Arithmétique
FICHE III: Arithmétique élémentaire et congruences

Exercice 1. Trouver toutes les solutions dans $\mathbb{N}$ et dans $\mathbb{Z}$ des équations suivantes :

(1) $41x - 77y = 3$

(2) $17x - 59y = 4$

(3) $59x - 18y = 1$

(4) $174x - 48y = 30$

Exercice 2. Montrer que $n+1$ est premier avec $2n+1$ pour tout $n \in \mathbb{N}$, et en déduire que $(n+1)|\binom{2n}{n}$.

Exercice 3. Soit $n \in \mathbb{Z}$. Montrer que $6|5n^3 + n$ et que $n^2 \equiv 1, 0 \text{ou} 4 \mod 8$.

Exercice 4. Trouver l'ensemble des solutions de :

(1) $23x \equiv 1 \mod 171$

(2) $3x + 5 \equiv 0 \mod 43$

(3) $12x \equiv 8 \mod 42$

(4) $8x \equiv 12 \mod 42$

(5) $x \equiv 2 \mod 15$ et $x \equiv 8 \mod 28$

Exercice 5. Montrer que pour tout $n \in \mathbb{N}$ on a :

(1) $49|2^{3n+3} - 7n - 8$

(2) $7|3^{2n+1} + 2^{n+2}$

(3) $11|(3^{8n} \times 5^4) + (5^{6n} \times 7^3)$

Exercice 6. Montrer que si p est un nombre premier, alors pour tout k tel que $0 < k < p$, on a $p|\binom{p}{k}$.

Exercice 7. (1) Combien de 0 possède le nombre $63!$? On pourra calculer les puissances de 2 et de 5 intervenant dans $63!$. (On pourra même écrire $63!$ en produit de facteurs premiers).

(2) Écrivons un nombre entier par son écriture décimale : $u = a_n a_{n-1} ... a_1 a_0$ où a_i est le chiffres des 10^i-aines, a_0 celui des unités. Montrer que $u \equiv \sum_{i \text{ pair}} a_i - \sum_{i \text{ impair}} a_i \mod 11$. En déduire un critère de divisibilité par 11 ou une "preuve" par 11.

(3) Trouver le chiffre des unités de l'entier 7^{2017}.

(4) Calculer $7^{395} \mod 11$, $12^{246} \mod 43$, $2^{10001001} \mod 121$.

Exercice 8. (1) Montrer que si $n \in \mathbb{N}$ n'est pas premier et $n > 4$ alors $(n-1)! \equiv 0 \mod n$.

(2) Si $p = 2$, montrer que $(p-1)! \equiv -1 \mod 2$.

(3) On suppose maintenant que p est premier impair. Montrer que si $x = x^{-1}$ dans $\mathbb{Z}/p\mathbb{Z}$ alors $x = 1$ ou $x = -1$. En déduire que l'on peut grouper "presque tous" les éléments de $\mathbb{Z}/p\mathbb{Z}$ non nuls par paires $\{x, x^{-1}\}$ et en conclure que $(p-1)! \equiv -1 \mod p$

Exercice 9. On veut montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4. Pour cela, on regarde les nombres de Fermat $\mathrm{F}_n = 2^{2^n} + 1$ pour $n \geq 1$.

(1) Calculer F_n pour $n = 1, 2$.

(2) Soit p un nombre premier impair divisant F_n. Montrer que dans $\mathbb{Z}/p\mathbb{Z}$, 2 est inversible.

(3) Trouver un nombre N en fonction de n, tel que $2^N \equiv -1 \mod p$.

(4) Montrer qu'il existe k tel que $2^{2^k} \equiv 1 \mod p$ et en déduire que le plus petit k vérifiant cela vaut $n + 1$.

(5) Montrer que 2^{n+1} divise $p - 1$ et donc que $p \equiv 1 \mod 4$ et $p > 2^{n+1}$.

