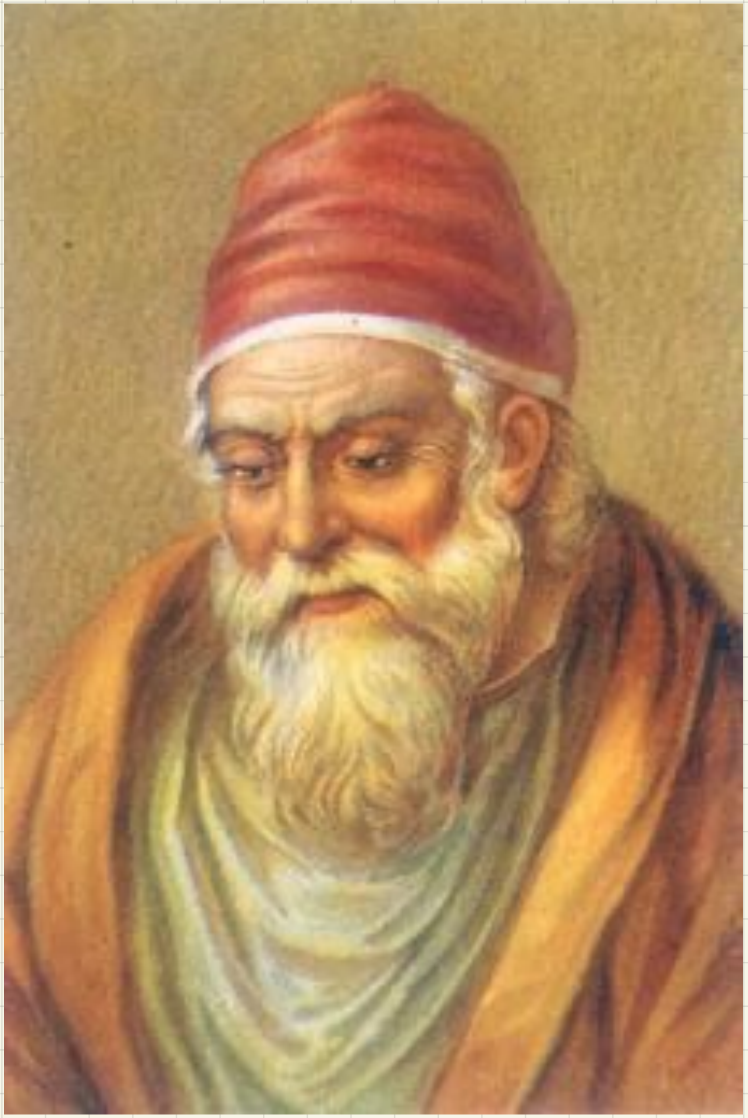


$\approx$ 325 – 270 B.C.

Euclid

Not Just Geometry!

$$\gcd(a,b) = ar - bs$$

Example:

300	18	12	6	0
1	0	1	-1	3
0	1	-16	17	-50

$$
\begin{aligned}
\gcd(300, 18) &= 300(-1) + 18(17) \\
&= 300(-1) - 18(-17) \qquad (\underset{=}{a}r - \underset{=}{b}s) \\
&= 300(-1 + \underbrace{18}) - 18(-17 + \underbrace{300}) \\
&= 300(\underset{\geq 0}{17}) - 18(\underset{\geq 0}{283})
\end{aligned}
$$

Application of Euclidean Alg.

Check if numbers are co-prime.

(They have only 1 common divisor, they share no prime factors)

Definition: $\boxed{a \text{ and } b \text{ are co-primes} \iff \gcd(a,b) = 1}$

We can conclude that (Extended Euclidean alg.)

$$a \,\&\, b \text{ are co-primes} \Rightarrow \gcd(a,b) = 1$$
$$\Rightarrow \exists\ r,s \geq 0.\ \ ar - bs = 1$$

The reverse direction also true. Assume $d \mid a \wedge d \mid b$

$$ar - bs = 1 \Rightarrow \underbrace{md}_{a}r - \underbrace{nd}_{b}s = 1 \Rightarrow d(mr - ns) = 1 \Rightarrow d = 1$$

$$\begin{tikzcd} & a \,\&\, b \text{ co-primes} \arrow[dr, bend left, "\text{Definition}"] & \\ ar-bs=1 \arrow[ur, bend left] & & \gcd(a,b)=1 \arrow[ll, bend left, "\text{Euclidean Alg.}"] \end{tikzcd}$$

All these statement are equivalent

- a & b are co-primes
- a & b have only one common divisor (it's 1)
- a & b share no prime factors
- $\gcd(a, b) = 1$
- $\exists\, r, s \geq 0.\ ar - bs = 1.$
- Also, we say a & b are relatively prime.

