Lesson 2
Divisions

Unit 1
Divisibility

Divisibility

$\mathbb{N} = \{0, 1, 2, 3, ...\}$ **Naturals**

$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ **Integers**

DEFINITION

Let $a, b \in \mathbb{Z}, b \neq 0$. We say that b divides a (we write $b \mid a$) if there is $c \in \mathbb{Z}$ such that

$$a = bc.$$

NO meaning if b=0

EXAMPLE $2 \mid 4$ **but** $2 \nmid 5$

QUESTION **Does 1 divide any integer?**

Divisibility

PROPOSITION **Let a, b, c be integers. $(a \neq 0)$**

(a) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

(b) *If* $a \mid b$ *and* $b \mid a$, *then* $a = \pm b$. $(b \neq 0)$

(c) *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (b + c)$ *and* $a \mid (b - c)$.

Proof.

Divisibility

DEFINITION

An *even* number is an integer that is divisible by 2, otherwise it is *odd*

The *divisors of a natural number* by convention are the positive divisors.

EXAMPLE $-2 \mid 6$ but the divisors of 6 are $1, 2, 3, 6.$

EXAMPLE **-4 is even, 13 is odd**

Euclidean division

PROPOSITION (Euclidean division)

Let a, b be naturals with $b > 0$. Then there exist unique integers q (the quotient) and r (the remainder) so that

Admitted

$$a = bq + r, \quad 0 \leq r < b$$

EXAMPLE b divides a if and only if $r = 0$!

EXAMPLE $a = 27, b = 7$: $q = 3, r = 6$.

EXAMPLE $a = 7 \times 4 - 5$

What is the quotient of $a : 7$? 3

What is the remainder of $a : 7$? 2

$$a = 7 \times 3 + 7 - 5 = 7 \times \boxed{3} + \boxed{2}, \; 0 \leq 2 < 7$$

Euclidean division in practice

Let a, b be naturals with $b > 0$. $a = bq + r, \quad 0 \leq r < b$

Then $q = \left[\frac{a}{b}\right], r = a - b\left[\frac{a}{b}\right].$

Indeed $\frac{a}{b} = q + \frac{r}{b}, 0 \leq \frac{r}{b} < 1.$

Thus $\left[\frac{a}{b}\right] = q. \quad r = a - bq = a - b\left[\frac{a}{b}\right].$

EXAMPLE $a = 15476, b = 137.$ Find $q, r.$

And now…VOTE!

Should universities prioritize job-market-oriented education over research and theoretical knowledge in postgraduate programs?

Answer soon:

- **YES**
- **NO**
- **X (abstain)**

Euclidean division

AN AMUSING CRYPTOGRAPHIC APPLICATION

You are *N* students: not too big, say less than 10

You vote either YES, or NO, or Abstain to a Proposition: decide your VOTE

Voters: One by one

- Voter n. 1: Vote YES? Add *N+1.* Vote NO? Add 1. Abstain: 0. Write just the sum in a paper.
- Voter n. 2. Give the paper to Voter n.2. Vote YES? Add *N+1.* Vote NO? Add 1. Abstain: 0

.....

Tell me just the final number: I will tell how many voted yes/no/abstain

Euclidean division

AN AMUSING APPLICATION

How does it work?

Binary representation

Every natural *m* can be expressed in binary code

DEFINITION

Let $m \in \mathbb{N}$. We write $m = (m_{B-1} \dots m_1 m_0)_2$ if $m = m_0 + m_1 \times 2 + \cdots + m_{B-1} 2^{B-1}$ and $m_i \in \{0, 1\}$.

$m_i \in \{0, 1\}$: bits

EXAMPLE

Convert 112 in binary

B=7 raws

a/b: Quotient Division of a by b	Remainder (R)

in the last raw: the quotient is 0

$$112 = 1110000_2 = 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$$

Binary representation

Every natural *m* can be expressed in binary code

DEFINITION

Let $m \in \mathbb{N}$. We write $m = (m_{B-1} \dots m_1 m_0)_2$ if $m = m_0 + m_1 \times 2 + \cdots + m_{B-1} 2^{B-1}$ and $m_i \in \{0, 1\}$.

