GOOD
OOD

Exercice 1

a) $(n-1)! \overset{?}{\equiv} -1 \mod n$ pour $2.3 = n$

$(2-1)! = 1! = 1 \equiv -1 \mod 2$

car $1 = 2 \cdot 1 \underline{-1}$

$(3-1)! = 2! = 2 \equiv -1 \mod 3$

car $2 = 3 \cdot 1 \underline{-1}$

b) On suppose que $n = p$ premier tq $n = p \geq 5$

trouver dans $\mathbb{Z}/p\mathbb{Z}$ les solutions de

$\bar{x}^2 - \bar{1} = 0$

$\Leftrightarrow \bar{x}^2 = \bar{1}$

$\Leftrightarrow \bar{x} = 1$ ou $\bar{x} = (p-1)$

car $(p-1)^2 = p^2 - 2p + 1$

$= p\underline{(p-2)} + \underset{\text{reste}}{1}$

Donc $\overline{(p-1)^2} = 1 \Rightarrow \overline{(p-1)}^2 - \bar{1} = 0$

c) Mq $\forall \bar{y} \in \mathbb{Z}/p\mathbb{Z}$ tq $2 \leq y \leq p-2$

$\exists! \bar{z} \in \mathbb{Z}/p\mathbb{Z}$ avec $2 \leq z \leq p-2$ tq

$\bar{1} = \bar{y} \cdot \bar{z}$

$\Leftrightarrow \bar{y} \cdot \bar{z} - 1 = 0$

Dans la question b) on a montrer que $\bar{x}^2 - \bar{1} = 0 \Leftrightarrow \bar{x}^2 = 1 \Leftrightarrow \bar{x} \cdot \bar{x} = \bar{1}$

si $\bar{x} = \bar{1}$ ou $\bar{x} = \overline{p-1}$ et pas d'autre.

Donc l'inverse d'un nombre dans $\mathbb{Z}/p\mathbb{Z}$ est lui même ssi $\bar{x} = \bar{1}$ ou $\bar{x} = p-1$

mais $2 \leq y \leq p-2$, donc $\bar{z} \neq \bar{y}$

Or p est premier et $2 \leq y \leq p-2$

donc $\bar{y} \wedge p = 1$, par le thm de Bézout

$\exists u, v \in \mathbb{Z}$ tq $u\bar{y} + vp = 1 \equiv 1 \bmod p$

$\Rightarrow u\bar{y} + vp \equiv 1 \bmod p$ $\quad vp \equiv 0 \bmod p$ car mult. de p

$\Rightarrow u\bar{y} \equiv 1 \bmod p$

donc $\bar{u}$ est un inverse de $\bar{y}$

$2 \leq \bar{u} \leq p-2$ car si $\bar{u} = 1$ donc $\underbrace{\bar{u}\bar{y}}_{\equiv 1 \bmod p} = 1 \cdot \bar{y} = \bar{y} \equiv 1 \bmod p$ mais $\bar{y} \geq 2$ contrad.

de même on suppose $\bar{u} = p-1$

donc $\bar{u}\bar{y} \equiv 1 \equiv (p-1)\bar{y} \equiv \underbrace{p\bar{y}}_{\equiv 0 \bmod p} - \bar{y}$

$\equiv -\bar{y} \bmod p$

$\equiv 1 \bmod p$

$\Rightarrow \bar{y} \equiv -1 \bmod p$

$\equiv p-1 \bmod p$

contrad.

On a montrer que $\forall 2 \leq y \leq p-2$ $\quad \exists\, 2 \leq \bar{z} \leq p-2$

Montrons que ce $\bar{z}$ inv. est unique.

On suppose par l'absurde que $\exists 2 \leq \bar{z}' \leq p-2$

tq $\bar{z}' \cdot \bar{y} \equiv 1 \bmod p$

Donc $\bar{y} \cdot \bar{z} \equiv \bar{y} \cdot \bar{z}' \equiv 1 \bmod p$

$\Leftrightarrow \bar{y} \cdot \bar{z} - \bar{y} \cdot \bar{z}' \equiv 0 \bmod p$

$\Leftrightarrow \bar{y}(\bar{z} - \bar{z}') \equiv 0 \bmod p$

$\Leftrightarrow \bar{y} \equiv 0 \bmod p$ ou $(\bar{z} - \bar{z}') \equiv 0 \bmod p$

$2 \leq \bar{y} \leq p-2 \Rightarrow \bar{y} \not\equiv 0 \bmod p$, donc c'est $\bar{z} - \bar{z}' \equiv 0 \bmod p$

$\Rightarrow \bar{z} \equiv \bar{z}' \bmod p$

mais on a supposé que $\bar{z} \neq \bar{z}'$ donc contradiction.

