d'où $\begin{cases} x = 3 \bmod(13) \\ x = 9 \bmod(19) \end{cases}$
soit M=$13 \times 19 = 247$
le système admet une solution unique modulo M
x=$3\times19 \times y_1 + 9 \times 13 \times y_2$
avec $y_1 = 13^{-1} \bmod(19)$ $\quad$ $y_2 = 19^{-1} \bmod(13)$
on a 19=13+6
$13=6\times2 + 1 \Longrightarrow 1 = 13 - 6 \times 2$
$1=13-(19-13)\times2$
$1=13\times3 - 19 \times 2$
donc $13^{-1} \bmod(19) = 3 \bmod(19) \Longrightarrow y_1 = 3$
$19^{-1} \bmod(13) = -2 \bmod(13) \Longrightarrow y_2 = 11$
x=$3 \times 19 \times 3 + 9 \times 13 \times 11 = 1458$
$1458 \div 247 = 5.902$
$1458 - 247 \times 5 = 223.$
x=223mod(19×13)

TD ARITHMETIQUE L2 MI : 19-20

EXERCICE 1

Soit n un entier naturel non nul et $q \in \mathbb{R}$ ou $\mathbb{C}$.
On pose $(n)_q = 1 + q + \cdots + q^{n-1}$, $(n!)_q = (1)_q (2)_q \cdots (n)_q$
$\left(\begin{array}{c} n \\ k \end{array} \right)_q = \dfrac{(n!)_q}{(k!)_q ((n-k)!)_q}$ et $(0!)_q = 1.$

a) Montrer que $(n!)_q = \frac{(q-1)(q^2-1)\cdots(q^n-1)}{(q-1)^n}$ avec $q \neq 1$

b) Montrer que $\left(\begin{array}{c} n \\ k \end{array} \right)_q = \left(\begin{array}{c} n \\ n-k \end{array} \right)_q$

c) Montrer que $\left(\begin{array}{c} n \\ k \end{array} \right)_q = \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right)_q + q^k \left(\begin{array}{c} n-1 \\ k \end{array} \right)_q = \left(\begin{array}{c} n-1 \\ k \end{array} \right)_q +$
$q^{n-k} \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right)_q$

EX 2

Soit G un groupe tel que l'application x$\longmapsto$x^{-1} soit un morphisme. Montrer que G est commutatif.

EX 3

Montrer qu'un sous-groupe d'indice 2 dans un groupe G est distingué dans G.

EX 4

Soit f : G $\longrightarrow$H un morphisme de groupes finis. Soit G' un sous-groupe de G. Montrer que

l'ordre de f(G') divise les ordres de G' et de H.

EX 5

Soit f : G$\longrightarrow$H un morphisme de groupes finis. Soit G' un sous-groupe de G d'ordre premier à l'ordre de H. Montrer que G'= ker(f).

Ex 6

Démontrer que pour tout $n \in \mathbb{N}$,

1. n^3 - n est divisible par 6 ,

2.n^5 - n est divisible par 30 ,

3. n^7 - n est divisible par 42 .

Ex 7

Pour tout $n \in \mathbb{N}$, on définit deux propriétés :

P_n : 3 divise 4^n-1 et Q_n : 3 divise 4^n+1 .

2. Montrer que P_n est vraie pour tout $n \in \mathbb{N}$.

3. Que penser de l'assertion :$\exists n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0$ Q_n est vraie.

Ex 8

Démontrer par récurrence que :

a) $2^{2\times 3^n} - 1$ est divisible par 3^{n+1} pour tout entier n$\geq$ 0.

b) $5^{3^n} + 1$ est divisible par 3^{n+1} pour tout entier n$\geq$ 0.:

Ex 9

1.Montrer que pour tout n$\in \mathbb{N}$ et tout p$\in \mathbb{Z}$: $\mathrm{p}\begin{pmatrix} n \\ p \end{pmatrix} = n \begin{pmatrix} n-1 \\ p-1 \end{pmatrix}$

2.Calculer pour tout n

$\mathrm{S}_0 = \sum_{p=0}^{n} \begin{pmatrix} n \\ p \end{pmatrix}$; $\mathrm{S}_1 = \sum_{p=0}^{n} \mathrm{p}\begin{pmatrix} n \\ p \end{pmatrix}$; $\mathrm{S}_2 = \sum_{p=0}^{n} \mathrm{p}^2 \begin{pmatrix} n \\ p \end{pmatrix}$

EX 10

Soit $\sigma : \mathbb{Z} \longrightarrow \mathbb{N}$ qui à $n \in \mathbb{Z}$ associe le nombre de diviseurs positifs de n .

a) Soit p un nombre premier et $\alpha \in \mathbb{N}^*$ .Calculer $\sigma(p^\alpha)$.

b) Soient $a, b \in \mathbb{Z}$ premiers entre eux ,et $\varphi : \text{div}(a) \times \text{div}(b) \longrightarrow \text{div}(ab)$ définie par $\varphi(k,l) = kl$ montrer que φ est une bijection .div(n) désigne l'ensemble des diviseurs positifs d'un entier n

c) En déduire une relation entre $\sigma(ab)$, $\sigma(a)$ et $\sigma(b)$ si a et b sont premiers entre eux .

d) Soit n un entier naturel, $p_1^{\alpha_1}.\ p_2^{\alpha_2} \cdots\ p_r^{\alpha_r}$ la décomposition en nombre premiers de n .Exprimer $\sigma(n)$ en fonction des α_i .

Ex 11

On suppose que

n est un entier ≥ 2 tels que $2^n - 1$ est premier.

Montrer que n est un nombre premier.

Ex 12

Soient a et p deux entiers supérieurs à 2.

Montrer que si $a^p - 1$ est premier alors a=2 et p est premier.

Ex 13

Soit p un nombre premier, p$\geq$ 5. Montrer que p^2 - 1 est divisible par 24.

EX 14

Résoudre dans Z^2 les équations suivantes :

a) 17x + 6y = 1 b) 27x + 25y = 1 c) 118x + 35y = 1 d) 39x + 26y = 1

EX 15

1.Résoudre dans Z les équations : $x^2 = 2 \bmod 6$; $x^3 = 3 \bmod 9$.

2. Résoudre dans Z^2 les équations suivantes :

$5x^2 + 2xy - 3 = 0$; $y^2 + 4xy - 2 = 0$.

Ex 16

Résoudre dans $\mathbb{Z}$

$$1)\begin{cases} x = 2 \bmod 10 \\ x = 5 \bmod 13 \end{cases} \qquad 2)\begin{cases} x = 4 mod 6 \\ x = 7 mod 9 \end{cases} \quad 3)\begin{cases} 5x = 4 (mod 27) \\ 12x = 9 (mod 51) \end{cases}$$

Ex 17

Une bande de 17 pirates dipose d'un butin de N pièces d'or d'égale valeur. Ils décident de se le partager équitablement et de donner le reste au cuisinier (non pirate). Celui i reçoit 3 pièces. Mais une dispute éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment; le cusinier reçoit alors 4 pièces. Dans un naufrage ultérieur, seul le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pices.

Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates?

EX18

Combien l'armée de Han Xing comporte-t-elle de soldats (au minimum) si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?

Exercice 19

résoudre dans $\mathbb{Z}$ le système de congruence :

$$\begin{cases} x \equiv 3 \bmod 4 \\ x \equiv -2 \bmod 3 \\ x \equiv 7 \bmod 5 \end{cases}$$

Ex 20

Trouver le reste de la division euclidienne de
10^{2020} par 42.