$m_i \in \{0, 1\}$: bits

EXAMPLE

Convert 112 in binary

B=7 raws

a/b: Quotient Division of a by b	Remainder (R)
112 / 2 = 56	0
56 / 2 = 28	0
28 / 2 = 14	0
14 / 2 = 7	0
7 / 2 = 3	1
3 / 2 = 1	1
1 / 2 = 0	1

in the last raw: the quotient is 0

$$112 = 1110000_2 = 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$$

Binary representation

EXAMPLE

Write 33 in base 2

Binary representation

REMARK

If $m = (m_{B-1} \dots m_1 m_0)_2$ then $m < 2^B$.

If m has B bits in base 2 then $m < 2^B$.

Indeed, $m = m_0 + m_1 \times 2 + \cdots + m_{B-1} 2^{B-1} \leq 1 + 2 + \cdots + 2^{B-1}$

$$= \frac{2^B - 1}{2 - 1} = 2^B - 1.$$

Binary representation

PROPOSITION Let $m \in \mathbb{N}$, $m < 2^B$ and consider the following division by 2 process:

B raws

$$
\begin{aligned}
m &= 2q_0 + m_0, 0 \leq m_0 < 2,\\
q_0 &= 2q_1 + m_1, 0 \leq m_1 < 2,\\
q_1 &= 2q_2 + m_2, 0 \leq m_2 < 2,\\
&\cdots
\end{aligned}
$$

in the last raw: the quotient is 0

$$q_{B-2} = 2 \times q_{B-1} + m_{B-1}, 0 \leq m_{B-1} < 2.$$

Then $q_{B-1} = 0$ and $m = m_0 + 2m_1 + \cdots 2^{B-1}m_{B-1}$.

Proof. **Try with B=3**

$$m = 2q_0 + m_0 < 2^3 \Rightarrow 2q_0 < 2^3 \Rightarrow q_0 < 2^2$$

$$q_0 = 2q_1 + m_1 < 2^2 \Rightarrow q_1 < 2$$

$$q_1 = 2q_2 + m_2 < 2 \Rightarrow q_2 < 1 \Leftrightarrow q_2 = 0$$

$$
\begin{aligned}
m &= 2q_0 + m_0\\
&= 2(2q_1 + m_1) + m_0\\
&= 2(2m_2 + m_1) + m_0 \ = 2^2m_2 + 2m_1 + m_0
\end{aligned}
$$

□

Binary representation

PROPOSITION Let $m \in \mathbb{N}$, $m < 2^B$ and consider the following division by 2 process:

B raws

$$
\begin{aligned}
m &= 2q_0 + m_0, 0 \leq m_0 < 2, \\
q_0 &= 2q_1 + m_1, 0 \leq m_1 < 2, \\
q_1 &= 2q_2 + m_2, 0 \leq m_2 < 2, \\
&\cdots \\
q_{B-2} &= 2 \times q_{B-1} + m_{B-1}, 0 \leq m_{B-1} < 2.
\end{aligned}
$$

in the last raw: the quotient is 0

Then $q_{B-1} = 0$ and $m = m_0 + 2m_1 + \cdots 2^{B-1} m_{B-1}$.

$m < 2^B$

$m = 2q_0 + m_0, 0 \leq m_0 < 2,$
$q_0 = 2q_1 + m_1, 0 \leq m_1 < 2,$
$q_1 = 2q_2 + m_2, 0 \leq m_2 < 2,$
$\cdots$
$q_{B-2} = 2 \times q_{B-1} + m_{B-1}, 0 \leq m_{B-1} < 2.$
Then $q_{B-1} = 0$ and $m = m_0 + 2m_1 + \cdots 2^{B-1}m_{B-1}.$

Proof. $m = 2q_0 + m_0$:

$2q_0 \leq m < 2^B \Rightarrow$

$2q_1 \leq q_0 < 2^{B-1} \Rightarrow$

.....

The last line is $q_{B-2} = 2q_{B-1} + m_{B-1} = m_{B-1}.$

$$m = 2q_0 + m_0$$
$$= 2(2q_1 + m_1) + m_0 = 2^2 q_1 + 2m_1 + m_0$$
$$= 2^2(2q_2 + m_2) + 2m_1 + m_0 = 2^3 q_2 + 2^2 m_2 + 2m_1 + m_0$$
$$= \cdots\cdots$$
$$= 2^{B-1} q_{B-2} + 2^{B-2} m_{B-2} + \cdots + 2m_1 + m_0$$
$$= 2^{B-1} m_{B-1} + 2^{B-2} m_{B-2} + \cdots + 2m_1 + m_0 \quad \square$$

Binary representation

NUMBER OF BITS

COROLLARY **A natural m has a binary representation with $B \geq 1$ bits ($m = m_{B-1}...m_0$ with $m_{B-1} = 1$) iff**

$$2^{B-1} \leq m < 2^B.$$

In particular $B = [\log_2 m] + 1$.