Donc $\bar{z}$ est une seule inverse de $\bar{y}$ dans $\mathbb{Z}/p\mathbb{Z}$

d) Dans la question précédente,
on a montré que $\forall \bar{y} \in \{2, \dots, p-2\}$ $\exists! \, \bar{z} \in \{2, \dots, p-2\}$
tq $\bar{y} \cdot \bar{z} = 1$

$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot p-2 \cdot p-1$

Donc pour chaque nombre dans $\{2, \dots, p-1\}$
il existe un et un seul inverse aussi
dans $\{2, \dots, p-1\}$ tq donc

$$\overline{(p-1)!} = \bar{1} \cdot \underbrace{\bar{2} \cdot \bar{3} \cdot \dots \cdot \overline{p-2}} \cdot \overline{p-1}$$
$$= \bar{1} \cdot \bar{1} \cdot \overline{p-1}$$

e) On suppose que $n \notin \mathcal{P}$ et $\exists \; 2 \leq m, d \leq n-1$
tq $n = dm$ et $n \geq 4$

<u>1 cas:</u> $d \neq m$

Alors $(p-1)! = 1 \cdot 2 \cdot \dots \cdot d \cdot \dots \cdot m \cdot \dots \cdot p-1$
$= 1 \cdot 2 \cdot \dots \cdot p-1 \cdot \dots \cdot d \cdot m$
$= 1 \cdot 2 \cdot \dots \cdot p-1 \cdot n \equiv 0 \mod n$
$\not\equiv -1 \mod n$

<u>2 cas:</u> $d = m$ donc $n = d^2$

Alors $(p-1)! = 1 \cdot 2 \cdot \dots \cdot d \cdot \dots \cdot p-1$
$= 1 \cdot 2 \cdot \dots \cdot p-1 \cdot d$
$1 \cdot 2 \cdot \dots \cdot p-1 \cdot d = \ell n + r = \ell d \cdot d + r$
$\Leftrightarrow d(1 \cdot 2 \cdot \dots \cdot i-1 \cdot \dots \cdot i+1 \cdot \dots \cdot p-1 - \ell d) = r$

$2d \leq d^2 - 1$
$\Leftrightarrow d^2 - 2d - 1 \geq 0$
$\Delta = 4 + 4 = 8$
$x_1 = \frac{2 - \sqrt{8}}{2} = 1 - \sqrt{2} \approx -0{,}4$
$x_2 = \frac{2 + \sqrt{8}}{2} = 1 + \sqrt{2} \approx 2{,}4$

donc un facteur $2d$ est dans $(n-1)!$
$(d^2-1)!$

si $d \geq 2{,}4 \Rightarrow d \geq 3 \Leftrightarrow \sqrt{n} \geq 3$
donc pour $n \geq 9$ $(n-1)! \equiv 0 \mod n$
pour cas $n = 4$ on a $(4-1)! = 3! = 6 \equiv 2 \mod 4$

Exercice 2

Soit $n \geq 1$ et $\{F_n\}_{n=0}^{\infty}$ tq $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ $\forall n \geq 1$

montrons que $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$

raisonnons par récurrence : $P(1)$: $n = 1$

$F_2 = F_1 + F_0 = 1 + 0 = 1$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^1 = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

vrai.

hérédité : $P(n)$: $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$

$P(n+1)$: $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{bmatrix}$

$F_{n+2} = F_{n+1} + F_n$

$$= \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} F_{n+1} + F_n & F_{n+1} \\ \underbrace{F_n + F_{n-1}}_{= F_{n+1}} & F_n \end{bmatrix} = \begin{bmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{bmatrix}$$

Donc $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ par récurrence !

b) $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ $\sim L_1 \to L_1 - L_2$

$\begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} = 1 \cdot 0 - 1 \cdot 1 = -1$

Or $\det(A^n) = \det(A)^n$

donc $\det\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)^n = \det\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)^n = (-1)^n$

Or $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$

donc $\det\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n\right) = \det\left(\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}\right)$

$= (-1)^n$

$\det\left(\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}\right) = F_{n+1} F_{n-1} - F_n \cdot F_n$

<u>donc $(-1)^n = F_{n+1} \cdot F_{n-1} - F_n \cdot F_n$</u>

c) D'après a) $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$

Soit $n \geq 0$ $m \geq 1$

On écrit

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^m = \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{m+n} = \begin{bmatrix} F_{m+n+1} & F_{m+n} \\ F_{m+n} & F_{m+n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^m \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n$$

$$= \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} F_{m+1} F_{n+1} + F_m F_n & F_{m+1} \cdot F_n + F_m F_{n-1} \\ \underbrace{F_m F_{n+1} + F_{m-1} F_n}_{= F_{n+m}} & F_n F_m + F_{n-1} F_{n-1} \end{bmatrix}$$

<u>donc $F_{n+m} = F_{n+1} F_m + F_n F_{m-1}$</u>

d) On remplace $u := \pm F_{m+1}$

$v := \pm F_m$

donc on a : $u F_{m-1} + v F_m = 1$

par Bezout cela signifie que

$\text{pgcd}(F_{m-1}, F_m) = 1$ ou que ces nombres sont premiers entre eux.

e) D'après (c) pour $n \geq 0$ et $m \geq 1$

$$F_{n+m} = F_{n+1} F_m + F_n F_{m-1}$$

Soit $e \geq 2$

1. Supposons que $e \mid F_m$ et $e \mid F_n$

Alors $\exists k_1,\ F_m = k_1 e$ $\quad F_m \equiv 0 \mod e \Rightarrow F_{n+1} F_m \equiv 0 \mod e$

$\exists k_2,\ F_n = k_2 e$ $\quad F_n \equiv 0 \mod e \Rightarrow F_{m-1} F_m \equiv 0 \mod e$

$F_{n+m} = F_{n+1} F_m + F_n F_{m-1} \equiv 0 + 0 \mod e$

Alors $F_{n+m} = F_{n+1} k_1 e + k_2 e F_{m-1}$

$= e(F_{n+1} k_1 + k_2 F_{m-1}) = F_{n+m}$

Donc F_{n+m} est un multiple de e

donc $e \mid F_{n+m}$

2. Supposons $(e \mid F_m$ et $e \mid F_{n+m})$

$F_m \equiv 0 \mod$.

