The Euclidean Algorithm

(Euklids Algoritme)

Described in the book **Elements** by **Euclid** who lived 325 B.C. – 265 B.C.

Ex:

$$\gcd(287, 91) = ?$$

$$287 = 91 \cdot 3 + 14$$
$$91 = 14 \cdot 6 + 7$$
$$14 = 7 \cdot 2$$

Last remainder $\neq 0$

$$\gcd(287, 91) = 7$$

Check:

$$287 = 7 \cdot 41$$
$$91 = 7 \cdot 13$$

Why does it work?

The Euclidean Algorithm is correct:

Lemma 4.3.1

$$a = bq + r, \quad a,b,q,r \in \mathbb{Z}$$
$$\Downarrow$$
$$\gcd(a,b) = \gcd(b,r)$$

Proof:

We will prove that

$$d \mid a \wedge d \mid b \iff d \mid b \wedge d \mid r$$

(I.e., the set of common divisors of a and b is the same as for b and r: „$cd(a,b) = cd(b,r)$". This is a stronger statement than $\gcd(a,b) = \gcd(b,r)$.)

$$d \mid b \wedge d \mid r \implies d \mid \underbrace{(bq+r)}_{=a}, \quad \text{by Cor. 4.1.1}$$

$$d \mid a \wedge d \mid b \implies d \mid \underbrace{(a-bq)}_{=r}, \quad \text{by Cor. 4.1.1}$$

$\square$

Ex (from before)

$$287 = 91 \cdot 3 + 14 \qquad (*)$$
$$91 = 14 \cdot 6 + 7 \qquad (**)$$
$$14 = 7 \cdot 2 \qquad (***)$$

By Lemma 4.3.1,

$$\begin{aligned} \gcd(287, 91) &= \gcd(91, 14), \text{ by } (*) \\ &= \gcd(14, 7), \text{ by } (**) \\ &= 7, \text{ by } (***) \end{aligned}$$

We can write 7 as a linear combination of 287 and 91 by working backwards through the steps of the Euclidean Algorithm:

$$\begin{aligned} 7 &= 91 - 14 \cdot 6, \quad \text{by } (**) \\ &= 91 - (287 - 91 \cdot 3) \cdot 6, \text{ by } (*) \\ &= 91 - 287 \cdot 6 + 91 \cdot 18 \\ &= 91 \cdot 19 - 287 \cdot 6 \end{aligned}$$

Generalizing this observation, we obtain:

Theorem 4.3.6

$$\forall a, b \in \mathbb{Z} : \exists s, t \in \mathbb{Z} : \gcd(a, b) = sa + tb$$

I.e., $\gcd(a,b)$ can be written as a linear combination of a and b.

We will now work towards answering the question from last time:

When is <u>division</u> of congruences allowed?

<u>Lemma 4.3.2</u>

For any $a, b, c \in \mathbb{Z}^+$,

$$a \mid bc \ \wedge \ \gcd(a,b) = 1$$
$$\Downarrow$$
$$a \mid c$$

Intuition: bc contains all of a's prime factors. Thus, if b contains none of a's prime factors, then c must contain them all.

Ex:

$4 \mid 9 \cdot 12 \quad \Rightarrow \quad 4 \mid 12$, since $\gcd(4,9) = 1$

$4 \mid 2 \cdot 18$, but $4 \nmid 18 \qquad (\gcd(4,2) = 2)$

$4 \mid 2 \cdot 20$, and $4 \mid 20$ even though $\gcd(4,2) = 2$

Lemma 4.3.2 will be used to prove:

Theorem 4.3.7

Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then,

$$\begin{aligned} & ac \equiv bc \pmod{m} \ \wedge\ \gcd(c,m)=1 \\ \Downarrow\ & \\ & a \equiv b \pmod{m} \end{aligned}$$

I.e., if c divides the LHS as well as the RHS, and c does not have any prime factors in common with m, then we are allowed to divide both sides by c.