Proof. **$m < 2^B \Rightarrow$ at most B bits.**

If $B - 1$ bits are enough then $m < 2^{B-1}$, a contradiction. $\square$

EXAMPLE **What is the number of bits of 368932 in base 2?**

$\log_2(368932) = 18.4...$ $\quad B = [\log_2(368932)] + 1 = 19$

Indeed $368932 = 1011010000100100100_2$

Unit 2
Greatest Common Divisor

gcd: Greatest Common Divisor

The divisors of 12 are 1, 2, 3, 4, 6, 12

The divisors of 18 are 1, 2, 3, 6, 9

The set of common divisors of 18 and 12 is $\{1, 2, 3, 6\}$

Its largest element is 6. We say that 6 := gcd(18, 12)

DEFINITION When we write $\gcd(a, b)$ we subsume that a or b is non-zero

Let a, b be integers not both 0. Then the set of common divisors has a largest element d called the greatest common divisor of a and b. We write $d = \gcd(a, b)$ It is well defined!

EXAMPLE **gcd(12, 0)=?**

gcd: Greatest Common Divisor

THE EUCLIDEAN ALGORITHM

EXAMPLE Find $\gcd(119, 259)$

7 is the last non-zero remainder

7=gcd(119, 259)

$$259 = 2 \cdot 119 + 21 \qquad 7 \mid 259 \qquad c \mid 21$$

$$119 = 5 \cdot 21 + 14 \qquad 7 \mid 119 \qquad c \mid 14$$

$$21 = 1 \cdot 14 + \boxed{7} \qquad 7 \mid 21 \qquad c \mid 7$$

$$14 = 2 \cdot 7 + 0. \qquad 7 \mid 14$$

Proof. a) $7 \mid 119$ and $7 \mid 259$

b) If $c \mid 119$ and $c \mid 259$ then $c \mid 7$

gcd: Greatest Common Divisor

THE EUCLIDEAN ALGORITHM

THEOREM (Euclidean Algorithm) Let $a, b > 0$ with $a \geq b$.

The following algorithm computes $\gcd(a, b)$ in a finite number of steps:

1. Let $r_0 := a, r_1 := b$.
2. Set $i = 1$.
3. Divide r_{i-1} by r_i to get a quotient q_i and remainder r_{i+1}:

$$r_{i-1} = r_i q_i + r_{i+1} \text{ with } 0 \leq r_{i+1} < r_i.$$

4. If $r_{i+1} = 0$ then $r_i = \gcd(a, b)$.
5. Otherwise $r_{i+1} > 0$: replace i by $i + 1$ and go to Step 3.

gcd: Greatest Common Divisor

THE EUCLIDEAN ALGORITHM

THEOREM (Euclidean Algorithm) Let $a, b > 0$ with $a \geq b$.

The following algorithm computes $\gcd(a, b)$ in a finite number of steps:

1. Let $r_0 := a, r_1 := b$.
2. Set $i = 1$.
3. Divide r_{i-1} by r_i to get a quotient q_i and remainder r_{i+1}:
$$r_{i-1} = r_i q_i + r_{i+1} \text{ with } 0 \leq r_{i+1} < r_i.$$
4. If $r_{i+1} = 0$ then $r_i = \gcd(a, b)$.
5. Otherwise $r_{i+1} > 0$: replace i by $i + 1$ and go to Step 3.

The process ends because $r_0 > r_1 > r_2 > \ldots \geq 0$.

Proof.

The process ends because $r_0 > r_1 > r_2 > \ldots \geq 0$.