$F_{n+m} \equiv 0 \mod e$

$F_{n+m} = F_{n+1} F_m + F_n F_{m-1} \equiv 0 \mod e$

$\equiv F_n F_{m-1} \equiv 0 \mod e$

$\Rightarrow (F_n \equiv 0 \mod e$ ou $F_{m-1} \equiv 0 \mod e)$

Or $F_m \wedge F_{m-1} = 1$ par (d)

$e \geq 2$ et $e \mid F_m$ donc $e \nmid F_{m-1}$ d'où $F_{m-1} \not\equiv 0 \mod e$ donc $F_n \equiv 0 \mod e$

$\Rightarrow \underline{e \mid F_n}$

f) Posons $d := pgcd(F_{n+m}, F_m)$

donc $d \mid F_{n+m}$ et $d \mid F_m$ $\Leftrightarrow$ $F_{n+m} \equiv 0 \mod d$
$F_m \equiv 0 \mod d$

D'après (e) $(d \mid F_{n+m}$ et $d \mid F_m) \Rightarrow d \mid F_n$

Montrons que d est le plus grand nombre qui divise à la fois F_n et F_m

Supposons par l'absurde que $\exists\, e > d$ tq $e \mid F_n$ et $e \mid F_m$

D'après (e) $(e \mid F_n$ et $e \mid F_m) \Rightarrow e \mid F_{n+m}$

Or $e \mid F_m$ et $e \mid F_{n+m}$ donc $e \leq pgcd(F_m, F_{n+m}) = d$
$\Rightarrow e \leq d$

Contradiction. Alors $\underline{d = pgcd(F_n, F_m) = pgcd(F_{n+m}, F_m)}$

g) Soit $0 \leq b < a$

Posons $d := pgcd(F_a, F_b)$

On pose $a - b = n$
et $b = m$
alors $a = a - b + b = n + m$

donc $d := pgcd(F_a, F_b) = pgcd(F_{n+m}, F_m)$
$= pgcd(F_n, F_m)$ d'après (f)
$= pgcd(F_{a-b}, F_b)$

h) $pgcd(F_{n+m}, F_m) = pgcd(F_n, F_m)$
$pgcd(F_a, F_b) = pgcd(F_{a-b}, F_b)$

$pgcd(F_{qb+r}, F_r) = pgcd(F_{qb}, F_r)$
$a = qb + r, b = b$
$pgcd(F_{qb+r}, F_b) = pgcd(F_{qb+r-b}, F_b) = pgcd(F_{(q-1)b+r}, F_b)$
$= \dots = pgcd(F_{b+r}, F_b)$
$= pgcd(F_r, F_b)$

(i) D'après (h) $pgcd(F_a, F_b) = pgcd(F_b, F_r)$ où r est le reste de la division euclidienne de a par b
Alors si on note r_1 le reste de la division de b par r alors $pgcd(F_a, F_b) = pgcd(F_b, F_r) = pgcd(F_r, F_{r_1})$ par (h)
On peut continuer de même jusqu'au moment où on obtient le dernier reste non nul r' ... $= pgcd(F_{r'}, F_0)$

qui par l'algorithme d'Euclide est le pgcd de a et b.
$\Rightarrow r' = pgcd(a, b)$
$= pgcd(F_{r'}, 0) = F_{r'} = F_{pgcd(a,b)}$
Donc $pgcd(F_a, F_b) = F_{pgcd(a,b)}$

h) $pgcd(F_{n+m}, F_m) = pgcd(F_n, F_m)$
$pgcd(F_a, F_b) = pgcd(F_{a-b}, F_b)$

$pgcd(F_{qb+r}, F_r) = pgcd(F_{qb}, F_r)$
$a = qb+r, b = b$
$pgcd(F_{qb+r}, F_b) = pgcd(F_{qb+r-b}, F_b) = pgcd(F_{(q-1)b+r}, F_b)$
$= \dots = pgcd(F_{b+r}, F_b)$
$= pgcd(F_r, F_b)$

h) Soit r le reste de la division euclidienne de a par b donc $\exists q$ tq $a = qb+r$. Montrons que $pgcd(F_a, F_b) = pgcd(F_b, F_r)$

$pgcd(F_a, F_b) = pgcd(F_{a-b}, F_b)$ d'après (g)

$= pgcd(F_{a-2b}, F_b)$

$pgcd(F_{a-b}, F_b) = pgcd(F_{qb+r-b}, F_r) = pgcd(F_{(q-1)b+r}, F_b)$
$= pgcd\, F_{(q-2)b+r}, F_b)$
$\vdots$
$= pgcd(F_{(q-q)b+r}, F_b)$
$= \underline{pgcd(F_r, F_b)}$

