RATIONAL AND IRRATIONAL NUMBERS

Greatest common divisor

- Let $a \in \mathbb{Z}$. The set of divisors of a, Δa, is defined as:

$$\boxed{\Delta a = \{ x \in \mathbb{Z} \mid x | a \}}$$

- Let $a, b \in \mathbb{Z}$. The greatest common divisor $gcd(a,b)$ of a and b is defined as

$$\boxed{gcd(a,b) = \max(\Delta a \cap \Delta b)}$$

- Note that since $\Delta a = \Delta -a$, it follows that

$$\boxed{gcd(-a,b) = gcd(a,-b) = gcd(-a,-b) = gcd(a,b)}$$

Thm: Let $a, b \in \mathbb{Z} : a \neq 0 \vee b \neq 0$. Then

$$\boxed{gcd(a,b) = \min \{ ax + by \mid x, y \in \mathbb{Z} \wedge ax + by > 0 \}}$$

Proof

Let $S = \{ax+by \mid x,y \in \mathbb{Z} \wedge ax+by > 0\}$.
Since
$a \neq 0 \vee b \neq 0 \Rightarrow a^2+b^2 > 0 \Rightarrow a^2+b^2 \in S \Rightarrow$
$\Rightarrow S \neq \emptyset \Rightarrow \exists m \in S : m = \min S$.
Also note that
$m \in S \Rightarrow \exists\, x_0, y_0 \in \mathbb{Z} : m = ax_0 + by_0$.

- We will show that $m \in \Delta a$.
  From the division theorem:
  $\exists q, r \in \mathbb{Z} : a = mq + r \wedge 0 \leq r < m$
  We claim that $r = 0$. Assume that $r > 0$.
  $r = a - mq = a - (ax_0 + by_0)q =$
  $= a(1 - qx_0) + b(-qy_0) \Rightarrow r \in S \Rightarrow$
  $\Rightarrow r \geqslant \min S = m \Rightarrow r \geqslant m$ ← contradiction.

  Thus $r = 0 \Rightarrow a = mq \Rightarrow m \mid a \Rightarrow m \in \Delta a$.
  Similar argument gives $m \in \Delta b$.
  Thus $m \in \Delta a \cap \Delta b$.

- We will show that $\forall x \in \Delta a \cap \Delta b : x \leq m$.
  Let $x \in \Delta a \cap \Delta b$ be given. Then
  $x \in \Delta a \wedge x \in \Delta b \Rightarrow x \mid a \wedge x \mid b \Rightarrow$
  $\Rightarrow x \mid ax_0 + by_0 \Rightarrow x \mid m \Rightarrow x \leq m$
  Thus $\forall x \in \Delta a \cap \Delta b : x \leq m \Rightarrow$
  $\Rightarrow m = \max(\Delta a \cap \Delta b) = \gcd(a,b)$ □

Relatively prime numbers

- Let $a, b \in \mathbb{Z}$ such that $a \neq 0 \vee b \neq 0$.
  We say that

$$\boxed{a, b \text{ relatively prime} \Leftrightarrow \gcd(a,b) = 1}$$

Thm: $\boxed{a, b \text{ relatively prime} \Leftrightarrow \exists x_0, y_0 \in \mathbb{Z} : ax_0 + by_0 = 1}$

Proof

Define $S_{ab} = \{ax + by \mid x, y \in \mathbb{Z} \wedge ax + by > 0\}$.

($\Rightarrow$): Assume that
a, b relatively prime $\Rightarrow \gcd(a,b) = 1 \Rightarrow$
$\Rightarrow \min S_{ab} = 1 \Rightarrow \quad 1 \in S_{ab} \Rightarrow$
$\Rightarrow \exists x_0, y_0 \in \mathbb{Z} : ax_0 + by_0 = 1$.