Let $d := r_{n+1}$ be the last non zero remainder, $n \geq 0$.

$$\begin{array}{l|l|l}
d \mid r_2, d \mid r_1 \Rightarrow d \mid r_0 & r_0 = r_1 q_1 + r_2 & c \mid a = r_0, c \mid b = r_1 \Rightarrow c \mid r_2 \\
d \mid r_3, d \mid r_2 \Rightarrow d \mid r_1 & r_1 = r_2 q_2 + r_3 & c \mid r_1, c \mid r_2 \Rightarrow c \mid r_3 \\
\ldots\ldots\ldots & \ldots\ldots\ldots & \ldots\ldots\ldots \\
d \mid r_{n+1}, d \mid r_n \Rightarrow d \mid r_{n-1} & r_{n-1} = r_n q_n + r_{n+1} & c \mid r_{n-1}, c \mid r_n \Rightarrow c \mid r_{n+1} = d \\
d = r_{n+1} \mid r_n & r_n = r_{n+1} q_{n+1} = d q_{n+1} &
\end{array}$$

i) d divides a, b: $d \mid a$ and $d \mid b$.

ii) d is the greatest common divisor: if $c \mid a$ and $c \mid b$ then $c \mid d$. $\square$

gcd: Greatest Common Divisor

THE EUCLIDEAN ALGORITHM

EXAMPLE **Find gcd(123, 456) by means of the Euclidean algorithm:**

EXAMPLE **Find gcd(1776, 1848) by means of the Euclidean algorithm:**

Unit 3
Extended Euclidean algorithm

gcd: the extended Euclidean algorithm

EXAMPLE

a b

$$259 = 2 \cdot 119 + \boxed{21} \qquad 21 = a - 2b$$

$$119 = 5 \cdot 21 + \boxed{14} \qquad 14 = b - 5(a - 2b) = -5a + 11b$$

$$21 = 1 \cdot 14 + \boxed{7} \qquad 7 = (a - 2b) - (-5a + 11b) = 6a - 13b$$

$$14 = 2 \cdot 7 + 0.$$

$$\gcd(a, b) = 7 = 6a - 13b$$

$\gcd(a, b)$ is a linear combination of a, b

gcd: the extended Euclidean algorithm

PROPOSITION (Extended Euclidean algorithm)

Let a, b naturals non all zero. If $d = \gcd(a, b)$ then there are $u, v \in \mathbb{Z}$ satisfying

$$d = au + bv$$

Proof.

If d=gcd(a,b):

$$a = q_1 b + r_1, \quad with\ 0 \le r_1 < b$$
$$b = q_2 r_1 + r_2, \quad with\ 0 \le r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3, \quad with\ 0 \le r_3 < r_2$$
$$\vdots$$
$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, \quad with\ 0 \le r_{n-1} < r_{n-2}$$
$$r_{n-2} = q_n r_{n-1} + 0.$$

$r_{n-1} = d$

r_1 **lin. comb. of** a, b

r_2 **lin. comb. of** b, r_1

r_3 **lin. comb. of** r_1, r_2

$\vdots$

$d = r_{n-1}$ **lin. comb. of** r_{n-3}, r_{n-2}

gcd: the extended Euclidean algorithm

EXERCISE **Evaluate $\gcd(14, 100)$ and express it as a linear combination of 14 and 100.**

gcd: the extended Euclidean algorithm

EXERCISE **Evaluate $\gcd(182, 630)$ and express it as a linear combination of 182 and 630.**

gcd: the extended Euclidean algorithm

Let a, b naturals non all zero. If $d = \gcd(a, b)$ then there are $u, v \in \mathbb{Z}$ satisfying

$$d = au + bv$$

REMARK u, v are not unique!

$$u' = u + kb, v' = v - ka \quad (k \in \mathbb{Z})$$

$$au + bv' = a(u + kb) + b(v - ka) = au + \cancel{kab} + bv - \cancel{kab} = au + bv = d$$

Unit 4
Coprime numbers

Coprime integers

DEFINITION Two integers are relatively prime (or coprime) if $\gcd(a, b) = 1$.

EXAMPLE 32 and 15 are relatively prime.

PROPOSITION (Characterisation of coprime numbers)

a, b are relatively prime if and only if there are integers u, v such that $au + bv = 1$

Proof. If $\gcd(a, b) = 1$ then there are $u, v \in \mathbb{Z}$: $au + bv = 1$.