Exercice 3

(a)

$24x + 8y = a$ ssi $pgcd(24,8) \mid a$

$\Rightarrow$ Soit $d := pgcd(24,8)$ Supposons que $24x + 8y = a$

Alors $\exists a'$ $24 = a' \cdot d$ alors on a : $a'dx + b'dy = a$

$\exists b'$ $8 = b' \cdot d$ $\Leftrightarrow d(a'x + b'y) = a$

Alors $d \mid a$ où $d = pgcd(24,8)$

$\Leftarrow$ Supposons que $d := pgcd(24,8)$ $d \mid a$ alors $\exists k$, $a = d \cdot k$

donc $24x + 8y = d \cdot k$ par euclide

$\exists u, v$ tq $(24u + 8v = d)k$

$\Leftrightarrow 24(u \cdot k) + 8(v \cdot k) = d \cdot k = a$

Alors il existe une solution de $24x + 8y = a$

$(x,y) \in \mathbb{Z}^2$

(b) $24x + 8y = a$ on pose $a = 3$

Alors $24x + 8y = 3$

$\Leftrightarrow 8x + 3y = 1$ $8 \wedge 3 = 1$ par le Bézout

$\exists u, v$ tq $8u + 3v = 1$

On cherche une solution particulière par Bézout

$8 = 2 \cdot 3 + 2$

$3 = 2 \cdot 1 + 1$

$1 = 3 - 2$

$= 3 - (8 - 2 \cdot 3)$

$= 3 - 8 + 2 \cdot 3$

$= 3 \cdot 3 - 8$

$= (-1)8 + (3) \cdot 3$

$S_p = (-1, 3) = (x_0, y_0)$

$8\underbrace{(x - x_0)}_{X} + 3\underbrace{(y - y_0)}_{Y} = 0$

$\Leftrightarrow 8X + 3Y = 0$

$\Leftrightarrow 8X = -3Y \Rightarrow \begin{cases} 3 \mid 8X \overset{\text{Gauss}}{\Rightarrow} 3 \mid X \Rightarrow X = 3k \\ 8 \mid 3Y \Rightarrow 8 \mid Y \Rightarrow Y = 8k' \end{cases}$

$\Rightarrow 8 \cdot \underbrace{3 \cdot k} = -3 \cdot 8 \cdot k'$

$\Rightarrow k = -k' \Rightarrow (E) \{(k, -k) : k \in \mathbb{Z}\}$

$\Rightarrow (S) = \{(3 \cdot k + x_0, -8 \cdot k + y_0) : k \in \mathbb{Z}\}$

$= \{(3 \cdot k - 1, -8 \cdot k + 3) : k \in \mathbb{Z}\}$

(c) On pose $3 = 3\alpha$

Alors $24x + 9y = 3\alpha$

$\iff 8x + 3y = \alpha$

D'après (b) $\left[8\cdot(-1) + 3\cdot(3) = 1 \right] \alpha$

$\iff 8\cdot(-\alpha) + 3(3\alpha) = \alpha$

Alors $(x_0, y_0) = (-\alpha, 3\alpha)$

De même posons $X = x - x_0$, $Y = y - y_0$

Alors $8X + 3Y = 0$ Gauss $\Rightarrow \begin{cases} 8 \mid Y \\ 3 \mid X \end{cases}$ $\exists x, y$ $\quad y = 8y'$, $X = 3x'$