Proof:

Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.
Assume that $\gcd(c,m)=1$.
Then,

$$\begin{aligned} & ac \equiv bc \pmod{m} \\ \Updownarrow\ & \\ & m \mid (ac-bc), \text{ by Def } 4.1.3 \\ \Updownarrow\ & \\ & m \mid (a-b)c \\ \Updownarrow\ & \\ & m \mid (a-b), \text{ by Lemma } 4.3.2, \text{ since } \gcd(c,m)=1 \\ \Updownarrow\ & \\ & a \equiv b \pmod{m}, \text{ by Def. } 4.1.3 \end{aligned}$$

$\square$

Ex:

$9 \equiv 45 \pmod{4} \Rightarrow 3 \equiv 15 \pmod{4}$, since $\gcd(3,4)=1$

$10 \equiv 22 \pmod{4}$ but $5 \not\equiv 11 \pmod{4}$ $(\gcd(2,4)=2)$

$12 \equiv 20 \pmod{4}$ and $6 \equiv 10 \pmod{4}$ even though $\gcd(2,4)=2$.

Linear Congruences and Multiplicative Inverses (Section 4.4)

Ex: $4x \equiv 5 \pmod{11}$ $\qquad (\gcd(4,11) = 1)$

$x = 4$ is a solution:

x	0	1	2	3	4	5	6	7	8	9	10	11
$4x \bmod 11$	0	4	8	1	5	9	2	6	10	3	7	0

Ex: $4x \equiv 5 \pmod{10}$ $\qquad (\gcd(4,10) = 2)$

No solution, since $4x \bmod 10$ is even and $5 \bmod 10$ is odd:

x	0	1	2	3	4	5	6	7	8	9	10	11
$4x \bmod 10$	0	4	8	2	6	0	4	8	2	6	4	8

Ex: $4x \equiv 2 \pmod{10}$ $\qquad (\gcd(4,10) = 2)$

$x = 3$ is a solution:

x	0	1	2	3	4	5	6	7	8	9	10	11
$4x \bmod 10$	0	4	8	2	6	0	4	8	2	6	4	8

How to decide whether a given congruence has a solution?

A linear equation always has a solution.
It can be found by multiplying by $\frac{1}{a}$:

$$ax = b \iff \frac{1}{a} \cdot ax = \frac{1}{a} \cdot b \iff x = \frac{b}{a}$$

Note that $\frac{1}{a}$ is the multiplicative inverse of a,
since $\frac{1}{a} \cdot a = 1$.

Can we do something similar with a congruence?
I.e., can we find an $\bar{a}$ such that

$$\bar{a} \cdot a \equiv 1 \pmod{m} \text{ ?}$$

In that case, $\bar{a}$ would be the multiplicative inverse of a modulo m.

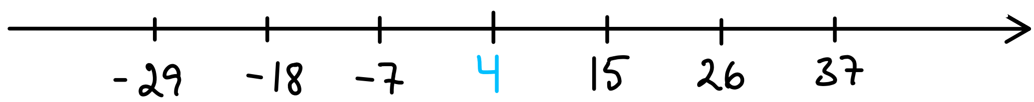
Ex: 3 is a multiplicative inverse of 4 modulo 11:

$$3 \cdot 4 \bmod 11 = 12 \bmod 11 = 1$$

This is useful in the example from before:

$$\begin{aligned} & 4x \equiv 5 \pmod{11} \\ \Updownarrow \; & \\ & 3 \cdot 4x \equiv 3 \cdot 5 \pmod{11}, \quad \text{by Theorems 4.1.5 and 4.3.7} \\ \Updownarrow \; & \\ & 12x \equiv 15 \pmod{11} \\ \Updownarrow \; & \\ & x \equiv 4 \pmod{11} \end{aligned}$$

Solution set: $\{4 + 11k \mid k \in \mathbb{Z}\}$



Ex: 4 has no multiplicative inverse modulo 10, since $4k \bmod 10$ is even for any $k \in \mathbb{Z}$.

If $\gcd(a, m) = 1$, $\bar{a}$ exists and we can find it using the Euclidean Algorithm and working backwards.

