Soit A l'ensemble des entiers naturels de l'intervalle [1 ; 46].

1. On considère l'équation (E) : $23x + 47y = 1$ où x et y sont des entiers relatifs.

a. Donner une solution particulière (x_0, y_0) de (E).

b. Déterminer l'ensemble des couples (x, y) solutions de (E).

c. En déduire qu'il existe un unique entier x appartenant à A tel que $23x \equiv 1$ (47).

2. Soient a et b deux entiers relatifs.

a. Montrer que si $ab \equiv 0$ (47) alors $a \equiv 0$ (47) ou $b \equiv 0$ (47).

b. En déduire que si $a^2 \equiv 1$ (47) alors $a \equiv 1$ (47) ou $a \equiv -1$ (47).

3. *a*. Montrer que pour tout entier p de A, il existe un entier relatif q tel que $p \times q \equiv 1$ (47) .

Pour la suite, on admet que pour tout entier p de A, il existe un unique entier, noté $inv(p)$, appartenant à A tel que $p \times inv(p) \equiv 1$ (47) .

Par exemple :

$inv(1) = 1$ car $1 \times 1 \equiv 1$ (47), $inv(2) = 24$ car $2 \times 24 \equiv 1$ (47), $inv(3) = 16$ car $3 \times 16 \equiv 1$ (47).

b. Quels sont les entiers p de A qui vérifient $p = inv(p)$?

c. Montrer que $46 ! \equiv -1$ (47).

CORRECTION

1. *a*. $2 \times 23 = 46$ donc $-2 \times 23 + 47 \times 1 = 1$ donc $(-2 ; 1)$ est une solution particulière de (E).

b. $23x + 47y = 1$

$-2 \times 23 + 47 \times 1 = 1$ donc par différence membre à membre : $23(x + 2) + 47(y - 1) = 0$ soit $23(x + 2) = -47(y - 1)$

47 divise $23(x + 2)$ or 23 et 47 sont premiers entre eux donc 47 divise $x + 2$(théorème de Gauss)

Il existe un entier relatif k tel que $x + 2 = 47k$

En remplaçant dans $23(x + 2) = -47(y - 1)$, $x + 2$ par $47k$ on obtient que $y - 1 = -23k$

Si $(x ; y)$ est solution de (E), il existe un entier relatif k tel que $y = -23k + 1$ et $x = 47k - 2$

Vérification :

Si $x = 47k - 2$ et $y = -23k + 1$: $23x + 47y = 23(47k - 2) + 47(-23k + 1) = 23 \times 47k - 2 \times 23 - 47 \times 23k + 47$

$23x + 47y = 1$ donc $(47k - 2 ; -23k + 1)$ est solution de (E)

L'ensemble des solutions de (E) sont les couples $(-47k - 2 ; -23k + 1)$ avec $k \in \nearrow$.

c. Si x est solution de $23x \equiv 1$ (47), il existe un entier relatif y tel que $23x = 47y + 1$ soit $23x - 47y = 1$

soit $23x + 47 \times (-y) = 1$. D'après la question précédente, $x = 47k - 2$ et $-y = -23k + 1$ avec $k \in \nearrow$

$x \in$ A donc $1 \leq 47k - 2 \leq 46$

$3 \leq 47k \leq 48 \Leftrightarrow \frac{3}{47} \leq k \leq \frac{48}{47} \Leftrightarrow k = 1 \Leftrightarrow x = 45$ donc 45 est l'unique entier x appartenant à A tel que $23x \equiv 1$ (47).

2. *a*. Si $ab \equiv 0$ (47) alors 47 divise ab

or 47 est un nombre premier donc soit 47 divise a soit 47 divise b donc $a \equiv 0$ (47) ou $b \equiv 0$ (47).

b. $a^2 \equiv 1$ (47) $\Leftrightarrow a^2 - 1 \equiv 0$ (47) $\Leftrightarrow (a - 1)(a + 1) \equiv 0$ (47)

alors d'après la question précédente : $a - 1 \equiv 0$ (47) ou $a + 1 \equiv 0$ (47) c'est-à-dire $a \equiv 1$ (47) ou $a \equiv -1$ (47).

3. *a*.

petit théorème de Fermat : Soit a un entier relatif et p un nombre premier. Si p ne divise pas a alors $a^{p-1} \equiv 1$ [p]

$1 \leq p \leq 46$ donc 47 ne divise pas p

47 est un nombre premier, 47 ne divise pas p donc d'après le petit théorème de Fermat : $p^{46} \equiv 1$ [47] soit $p \times p^{45} \equiv 1$ [47]

pour tout entier p de A, il existe un entier relatif q ($q = p^{45}$) tel que $p \times q \equiv 1$ (47) .

b. Soit p un entier de A tel que $p = inv(p)$

Par définition $p \times inv(p) \equiv 1$(47) or $p = inv(p)$ donc $p \times p \equiv 1$(47) soit $p^2 \equiv 1$ (47) donc $p \equiv 1$(47) ou $p \equiv -1$(47) d'après 2. *b*.