$\iff 8X = -3Y$

$\iff 8\cdot 3x' = -3\cdot 8\cdot y'$

$\iff x' = -y' \Rightarrow \exists k,\ \underline{x' = k},\ \underline{y' = -k}$

$\iff 8\cdot(3k) = -3(-8k)$

Donc $x = X + x_0 = 3k - \alpha$

$y = X + y_0 = -8k + 3\alpha$

Alors $(S) \iff \{ (3k - \alpha, -8k + 3\alpha) : k \in \mathbb{Z} \}$

(d) Trouver $\omega \in \mathbb{Z}$

$$\begin{cases} \omega \equiv 20 \ [24] \\ \omega \equiv 5 \ [9] \end{cases}$$

$\omega = 9\cdot k + 5$

$\omega = 24\cdot l + 20$

$\iff 9k + 5 = 24l + 20$

$\iff 24l + 9(-k) = -15 \quad | \ l = x,\ y = -k$

$24x + 9y = -15$ $\qquad -15 = 5\cdot(-3) \Rightarrow \alpha = -5$

$x = 3k - \alpha = l$

$y = -8k + 3\alpha = -k \Rightarrow k = 8k - 3\alpha$

$\omega = 24l + 20 = 24(3k + 5) + 20 = 72k + 140$ $\quad$ On pose $q = k + 1$

$= 72q + 68$

Alors $(S) \iff \{ 72q + 68 : q \in \mathbb{Z} \}$

Exercice 4

Soit $a \in \mathbb{N}$

$x := a^2+5a+2$ $\qquad d := pgcd(x,y)$

$y := a-5$

(a) $d := pgcd(x,y) = pgcd(y,x) = pgcd(y, x+ny)$ avec $n \in \mathbb{N}$

On pose $n = (-a)$

$a^2+5a+2 \quad -a(a-5) = 10a+2$

$x \quad + ny$

Alors $d := pgcd(x,y) = pgcd(a^2+5a+2, a-5) = pgcd(a-5, 10a+2)$

b) On pose $z = 10a+2$

Alors on a : $d := pgcd(a-5, 10a+2) = pgcd(x,z) = pgcd(x, z+nx)$

On pose $n = (-10)$

alors $z+nx = 10a+2 - 10(a-5) = 10a+2 - 10a+50 = 52$

Alors $d := pgcd(a-5, 52)$

c) x et y sont premiers entre eux ssi $pgcd(x,y) = d = 1$

D'après (c) $d := pgcd(a-5, 52)$

Alors cherchons tels a tel que $d = 1$

1) Si a est impair, alors $\exists \alpha$ tq $a = 2\alpha+1$

$a-5 = 2\alpha+1-5 = 2\alpha-4 = 2(\alpha-2)$

$pgcd(2(\alpha-2), 52) = pgcd(2(\alpha-2), 26\cdot 2) = 2\cdot pgcd(\alpha-2, 26)$

Cela signifie que $2 | a-5$ et $2 | 52$

donc on a trouvé un nombre qui divise

à la fois $a-5$ et 52, donc $d \geq 2$, mais

On cherche a tel que $d=1$, donc a doit être pair

Supposons que a est pair alors $\exists \alpha$ tq $a = 2\alpha$

Alors $a-5 = 2\alpha-5$ donc $2\alpha-5$ est toujours impair

donc n'est pas divisible par 2, donc $d \neq 2$

2) pour que $d = 1$ on doit trouver tel a tel que $52 = 4 \cdot 13$ ne divise pas $a-5$. On suppose a pair, donc $a-5$ impair.

Si $4 \cdot 13 \mid a-5$ 4 est premier à $a-5$ alors si 13 est premier à $a-5$ donc $4 \cdot 13$ est premier à $a-5$

Donc pour que 52 ne divise pas $a-5$ il faut que $a-5 \not\equiv 0 \mod 13$

$\Leftrightarrow a \not\equiv 5 \mod 13$

A l'inverse, on cherche tel a tel que $a-5 \nmid 52 \Leftrightarrow a-5 \nmid 4 \cdot 13$

On a supposé que a est pair, donc $a-5$ impair, donc $a-5 \wedge 4 = 1$, donc si $a-5 \mid 52$, par Gauss $a-5 \mid 13$, donc pour que $d=1$ il faut que $13 \not\equiv 0 \mod a-5 \Leftrightarrow 13 \neq (a-5)n \quad \forall n$

Seul a tel que $a-5 \mid 13$ est $a = 18 \Rightarrow a \equiv 5 \mod 13$.

Donc x et y sont premiers entre eux si $\underline{a \in 2\mathbb{N} \text{ et } a \not\equiv 5 \mod 13}$

<u>Exercice 5</u>

a) Soit $n \in \mathbb{N}$ et $n \geq 1$

Soit k le nombre de chiffre de n

On note a_i $(1 \leq i \leq k)$ $i^{\text{ème}}$ chiffre de n

donc on peut écrire $n = a_1 10^{k-1} + a_2 10^{k-2} + \dots + a_k 10^0$

$10 \equiv 1 \mod 9$ et $10^j \equiv 1^j \equiv 1 \mod 9 \quad \forall j \in \mathbb{N}$

Donc $n \equiv a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \dots + a_k 10^0 \; [9]$

$\Leftrightarrow n \equiv a_1 \cdot 1 + a_2 \cdot 1 + \dots + a_k \cdot 1 \; [9]$

$\Leftrightarrow n \equiv a_1 + a_2 + \dots + a_k \; [9]$

Donc tout nombre n est congrus à la somme de ses chiffres modulo 9.

b)

$$4444 \equiv 4+4+4+4 \ [9]$$
$$\equiv 16 \ [9]$$
$$\equiv 7 \ [9]$$
$$4444 = 3 \cdot 1481 + 1$$

$$4444^{4444} \equiv 7^{4444} \ [9]$$
$$\equiv 7^{4443} \cdot 7 \ [9]$$
$$\equiv 7^{3 \cdot 1481} \cdot 7 \ [9]$$
$$\equiv (7^3)^{1481} \cdot 7 \ [9]$$

c) $7^3 = 343 = 342 + 1 = 9 \cdot 38 + 1$

Donc $7^3 \equiv 1 \ [9]$

Alors $(7^3)^{1481} \cdot 7 \equiv (1)^{1481} \cdot 7 [9]$
$$\equiv 1 \cdot 7 \ [9]$$
$$\equiv 7 \ [9]$$

Donc $4444^{4444} \equiv 7 \ [9]$

d) $4444 < 10000$
$\Leftrightarrow 4444^{4444} < 10000^{4444} = 10^{4 \cdot 4444}$

Cela signifie que 4444^{4444} est écrit avec moins de $4 \cdot 4444$ chiffres.

e) $10^6 = 1000\,000$

$4 \cdot 4444 = 17776$

d'après (d) nombre de chiffres de $4444^{4444} < 4 \cdot 4444 = 17776$

Le plus grand nombres écrit avec 17776 chiffres est le nombre où tous les chiffres sont 9

