Arithmétique – Fiche de cours

1. Nombres premiers

a. Définition

Un entier naturel est premier s'il a deux diviseurs : 1 et lui-même.

b. Critère d'arrêt

Tout entier naturel n, $n \geq 2$, admet un diviseur premier.

Si n n'est pas premier, alors il admet un diviseur premier p tel que :

$$2 \leq p \leq \sqrt{n}$$

c. Infinité de nombres premiers

Il existe une infinité de nombres premiers.

d. Crible d'Eratosthène

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

e. Théorème de Gauss

Un nombre premier divise un produit de facteurs si, et seulement si, il divise l'un de ces facteurs.

Si p divise ab $\Leftrightarrow$ p divise a ou p divise b

f. Théorème fondamental de l'arithmétique

Tout entier A > 2, peut se décomposer de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers.

$$A = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n}$$

Le nombre N de diviseurs d'un nombre entier est :

$$N = (\alpha_1 + 1) \times (\alpha_2 + 1) \times \ldots \times (\alpha_n + 1)$$

2. Multiples et diviseurs

a. Définition

Soit a, b et k des entiers relatifs avec $a = k \cdot b$

- a est un multiple de b
- b est un diviseur de a

b. Critères de divisibilité

- divisibilité par 2 : le chiffre des unités est 0, 2, 4, 6 ou 8 (nombre pair)
- divisibilité par 3 : la somme des chiffres est un multiple de 3
- divisibilité par 4 : les deux derniers chiffres sont multiples de 4
- divisibilité par 5 : le chiffre des unités est 0 ou 5
- divisibilité par 9 : la somme des chiffres est un multiple de 9
- divisibilité par 10 : le chiffre des unités est 0
- divisibilité par 11 : pour un nombre à 3 chiffres ; le chiffre du milieu = la somme des 2 autres chiffres

c. Opération sur les multiples

Soit trois entiers relatifs a, b et c.

Si a divise b et c alors a divise $b + c$, $b - c$ ou toute combinaison linéaire de b et de c.

d. Division Euclidienne

Soit a un entier relatif et b un entier naturel non nul.

On appelle division euclidienne de a par b, l'opération qui au couple $(a; b)$ associe le couple $(q; r)$ tel que :

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b$$

a s'appelle le *dividende*, b le *diviseur*, q le *quotient* et r le *reste*.

e. Congruence

Soit n un entier naturel ($n > 2$), a et b deux entiers relatifs.
On dit que deux entiers a et b sont congrus modulo n si, et seulement si, a et b ont même reste par la division euclidienne par n.
On note alors : $a \equiv b \bmod n$ ou $a \equiv b\,(n)$

Propriétés :
Soit n un entier naturel ($n > 2$), a, b, c, d des entiers relatifs vérifiant :

$$a \equiv b\ (n) \text{ et } c \equiv d\ (n)$$

- addition : $a + c \equiv b + d\ (n)$
- multiplication : $ac \equiv bd\ (n)$
- puissances : $\forall k \in \mathbb{N} \quad a^k \equiv b^k\,(n)$

f. pgcd

Soit a et b deux entiers relatifs non nuls. L'ensemble des diviseurs communs à a et b admet un plus grand élément D, appelé plus grand commun diviseur.
On note : $D = pgcd(a\,;b)$

g. ppcm

Soit a et b deux entiers relatifs non nuls.
L'ensemble des multiples strictement positifs communs à a et à b admet un plus petit élément M, appelé plus petit commun multiple.
On le note : $M = ppcm(a\,;b)$

h. Lien entre pgcd et ppcm

Soit a et b deux entiers relatifs non nuls

$$a \times b = pgcd(a\,;b) \times ppcm(a\,;b)$$

i. Egalité de Bézout

Soit a et b deux entiers non nuls et $D = pgcd(a\,;b)$
Il existe alors un couple (x,y) d'entiers relatifs tels que : $ax + by = D$

j. Théorème de Bézout

Deux entiers relatifs a et b sont premiers entre eux **si et seulement si**, il existe deux entiers relatifs x et y tels que : $ax + by = 1$

k. Corollaire du théorème de Bézout

L'équation $a \cdot x + b \cdot y = c$ admet des solutions entières si et seulement si c est un multiple du $pgcd(a\,;b)$

k. Petit théorème de fermat

Si p est premier est a n'est pas divisible par p alors :

$$a^{p-1} \equiv 1\,(p)$$