$p \equiv 1$(47) $\Leftrightarrow p = 1 + 47k$ ($k \in \nearrow$) or $p \in$ [1 , 46] donc $0 \leq 47k \leq 45$ soit $k = 0$ donc $p = 1$

$p \equiv -1$(47) $\Leftrightarrow p = -1 + 47k$ ($k \in \nearrow$) or $p \in$ [1 , 46] donc $2 \leq 47k \leq 47$ soit $k = 1$ donc $p = 46$

Sans idées mais avec du courage :

$inv(1) = 1$

$46 \equiv -1$ (47) donc $46 \times 46 \equiv 1$ (47) soit $inv(46) = 46$

$4 \times 12 = 48$ donc $inv(4) = 12$ et $inv(12) = 4$

$5 \times 19 = 95 = 2 \times 47 + 1$ donc $inv(5) = 19$ et $inv(19) = 5$

$6 \times 8 = 48$ donc $inv(6) = 8$ et $inv(8) = 6$

$7 \times 27 = 149 = 47 \times 47 + 1$ donc $inv(7) = 27$ et $inv(27) = 7$

$9 \times 21 = 189 = 47 \times 47 + 1$ donc $inv(9) = 21$ et $inv(21) = 9$

$10 \times 33 = 330 = 47 \times 47 + 1$ donc $inv(10) = 33$ et $inv(33) = 10$

$11 \times 30 = 330 = 47 \times 47 + 1$ donc $inv(11) = 30$ et $inv(30) = 11$

$13 \times 29 = 377 = 8 \times 47 + 1$ donc $inv(13) = 29$ et $inv(29) = 13$

$14 \times 37 = 518 = 11 \times 47 + 1$ donc $inv(14) = 37$ et $inv(37) = 14$
$15 \times 22 = 330 = 7 \times 47 + 1$ donc $inv(15) = 22$ et $inv(22) = 15$
$17 \times 36 = 612 = 13 \times 47 + 1$ donc $inv(17) = 36$ et $inv(36) = 17$
$18 \times 34 = 612 = 13 \times 47 + 1$ donc $inv(18) = 34$ et $inv(34) = 18$
$20 \times 40 = 800 = 17 \times 47 + 1$ donc $inv(20) = 40$ et $inv(40) = 20$
$23 \times 45 = 1035 = 22 \times 47 + 1$ donc $inv(23) = 45$ et $inv(45) = 23$
$25 \times 32 = 800 = 17 \times 47 + 1$ donc $inv(25) = 32$ et $inv(32) = 25$
$26 \times 38 = 988 = 21 \times 47 + 1$ donc $inv(26) = 38$ et $inv(38) = 26$
$28 \times 42 = 1176 = 25 \times 47 + 1$ donc $inv(28) = 42$ et $inv(42) = 28$
$31 \times 44 = 1364 = 29 \times 47 + 1$ donc $inv(31) = 44$ et $inv(44) = 31$
$35 \times 43 = 1505 = 32 \times 47 + 1$ donc $inv(35) = 43$ et $inv(43) = 35$
$39 \times 41 = 1599 = 34 \times 47 + 1$ donc $inv(39) = 41$ et $inv(41) = 39$

p	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
$inv(p)$	1	24	16	12	19	8	27	6	21	33	30	4	29	37	22	3	36	34	5	40	9	15	45

p	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
$inv(p)$	2	32	38	7	42	13	11	44	25	10	18	43	17	14	26	41	20	39	28	35	31	23	46

Seuls 1 et 46 vérifient $p \in A$ et $p = inv(p)$

c. $46 ! = 1 \times 2 \times \ldots \times 45 \times 46$
$46 ! = (2 \times 24) \times (3 \times 16) \times (4 \times 12) \times (5 \times 19) \times (6 \times 8) \times (7 \times 27) \times (9 \times 21) \times (11 \times 30) \times (13 \times 29) \times (14 \times 37) \times (14 \times 37) \times (15 \times 22) \times (17 \times 36) \times (18 \times 34) \times (23 \times 45) \times (25 \times 32) \times (26 \times 38) \times (28 \times 42) \times (31 \times 44) \times (35 \times 43) \times (39 \times 41) \times 46$
Tous les produits entre parenthèses sont de la forme $p \times inv(p)$ donc congrus à 1 modulo 47
$46 ! \equiv 46 \ (47)$ donc $46 ! \equiv -1 \ (47)$.