Prime numbers

Definition: A **prime** number p is an integer such that

- $p \geqslant 2$
- $d \mid p \Rightarrow (d=1 \vee d=p)$

In English, p is divisible by (a multiple of) only 1 and p.

If a number $\neq 1$ is not prime, it's called **composite**.

Two facts:

[prime factorization]
Every number >0 can be expressed as a product of primes

[Fundamental theorem of arithmetics]
Prime factorization is **UNIQUE**

proofs: see notes

Some nice properties of primes: (below p is prime)

- $p \mid ab \Rightarrow (p \mid a \vee p \mid b)$

Proof: $p \mid ab \Rightarrow ab = mp$ (ab is a multiple of p)

factor a, b, and m into primes. Since ab and mp are the same number, and prime factorization is unique p must appear on the left as one of the factors. So p is a factor of a or a factor of b (or both)

Note: the statement is not true if p is not prime.

$$10 \mid 4 \times 5 \quad \text{but} \quad 10 \nmid 4 \wedge 10 \nmid 5.$$

- $p \mid b \wedge p \nmid a \Rightarrow p \mid \frac{b}{a}$ (if $\frac{b}{a}$ is integer)

let $\frac{b}{a} = k$. Then $b = ak \Rightarrow \underbrace{mp}_{b} = ak$

Using the uniqueness, p must be one of the prime factors of ak, so

$$p \mid ak \Rightarrow (p \mid a \vee p \mid k)$$

But $p \nmid a$. Therefore $p \mid k$.

Also not necessarily true if p is not prime.

e.g. $4 \mid 12 \wedge 4 \nmid 6$, but $4 \nmid \frac{12}{6} = 2$

Conclusion: P is prime, then

- if p divides a product, it must divide one of the factors

- if p divides the numerator, but not the denominator, it must divide the ratio.

- other properties can be found in the notes

Equivalence Relation

Consider a set S and a relation R on $S \times S$

We will use the notation $\equiv$ when talking about "equivalence"

$a \equiv b$ to mean $(a,b) \in R$.

R is an equivalence relation on S means:

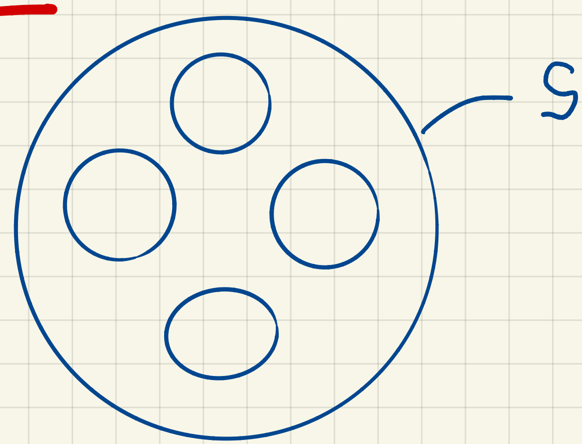
Reflexive : $a \equiv a$ $\qquad (a,a) \in R$

Symmetric : $a \equiv b \Rightarrow b \equiv a$ $\qquad (a,b) \in R \Rightarrow (b,a) \in R$

Transitive : $(a \equiv b \wedge b \equiv c) \Rightarrow a \equiv c$ $\qquad \left.\begin{array}{l}(a,b) \in R \\ (b,c) \in R\end{array}\right| \Rightarrow (a,c) \in R$

Example : '$=$' is an equivalence relation on $\mathbb{R}$

An equivalence relation on S partitions S into sets called classes of equivalence.