Ex: Multiplicative inverse of 4 modulo 11

$$11 = 4 \cdot 2 + 3$$
$$4 = 3 \cdot 1 + 1$$

$$1 = 4 - 3 \cdot 1 = 4 - (11 - 4 \cdot 2) \cdot 1 = 3 \cdot 4 - 11$$
$$\Downarrow$$
$$3 \cdot 4 = 1 + 11$$
$$\Downarrow$$
$$3 \cdot 4 \equiv 1 \pmod{11}$$

Thus, 3 is a multiplicative inverse of 4 modulo 11.
(And hence, 4 is a multiplicative inverse of 3 modulo 11.)
Moreover, 3 is the only multiplicative inverse of 4 in $\mathbb{Z}_{11}$:

Theorem 4.4.1

Let $a, m \in \mathbb{Z}$, $m \geq 2$. Then,

$$\gcd(a, m) = 1$$
$$\Downarrow$$
$$\exists! \, \bar{a} \in \mathbb{Z}_m : \bar{a} a \equiv 1 \pmod{m}$$

Proof of uniqueness: Exercise 4.4.7

Does a have a multiplicative inverse modulo m?

If $\gcd(a,m) = 1$,

Yes (Theorem 4.4.1)

Otherwise,

No (Exercise 4.4.8)

Does $ax \equiv b \pmod{m}$ have a solution?

If $\gcd(a,m) = 1$,

Yes (Theorem 4.4.1)

Otherwise,

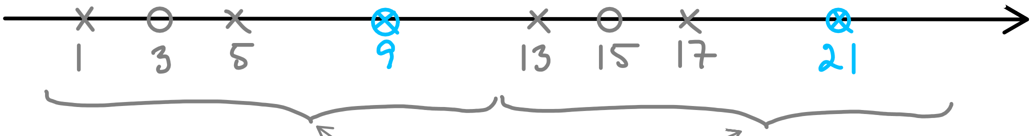
Maybe (Examples above)

Systems of Linear Congruences

Ex:

$x \equiv 1 \pmod{4}$ 1, 5, 9, 13, 17, 21, 25, ...   ×

$x \equiv 3 \pmod{6}$ 3, 9, 15, 21, 27, ...   ○



Same pattern
(why?)

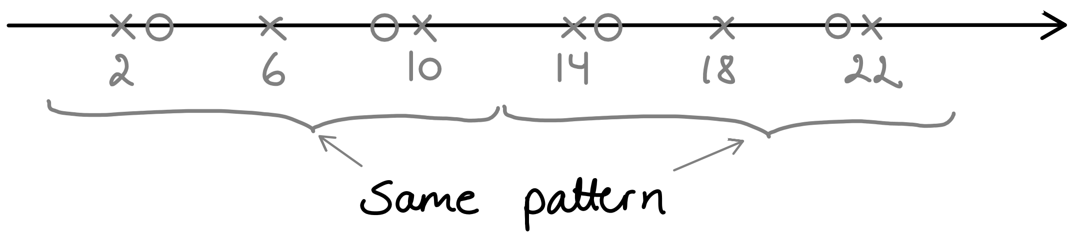
Adding (a multiple of) 12, both congruences are unchanged, since 12 is a multiple of 4 as well as 6.

Thus, since $x = 9$ is a solution, $x = 9 + 12k$ is a solution for any $k \in \mathbb{Z}$.

Ex:

$x \equiv 2 \pmod 4$ $2, 6, 10, 14, 18, 22, 26, \ldots$ $\times$

$x \equiv 3 \pmod 6$ $3, 9, 15, 21, 27, 33, \ldots$ $\circ$



Since $\mathbb{Z}_{12}$ does not contain a common solution, there is no common solution.

Note that $\operatorname{lcm}(4,6) = 12$.

In general:

$$\boxed{\begin{array}{l}\text{For } n \text{ congruences with moduli } m_1, m_2, \ldots, m_n, \\ \quad \exists \text{ solution} \iff \exists! \text{ solution in } \mathbb{Z}_{\operatorname{lcm}(m_1, m_2, \ldots, m_n)}\end{array}}$$

We shall see that if $m_1, m_2, \ldots, m_n$ are pairwise relatively prime (and hence $\operatorname{lcm}(m_1, m_2, \ldots, m_n) = m_1 \cdot m_2 \cdot \ldots \cdot m_n$), there is a solution.