Conversely, if $au + bv = 1$ for some $u, v \in \mathbb{Z}$ and $d \mid a, d \mid b$, then $d \mid (au + bv) = 1$. Thus $\gcd(a, b) = 1$. □

Integers that are relatively prime

REMARK $a \mid bc \not\Rightarrow a \mid b$ or $a \mid c$.

EXAMPLE $4 \mid 2 \times 6$ but $4 \nmid 2, 4 \nmid 6$

An important application of the characterisation of coprime numbers

PROPOSITION Let a, b be coprime, $a \neq 0$, and $a \mid bc$. Then $a \mid c$.

COPRIME

Proof. Let $u, v \in \mathbb{Z}$ such that $au + bv = 1$. Then $auc + bvc = c$.

Now $a \mid a(uc)$, $a \mid (bc)v$ whence $a \mid auc + bvc = c$. $\square$

Linear Diophantine EQUATION au+bv=c

a, b coprime

COROLLARY Let a, b be relatively prime. For all $c \in \mathbb{Z}$ the equation $au + bv = c$ has integer solutions u, v.

How to find a particular solution?

1. Find $u_0, v_0 \in \mathbb{Z}$: $au_0 + bv_0 = 1$ (extended Euclidean algorithm)

2. $c(au_0 + bv_0) = c$: $\quad a(cu_0) + b(cv_0) = c.$

EXAMPLE **Find a solution to 10u+21v=5**

All the solutions of the linear Diophantine EQUATION au+bv=c

a, b coprime

PROPOSITION (ALL the integer solutions to au+bv=c)

Let a, b be relatively prime and $u_0, v_0 \in \mathbb{Z}$ such that $au_0 + bv_0 = c$. Then all the solutions to $au + bv = c$ are of the form $u = u_0 + kb, v = v_0 - ka$ for any $k \in \mathbb{Z}$.

Proof. Clearly $u = u_0 + kb, v = v_0 - ka$ are solutions:
$a(u_0 + kb) + b(v_0 - ka) = au_0 + bv_0 = c.$

Conversely, assume $au + bv = au_0 + bv_0 = c$. Then $a(u - u_0) = b(v_0 - v)$.

Assume $a \neq 0$. Then $a \mid b(v_0 - v)$: since $\gcd(a, b) = 1$ we have $a \mid v_0 - v$.

Let $k \in \mathbb{Z}$ be such that $v_0 - v = ka$. Thus $a(u - u_0) = b(ka) = a(kb)$.

It follows that $u - u_0 = kb$. $\square$

All the solutions of the linear Diophantine EQUATION au+bv=c

a, b coprime

EXAMPLE

A solution to $10u+21v=5$ is ($u_0=-10$, $v_0=5$). Find all the solutions.

generalisation to more than 2 numbers

DEFINITION

If $x_1, ..., x_m$ $\gcd(x_1, ..., x_m)$ is the greatest common divisor to $x_1, ..., x_m$.

PROPOSITION **If $x_1, ..., x_m$ are integers with $\gcd(x_1, ..., x_m) = 1$ there are**

$u_1, ..., u_m \in \mathbb{Z}$: $\quad u_1 x_1 + \cdots + u_m x_m = 1.$

Unit 5
The Linear Diophantine equation au+bv=c
The general case

The linear Diophantine equation au+bv=c in the general case

We do not assume anymore that a, b are coprime

PROPOSITION Let a, b integers not all 0. The equation $au + bv = c$ has solutions $u, v \in \mathbb{Z}$ if and only if $\gcd(a, b) \mid c$.

Proof. Assume $c = k \gcd(a, b)$. There are $u, v \in \mathbb{Z}$: $au + bv = \gcd(a, b)$.

Thus $c = k \gcd(a, b) = a(ku) + b(kv)v$.

Conversely let u, v: $au + bv = c$.

Since $\gcd(a, b) \mid a, \gcd(a, b) \mid b$ then $\gcd(a, b) \mid au + bv = c$. $\square$

How to find a solution to au+bv=c

THE GENERAL CASE

The equation $au + bv = c$.

