Correction séance 2 (15 septembre)

† *Divisibilité*.

Exercice 5. (Crible d'Ératosthène)
Si n n'est pas premier, on a une décomposition $n = ab$ avec $a, b \geqslant 2$. Si $a \leqslant \sqrt{n}$, on a terminé. Si $a > \sqrt{n}$, alors $ab = n > b\sqrt{n}$ et on obtient $\sqrt{n} > b$, donc n admet un diviseur inférieur ou égal à $\sqrt{n}$.

2. A chaque étape, le plus petit entier de la liste est premier : si il n'a pas été retiré dans les étapes précédentes, il n'est multiple d'aucun entier qui lui est inférieur. Si un nombre est premier, il est forcément le plus petit nombre qui n'a pas été retiré de la liste a une certaine étape (puisqu'on a retiré que des nombres composites).
Notons que, quand on a trouvé les nombres premiers inférieurs à $\sqrt{N}$, tous les nombres restant de la liste sont premiers : les nombres composites inférieurs à N ont un diviseur premier inférieur à $\sqrt{N}$, ils ont donc déjà été retirés de la liste.

3.

Algorithm 1 Crible d'Eratosthene

$L := [2, 3, \ldots, N]$
$P := [\,]$
while $L \neq \varnothing$ et $L[1] < \sqrt{N}$ **do**
  $P := [P, L[1]]$
  $L := L \setminus ((L[1] * L) \cap L)$
end while
return P

4. On applique l'algorithme précédent à notre liste.

(a) - 2 est premier, on retire ses multiples. Il reste

3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61
63	65	67	69	71	73	75	77	79	81	83	85	87	89	91
93	95	97	99	101	103	105	107	109	111	113	115	117	119	

(b) - 3 est premier, on retire ses multiples. Il reste

5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
49	53	55	59	61	65	67	71	73	77	79	83	85	89	91
95	97	101	103	107	109	113	115	119						

(c) - 5 est premier, on retire ses multiples. Il reste

7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
61	67	71	73	77	79	83	89	91	97	101	103	107	109	113
119														

(d) - 7 est premier, on retire ses multiples. Il reste

11	13	17	19	23	29	31	37	41	43	47	53	59	
61	67	71	73	79	83	89	97	101	103	107	109	113	

(e) - Le prochain nombre sur la liste est $11 > \sqrt{120}$, par la question 2, tous les nombres de la liste sont premiers. D'où la liste des nombres premiers inférieurs à 120 :

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
53	59	61	67	71	73	79	83	89	97	101	103	107	109	113

5.

Algorithm 2 EstPremier

```
L :=Eratosthene(⌊√N⌋)
for i in L do
  if i divide N then
    return false
  end if
end for
return true
```

Cet algorithme est bien gentil, mais il demande de calculer la liste des nombres premiers inférieurs à $\sqrt{N}$ via le crible d'Ératosthène, ce qui est très couteux !

† *PGCD, Algorithme d'Euclide*

Exercice 7. Soit d un diviseur commun à $a+b$ et $a-b$. Par somme et par différence, on obtient que d divise

$$2a = a+b+a-b \text{ et } 2b = a+b-(a-b)$$

Donc d divise $2a \wedge 2b = 2(a \wedge b) = 2$.
Si a et b sont tous deux impairs, alors $a+b$ et $a-b$ sont pairs, et 2 est leur pgcd.
Si a et b sont de parité différentes, alors $a+b$ et $a-b$ sont impairs et premiers entre eux.

Exercice 8.
1. On utilise l'algorithme d'Euclide :

$$\begin{aligned} 165 &= 4 \cdot 35 + 25 \\ 35 &= 1 \cdot 25 + 10 \\ 25 &= 2 \cdot 10 + 5 \\ 10 &= 2 \cdot 5 + 0 \end{aligned}$$

Le dernier reste non nul est 5, c'est le pgcd de 165 et de 35. Le ppcm de 165 et de 35 est donné par le produit, divisé par le pgcd, ici $\frac{165*35}{5} = 33*35 = 1155$.

2.

$$\begin{aligned} 28 &= 1 \cdot 16 + 12 \\ 16 &= 1 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0 \end{aligned}$$

Le dernier reste non nul est 4, c'est le pgcd de 28 et de 16.

3. La décomposition en produit de facteurs premiers de 27 est 3^3, celle de 8 est 2^3. Ces décompositions n'ayant aucun facteur commun, 27 et 8 sont premiers entre eux.

4. On a $24 = 8*3$, donc 8 divise 24 et est le pgcd de 8 et 24.

Exercice 9.
1.

Algorithm 3 Division

$m, n \in \mathbb{N}$
$b := 1$
while $m > nd$ **do**
  $b := b + 1$
end while
$b := b - 1$
return $(b, m - bn)$

2.

Algorithm 4 AlgEuclide

$m, n \in \mathbb{N}$
$(b, r) :=$`Division`(m, n)
if $r = 0$ **then**
  return n
end if
return `AlgEuclide`(n, r)

Exercice 10.
1. C'est la définition du pgcd.