($\Leftarrow$): Assume that
$\exists x_0, y_0 \in \mathbb{Z} : ax_0 + by_0 = 1 \Rightarrow 1 \in S_{ab}$
$\forall x \in S_{ab} : x > 0$ $\Rightarrow$
$\Rightarrow 1 = \min S_{ab}$
$\gcd(a,b) = \min S_{ab}$ $\Rightarrow \gcd(a,b) = 1 \Rightarrow$

$\Rightarrow a, b$ relatively prime $\square$

Thm: (Euclid's Lemma)

$$\left.\begin{array}{l} a, b, c \in \mathbb{Z} \wedge a \neq 0 \\ a \mid bc \\ a, b \text{ relatively prime} \end{array}\right\} \Rightarrow a \mid c$$

Proof

$a \mid bc \Rightarrow \exists q \in \mathbb{Z} : bc = aq.$ (1)

a, b rel. prime $\Rightarrow \exists x_0, y_0 \in \mathbb{Z} : ax_0 + by_0 = 1$

It follows that

$$c = c \cdot 1 = c(ax_0 + by_0) = cax_0 + bcy_0 =$$
$$= cax_0 + aqy_0 = a(cx_0 + qy_0) \Rightarrow a \mid c.$$

Thm:

$$\left.\begin{array}{l} a, b, c \in \mathbb{Z} - \{0\} \\ a, b \text{ relatively prime} \\ a \mid c \wedge b \mid c \end{array}\right\} \Rightarrow ab \mid c$$

Proof

a, b relatively prime $\Rightarrow \exists x_0, y_0 \in \mathbb{Z} : ax_0 + by_0 = 1$ (1)

$a \mid c \Rightarrow \exists q_1 \in \mathbb{Z} : c = aq_1$ (2)

$b \mid c \Rightarrow \exists q_2 \in \mathbb{Z} : c = bq_2.$ (3)

Thus

$$c = c \cdot 1 = c(ax_0 + by_0) = acx_0 + bcy_0 =$$
$$= a(bq_2)x_0 + b(aq_1)y_0 = ab(q_2 x_0 + q_1 y_0) \Rightarrow ab \mid c.$$

EXERCISES

(1) Write a necessary and sufficient condition, using quantifiers, for the statement:
$a, b \in \mathbb{Z}$ are NOT relatively prime
by negating the relevant theorem.

(2) Show that the following pairs are always relatively prime
a) $2n+1, 3n+2$ with $n \in \mathbb{Z}$
b) $2n^2+3, 3n^2+4$ with $n \in \mathbb{Z}$

(3) Let $a, b, c \in \mathbb{Z}$. Prove the following properties of the greatest-common-divisor:

a) $\gcd(ca, cb) = c \gcd(a, b)$
b) $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$
c) $\gcd(a, bc) = \gcd(a, \gcd(a,b)c)$
d) $\gcd(a,b) = 1 \Rightarrow \gcd(a^2, b^2) = 1$
e) $\gcd(a^2, b^2) = [\gcd(a,b)]^2$

[Hint: Use (a) to prove (b). Use (c) to prove (d). Use (d) to prove (e)]

(4) Let $a, b, c \in \mathbb{Z}$. Prove that $\gcd(a+Bc, b) = \gcd(a, b)$.
[Hint: Show that $\Delta a \cap \Delta b = \Delta a+bc \cap \Delta b$]

⑤ Let $a, b, c \in \mathbb{Z} - \{0\}$ with a, b relatively prime. Prove that

a) $a^2 \mid b^2 c \Rightarrow a^2 \mid c$

b) $a^2 \mid c \wedge b^2 \mid c \Rightarrow (ab)^2 \mid c$

⑥ Let $a, b, c \in \mathbb{Z} - \{0\}$ such that a, b are relatively prime and a, c are relatively prime Show that a, bc are relatively prime.

↳ For ⑤ and ⑥ you may use the results of ③ without proof.

Prime numbers

- Let $p \in \mathbb{Z}$. We say that
  p prime $\Leftrightarrow \Delta_p = \{\pm 1, \pm p\}$
  p composite $\Leftrightarrow$ p not prime.

