TD Mathématiques pour la cryptographie I

Exercice 1

Trouver le quotient et le reste dans les divisions suivantes :

1. 2008 par 52 2. 1025 par -8 3. -2012 par -60

Correction

1. $2008 = 38.52 + 32$
2. $1025 = -128.(-8) + 1$
3. $-2012 = 34.(-60) + 28$

Exercice 2

Montrer que le reste de la division euclidienne par 8 du carré d'un nombre impair est 1.

Correction Un nombre impair n s'écrit $n = 2k + 1$ avec $k \in \mathbb{Z}$. Son carré est

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$$

L'un des entiers k ou $k+1$ est pair donc leur produit est pair et $4k(k+1)$ est multiple de 8. Ainsi n^2 est de la forme $8q + 1$ ce qui montre le résultat.

Exercice 3

1. Trouver tous les diviseurs de 312.
2. Faire de même avec 276 et calculer $312 \wedge 276$.
3. Recalculer $312 \wedge 276$ en utilisant l'algorithme d'Euclide.

Correction

1. Diviseurs de 312 : $\{1, 2, 4, 8, 3, 6, 12, 24, 13, 26, 39, 52, 78, 104, 156, 312\}$ et leurs opposés.
2. On fait de même avec 276 et on trouve $\{1, 2, 3, 4, 6, 12, 23, 46, 69, 92, 138, 276\}$ et leurs opposés. On en déduit que le PGCD est 12.
3. On effectue successivement les divisions :

$$312 = 276 \cdot 1 + 36$$
$$276 = 36 \cdot 7 + 24$$
$$36 = 24 \cdot 1 + 12$$
$$24 = 12 \cdot 2 + 0$$

Le PGCD est le dernier reste non-nul, c'est à dire 12.

Exercice 4

1. Calculer $4\,820 \wedge 520$ à l'aide de l'algorithme d'Euclide.
2. Déterminer deux entiers relatifs u et v tels que $4\,820u + 520v = 4\,820 \wedge 520$

Correction

1. On trouve $4\,820 \wedge 520 = 20$.
2. On remonte l'algorithme d'Euclide et on trouve $-11.4\,820 + 102.520 = 20$.

Exercice 5

Donner la décomposition en produit de facteurs premiers de $12\,600$.

Correction $12\,600 = 2^3.3^2.5^2.7$

Exercice 6

1. Les nombres premiers consécutifs 2, 3 et 5 sont de la forme p, $p+1$ et $p+3$.
   Montrer que c'est le seul triplet ayant cette propriété.
2. Les nombres premiers consécutifs 3, 5 et 7 sont de la forme p, $p+2$ et $p+4$.
   Montrer que c'est le seul triplet de nombres premiers ayant cette propriété.

Correction

1. Si p est un premier non-égal à 2 alors il est impair et $p+1$ est pair : $p+1$ n'est pas premier.
2. Si p est un premier supérieur à 3 alors il est de la forme $3k+1$ ou $3k+2$. Dans le premier cas $p+2$ est multiple de 3 et dans le second cas c'est $p+4$.

Exercice 7

Montrer que, sauf une exception, tout nombre premier p peut s'écrire comme différence de deux carrés d'entiers naturels.
Décomposer de cette façon le nombre premier 439.

Correction On cherche deux entiers naturels a et b tels que, si p est un nombre premier, $p = a^2 - b^2 = (a+b)(a-b)$.
Comme p est premier, on a forcément $a+b = p$ et $a-b = 1$ ce qui après résolution donne $a = \frac{p+1}{2}$ et $b = \frac{p-1}{2}$. On remarque que p doit être impair ce qui exclut 2, c'est l'exception.
Application à 439 : $a = \frac{440}{2} = 220$ et $b = \frac{438}{2} = 219$ et on a bien $439 = 220^2 - 219^2$.

