55

Rappel : Si p est premier, alors $(p-1)! = -1 \ [p]$ (Théorème de Wilson)

Si $p = 29$, $28! = -1 \ [29]$

$28! = 26! \times 27 \times 28 = 26! \times (-2) \times (-1) \ [29]$

donc $26! \times 2 = -1 \ [29]$

On dans $\mathbb{Z}/29\mathbb{Z}$, $\overline{2}$ est inversible pour la multiplication

$2 \times 15 = 1 \ [29]$

donc $26! \times \underbrace{2 \times 15}_{1 \ [29]} = -15 \ [29]$

$\Leftrightarrow 26! = -15 \ [29] = 14 \ [29]$

Comme $0 \leqslant 14 < 29$, le reste de la division euclidienne de $26!$ par 29 c'est 14.

3.4.

$$7x - 4y^3 = 1$$

Raisonnement par l'absurde : Si $x, y \in \mathbb{Z}$ tels que $7x - 4y^3 = 1$

alors $\quad -4y^3 = 1 \ [7]$

Or dans $\mathbb{Z}/7\mathbb{Z}$, $\quad y = 0, \pm 1, \pm 2, \pm 3 \ [7]$

ou

donc $-4y^3 = \begin{cases} 0 \ [7] & \text{si } y = 0 \ [7] \\ \pm 4 \ [7] & \text{si } y = \pm 1, \pm 2 \text{ ou } \pm 3 \ [7] \end{cases}$

donc $\neq 1 \ [7]$ contradiction.

(ii) Par l'absurde. Si $x, y, z, t \in \mathbb{Z}$ et $x^3 + y^3 + z^3 + 9t = 4$

alors : $\quad x^3 + y^3 + z^3 = 4 \ [9]$

Or $\quad \mathbb{Z}/9\mathbb{Z} = \{ \bar{0}, \pm\bar{1}, \pm\bar{2}, \pm\bar{3}, \pm\bar{4} \}$

donc $\forall x \in \mathbb{Z}, \quad x^3 = 0, \pm 1 \ (\pm 1, 0, \text{ou } \pm 1) \ [9]$

de même pour y^3, z^3

en particulier $x^3+y^3+z^3 \neq 4 \ [9]$. Contradiction.

(iii) Par l'absurde si $x, y \in \mathbb{Z}$ sont tels que $x^2+xy+2y^2 = 7003$

$(x+y)x = x^2+xy = 1 \ [2]$

$$(*) \quad \left(x+\frac{1}{2}y\right)^2 + \frac{7}{4}y^2 = 7003$$

Dans $\mathbb{Z}/7\mathbb{Z}$: $x^2+xy+2y^2 = 3 \ [7]$

$x = 0, \pm 1, \pm 2, \pm 3 \ [7] \Rightarrow x^2 = 0, 1, 4, 2 \ [7]$

$2y^2 = 0, 2, 1, 4 \ [7]$

Or y est pair car $x(x+y)$ impair $\Rightarrow$ x impair, y pair

$y = 2y'$, $y' \in \mathbb{Z}$ donc $(*) \Rightarrow (x+y')^2 + 7y'^2 = 7003$

$\Rightarrow (x+y')^2 = 3 \ [7]$

Or 3 n'est pas un carré modulo 7 $\Rightarrow$

Contradiction car $x+y' \in \mathbb{Z}$.

3.5.

a, b, c entiers impairs

$$(a+b+c)^2 = a^2+b^2+c^2+2(ab+bc+ca)$$

Dans $\mathbb{Z}/8\mathbb{Z}$

x	0	± 1	± 2	± 3	4
x^2	0	1	4	1	0

donc $(a+b+c)^2 = 1 \ [8]$ car $a+b+c$ impair

$a^2+b^2+c^2 = 1+1+1 \ [8] = 3 \ [8]$

donc $2(ab+bc+ca) = 1-3 \ [8] = -2 \ [8]$

($2(ab+bc+ca) = (a+b+c)^2 - a^2 - b^2 - c^2$

$\forall x$ impair, $x^2 = 1 \ [8]$)

En divisant par 2 : $ab+bc+ca = -1 \ [4]$

Si $ab+bc+ca \in \mathbb{N}$ et si $\sqrt{ab+bc+ca} \in \mathbb{N}$

alors $ab+bc+ca = \left(\sqrt{ab+bc+ca}\right)^2 = n^2$

Or $\forall n \in \mathbb{N}$, $n^2 = 1$ ou $0 \ [4] \neq -1 \ [4]$ contradiction.