(6) Conclure.

Exercice 10. On veut montrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 4. Pour cela on suppose par l'absurde qu'il n'en existe qu'un nombre fini : $p_1 < \cdots < p_r$.

(1) Que valent p_1 et p_2 ?

(2) Soit n un nombre entier montrer que si $n \equiv -1 \mod 4$ alors il existe un nombre premier p_i qui le divise.

(3) On regarde $n = 4 \prod_{i=1}^{r} p_i - 1$. En déduire une contradiction en utilisant la question précédente.

Exercice 11. On cherche à trouver tous les entiers $0 < a < b$ tels que $a^b = b^a$.

(1) Montrer que les nombres premiers divisant a sont les mêmes que ceux divisant b.

(2) Soit p l'un d'entre eux, montrer que si r (resp. s) est l'exposant de p dans la décomposition de a (resp. de b) alors $r < s$ et en déduire que a divise b.

(3) Montrer que si on écrit $b = an$ alors $an = a^n$.

(4) Montrer que $a^2 \geq 2a$ et par suite que $a^n > na$ pour $n > 2$. En déduire que $a = n = 2$ et par suite que $a = 2$ et $b = 4$ est l'unique solution.

Exercice 12. On cherche à résoudre dans $\mathbb{N}^*$, l'équation $x^2 + y^2 = z^2$.

(1) Trouver une solution.

(2) Montrer que si (x, y, z) est solution alors (y, x, z) est aussi solution.

(3) On pose $d = \mathrm{pgcd}(x, y)$, montrer que d divise z.

(4) En déduire que les solutions sont toutes de la forme (dx_1, dy_1, dz_1) où $d \in \mathbb{N}^*$ et $\mathrm{pgcd}(x_1, y_1) = 1$.

On suppose dorénavant que x et y sont premiers entre eux.

(5) Montrer que x et y ne sont pas de même parité.

(6) En déduire qu'on peut supposer que y est pair.

(7) Montrer que x et z sont impairs et premiers entre eux.

(8) Montrer que $(z-x)/2$ et $(z+x)/2$ sont premiers entre eux et sont des carrés.

(9) En déduire qu'on peut écrire $x = v^2 - u^2$, $y = 2uv$ et $z = u^2 + v^2$, avec $u < v$ premiers entre eux pas de même parité.

(10) Réciproquement si on a $u < v$ premiers entre eux et pas de même parité, montrer que $x = v^2 - u^2$ et $y = 2uv$ sont premiers entre eux, y est pair et il existe z tel que $x^2 + y^2 = z^2$.

On ne suppose plus que x et y sont premiers entre eux.

(11) Finalement, écrire la forme de tous les (x, y, z) possibles et décrire ceux pour lesquels $x < y < z < 50$.

Exercice 13. Soit p un nombre premier impair et $n = p^r$ pour $r > 0$.

(1) Soit $u \geq 0$, montrer que $(1 + up^k)^p = 1 + vp^{k+1}$ avec $v \equiv u \mod p$. On pourra développer avec le binôme de Newton et vérifier que si $i \geq 2$, p^{k+2} divise $\binom{p}{i} u^i p^{ki}$ pour $i \geq 2$ et $k \geq 1$.

(2) Montrer en utilisant le théorème d'Euler que l'on a pour tout $r > 0$, $k^{p^r} \equiv k^{p^{r-1}} \mod p^r$. En déduire par récurrence sur r que $k^{p^{r-1}} \equiv 1 \mod p^r$ entraîne que $k \equiv 1 \mod p$.

(3) En utilisant la première question, montrer la réciproque et montrer que $(1 + p)^{p^{r-2}} \equiv 1 + p^{r-1} \mod p^r$ par récurrence sur $r \geq 2$.

(4) Montrer que $1 + p$ est d'ordre p^{r-1} dans $(\mathbb{Z}/p^r\mathbb{Z})^\times$ pour $r \geq 2$.