Exercice 8

1. Calculer modulo 8 : $65 \times (25+41)$; 8002×15 ; $39 \times (15-21)^3$
2. Calculer modulo 11 : 12^{15} ; 10^7 ; 78^{15} ; 13^{12}
3. Calculer modulo 7 : $91\,234^{2002}$; $1\,234^{1\,234}$

Correction

1. $65 \times (25+41) \equiv 1 \times 66 \equiv 1 \times 2 \equiv 2$ [8].
   $8002 \times 15 \equiv 2 \times (-1) \equiv -2 \equiv 6$ [8].
   $39 \times (15-21)^3 \equiv -1 \times (-6)^3 \equiv -1 \times 2^3 \equiv 0$ [8]
2. $12^{15} \equiv 1^{15} \equiv 1$ [11]
   $10^7 \equiv (-1)^7 \equiv -1 \equiv 10$ [11]
   $78^{15} \equiv 1^{15} \equiv 1$ [11]
   $13^{12} \equiv 2^{12} \equiv 2^{5\cdot2+2} \equiv 32^2 \cdot 2^2 \equiv (-1)^2 \cdot 4 \equiv 4$ [11]
3. $91\,234^{2002} \equiv (70000 + 21000 + 234)^{2002} \equiv 234^{2002} \equiv 24^{2002} \equiv 3^{2002} \equiv 3^{3\cdot667+1} \equiv 27^{667} \cdot 3 \equiv (-1)^{667} \cdot 3 \equiv -3 \equiv 4$ [7] car on a au préalable calculé les premières puissances de 3 et on a vu que $3^3 \equiv -1$ [7]
   $1\,234^{1\,234} \equiv 534^{1\,234} \equiv 44^{1\,234} \equiv 2^{1\,234} \equiv 2^{3.411+1} \equiv 8^{411}.2 \equiv 1^{411}.1 \equiv 2$ [7] car on a au préalable calculé les premières puissances de 2 et on a vu que $2^3 \equiv 1$ [7]

Exercice 9

Résoudre les équations suivantes modulo 26.

1. $7x + 22 \equiv 6 \mod 26$
2. $16x - 21 \equiv 12 \mod 26$
3. $20x + 20 \equiv 14 \mod 26$
4. $x^2 + 2x - 4 \equiv 7 \mod 26$

Correction

1. $7x + 22 \equiv 6 \mod 26$ d'où $7x \equiv -16 \equiv 10$ et $x \equiv 20 \mod 26$
2. $16x - 21 \equiv 12 \mod 26$ d'où $16x \equiv 33 \equiv 7$ et il n'y a pas de solution.
3. $20x + 20 \equiv 14 \mod 26$ d'où $20x \equiv -6 \equiv 20$ et il y a deux solutions : 1 et 14 modulo 26.
4. $x^2 + 2x - 4 \equiv 7 \mod 26$ d'où $x(x+2) \equiv 11 \mod 26$ et on trouve les solutions 7 et 17 grâce à la table de multiplication de $(\mathbb{Z}/26\mathbb{Z})$ car $7(7+2) \equiv 11 \mod 26$ et $17(17+2) \equiv 11 \mod 26$.

∼∼∼∼∼∼∼∼∼∼∼∼∼∼ vers crypto

Exercice 10

1. Calculer $\varphi(n)$ pour $2 \leqslant n \leqslant 10$.
2. Calculer $\varphi(70)$.
3. Calculer $\varphi(12\,600)$.

Correction

1.

n	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	2	2	4	2	6	4	6	4

2. On a $70 = 7 \cdot 10$ d'où $\varphi(70) = \varphi(7) \cdot \varphi(10) = 6 \cdot 1 \cdot 4 = 24$.
3. On a vu dans un exercice précédent que $12\,600 = 2^3.3^2.5^2.7$ alors

$$\varphi(12\,600) = 12\,600\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 2\,880$$

Exercice 11

1. Vérifier à l'aide de l'algorithme d'Euclide que 37 et 1 243 sont premiers entre-eux.
2. En utilisant l'algorithme d'Euclide étendu, calculer l'inverse de 37 modulo 1 243.
3. Résoudre l'équation $37(x+12) \equiv 548\ [1\,243]$.
4. Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/1\,243\mathbb{Z}$?