Donc $\sqrt{ab+bc+ca} \notin \mathbb{Q}$ (cf exo 2.4).

3.6 Résoudre $2^x - 3^y = 1$ dans $\mathbb{N}^2$

$\Leftrightarrow (x,y) = (2,1), (1,0)$

En effet ce sont des solutions.

Réciproquement, $2^x - 3^y = 1$, $x, y \in \mathbb{N}$

$y = 0 \Rightarrow x = 1$

$y = 1 \Rightarrow x = 2$

$y \geq 2 \Rightarrow$ impossible

car alors $2^x - 3^y = 1 \Rightarrow 2^x = 1 + 3^y = 1 [9]$

Or si $x \in \mathbb{N}$, $2^x = \pm 1, \pm 2, \pm 4 \mod 9$ (récurrence)

$2^0 = 1 [9]$, $2^1 = 2 [9]$, $2^2 = 4 [9]$, $2^3 = -1 [9]$

$2^4 = -2 [9]$, $2^5 = -4 [9]$, $2^6 = 1 [9]$

$2^7 = 2 [9]$ etc. ...

si $x \geq 3$, alors $2^x - 3^y = 1 \Rightarrow -3^y = 1 - 2^x$

$8 = 2^3 \mid 2^x$

$= 1 \ [8]$

or $3^2 = 1 \ [8]$

donc $3^y = 1$ ou $3 \ [8]$ $(\forall y \in \mathbb{N})$

donc $-3^y = -1$ ou $-3 \ [8] \neq 1 \ [8]$ $(\forall y \in \mathbb{N})$

Contradiction. Dòù: $x \leq 2 \Rightarrow x = \cancel{0}, 1$ ou 2

$\Rightarrow x = 1$ et $y = 0$

ou $x = 2$ et $y = 1$

2.4.

1) $P(X) = X^n + a_{n-1} X^{n-1} + \cdots + a_0$, $a_i \in \mathbb{Z}$

$n \geq 1$

si $x = \frac{p}{q} \in \mathbb{Q}$ où $p, q \in \mathbb{Z}$, $q \neq 0$, $p \wedge q = 1$

si $P(x) = 0$ alors $x \in \mathbb{Z}$

En effet, $P(x) = \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_0 = 0$

$\Rightarrow p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n = 0$

$\Rightarrow p^n = q \left(-a_{n-1} p^{n-1} - \cdots - a_0 q^{n-1} \right)$

$\Rightarrow \quad q \mid p^n \quad \xrightarrow{\text{lemme de Gauss}} \quad q \mid p^{n-1} \Rightarrow q \mid p^{n-2} \Rightarrow \cdots \Rightarrow q \mid p$

$\Rightarrow \quad q = \pm 1 .$

ex: $X^2 - 2$ n'a pas de racine rationnelle car n'a pas de racine entière

2) Considérer $X^k - n \in \mathbb{Z}[X]$ unitaire

si $n^{1/k} \in \mathbb{Q}$, alors c'est une racine de $X^k - n$

donc $n^{1/k} \in \mathbb{Z}$

$\Rightarrow \quad n = (n^{1/k})^k$

$\Rightarrow$ les facteurs premiers de n apparaissent avec un exposant dans $k\mathbb{N}$.

3) $r = \frac{p}{q}$, $p, q \in \mathbb{Z}$, $q \neq 0$, $p \wedge q = 1$

Si $P(r) = 0$, alors $a_n r^n + \cdots + a_0 = 0$

$\Rightarrow \quad a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n = 0$

$\Rightarrow \quad p \mid a_0 q^n$ et $q \mid a_n p^n$

Or $p \wedge q = 1 \Rightarrow p \wedge q^n = 1$ et $q \wedge p^n = 1$

(si l nombre premier divise p et q^n alors l divise p et q)

donc lemme de Gauss $\Rightarrow$ $p \mid a_0$ et $q \mid a_n$

Application $X^3 - 3X + 1$ n'a pas de racine dans $\mathbb{Q}$.

$\left(2\cos\frac{2\pi}{9}, 2\cos\frac{4\pi}{9}, 2\cos 8\pi/9\right)$

2.5 x^n et $x^{n+1} \in \mathbb{Z} \Rightarrow x = 0$ ou $x = \frac{x^{n+1}}{x^n} \in \mathbb{Q}$.

et $x = (x^n)^{1/n}$ ...