Thm: Let $n \in \mathbb{N}$ with $n \geq 2$.

$$n \text{ composite} \Leftrightarrow \exists a, b \in \mathbb{Z}: \begin{cases} n = ab \\ 1 < a < n \wedge 1 < b < n \end{cases}$$

Proof

We note that $\{\pm 1, \pm n\} \subseteq \Delta_n$. Le
n composite $\Rightarrow \Delta_n \neq \{\pm 1, \pm n\} \Rightarrow \{\pm 1, \pm n\} \subset \Delta_n$
Let $\xi = \Delta_n - \{\pm 1, \pm n\} \neq \emptyset$. Choose $a \in \xi$.
Then $a \mid n \Rightarrow \exists b \in \mathbb{Z}: n = ab$
Since $a \mid n$ and $a \in \xi \Rightarrow 1 < a < n$.
Likewise, since $a < n$ and b is the quotient, $1 < b < n$.

Thm: Let $b, c, p \in \mathbb{Z}$. Then

$$p \text{ prime} \wedge p \mid bc \Rightarrow p \mid b \vee p \mid c$$

Proof

Case 1: If $p \mid b \Rightarrow p \mid b \vee p \mid c$.

Case 2: Assume $p \nmid b \Rightarrow \pm p \notin \Delta_b \Rightarrow$

$\Rightarrow \Delta_b \cap \Delta_p = \Delta_b \cap \{\pm 1, \pm p\} = \{\pm 1\} \Rightarrow$

$\Rightarrow \gcd(b,p) = \max \Delta_b \cap \Delta_p = \max\{\pm 1\} = 1$

$\Rightarrow$ b, p relatively prime $\Longrightarrow p \mid c \Rightarrow$ ($p \mid bc$)

Euclid Lemma

$\Rightarrow p \mid b \vee p \mid c$. ∎

- Using the method of induction we can prove the stronger result:

$$\left.\begin{array}{l} p, b_1, b_2, \ldots, b_n \in \mathbb{Z} - \{0\} \\ p \text{ prime} \wedge p \mid b_1 b_2 \cdots b_n \end{array}\right\} \Rightarrow \exists a \in [n] : p \mid b_a$$

Here $[n] = \{1, 2, 3, \ldots, n\}$.

↳ Fundamental Theorem of Arithmetic

- Let $b \in \mathbb{N}$ with $b \geq 2$. A sequence $(p_1, p_2, \ldots, p_n)$ is a prime number factorization of b if and only if:

a) $b = p_1 p_2 \cdots p_n$ AND

b) $p_1 \leq p_2 \leq \cdots \leq p_n$

• We will now show:

Thm: If $b \in \mathbb{N}$ with $b \geq 2$, then b has a unique prime number factorization.

Proof

• Existence

$b = 2$ has the obvious prime factorization (2).

Assume that

$\forall x \in \mathbb{N}: (2 \leq x \leq k) \Rightarrow x$ has a prime factorization.

We will show that $k+1$ has a prime factorization.

Case 1: If $k+1$ prime $\Rightarrow (k+1)$ is the obvious prime factorization.

Case 2: If $k+1$ composite $\Rightarrow$

$$\Rightarrow \exists x, y \in \mathbb{Z}: \begin{cases} k+1 = xy & (1) \\ 1 < x < k+1 \wedge 1 < y < k+1 & (2) \end{cases}$$

From (2): x, y have a prime factorization $\Rightarrow$

$\Rightarrow k+1 = xy$ has a prime factorization.

• Uniqueness

Assume that $k+1$ has two distinct prime factorizations

$$k+1 = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

such that for some $a \in [\min\{m,n\}]$

$p_a \neq q_a$, and

$p_\lambda = q_\lambda$, $\forall \lambda \in [a-1]$ if $a > 1$.

It follows that

$$p_a \cdots p_n = q_a \cdots q_m \Rightarrow p_a \mid q_a \cdots q_m \Rightarrow$$

$$\Rightarrow \exists b \in \mathbb{Z}_{a,m} : \left.\begin{matrix} p_a \mid q_b \\ q_b \text{ } p_a \text{ prime} \end{matrix}\right\} \Rightarrow \underline{p_a = q_b}$$

It follows that $p_a = q_b \geq q_a \Rightarrow p_a \geq q_a$ (1)
and

$$p_a \mid q_a \cdots q_m \Rightarrow$$
$$\Rightarrow p_a \leq q_a \cdots q_m \leq q_a \Rightarrow p_a \leq q_a \quad (2)$$

From (1) and (2): $p_a = q_a \leftarrow$ contradiction since $p_a \neq q_a$. ∎

- An immediate consequence of this result is that if $p_1, p_2, \ldots, p_n, \ldots$ is the increasing sequence of all prime numbers, then any $b \in \mathbb{N}$ with $b \geq 2$ has a unique canonical factorization of the form

$$\boxed{b = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}}$$

with $a_k \in \mathbb{N}$, $\forall k \in [n]$.

