Corrigé succinct Examen.
Arith. 2023.

Ex1 : 1) p premier, $a \in \mathbb{Z}$ $\text{pgcd}(a,p) = 1$

$a^{p-1} \equiv 1 [p]$.

2). 13 premier $\Rightarrow$ $2^{12} \equiv 1 [13]$., $\text{pgcd}(2,13) = 1$

$70 = 5 \times 12 + 10$.

$2^{70} + 3^{70} = 2^{12 \times 5 + 10} + 3^{12 \times 5 + 10}$

$\equiv 2^{10} + 3^{10} [13]$.

$\equiv 2^2 \times 4 + 3^{3 \times 3} \times 3. [13]$

$\equiv -3 + 3 [13]$

$\equiv 0 [13]$.

$2^4 = 16 \equiv 3 (13)$

$3^3 = 27 \equiv 1 [13]$.

Ex2 : voir cours

Ex3 ①: $x^2 - \bar{3}1x + \bar{8} = x^2 + \bar{6}x + \bar{8}$

$= (x+\bar{3})^2 - \bar{9} + \bar{8} = (x+\bar{3})^2 - \bar{1}$

$= (x+\bar{3}-\bar{1})(x+\bar{3}+\bar{1})$

$= (x+\bar{2})(x+\bar{4})$.

les solutions sont -2 et -4 ou encore 35 et 33

② Appliquer l'algorithme d'euclide étendu :

On trouve : $(\bar{89})^{-1} = \bar{89}$;

$\bar{172} = -\bar{8}$

$x = \bar{89} \times 2 =$

Exo : ① $|A^*| = \varphi(54)$.

$54 = 27 \times 2 = 9 \times 3 \times 2 = 3^3 \times 2$.

$\varphi(54) = (3^3 - 3^2) \times (2-1)$

$= (27-9) = 18$.

② $a^9 = a^6 \times a^3 = \bar{17} \times \bar{19} = 3\bar{23} \equiv -1 \ [54]$.

$a^{18} = 1$; On sait que $\omega(a) \mid 18$.

$\omega(a) \in \{1, 2, 3, 6, 9, 18\}$. Le calcul precedent montre que $\omega(a) = 18 = |A^*|$.

ie: A^* est cyclique et a est un generateur de ce groupe.

③ $\bar{19}\, x = 1$; il s'agit de trouver $(\bar{19})^{-1}$;

on a trouvé : $\bar{19} \times \bar{17} = -1$ d'ou :

$\bar{19} \times (-\bar{17}) = 1 \Rightarrow (\bar{19})^{-1} = -\bar{17} = 3\bar{7}$

une autre facon de trouver $\bar{19}^{-1}$.

$\bar{19} = a^6$; $\bar{19}^{-1} = a^{18-6} = a^{12} = a^9 \times a^3$

$= -a^3 = -17$

l'equation $x^3 = \bar{1}$; on remarque d'abord que si x est solution, x est inversible, $x \in A^*$; $\exists k \in \{1, \dots, 17\}$

$x = a^k$; $x^3 = \bar{1}$ devient.

$(a^k)^3 = a^{3k} = \bar{1} = a^{18}$

$\Rightarrow 3k \equiv 0 \ [18]$; ou encore $k \equiv 0 \ [6]$;

On trouve $k = 0$; $k = 6$; $k \neq 12$;

Ce qui donne :

$x = a^0 = 1$ ou $x = a^6$ ou $x = a^{12}$

autrement dit : $x = 1$, $x = \bar{19}$; $x = \bar{37}$.

Ex 5 ① $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe ; $\bar{2} \neq \bar{0}$ (car $p \neq 2$)

$\exists\, b \in \mathbb{Z}$: $\bar{2}\bar{b} = \bar{1}$ ou encore :

$2b \equiv 1 [p]$.

(b) $(ba)^2 + 1 \equiv b^2a^2 + 1 [p]$ or $a^2 \equiv -4 [p]$

on a donc : $(ba)^2 + 1 \equiv b^2(-4) + 1 \; [p]$

$\equiv -(b \times 2)^2 + 1 \; [p]$

$\equiv -1 + 1 \; [p]$

$\equiv 0 [p]$.

c). $(ba)^2 + 1 \equiv 0 [p]$; signifie de $\bar{-1}$ est un carré dans $(\mathbb{Z}/p\mathbb{Z})$; on conclut que $p \equiv 1 [4]$ (cours)

② 5 est premier, $5 \equiv 5 [8]$: $5 \in E$, $E \neq \emptyset$:

On remarque tous les p_i sont impairs $\Rightarrow p^2$ aussi.

③ 2 ne peut donc diviser $Q = P^2 + 4$.

$p_i \mid P$, $p_i \mid P^2$; si $p_i \mid Q \Rightarrow p_i \mid 4$ Absurde.

donc $q \notin E$.

(4). On a: $q \mid p^2+4$, i.e:

$p^2+4 \equiv 0 \ [q]$, q premier:

D'après la question 1 $\Rightarrow$ $q \equiv 1 \ [4]$.

(5) $p_i \equiv 5 \ [8]$, $p_i^2 \equiv 1 \ [8]$.

donc $p^2 \equiv 1 \ [8]$; et $Q \equiv (1+4) \ [8]$
$\equiv 5 \ [8]$.

(6) Soit q un diviseur premier de Q;

$q \equiv 1 \ [4] \Rightarrow q = 4k+1$;

Regardons les congruences de q modulo 8;

q peut donc être congru à $1 \ [8]$. ou; $q \equiv 5 \ [8]$.

et c'est tout!

si tous les diviseurs premier de Q sont $\equiv 1 \ [8]$:

on aura: $Q \equiv 1 \ [8]$ Absurde, il existe bien

un diviseur q premier $\equiv 5 \ [8]$, $(q \mid Q)$

(7): q est premier, $q \equiv 5 \ [8]$; et $q \notin E$;

Absurde.

Ex 6 — $6x^2+5x+1 = 0$, si $x \in \mathbb{Z}$.

x solution on aura: $x(6x+5) = -1 \Rightarrow$

$x \in \{1, -1\}$. or ni 1 ni -1 ne sont solutions

... dans $\mathbb{Z}/p\mathbb{Z}$: $p \neq 2$; $p \neq 3$.

$\bar{6}x^2 + \bar{5}x + \bar{1}$;

$\Delta = \bar{25} - 4 \times 6 \times \bar{1} = \bar{1}$ est toujours un carré

dans $\mathbb{Z}/p\mathbb{Z}$; l'équation a des solutions.

si $p = 2$; $x = 1$ est solution ; (l'équation devient une équation du premier ordre.)

ou $p = 3$

Ex 7 : On calcule le déterminant de M de la manière suivante ; $C_2 \to C_2 + C_1$, $C_3 \to C_3 + C_1$, ... , $C_n \to C_n + C_1$

On trouve une matrice dont les colonnes 2 jusqu'à n sont formées par : soit 0, soit 2, soit -2 ;

donc : $\det M = \underbrace{2 \times 2 \cdots \times 2}_{(n-1) \text{ fois}} \det B = 2^{n-1} \det B$.

la matrice B qui reste ne contient que des 1, -1, 0.

$\det B \in \mathbb{Z}$; donc on a bien.

$\det M$ est un entier multiple de 2^{n-1}.