1. **Find $d = \gcd(a, b)$. If $d \nmid c$: no integer solutions.**

2. **If $d \mid c$ then**

$$au + bv = c \Leftrightarrow \frac{a}{\gcd(a,b)}u + \frac{b}{\gcd(a,b)}v = \frac{c}{\gcd(a,b)}$$

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

Find all the SOLUTIONS TO au+bv=c

THE GENERAL CASE

REMARK **Divide everything by gcd(a,b)**

$$au + bv = c \Leftrightarrow \frac{a}{\gcd(a,b)}u + \frac{b}{\gcd(a,b)}v = \frac{c}{\gcd(a,b)}.$$

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

If u_0, v_0 is a solution to $au + bv = c$ the others solutions are

$$u = u_0 + k\frac{b}{\gcd(a,b)}, v = v_0 - k\frac{a}{\gcd(a,b)}, k \in \mathbb{Z}.$$

Do not remember the formula (but know how to find it).

SOLUTIONS TO the linear Diophantine equation au+bv=c in the general case

EXERCISE

Find all integer solutions to $8u + 6v = 14$.

Solution.

SOLUTIONS TO the linear Diophantine equation au+bv=d in the general case

EXAMPLE **Does $48u + 92v = 12$ have a solution (u, v)? If yes, find one.**

Describe all the solutions to the equation.

An application: The postage stamp problem

At the post office they have only 3 cents and 5 cents stamps.

What postage values would you be able to put on your mail?

Which values are unavailable?

MATHEMATICAL VERSION Let a, b be relatively prime.

What positive integers d can be written as
$d = au + bv$ with $u, v \in \mathbb{N}$?

feasible number

not $\mathbb{Z}$!

The postage stamp problem

What is the answer if we allow u, v to be negative? $\mathbb{N}$

How about if we want u, v positive (≥ 0) **?**

Let a, b be relatively prime.
What positive integers d can be written as $d = au + bv$ with $u, v \in \mathbb{N}$?

$a = 3, b = 5$

Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Feasible														

$a = 2, b = 7$

Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Feasible														

The postage stamp problem

PROPOSITION **Let $a, b \geq 1$ relatively prime.**
1. $n = ab - a - b$ is NOT feasible;
2. $n > ab - a - b$ is feasible.

Proof. **1. $n = ab - a - b$ is not feasible.**

The postage stamp problem

2. $n > ab - a - b$ **is feasible.**

Unit 5
Prime numbers

Prime numbers

DEFINITION A natural $p \geq 2$ is prime if the only divisors of p are 1 and p.

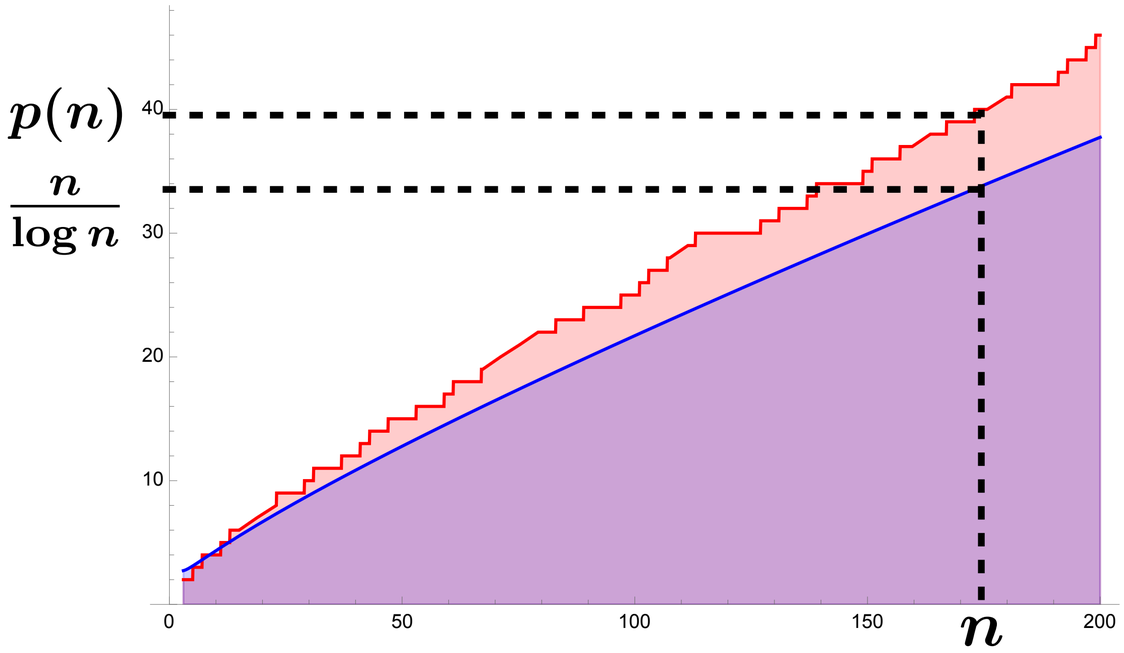
The first primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