Correction

1. Les divisions successives sont :

$$\begin{aligned} 1\,243 &= 37 \cdot 33 + 22 \\ 37 &= 22 \cdot 1 + 15 \\ 22 &= 15 \cdot 1 + 7 \\ 15 &= 7 \cdot 2 + 1 \end{aligned}$$

D'où $37 \wedge 1\,243 = 1$.

2. On remonte les divisions et on trouve $1 = 168 \cdot 37 - 5 \cdot 1\,243$. En passant modulo $1\,243$ on obtient :

$$37 \cdot 168 \equiv 1 \quad [1\,243]$$

ce qui indique que 168 est l'inverse de 37 modulo $1\,243$.

3. On a
$$37(x+12) \equiv 548 \ [1\,243]$$
D'après la question précédente, en multipliant des deux côtés par l'inverse de 37 on obtient
$$x+12 \equiv 548 \cdot 168 \equiv 92\,064 \equiv 82 \ [1243]$$
d'où
$$x \equiv 70 \ [1243]$$
4. Le nombre d'éléments inversibles est donné par $\varphi(1\,243)$. Pour obtenir le résultat il faut la décomposition primaire de $1\,243$ qui est $11 \cdot 113$. On a donc
$$\varphi(1\,243) = \varphi(11) \cdot \varphi(113) = 10 \cdot 112 = 1\,120$$

∼∼∼∼∼∼∼∼∼∼∼∼∼∼ vers crypto

★ EXERCICES SUPPLÉMENTAIRES D'ENTRAÎNEMENT ★

Exercice 12

1. Calculer $58 \cdot (38+27)$ modulo 8.
2. Calculer 55^{100} modulo 13.
3. Calculer 101^{3333} modulo 9.

Correction

1. $58 \cdot (38+27) \equiv 2 \cdot (6+3) \equiv 2 \ [8]$
2. Calculer $55^{100} \equiv 3^{100} \ [13]$. Or $3^3 \equiv 1 \ [13]$ donc $3^{100} \equiv 3^{3 \cdot 33+1} \equiv (3^3)^{33} \cdot 3 \equiv 3 \ [13]$
3. $101^{3333} \equiv 2^{3333}$. Or $2^3 \equiv -1 \ [9]$ d'où $2^{3333} \equiv (2^3)^{1111} \equiv (-1)^{1111} \equiv -1 \ [9]$

Exercice 13

1. Soit n un entier naturel dont le reste de la division par 5 vaut 2 ou 3. Montrer que n^2+1 est divisible par 5.
2. Montrer que pour tout entier naturel n, l'entier $n^5 - n$ est divisible par 5.

Correction

1. Si $n \equiv 2 \ [5]$ alors $n^2+1 \equiv 4+1 \equiv 0 \ [5]$. De même si $n \equiv 3 \ [5]$ alors $n^2+1 \equiv 9+1 \equiv 0 \ [5]$.
2. $n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = n(n-1)(n+1)(n^2+1)$.
   Si n est congru à 0 ou 1 ou -1 (c'est à dire 4) alors $n(n-1)(n+1)$ est congru à 0. Si n est congru à 2 ou 3 alors c'est n^2+1 qui est congru à 0 d'après la question précédente.
   Dans les cinq cas, $n^5 - n$ est congru à 0 modulo 5.

Exercice 14

Soit $n > 3$.

1. Les nombres n, $n+2$ et $n+4$ peuvent-ils être tous premiers ?
2. Les nombres n, $n+2$ et $n+6$ peuvent-ils être tous premiers ?

Correction

1. On raisonne modulo 3 : si n vaut 0 alors le premier nombre n'est pas premier, s'il vaut 1 c'est le deuxième qui n'est pas premier, s'il vaut 2 c'est le troisième.
2. Oui c'est possible, par exemple 17, 19 et 23.