COURS ARITHMETIQUE TERMINALE L

1. La division dans $\mathbb{Z}$

Définition: Soient a et b deux nombres entiers relatifs. On dit que a est divisible par b ou encore que a est un multiple de b s'il existe un entier relatif q tel que $a = qb$. Le nombre b et un diviseur de a.

Théorème : Soient a et b deux nombres entiers relatifs.

Il existe un unique couple d'entiers q et r tels que $a = bq + r$ et $0 \leqslant r < |b|$.

C'est la division euclidienne de a par b. Le nombre q s'appelle le quotient et r le reste de la division.

Exercices : Quel est le résultat de la division de 21 par 5 ? De 153 par 11 ?

Le nombre 21 est-il divisible par 5 ? par 7 ?

2. Nombres premiers

Définition: Un entier naturel qui admet exactement deux diviseurs positifs, 1 et lui-même, est appelé un nombre premier.

Attention: 1 n'est pas un nombre premier. Le plus petit nombre premier est 2.

Exercice : Les nombres suivants sont-ils premiers : 27, 37, 91 et 143 ?

Crible d'Erathostène: La méthode suivante permet de déterminer tous les nombres premiers inférieurs à un nombre fixé à l'avance (ici, 200). Cette méthode est connue depuis longtemps: Erathostène(276 av JC – 194 av JC) .

On prépare un tableau contenant tous les nombres que l'on souhaite étudier.

Puis on le lit de gauche à droite et de haut en bas : 2 est premier ? Oui, donc on va barrer tous ses multiples.

Cela montre que le nombre suivant non barré est à son tour premier ; c'est 3 : on barre tous ses multiples.

Puis le nombre suivant non encore barré est 5 : il est premier, et on barre tous ses multiples. Ainsi de suite : à la fin, les nombres non barrés sont exactement les nombres premiers.

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	151	152	153	154	155
156	157	158	159	160	161	162	163	164	165	166	167	168	169
170	171	172	173	174	175	176	177	178	179	180	181	182	183
184	185	186	187	188	189	190	191	192	193	194	195	196	197
198	199	200											

Théorème : Tout entier naturel peut s'écrire, de façon unique, comme un produit de nombres premiers. Ce produit s'appelle la décomposition du nombre en produit de facteurs premiers.

3. Congruences

3.1 Une question pratique:

Un élève qui aime bien les vacances constate qu'en 2005, le premier mai tombait un dimanche.
Comment peut-il savoir, sans trop se fatiguer, si en 2006 et en 2007 le premier mai donnera un jour de congé de plus, ou s'il tombera pendant un week-end ?
Il s'agit donc de savoir, quand on rajoute 365 jours à un samedi, sur quel jour de la semaine on tombe.
La remarque fondamentale est que rajouter 7 jours ne change rien ! Et donc 14 jours non plus, 21 jours non plus... ni n'importe quel multiple de 7.
Ainsi, on peut écrire la division euclidienne de 365 par 7 : $365 = 52\times7 + 1$.
On voit donc que le premier mai 2006 tombera 52 semaines et un jour après le premier mai 2005 : il tombera un lundi. Et le premier mai 2007, un mardi. Et le premier mai 2008 ?

Nous venons de faire notre premier calcul de congruence : au lieu de faire un calcul exact sur des entiers, nous venons de faire un calcul modulo 7, en conservant seulement l'information "jour de la semaine".

3.2 La notion de congruence

On fixe un entier naturel n, supérieur ou égal à 2.
Définition : On dit que deux nombres entiers x et y sont congrus modulo n, et on note $x \equiv y \pmod n$, ou $x \equiv y\ [n]$ s'ils ont le même reste dans leurs divisions euclidiennes respectives par n.

Exemple : On a les divisions $365 = 52\times7 + 1$, $15 = 2\times7 + 1$, $1 = 0\times7 + 1$et $-6 = -1\times 7 + 1$. Le reste est 1 à chaque fois, ce qui signifie que ces nombres sont congrus modulo 7 : $365 \equiv 15 \equiv -6 \equiv 1 \pmod 7$.

Propriétés: a) Tout nombre entier relatif est congru modulo n à un unique nombre entier compris entre 0 et $n - 1$.
b) Si $x \equiv y \pmod n$ et $y \equiv z \pmod n$, alors $x \equiv z \pmod n$.
c) Si x est divisible par n alors $x \equiv 0 \pmod n$.

Deux propriétés fondamentales :
On peut additionner et multiplier les congruences modulo n :
si $x \equiv y \pmod n$ et $x' \equiv y' \pmod n$, alors $x + x' \equiv y + y' \pmod n$ et $xx' \equiv yy' \pmod n$.
Démonstration : $x \equiv y \pmod n$ signifie que $x = qn + r$ et $y = q'n + r$ et $0 \leqslant r < n$.
De même, $x' \equiv y' \pmod n$ signifie que $x' = pn + r'$ et $y' = p'n + r'$ et $0 \leqslant r' < n$.
Pour la somme:
Ainsi $x + x' = qn + r + pn + r' = (q + p)n + (r + r')$ et $y + y' = q'n + r + p'n + r' = (q' + p')n + (r + r')$.
Si $r + r'$ est plus grand que n , alors il existe des entiers a et b tels que $r + r' = an + b$ et $0 \leqslant b < n$.
Et b est le reste de la division de $x + x'$ et de $y + y'$ par n.
Si $r + r'$ est strictement plus petit que n , alors $r + r'$ est le reste de la division de $x + x'$ et de $y + y'$ par n.
Donc $x + x'$ et $y + y'$ ont le même reste dans la division euclidienne par n.
Pour le produit:
$xx' = (qn + r)(pn + r') = (qpn + qr' + pr)n + rr'$ et $yy' = (q'n + r)(p'n + r') = (q'p'n + q'r' + p'r)n + rr'$.
Si rr' est plus grand que n , alors il existe des entiers c et d tels que $rr' = cn + d$ et $0 \leqslant d < n$. Et d est le reste de la division de xx' et de yy' par n.
Si rr' est strictement plus petit que n , alors rr' est le reste de la division de xx' et de yy' par n.
Donc xx' et yy' ont le même reste dans la division euclidienne par n.

Exemples : $40 \equiv 1 \pmod{13}$ et $168 \equiv -1 \pmod{13}$ donc $208 = 40 + 168 \equiv 1 - 1 \equiv 0 \pmod{13}$.
$36 \equiv 1 \pmod 7$ donc $36^5 \equiv 1 \pmod 7$.