Bachelor of Ecole Polytechnique
Algorithms for Discrete Mathematics, year 2, semester 1

Experimental Maths 1: Primes and Euclid

Table of contents


```python
# execute this part to modify the css style
from IPython.core.display import HTML
def css_styling():
    styles = open("./style/custom2.css").read()
    return HTML(styles)
css_styling()
```

```python
## loading python libraries

# necessary to display plots inline:
%matplotlib inline

# load the libraries
import matplotlib.pyplot as plt # 2D plotting library
import numpy as np              # package for scientific computing
from math import *              # package for mathematics (pi, arctan, sqrt, factorial
```

Please read!

Guidelines for the notebooks

- Try to write simple and elegant programs. Think recursive!
- Each function must be tested (for your sake, it also must be

commented).

- Draw plots that illustrate interesting phenomena (play with parameters).
- **It doesn't matter not to finish the Notebook!**
- For the mathematical questions try to be rigorous and concise. Compare your claims with experiments.
- Do not hesite to ask the TA for help.
- The notebook with complete solutions will be uploaded on moodle after the lab.

Prime numbers and divisibility

We aim to investigate the distribution of primes among integers. Namely, how many prime numbers are there (approximately) between 1 and n?

Do it yourself.

Write a boolean function IsPrime(n) which returns `True` if and only n is prime.

(In python $a \pmod p$ is obtained with `a%p` *.)*

```
def IsPrime(n):
    # input: integer n
    # output: True or False depending on whether n is prime or not
    return ????
```

Now we are ready for experiment. For $n \geq 2$, let $P(n)$ denote the number of primes less than n. For example, $P(11) = 5$ since $2, 3, 5, 7, 11$ are prime.

Do it yourself.

1. Write a script which takes as input n and returns the list $[P(2), P(3), \dots, P(n)]$.
2. Plot the function $n \mapsto P(n)$ (try $n = 100, 1000, 10000$).

Do it yourself. Modify your previous plot to guess (by trials and errors) what is the asymptotic behaviour of $P(n)$ when $n \to +\infty$: find a sequence a_n such that $P(n) \sim a_n$. *In order to improve your guess you can plot* $\frac{P_n}{a_n}$ *in some interval* $(T/2, T)$ *(instead of* $(0, T)$*).*

Answers.

Factorization

Do it yourself. Write a function `Factorize(n)` which returns the factorization of `n` into primes. For example your function should return:

```
Factorize(2158884)
[2, 2, 3, 3, 7, 13, 659]
```

Hint: Think recursive!

```
def Factorize(n):
    # input: integer n
    # output: list of factors of n

print(Factorize(2158884))
```

For $n \geq 2$ we introduce

$$F(n) = \text{Number of prime factors of } n\text{, counted with multiplicity.}$$

For example, $F(2158884) = 7$.

Do it yourself. Plot the function $n \mapsto F(n)$ (try $n = 100, 1000, 5000$).

Do it yourself. (Theory)

1. Plot on the previous picture $n \mapsto F(n)$ and $n \mapsto \log_2(n)$ (logarithm in basis two).
2. Prove the following:
   - **(lower bound)** There are infinitely many n's for which $F(n) = \log_2(n)$.
   - **(upper bound)** $F(n) \leq \log_2(n)$ for every n.

Answers.

1.
2.

3. The Euclid algorithm

We recall that Euclid's algorithm (which computes the gcd of two non-negative integers) relies on the fact that for every a, b we have

$$\begin{cases} \gcd(a,b) & = \gcd(b, a\%b), \\ \gcd(a,0) & = a, \end{cases}$$

where $a\%b$ is the remainder of the euclidean division a/b.

Do it yourself. Write a function `GreatestCommonDivisor(a,b)` which returns $\gcd(a,b)$ using the Euclid algorithm.

```
def GreatestCommonDivisor(a,b):
    # input: a,b: non-negative integers
    # output: returns the gcd of a and b
```

Integers m, n are said to be *coprime* if $\gcd(m,n) = 1$. For example, $14, 9$ are coprime.

In many references (see e.g. [Wikipedia (https://en.wikipedia.org/wiki/Coprime_integers#Probability_of_coprimality)](https://en.wikipedia.org/wiki/Coprime_integers#Probability_of_coprimality)) one can read that

"*The probability that two numbers randomly chosen are coprime is* $\frac{6}{\pi^2}$."

Yet there is no obvious way to rigorously define what are "two numbers randomly chosen". A possible interpretation is the following:

$$\frac{\mathrm{card}\left\{(i,j) \in [1,n]^2 \text{ such that } \gcd(i,j) = 1\right\}}{\mathrm{card}\left\{(i,j) \in [1,n]^2\right\}} \overset{n\to+\infty}{\to} \frac{6}{\pi^2}.$$

Do it yourself. Use your function `GreatestCommonDivisor` to draw a plot which illustrates the above convergence towards $\frac{6}{\pi^2}$ ($n = 200$ should be enough).

Do it yourself. Write a function `GreatestCommonDivisor_3(a,b,c)` which returns the gcd of three numbers.

A mysterious function

Do it yourself. What does the following function return? Can you prove it?

```python
def Mystery(MysteriousVariable):
    # input: ???
    # output: ???
    if MysteriousVariable==0:
        return []
    else:
        return Mystery(MysteriousVariable//2) + [MysteriousVariable%2]
```

Answers.

Change of basis

Do it yourself. Write a function `ChangeBasis(a,b,n_InBasis_a)` which takes as inputs: * Two basis a, b (integers ≥ 2) * A list which gives the decomposition of some integer n in basis a

and which returns the decomposition of n in basis b.

For example

```python
ChangeBasis(5,2,[4,1])
```

```
[1, 0, 1, 0, 1]
```

(Since $[4, 1]$ in basis 5 is 21 *i.e.* $[1, 0, 1, 0, 1]$.)

```python
def ChangeBasis(a,b,n_InBasis_a):
    # inputs: basis a,b, integer n in basis a (as a list)
    # output: n in basis b (as a list)
```