2. Soit p un nombre premier, on considère p^i et p^j les deux plus grandes puissances de p divisant m et n (ce sont celles qui apparaissent dans la décomposition de m et n en produits de facteurs premiers). Par définition la plus grande puissance de p divisant $m \wedge n$ est $p^{\min(i,j)}$. Si les décompositions de m et n sont

$$\prod_{p \in ¶} p^{j_p} \quad \text{et} \quad \prod_{p \in ¶} p^{i_p}$$

On a

$$m \wedge n = \prod_{p \in ¶} p^{\min(j_p, i_p)}$$

3.

Algorithm 5 Bourrin

$d := 1$
$N :=$ Minimum(n, m)
$P :=$ `Eratosthene`(N)
for p dans P **do**
  $i := 0$
  while p^{i+1} divise m et n **do**
    $i := i + 1$
  end while
  $d := d \cdot p^i$
end for
return d

4. Evidemment, `AlgEuclide` est nettement plus efficace : il ne fait appel qu'à des divisions euclidiennes, relativement faciles à obtenir, par opposition à la décomposition en produit de facteurs premiers.

Exercice 11.

1. Premièrement, notre recherche n'est pas vaine : 15 et 22 sont premiers entre eux, l'équation considérée admet donc des solutions. Commençons par trouver une telle solution via l'algorithme d'Euclide.

$$\begin{aligned} 22 &= 15 \cdot 1 + 7 \\ 15 &= 7 \cdot 2 + 1 \\ 7 &= 1 \cdot 7 + 0 \end{aligned}$$

On a donc

$$\begin{aligned} 1 &= 15 - 7 \cdot 2 \\ &= 15 - (22 - 15) \cdot 2 \\ &= 15 \cdot 3 - 22 \cdot 2 \end{aligned}$$

On a donc une solution particulière $x = 3, y = 2$.

Détaillons l'autre méthode donnée via la notation $15x - 22y = (x, y)$ (attention il y a un moins qui s'est invité !). Avec cette notation, on a

$$\begin{aligned} 7 &= 22 - 15 = (-1, -1) \\ 1 &= 15 - 2 \cdot 7 \\ &= (1, 0) - 2(-1, -1) \\ &= (1, 0) + (2, 2) = (3, 2) \end{aligned}$$

On retrouve (bien-sûr) la même solution $(x, y) = (3, 2)$.

On cherche maintenant la totalité des solutions. Soit une autre solution x et y, on a

$$15x - 22y = 15 \cdot 3 - 22 \cdot 2 \Leftrightarrow 15(x - 3) = 22(y - 2)$$

autrement dit, un multiple commun à 15 et à 22, comme ces deux nombres sont premiers entre eux, il existe un entier k tel que

$$\begin{aligned} \frac{15 \vee 22}{15} k = x - 3 \quad \text{et} \quad \frac{15 \vee 22}{22} k = y - 2 \\ 22k + 3 = x \quad \text{et} \quad 15k + 2 = y \end{aligned}$$

Les solutions sont donc les couples de la forme $x = 22k + 3, y = 15k + 2$ pour un entier k.

2. Là c'est directement plus simple : on a $15x = 22y$, donc il existe un entier k tel que $x = 22k$ et $y = 15k$, les solutions sont les couples de la forme $(22k, 15k)$.

3. Le pgdc de 15 et 24 est 3, qui ne divise pas 5, cette équation n'a donc pas de solutions entières.

4. Calculons le pgcd de 24 et 87 par l'algorithme d'Euclide.

$$\begin{aligned} 87 &= 24 \cdot 3 + 15 \\ 24 &= 15 \cdot 1 + 9 \\ 15 &= 9 \cdot 1 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

On a donc $87 \wedge 24 = 3$, $87 = 3 \cdot 29$ et $24 = 3 \cdot 8$. L'équation considérée admet des solutions si et seulement si $c = 3c'$ est un multiple de 3. Dans ce cas, l'équation devient

$$8x + 29y = c' \tag{1}$$

C'est cette équation là que l'on va résoudre. Commençons par trouver une solution à l'équation

$$8u + 29v = 1$$

On peut trouver en remontant l'algorithme d'Euclide précédent que

$$8 \cdot 11 + 29 \cdot (-3) = 1$$

Autrement dit, pour tout $c' \in \mathbb{Z}$ une solution de l'équation 1 est donnée par

$$8 \cdot (11c') + 29 \cdot (-3c') = c'$$

Soit maintenant une solution quelconque de l'équation 1, on a

$$8 \cdot (11c') + 29 \cdot (-3c') = 8x + 29y \Leftrightarrow 8(11c' - x) = 29(y + 3c')$$

Toujours comme $8 \cdot 29 = 29 \cdot 8$ est le ppcm de 29 et 8, on a qu'il existe un entier k tel que

$$29k = 11c' - x \quad \text{et} \quad 8k = y + 3c'$$

Les solutions recherchées sont donc les couples de la forme $(x, y) = (11c' - 29k, 8k - 3c')$ pour k dans $\mathbb{Z}$.