Corrigé succinct de l'examen

Ex 1 : 13 est premier ; On peut utiliser le Corollaire du petit th de Fermat :

$a^{13-1} = a^{12} \equiv 1\ [13]$ si $\text{pgcd}(a, 13) = 1$.

$126 = 12 \times 10 + 6$.

$3^{126} \equiv (3^{12})^{10} \times 3^6 \equiv 3^6 \equiv (3^3)^2 \equiv 1^2 \equiv 1\ [13]$.

$5^{126} \equiv (5^{12})^{10} \times 5^6 \equiv (5^2)^3 \equiv (-1)^3 \equiv -1$

$3^{126} + 5^{126} \equiv 1 - 1 \equiv 0\ [13]$.

Remarque : On peut également remarquer que :

$3^3 \equiv 1\ [13]$ et $5^2 \equiv -1\ [13]$ et faire le même calcul.

Ex 2 : C'est une question du cours ; peu d'étudiants l'ont traité complètement.

Ex 3 : ① $|A^*| = \varphi(22) = \varphi(2 \times 11) = \varphi(2)\varphi(11) = 1 \times 10 = 10$

② $k \in A^* \iff \text{pgcd}(k, 22) = 1$

$A^* = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$

③ $\omega(\bar{7}) \mid 10 \Rightarrow \omega(\bar{7}) \in \{1, 2, 5, 10\}$

$\bar{7}^5 = -1 \Rightarrow \omega(\bar{7}) = 10$.

$\bar{7}$ ∗ donc un générateur du groupe A^* :
A^* est cyclique.

4) $A^* = \{\bar{7}, \bar{7}^2, \bar{7}^3, \dots, \bar{7}^{10}\}$.

$\bar{7}^k$ est un générateur ssi $\omega(\bar{7}^k) = 10$
ie. $\omega(\bar{7}^k) = \frac{10}{pgcd(k,10)}$, i.e.

$\bar{7}^k$ ∗ un générateur ssi. $pgcd(k,10) = 1$
le nombre de generateur ∗ donc égale à
$\varphi(10) = \varphi(2)\varphi(5) = 4$.
On peut les citer tous :
$\bar{7}, \bar{7}^3, \bar{7}^7, \bar{7}^9$

Ex 4 : ① On fait le tableau des carrés et on voit que la solution de $x^2 = 5$ ∗ et 4 et -4

② $z^2 - 4z + 10 = (z-2)^2 - 6 = 0$
$\Leftrightarrow (z-2)^2 = 5 \Leftrightarrow z-2 \in \{4, -4\}$
$\Leftrightarrow z \in \{6, -2\}$

(3) $\begin{cases} xy = 4 \\ x+y = 10 \end{cases}$ x, y sont donc les racines du polynôme : $Z^2 - 10Z + 4$

$\Delta = (10)^2 - 16 = +1 - 16 = -15 = -5$

5 est un carré, (-1) un non carré car $11 \not\equiv 1 [4]$.

et -5 est un non carré, pas de solution pour cette équation.

(5) (1) $2 = 1^2 + 1^2$.

$5 = 2^2 + 1^2$

$13 = 3^2 + 2^2$

$17 = 4^2 + 1^2$.

(2) $p = a^2 + b^2 \Leftrightarrow a^2 = -b^2$ dans $(\mathbb{Z}/p\mathbb{Z})^*$

$a \neq 0, b \neq 0, \quad a^2 \times (b^{-1})^2 = -1 \Leftrightarrow (ab^{-1})^2 = -1$

(-1) est un carré $\Leftrightarrow p \equiv 1 [4]$.

On peut également regarder les carrés modulo 4 ;

On trouve 0 et 1 ;

a^2 et b^2 ne peuvent être congrus à 0 ou à 1 en même temps car p est premier et $p \neq 2$;

on obtient facilement $p \equiv 1 [4]$

(3). $|S| = n+1$

$|S \times S| = (n+1)^2$;

$|\mathbb{F}_p| = p$; on $n^2 < p < (n+1)^2$

$\Rightarrow |S \times S| > |\mathbb{F}_p|$ et f ne peut donc être injective.

b). $f(x,y) = f(u,v) \iff$

$\bar{x} + \bar{\omega}\bar{y} = \bar{u} + \bar{\omega}\bar{v}$

$\bar{x} - \bar{u} = \bar{\omega}(\bar{v} - \bar{y})$.

$\iff \bar{a} = \bar{\omega}\bar{b} \iff \bar{a}^2 = -1\,\bar{b}^2$

$\iff \bar{a}^2 = \bar{\omega}^2 \bar{b}^2 \iff \bar{a}^2 + \bar{b}^2 = 0$ ie: ou encore: $p \mid a^2 + b^2$.

$(x,y) \neq (u,v) \Rightarrow (a \neq 0$ ou $b \neq 0$.

c). $\Rightarrow a^2 + b^2 > 0$;

$a, b \in S$; $a \leq n$

$a^2 + b^2 \leq 2n^2 < 2p$ $(n < \sqrt{p})$.

On sait que $p \mid a^2 + b^2 \Rightarrow$

$a^2 + b^2 = kp < 2p \Rightarrow k = 1$ et donc:

$a^2 + b^2 = p$.

Conclusion si $p = a^2 + b^2 \Rightarrow p \equiv 1 [4]$

et réciproquement si $p \equiv 1 [4]$; d'après $p = a^2 + b^2$.

EX6. n non premier ;

$n = pq$; $p \geq 2$, $q \geq 2$.

$p < n$, $q < n$. $\Rightarrow p \leq n-1$ et $q \leq n-1$

si $p \neq q$; $p \mid (n-1)! = 1 \times 2 \cdots \times (n-1)$

c'est même un des facteurs de ce produit et

Idem pour q ; donc $pq \mid (n-1)!$ i.e

$n \mid (n-1)!$.

si $p = q$, $n = p^2$. $(n-1)! = 1 \times 2 \cdots \times p \times \cdots (p^2-1)$

$p \mid (n-1)!$, regardons si $2p \nmid (n-1)!$

donc $2p \nmid (p^2-1)$ dans ce cas un encore.

$2p \nmid p^2 \iff p \neq 2$; $p > 2$.

$\iff$

En résumé si $p > 2$ i.e. $n = p^2 > 4$:

$p \neq 2p$ et p et $2p$ sont des facteurs de $(n-1)!$

donc $p \times 2p = 2n \mid (n-1)!$ en particulier

$n \mid (n-1)!$

Il reste donc juste le cas $n = p^2$ avec $p = 1$ ou 2 ; $n = 1$ exclu ; n non premier donc exclu

que $n > 2$).

le seul cas qui reste est $n = 2^2 = 4$:

$3! = 6$; et 4 ne

$(n-1) = 3$ divise pas 6

Ex 6. Soit G un groupe abélien.

U le sous ensemble des élément de G d'ordre fini;

U est un sous groupe de G.

preuve: $1 \in U$;

si $a, b \in U$; $a^n = 1$, $b^m = 1$

$(ab)^{nm} = a^{nm} b^{nm} = 1$ $(ab = ba)$

$a^n = 1 \Rightarrow (a^{-1})^n = 1$

il suffit donc de trouver un groupe infini abélien qui contient un infinité d'elements d'ordre fini; $\mathbb{C}^*$ remplit cette condition.

un autre exemple (voir si c'est le même!).

$\mathbb{Z}$ est un sous groupe additif de $\mathbb{R}$.

$\mathbb{R}/\mathbb{Z}$ (le groupe quotient) répond à la question