EXAMPLE The 10 000th prime number: 104729

```
In[159]:= Prime[10 000]

Out[159]= 104 729
```

Prime numbers



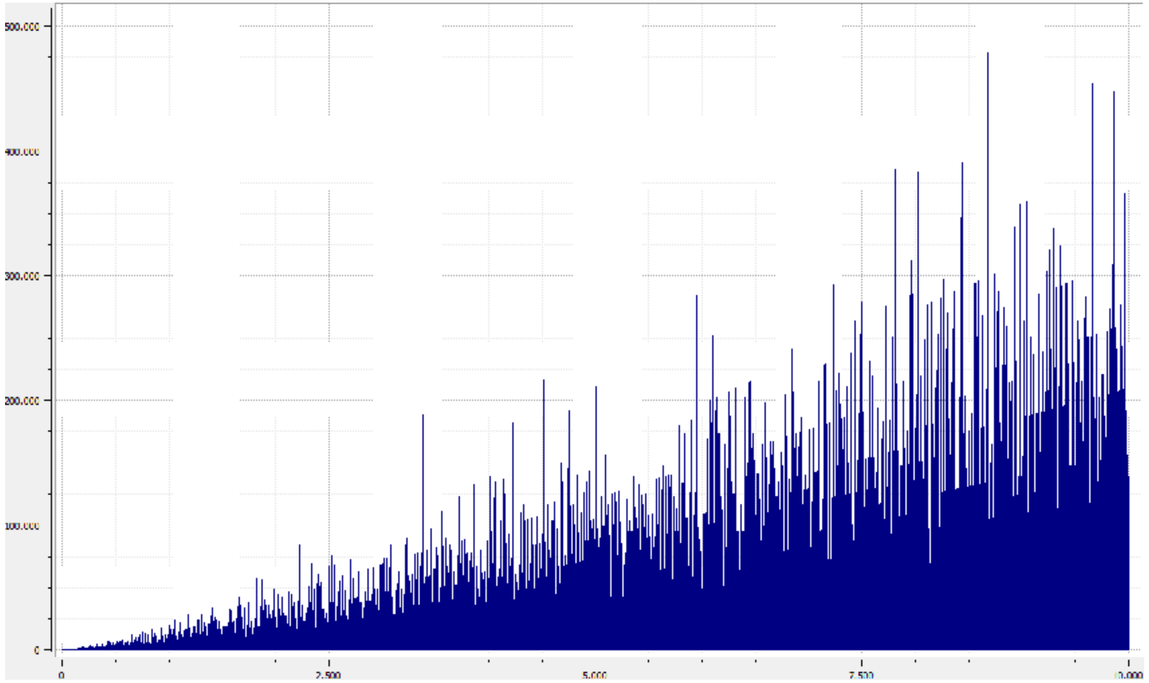
$$p(n) = \#\{\text{primes} \leq n\}$$

Prime number theorem:

$$p(n) \sim \frac{n}{\log n}, n \to +\infty$$

Distribution of the gap between consecutive prime numbers

$$m(k) = \frac{p_k^2 - p_{k-1}^2}{24} \qquad (k \geq 4)$$



Prime numbers: an infinite set

THEOREM (Euclid) **There are infinitely many prime numbers.**

Proof. **Assume the contrary: let $N \geq 2$ be such that**

$$\boxed{p \text{ prime} \Rightarrow p \leq N.}$$

Consider $N! + 1$: since $N! + 1 > N$ then it is not prime.

Let p be a prime divisor of $N! + 1$: necessarily $p \leq N$.

Then $p \mid N!$ (it is one of the factors of $N!$).

Thus $p \mid (N! + 1) - N! = 1$, a contradiction: there are primes $p > N$. $\square$

Recognize prime numbers

PROPOSITION If n is not prime then it has a divisor $1 < a \leq \sqrt{n}$.

Proof. If n is not prime there are $a, b > 1$ and $n = ab$.