Alors la somme des chiffres de ce nombre est

$9 \cdot 17776 = 159\,984 < 10^6$

Donc $A < 10^6$

f) D'après (e) $A < 10^6 = 1000000$

Alors $A \leq 999999$ Somme de ces chiffres est $6 \cdot 9 = 54$

Alors $B \leq 54$

g) D'après (f) $B \leq 54$, alors le nombre qui est ≤ 54 avec la plus grande somme des chiffres est 49 dont la somme des chiffres est 13

Alors $C \leq 13$

h) D'après (a) On peut écrire n'importe quel nombre comme $n = a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \dots + a_k \cdot 10^0$. où k : le nombre de chiffre

a_i avec $1 \leq i \leq k$ est le $i^{ème}$ chiffre.

De plus, ce nombre est congrus, à la somme de ces chiffres mod 9.

Donc on pose $4444^{4444} = a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \dots + a_k \cdot 10^0$ $k \in \mathbb{N}$

$\equiv a_1 + a_2 + \dots + a_k = A \ [9]$

avec a_i $i^{ème}$ chiffres de 4444^{4444}

De même, on ecrit $A = a_1 + a_2 + \dots + a_k = b_1 10^{l-1} + b_2 \cdot 10^{l-2} + \dots + b_l 10^0$ $l \in \mathbb{N}$ nbre de chiffres de A

$\equiv b_1 + b_2 + \dots + b_l = B \ [9]$

avec b_i le $i^{ème}$ chiffre de B

$B = b_1 + b_2 + \dots + b_l = c_1 \cdot 10^{m-1} + c_2 \cdot 10^{m-2} + \dots + c_m \cdot 10^0$ avec $m \in \mathbb{N}$ nbre de chiffres de B

c_i $i^{ème}$ chiffre de B $\equiv c_1 + c_2 + c_3 + \dots + c_m = C \ [9]$

Donc $4444^{4444} \equiv A \mod 9$

$A \equiv B \mod 9$

$B \equiv C \mod 9$

$\Rightarrow$ $\underline{4444^{4444} \equiv C \mod 9}$

(i) D'après (c) $4444^{4444} \equiv 7 \mod 9$

et d'après (h) $4444^{4444} \equiv C \mod 9$

Donc $C \equiv 7 \mod 9$

D'après (g) $C \leq 13$ $13 \equiv 4 \mod 9$

<u>Alors $C = 7$ car 7 est le seul nombre ≤ 13 tq $C \equiv 7 \ [9]$</u>

Exercice 7

a) Par le thm de Fermat, comme 13 est premier et 2 et 3 sont pas divisibles par 13, alors
$2^{12} \equiv 1 \mod 13$ et $3^{12} \equiv 1 \mod 13$

$2002 = 12 \cdot 166 + 10 = 1992 + 10$ $\qquad 12 \cdot 100 = 1200$

$2^{12 \cdot 166 + 10} = (2^{12})^{166} \cdot 2^{10}$ $\qquad 10 \cdot 12 \cdot 5 = 600$

$16 \cdot 12 = 192$ $\qquad 12 \cdot 16$

$(2^{12})^{166} \equiv 1^{166} = 1 \quad [13]$

$1992 + 10$

$2^{12 \cdot 166 + 10} \equiv 1 \cdot 2^{10} \quad [13]$

$2^{10} = 1024 \equiv 10 \quad [13]$ $\qquad 13 \cdot 80 - 13 - 13 = 13 \cdot 78 = 1014$

Donc $2^{12 \cdot 166 + 10} \equiv 1 \cdot 2^{10} \equiv 10 \; [13] \Rightarrow 2^{2002} \equiv 10 \; [13]$

$3^{12} \equiv 1 \quad [13]$ par le thm de Fermat

$3^{2002} = 3^{12 \cdot 166 + 10} = 3^{12 \cdot 166} \cdot 3^{10}$

$(3^{12})^{166} \equiv \underset{1}{1^{166}} \quad [13]$

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

$3^{3 \cdot 3} = (3^3)^3 \equiv 1^3 = 1 \; [13]$

$3^{10} = 3^{3 \cdot 3 + 1} = 3^{3 \cdot 3} \cdot 3 \equiv 1 \cdot 3 = 3 \; [13]$

$3^{2002} = 3^{12 \cdot 166} \cdot 3^{10} \equiv 1 \cdot 3 = 3 \; [13]$

Donc $2^{2002} + 3^{2002} \equiv 10 + 3 = 13 \; [13]$
$\equiv 0 \quad [13]$

Donc $13 \mid 2^{2002} + 3^{2002}$

6) $n \in \mathbb{N}$, $a \in \mathbb{Z}$ avec $a \wedge n = 1$

$k \in \mathbb{N}$ un exposant, r_k le reste de la division euclidienne de a^k par n.

Soit $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$, $k \longmapsto r_k$ une application.