We will prove this by giving a solution method
The running example will be:

Theorem 4.4.2: Chinese Remainder Theorem

If

$a_1, a_2, \dots, a_n \in \mathbb{Z}$,

$m_1, m_2, \dots, m_n \in \mathbb{Z} - \{1\}$ are

pairwise relatively prime, and

$m = m_1 \cdot m_2 \cdot \dots \cdot m_n$

Then,

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution in $\mathbb{Z}_m$.

Proof:

Uniqueness: Exercises 29 + 30

Existence: Constructive proof

Proof idea:

If we can find $b_1, b_2, \dots, b_n$ such that

$$b_k \equiv \begin{cases} 0 \pmod{m_i}, & \text{for each } i \neq k \\ 1 \pmod{m_k} \end{cases}$$

Then,

$$x = \sum_{k=1}^{n} b_k a_k$$

is a solution, since for each i, $1 \leq i \leq n$,

$$x = \sum_{k \neq i} b_k a_k + b_i a_i$$
$$\equiv \sum_{k \neq i} 0 \cdot a_k + 1 \cdot a_i \pmod{a_i}$$

For each k, $1 \le k \le n$:

Let $M_k = \frac{m}{m_k} = m_1 \cdot m_2 \cdot \ldots \cdot m_{k-1} \cdot m_{k+1} \cdot \ldots \cdot m_n$

By Theorem 4.4.1, there exists a y_k such that

$M_k y_k \equiv 1 \pmod{m_k}$, since $\gcd(M_k, m_k) = 1$

For each $i \neq k$,

$M_k \equiv 0 \pmod{m_i}$, since m_i is a factor in M_k.

and hence,

$M_k y_k \equiv 0 \pmod{m_i}$

Thus, we can choose $b_k = M_k y_k$, where y_k is a multiplicative inverse of M_k modulo m_k.

Hence,

$$\boxed{x = \sum_{k=1}^{n} M_k y_k a_k, \quad \text{where} \quad M_k y_k \equiv 1 \pmod{m_k}}$$

is a solution.

$\square$

Solution method

For $k = 1, 2, \ldots, n$

Let $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$

Let $M_k = \dfrac{m}{m_k}$

Determine y_k such that $M_k y_k \equiv 1 \pmod{m_k}$

Let $x = \sum_{k=1}^{n} M_k y_k a_k$

Note: If the moduli are <u>not</u> pairwise relatively prime, there <u>may</u> be a solution, but we cannot use the above method to find it (why not?)

Ex:

$x \equiv 2 \pmod{3}$ 2, 5, 8, 11, 14, 17, 20, 23, ...

$x \equiv 3 \pmod{5}$ 3, 8, 13, 18, 23, ...

$x \equiv 2 \pmod{7}$ 2, 9, 16, 23, ...

$m_1 = 3$

$M_1 = 5 \cdot 7 = 35$

$y_1 = 2$

$b_1 = M_1 y_1 = 70$

$$\equiv \begin{cases} 1 \pmod{3} \\ 0 \pmod{5} \\ 0 \pmod{7} \end{cases}$$

$m_2 = 5$

$M_2 = 3 \cdot 7 = 21$

$y_2 = 1$

$b_2 = M_2 y_2 = 21$

$$\equiv \begin{cases} 0 \pmod{3} \\ 1 \pmod{5} \\ 0 \pmod{7} \end{cases}$$

$m_3 = 7$

$M_3 = 3 \cdot 5 = 15$

$y_3 = 1$

$b_3 = M_3 y_3 = 15$

$$\equiv \begin{cases} 0 \pmod{3} \\ 0 \pmod{5} \\ 1 \pmod{7} \end{cases}$$

$m = 3 \cdot 5 \cdot 7 = 105$

$$\begin{aligned} x &= M_1 y_1 a_1 + M_2 y_2 a_2 + M_3 y_3 a_3 \\ &= 70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 \\ &= 233 \\ &= 23 + 2 \cdot 105 \end{aligned}$$

Set of solutions:

$\{ 23 + 105 \cdot k \mid k \in \mathbb{Z} \} =$

$\{ \ldots, -187, -82, 23, 128, 233, 338, \ldots \}$