If $a, b > \sqrt{n}$ then $n = ab > (\sqrt{n})^2 = n$, a contradiction. $\square$

EXAMPLE **Is 991 prime?**

Prime numbers and coprimality

QUESTION Assume $n \geq 1, m \in \mathbb{Z}$ and $n \nmid m$. True that m, n are coprime?

PROPOSITION (Coprimeness of a prime and non-multiple)

Let p be prime and $m \in \mathbb{Z}$. If $p \nmid m$ then p, m are coprime.

Proof. Let $d \geq 1$, $d \mid p$ and $d \mid m$.

p prime $\Rightarrow d = 1$ or $d = p$.

$d \mid m, p \nmid m \Rightarrow d = 1$. Thus $\gcd(p, m) = 1$. $\square$

Prime numbers and divisibility

QUESTION

Let $n \geq 1, n \mid ab$. True that $n \mid a$ or $n \mid b$?

COROLLARY(Prime divisor property)

p prime, a, b integers. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof. If $p \nmid a$ then p and a are coprime. Thus $p \mid b$. $\square$

The Fundamental Theorem of Arithmetic

THEOREM Let $a \geq 2$ be a natural. Then a can be factored as a product of primes.

$$a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} \qquad p_i \text{ distinct primes, } e_1, \ldots, e_m \geq 1.$$

The factorization into primes is unique modulo rearrangements of their order.

$e_i = \text{mult}_{p_i}(a)$ is the multiplicity of p_i in a, $i = 1, \ldots, m$.

REM: the multiplicity is sometimes called the order, we will use the term order for another concept

$$a = \prod_{p \text{ prime}} p^{\text{mult}_p(a)}$$

$(\text{mult}_p(a) := 0 \text{ if } p \neq p_i \text{ for some } i).$

EXAMPLE $1728 = 2^6 \cdot 3^3 \quad \text{mult}_2(1728) = 6, \text{mult}_3(1728) = 3.$

A formula for the divisors of a natural

PROPOSITION Let $a \geq 2$, $a = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, with $e_i \geq 1$.

The divisors of a are of the form $p_1^{f_1} \cdots p_m^{f_m}$ with $0 \leq f_1 \leq e_1$.

Proof. Let $d \geq 2$ with $d \mid a$ and q a prime in its factorization.

Then $q \mid p_1^{e_1} \cdots p_m^{e_m}$. q prime $\Rightarrow q \mid p_i$ for some i, i.e., $q = p_i$.

Necessarily $f_i = \text{mult}_{p_i}(d) \leq \text{mult}_{p_i}(a) = e_i$. $\square$

EXAMPLE Divisors of $3^4 \times 13^2$?

$1, 3, 3^2, 3^3, 3^4$

$1 \cdot 13 = 13, 3 \cdot 13, 3^2 \cdot 13, 3^3 \cdot 13, 3^4 \cdot 13$

$1 \cdot 13^2 = 13^2, 3 \cdot 13^2, 3^2 \cdot 13^2, 3^3 \cdot 13^2, 3^4 \cdot 13^2$

5×3 divisors

1, 3, 9, 13, 27, 39, 81, 117, 169, 351, 507, 1053, 1521, 4563, 13689

A formula for gcd

COROLLARY Let $a, b \geq 2$ and $a = p_1^{e_1} \cdots p_m^{e_m}, b = p_1^{f_1} \cdots p_m^{f_m}$

be their factorization into primes (possibly $e_i = 0$ or $f_i = 0$).

Then $\gcd(a, b) = p_1^{\min\{e_1, f_1\}} \cdots p_m^{\min\{e_m, f_m\}}$.

EXAMPLE $37800 = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7$ $\quad$ $2340 = 2^2 \cdot 3^2 \cdot 5 \cdot 13$

Then $\gcd(37800, 2340) = 2^2 \cdot 3^2 \cdot 5^1 = 180$.

COROLLARY Let $a, b \geq 2$ and $a = p_1^{e_1} \cdots p_m^{e_m}, b = q_1^{f_1} \cdots q_n^{f_n}$

be their factorization into primes, with $e_i, f_i \geq 1$.

Then a, b are coprime if and only if $\{p_1, \ldots, p_m\} \cap \{q_1, \ldots, q_n\} = \emptyset$.

END
of
Lesson 2
Divisions