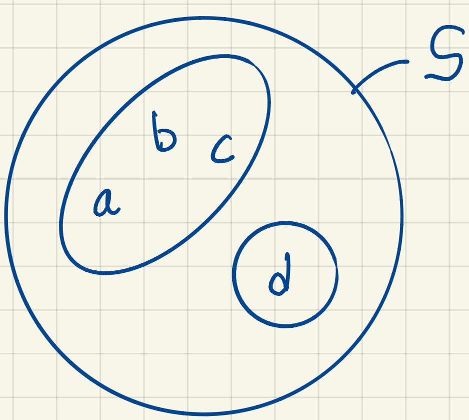
For all $a \in S$, define

$$C_a = \{x \in S : a \equiv x\}$$
$$= \{x \in S : (a, x) \in R\}$$

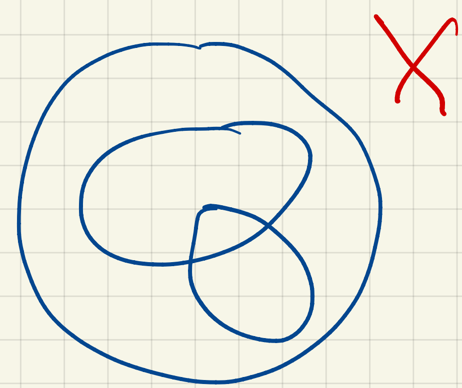
Example: $S = \{a, b, c, d\}$

$$R = \{(a,a), (b,b), (c,c), (d,d), (a,b), (b,c), (a,c), (b,a), (c,b), (c,a)\}$$

$C_a = \{a, b, c\}$ $\quad C_b = \{b, a, c\}$ $\quad C_c = \{c, a, b\}$ $\quad C_d = \{d\}$



Two classes of equivalence

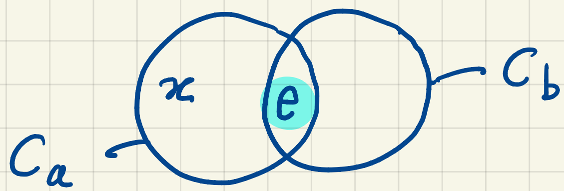


In general:

$$\bigcup_{a\in S} C_a = S \quad \left(\text{obvious, } \forall a \in S.\ a \in C_a \text{ since } a\equiv a\right)$$

$$C_a \cap C_b \neq \phi \implies C_a = C_b$$

Proof: Assume $C_a \cap C_b \neq \phi$



$e \in C_a \Rightarrow a \equiv e$

$e \in C_b \Rightarrow b \equiv e$

$$\left.\begin{array}{l} x\in C_a \Rightarrow a\equiv x \\ \underbrace{a\equiv e \Rightarrow e\equiv a}_{\text{symmetric}}\end{array}\right\} \Rightarrow \left.\begin{array}{c} b\equiv e\\ \underbrace{e\equiv x}_{\text{transitive}}\end{array}\right\} \xRightarrow[\text{transitive}]{} b\equiv x \Rightarrow x\in C_b$$

So $C_a \subset C_b$. Similarly $C_b \subset C_a$. Therefore $C_a = C_b$

Congruence

Notation: $a \equiv b \pmod{n}$ e.g. $7 \equiv 22 \pmod{5}$

- a & b have the same remainder in the division by n
- $n \mid a-b$ $(\underbrace{a-b}_{\text{could be negative, it's ok.}}$ is a multiple of $n)$
- We say "a is congruent to b modulo n"

Congruence is an equivalence relation. [from definition]

$$a \equiv a$$
$$a \equiv b \Rightarrow b \equiv a$$
$$(a \equiv b \wedge b \equiv c) \Rightarrow a \equiv c$$

Example: $n=7$, and the set $\mathbb{Z}$. 7 Equivalence classes

$$\{\ldots, -21, -14, -7, 0, 7, 14, 21, \ldots\}$$

$$\{\ldots, -20, -13, -6, 1, 8, 15, 22, \ldots\}$$

$$\{\ldots, -19, -12, -5, 2, 9, 16, 23, \ldots\}$$

$$\{\ldots, -18, -11, -4, 3, 10, 17, 24, \ldots\}$$

$$\{\ldots, -17, -10, -3, 4, 11, 18, 25, \ldots\}$$

$$\{\ldots, -16, -9, -2, 5, 12, 19, 26, \ldots\}$$

$$\{\ldots, -15, -8, -1, 6, 13, 20, 27, \ldots\}$$

Every number is equivalent to 0, 1, 2, 3, 4, 5, or 6.

- Imagine a "new world" of numbers where all numbers are $\{0, 1, 2, 3, 4, 5, 6\}$

- Not very imaginary! days of the week.

$$3 + 12 \equiv 1 \pmod 7 \qquad (15 \text{ is } 1)$$

Wed + 12 days = Monday

$$12 \equiv 5 \pmod 7$$

$$3 + 12 \equiv \underbrace{3 + 5}_{8} \equiv 1$$

$\equiv$ "behaves like" $=$