithm (II)

$$
\begin{aligned}
a_0 &= x_0 a_0 + y_0 a_1 \\
a_1 &= x_1 a_0 + y_1 a_1 \\
a_2 &= x_2 a_0 + y_2 a_1 \\
a_3 &= x_3 a_0 + y_3 a_1 \\
&\dots \\
a_k &= x_k a_0 + y_k a_1
\end{aligned}
$$

Extended Euclid's Algorithm (II)

$$
\begin{aligned}
a_0 &= x_0 a_0 + y_0 a_1 & a_0 &= 1a_0 + 0a_1, & x_0 &= 1, & y_0 &= 0, \\
a_1 &= x_1 a_0 + y_1 a_1 & a_1 &= 0a_0 + 1a_1, & x_1 &= 0, & y_1 &= 1, \\
a_2 &= x_2 a_0 + y_2 a_1 \\
a_3 &= x_3 a_0 + y_3 a_1 \\
&\dots \\
a_k &= x_k a_0 + y_k a_1
\end{aligned}
$$

Extended Euclid's Algorithm (II)

$$
\begin{aligned}
a_0 &= x_0 a_0 + y_0 a_1 & a_0 &= 1a_0 + 0a_1, & x_0 &= 1, & y_0 &= 0,\\
a_1 &= x_1 a_0 + y_1 a_1 & a_1 &= 0a_0 + 1a_1, & x_1 &= 0, & y_1 &= 1,\\
a_2 &= x_2 a_0 + y_2 a_1 \\
a_3 &= x_3 a_0 + y_3 a_1 \\
&\dots \\
a_k &= x_k a_0 + y_k a_1
\end{aligned}
$$

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 (II)

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

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

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

Extended Euclid's Algorithm (II)

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

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

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

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 (II)

$$x_i = x_{i-2} - \underbrace{\left(\frac{a_{i-2} - a_i}{a_{i-1}}\right)}_{=q_{i-1}} x_{i-1} \qquad y_i = y_{i-2} - \underbrace{\left(\frac{a_{i-2} - a_i}{a_{i-1}}\right)}_{=q_{i-1}} y_{i-1}$$

i	a_i	q	x_i	y_i
0	$a_0 = 4620$	-	1	0
1	$a_1 = 101$	-	0	1
2	$4620 = 45 \cdot 101 + 75$ $a_2 = 75$	45	$1 - 45 \cdot 0 =$ 1	$0 - 45 \cdot 1 =$ -45

Extended Euclid's Algorithm (II)

$$x_i = x_{i-2} - \underbrace{\left(\frac{a_{i-2} - a_i}{a_{i-1}}\right)}_{=q_{i-1}} x_{i-1} \qquad y_i = y_{i-2} - \underbrace{\left(\frac{a_{i-2} - a_i}{a_{i-1}}\right)}_{=q_{i-1}} y_{i-1}$$

i	a_i	q	x_i	y_i
0	$a_0 = 4620$	-	1	0
1	$a_1 = 101$	-	0	1
2	$4620 = 45 \cdot 101 + 75$ $a_2 = 75$	45	$1 - 45 \cdot 0 =$ 1	$0 - 45 \cdot 1 =$ -45
3	$101 = 1 \cdot 75 + 26$ $a_3 = 26$	1	$0 - 1 \cdot 1 =$ -1	$1 - 1 \cdot (-45) =$ 46
4	$75 = 2 \cdot 26 + 23$ $a_4 = 23$	2	$1 - 2 \cdot (-1) =$ 3	$-45 - 2 \cdot 46 =$ -137

Extended Euclid's Algorithm (II)

i	a_i	q	x_i	y_i
0	$a_0 = 4620$	-	1	0
1	$a_1 = 101$	-	0	1
2	$a_2 = 75$	45	1	-45
3	$a_3 = 26$	1	-1	46
4	$a_4 = 23$	2	3	-137
5	$26 = 1 \cdot 23 + 3$		$-1 - 1 \cdot 3 =$	$46 - 1 \cdot (-137) =$
	$a_5 = 3$	1	-4	183
6	$23 = 7 \cdot 3 + 2$		$3 - 7 \cdot (-4) =$	$-137 - 7 \cdot 183 =$
	$a_6 = 2$	7	31	-1418
7	$3 = 1 \cdot 2 + 1$		$-4 - 1 \cdot 31 =$	$183 - 1 \cdot 1418 =$
	$a_7 = 1$	1	-35	1601

Extended Euclid's Algorithm (II)

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

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

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

But from the last equation we can find the inverse of 101 modulo 4620, and the inverse of 4620 modulo 101.

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.