Mq $\exists\, 0 \leq k_1 < k_2$ avec $k_2 - k_1$ minimal possible tel que $\varphi(k_2) = \varphi(k_1)$

Or r_k est le reste de la division euclidienne de a^k par n, alors $r_k \in [\![0, n-1]\!]$

D'où φ est à valeurs de $\mathbb{N}$ à $[\![0, n-1]\!]$

$\mathrm{Card}(\mathbb{N}) > \mathrm{Card}([\![0, n-1]\!])$

Donc φ n'est pas injective, alors $\exists\, k_1 \neq k_2$ tq $\varphi(k_1) = \varphi_2(k_2)$

$r_k = a^k \bmod n$ est un entier compris entre 0 et $n-1$

Or l'ensemble des valeurs possible est fini (égal à $[\![0, n-1]\!]$

Donc il existe un point depuis lequel la suite (r_k) commence à se repeter periodiquement

On prend k_1 et $r_{k_1} = \varphi(k_1)$

On l'agrandi à 1 chaque fois notons k_2 jusqu'au moment où on obtient la première répétition $r_{k_1} = \varphi(k_2)$

$k_2 - k_1$ est donc la periode minimale.

c) On note $l := k_2 - k_1$

Montrons que $\forall n \in \mathbb{N}$ $a^{l+k} \equiv r_k \bmod n$ où $a^k \equiv r_k \bmod n$

$a^{l+k} = a^l \cdot a^k$

$a^l = a^{k_2 - k_1} = \dfrac{a^{k_2}}{a^{k_1}}$

Or $r_{k_1} = r_{k_2} =: r$, donc $a^{k_1} \equiv r \bmod n$ et $a^{k_2} \equiv r \bmod n$

$\underbrace{\dfrac{a^{k_2}}{a^{k_1}}}_{\equiv \frac{r}{r} = 1} \equiv \dfrac{r}{r} \bmod n$ donc $a^l \equiv 1 \bmod n$

D'où $a^{l+k} = a^l \cdot a^k \equiv 1 \cdot a^k \bmod n$

$\equiv r^k \bmod n$

d) $\forall m \in \mathbb{N} \quad \forall k \in \mathbb{N}$

$$a^{m \cdot l + k} = a^{m \cdot l} \cdot a^k = (a^l)^m \cdot a^k$$

$a^l \equiv 1 \mod n$ d'après (c) d'où $(a^l)^m \equiv \underset{=1}{1^m} \mod n$

Donc $a^{m \cdot l + k} \equiv a^k \mod n$, d'où r_k est l périodique.

65 130 520 1040 2080
260 1027 2054 4108 8190

e) $n = 13$, $a = 2$ 2 admet seulement 2 diviseurs : 2 et 1

$2 \nmid 13$, mais 1 divise. Alors $13 \wedge 2 = 1$

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14					
a^k	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192						
r_k	1	2	4	8	3	6	12	11	9	5	10	7	1	2						

Alors $12 - 0 = 12 = l$ est la periode de r_k

f) On pose $n = 13$, $a = 3$ On pose $r_k = a^k \wedge n$

Cherchons l' la periode de r_k

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16			
a^k	1	3	9	27	81	243	729	2187												
r_k	1	3	9	1	3	9														

$3 - 0 = 3 = l'$ est la periode de r^k

g) $2^{2002} = 2^{12 \cdot 166 + 10} \equiv 2^{10} \mod 13$ car $r_k = 2^k \wedge 13$ est 12 periodique et d'après c) $a^{l+k} \equiv a^k \mod n$ où l est la période.

$2^{10} \equiv 10 \mod 13$ alors $2^{2002} \equiv 10 \mod 13$

$3^{2002} = 3^{3 \cdot 667 + 1} \equiv 3 \mod 13$ car $3^k \wedge 13$ est 3 periodique

D'où $2^{2002} + 3^{2002} \equiv 10 + 3 \mod 13$
$\equiv 13 \mod 13$
$\equiv 0 \mod 13$

Donc $2^{2002} + 3^{2002}$ est bien divisible par 13

h)

$$2^{2002} + 3^{2002} = 2^{2\cdot 1001} + 3^{2\cdot 1001} = 4^{1001} + 9^{1001} = 4^{1001} - (-9)^{1001}$$

$$\begin{aligned} 4^{1001} - (-9)^{1001} &= (4-(-9))(4^{1000} + 4^{999}(-9) + \dots + 4(-9)^{999} + (-9)^{1000}) \\ &= (4+9)(4^{1000} + 4^{999}(-9) + \dots + 4(-9)^{999} + (-9)^{1000}) \\ &= 13(4^{1000} + 4^{999}(-9) + \dots + 4(-9)^{999} + (-9)^{1000}) \end{aligned}$$

Donc $2^{2002} + 3^{2002}$ est un multiple de 13,
alors est divisible par 13.