- Another Immediate consequence is the statement that every integer $m>1$ has a prime factor:

$$\boxed{m \in \mathbb{N} \wedge m > 1 \Rightarrow \exists p \in \mathbb{N} : p \text{ prime} \wedge p \mid m}$$

↳ No maximum prime number

- We will now show that there is no maximum prime number. This implies that there are infinite prime numbers.
- Let P be the set of all prime numbers:

$$\boxed{P = \{x \in \mathbb{N} \mid x \text{ prime}\}}$$

Thm : $\boxed{\forall x \in \mathbb{N} : \exists y \in P : y > x}$

Proof

Assume $\exists x \in \mathbb{N} : \forall y \in P : y \leq x \Rightarrow P \subseteq [x]$
$\Rightarrow P = \{p_1, p_2, \dots, p_n\}$ with $n \leq x$.
Let $p_n = \max P$. Define $m = p_1 p_2 \cdots p_n + 1$.
Since
$m = p_1 p_2 \cdots p_n + 1 > p_1 p_2 \cdots p_n > p_n \Rightarrow m \notin P \Rightarrow$
$\Rightarrow m$ composite $\Rightarrow \exists a \in [n] : p_a \mid m \Rightarrow$

$\Rightarrow \exists q \in \mathbb{Z} : m = p_a q$

It follows that

$$1 = m - p_1 p_2 \cdots p_n = p_a q - p_1 p_2 \cdots p_n =$$
$$= p_a (q - p_1 \cdots p_{a-1} p_{a+1} \cdots p_n) \Rightarrow$$

$\Rightarrow p_a \mid 1 \Rightarrow p_a \leq 1 \longleftarrow$ Contradiction.

EXERCISES

(7) Write a necessary and sufficient condition for the statement "p is prime", using quantifiers, by negating the definition of "p is composite". Note that the definition can be shortened if you first define:

$$A_n = \{(a,b) \in \mathbb{Z}\times\mathbb{Z} \mid 1 < a < n \wedge 1 < b < n\}$$

and use it appropriately.

(8) Let $n \in \mathbb{N}$. Show that

$$(\exists k \in \mathbb{Z} : n = k^3 + 1 \geq 3) \Rightarrow n \text{ not prime}$$

(9) Let $p \in \mathbb{N}$ be an odd prime. Prove that

a) $\exists k \in \mathbb{Z} : (p = 4k+1 \vee p = 4k+3)$

b) $\exists k \in \mathbb{Z} : (p = 6k+1 \vee p = 6k+5)$

(10) Let $p, q \in \mathbb{N}$. Show that

$$p, q \text{ primes} \wedge p \geq q \geq 5 \Rightarrow 24 \mid (p^2 - q^2)$$

(11) Let $k \in \mathbb{N} - \{0\}$. Show that

$$2^k - 1 \text{ prime} \Rightarrow k \text{ prime}.$$

(12) Use proof by induction to show that:

$$\left.\begin{array}{l} p, b_1, b_2, \ldots, b_n \in \mathbb{Z} - \{0\} \\ p \text{ prime} \wedge p \mid b_1 b_2 \cdots b_n \end{array}\right\} \Rightarrow \exists a \in [n] : p \mid b_a$$

Rational numbers and Irrationality proofs

- The set of all <u>rational numbers</u> is defined as

$$\boxed{\mathbb{Q} = \{ a/b \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z} - \{0\} \}}$$

therefore, equivalently, we have

$$\boxed{x \in \mathbb{Q} \Leftrightarrow \exists\, a \in \mathbb{Z} : \exists\, b \in \mathbb{Z} - \{0\} : x = a/b}$$

- If $x = a/b$ with $a \in \mathbb{Z}$ and $b \in \mathbb{Z} - \{0\}$ is a fractional representation of x, we say that a/b is <u>irreducible</u> if and only if $\gcd(a,b)$.