Exercice 6

a) par def $\mathrm{Card}\,(\mathbb{Z}/22\mathbb{Z})^\times = \varphi(22) = \varphi(2\cdot 11) = \varphi(2)\cdot\varphi(11)$
$= (2-1)\cdot(11-1) = 10$

b) Montrons que $\bar{2}$ engendre $(\mathbb{Z}/11\mathbb{Z})^\times$

$\bar{2}^1$	$\bar{2}^2$	$\bar{2}^3$	$\bar{2}^4$	$\bar{2}^5$	$\bar{2}^6$	$\bar{2}^7$	$\bar{2}^8$	$\bar{2}^9$	$\bar{2}^{10}$
$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{5}$	$\bar{10}$	$\bar{9}$	$\bar{7}$	$\bar{3}$	$\bar{6}$	$\bar{1}$

D'où $o(2) = \varphi(11) = 10$ et les puissances de $\bar{2}$ decrivent un le groupe $(\mathbb{Z}/11\mathbb{Z})^\times$

Or $(\mathbb{Z}/11\mathbb{Z})^\times$ est engendré par $\bar{2}$, donc monogène, de plus ce groupe est de cardinal fini, donc <u>cyclique</u>.

c) D'après le théorème du cours, si $m \wedge n = 1$

alors un morphisme des anneaux

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

est isomorphe.

De plus, l'autre theorème nous dit que si on a un iso-morphisme des anneaux
$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$
il offre un isomorphisme des groupe des inversibles:

$$\varphi' : (\mathbb{Z}/mn\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

Posons $m = 2$ $n = 11$, on a bien $m \wedge n = 2 \wedge 11 = 1$

d'où on obtient que $(\mathbb{Z}/22\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times$

d) Prenons $b = 13$

$13 \equiv 1 \mod 2$ et $13 \equiv 2 \mod 11$

e)

$\overline{13}^1$	$\overline{13}^2$	$\overline{13}^3$	$\overline{13}^4$	$\overline{13}^5$	$\overline{13}^6$	$\overline{13}^7$	$\overline{13}^8$	$\overline{13}^9$	$\overline{13}^{10}$
$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\shortparallel$
13	15	19	5	21	9	7	3	17	1

$o(13) = \varphi(22)$ d'où $\overline{13}$ genère $(\mathbb{Z}/22\mathbb{Z})^\times$

(f) On sait déjà que $(\mathbb{Z}/22\mathbb{Z})^\times$ est de l'ordre 10.

Donc le nombre de générateurs est $\varphi(10) = 4$.
Donc le nombre de generateurs de $(\mathbb{Z}/22\mathbb{Z})^\times$ est $\underline{4}$.

g) Les éléments de $(\mathbb{Z}/22\mathbb{Z})^\times$ sont:
$\{13, 15, 19, 5, 21, 9, 7, 3, 17, 1\}$

Un générateur g doit avoir ordre 10, i.e $g^{10} \equiv 1 \mod n$

$1^1 \equiv 1 \mod 22$
$3^5 \equiv 1 \mod 22$
$5^5 \equiv 1 \mod 22$
$\underline{7}^{10} \equiv 1 \mod 22$
$9^5 \equiv 1 \mod 22$
$\underline{13}^{10} \equiv 1 \mod 22$
$15^5 \equiv 1 \mod 22$
$\underline{17}^{10} \equiv 1 \mod 22$
$\underline{19}^{10} \equiv 1 \mod 22$
$21^2 \equiv 1 \mod 22$

Les nombre $g \in (\mathbb{Z}/22\mathbb{Z})^\times$ qui $g^k \equiv 1 \mod 22$ tq $k \neq 10$ ne sont pas de l'ordre 10, donc ne sont pas générateur
Les nombres $g \in (\mathbb{Z}/22\mathbb{Z})^\times$ qui ont $k = 10$ le plus petit exposant tel que $g^k \equiv 1 \mod 22$ sont de l'ordre 10 et donc sont des générateurs de $(\mathbb{Z}/22\mathbb{Z})^\times$
Tels nombres sont: $\underline{7, 13, 17, 19}$ - sont les générateurs de $(\mathbb{Z}/22\mathbb{Z})^\times$

h) De même façon comme dans (c)

$(\mathbb{Z}/33\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times$

Car $33 = 3 \cdot 11$ et $3 \wedge 11 = 1$

Donc $(\mathbb{Z}/33\mathbb{Z})^\times$ est cyclique ssi $(\mathbb{Z}/3\mathbb{Z})^\times$ est cyclique et $(\mathbb{Z}/11\mathbb{Z})^\times$ est cyclique.

D'après (B) $(\mathbb{Z}/11\mathbb{Z})^\times$ est cyclique.

Donc $(\mathbb{Z}/33\mathbb{Z})^\times$ est cyclique si $(\mathbb{Z}/3\mathbb{Z})^\times$ est cyclique, vérifions :

$(\mathbb{Z}/3\mathbb{Z})^\times$ $\quad \varphi(3) = (3-1) = 2$

$(\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}, \bar{2}\}$ $\quad \bar{2}^1 = 2 \not\equiv 1 \mod 3$
$\bar{2}^2 \equiv 1 \mod 3$

Donc $\bar{2}$ est de l'ordre 2 est génère $(\mathbb{Z}/3\mathbb{Z})^\times$
De plus $(\mathbb{Z}/3\mathbb{Z})^\times$ est de l'ordre fini.
D'où $(\mathbb{Z}/3\mathbb{Z})^\times$ est cyclique.

Or $(\mathbb{Z}/3\mathbb{Z})^\times$ et $(\mathbb{Z}/11\mathbb{Z})^\times$ sont cyclique
et $(\mathbb{Z}/33\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times$
donc $(\mathbb{Z}/33\mathbb{Z})^\times$ est cyclique.