- From the result (see homework) that

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

we see that any fractional representation a/b can be made irreducible by dividing both numerator a and denominator b

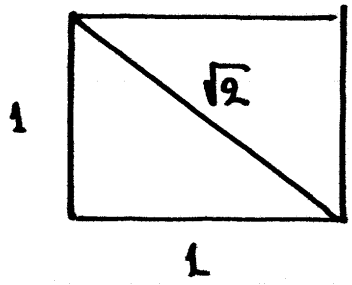
with the $\gcd(a,b)$. It follows that

$$x \in \mathbb{Q} \Leftrightarrow \exists a \in \mathbb{Z} : \exists b \in \mathbb{Z} - \{0\} : (x = a/b \wedge \gcd(a,b) = 1)$$

- More than 2500 years ago, the Pythagoreans discovered that there are numbers, arising from geometric constructions, that are NOT rational numbers.

Irrationality of $\sqrt{2}$

From the Pythagorean theorem we know that the diagonal of a square with side length 1, has length $\sqrt{2}$:



We will now show that

Thm : $\sqrt{2} \notin \mathbb{Q}$

Proof

Assume that

$\sqrt{2} \in \mathbb{Q} \Rightarrow \exists a \in \mathbb{Z} : \exists b \in \mathbb{Z} - \{0\} : (\sqrt{2} = a/b \wedge \gcd(a,b) = 1)$

It follows that

$$\sqrt{2} = \frac{a}{b} \Rightarrow a = \sqrt{2}\, b \Rightarrow a^2 = 2b^2 \Rightarrow a^2 \text{ even}$$

$$\Rightarrow a \text{ even} \Rightarrow \exists k \in \mathbb{Z} : a = 2k$$

and therefore

$$(2k)^2 = 2b^2 \Rightarrow 4k^2 = 2b^2 \Rightarrow b^2 \text{ even} \Rightarrow$$

$$\Rightarrow \left.\begin{array}{l} b \text{ even} \\ a \text{ even} \end{array}\right\} \Rightarrow \gcd(a,b) \geq 2$$

↑ contradiction.

Thus, $\sqrt{2} \notin \mathbb{Q}$. □

- This proof is a classic but it cannot be easily generalized for other square roots.

↳ Irrationality of $\sqrt{p}$

- Let $x \in \mathbb{Q} - \{0\}$. It is easy to see that x has a unique prime factorization

$$x = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

with $p_1, p_2, \ldots, p_n$ the first n prime numbers and with $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.
Thus

$$\boxed{x \in \mathbb{Q} \iff \forall k \in [n] : a_k \in \mathbb{Z}.}$$

- We say that

$$\boxed{x \text{ perfect square} \iff \exists y \in \mathbb{Q} : y^2 = x}$$

An immediate consequence of this definition is that

$$\boxed{x \text{ perfect square} \iff \forall k \in [n] : a_k \text{ even}}$$

- We may now prove that

$$\boxed{x \text{ not perfect square} \Rightarrow \sqrt{x} \notin \mathbb{Q}}$$

Proof (due to Gauss)

Let $x = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ with $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and $p_1, p_2, \ldots, p_n$ the n first prime numbers.
Assume $\sqrt{x} \in \mathbb{Q}$
Since $\sqrt{x} = (p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})^{1/2} =$

$$= p_1^{a_1/2} p_2^{a_2/2} \cdots p_n^{a_n/2}$$

It follows that

$$\sqrt{x} \in \mathbb{Q} \Rightarrow \forall k \in [n] : a_k/2 \in \mathbb{Z} \Rightarrow$$
$$\Rightarrow \forall k \in [n] : a_k \text{ even.} \quad (1)$$

On the other hand

$$x \text{ not a perfect square} \Rightarrow \exists k \in [n] : a_k \text{ odd} \quad (2)$$

From (1) and (2) we have a contradiction, thus $\sqrt{x} \notin \mathbb{Q}$. $\square$