Feuille 4 : Applications de l'arithmétique

Exercice 1 Soit $n \geq 2$ un entier. On considère les $n-1$ nombres

$$n!+2, \quad n!+3, \quad \ldots, \quad n!+(n-1), \quad n!+n.$$

1) Soit $n=3$. Démontrer que ces nombres ne sont pas premiers. Même question pour $n=4$ et $n=5$.

2) Traiter le cas général, $n \geq 1$.

3) Soit N un entier. Montrer que l'on peut trouver une suite de N nombres consécutifs non premiers.

Exercice 2 Jusqu'à combien peut-on compter sur les doigts d'une main ? et de deux mains ?
Indication : On pourra compter en binaire et identifier un doigt à un bit.

Exercice 3 Convertir en binaire les nombres suivants :

$$2, \quad 7, \quad 1024, \quad 1025, \quad 100.$$

Exercice 4 Écrire en base 10 les nombres binaires suivants :

$$101, \quad 11\,1001, \quad 10\,0101.$$

Exercice 5 On rappelle la formule suivante, valable pour $-1 < q < 1$

$$\sum_{k=0}^{+\infty} q^k = 1 + q + q^2 + \cdots + q^n + \cdots = \frac{1}{1-q}.$$

1) Calculer $1 + 2^{-2} + 2^{-4} + 2^{-6} + \cdots + 2^{-2n} + \cdots$

2) En déduire que le nombre $1/3$ s'écrit comme somme infinie d'inverses de puissances de 2.

Exercice 6 Donner le reste de la division euclidienne par 3 des nombres suivants. En déduire ceux qui sont divisibles par 3.

$$102, \quad 1273, \quad -1273, \quad 12401, \quad 12402.$$

Même question avec la division par 9.

Exercice 7 Le nombre suivant est premier : $N = 2^{74\,207\,281} - 1$.

1) Comment s'écrit ce nombre en base 2 ?

2) Combien de chiffres comprend l'écriture de ce nombre en base 10 ?

Exercice 8 Compléter les tables de multiplications suivantes, modulo n

modulo 5 :

$\times$	1	2	3	4
1				
2				
3				
4				

modulo 6 :

$\times$	1	2	3	4	5
1					
2					
3					
4					
5					

modulo 7 :

$\times$	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

Exercice 9 Montrer que pour tout $n \in \mathbb{N}$, $2^{3n} - 1$ est un multiple de 7.

Exercice 10 Déterminer le reste de la division euclidienne de 3^p par 8, pour $p \in \mathbb{N}$.
Indication : on pourra distinguer les cas $p = 2k$ et $p = 2k + 1$ avec $k \in \mathbb{N}$, selon que p est pair ou impair.

Exercice 11 (Jeu de Nim) Le maître du jeu dispose un certain nombre d'allumettes sur la table. Chaque joueur enlève à tour de rôle 1, 2 ou 3 allumettes.

1) On suppose que celui qui prend la dernière allumette perd. Montrer que la stratégie gagnante est de laisser à chaque fois un nombre d'allumettes congru à 1 modulo 4.

2) On suppose maintenant le vainqueur est celui qui peut jouer en dernier. Donner une stratégie gagnante.

Exercice 12 (Preuve par 9) Un élève a calculé $17 \cdot 123 = 2191$. A-t-il raison ?
Un autre a trouvé $17 \cdot 123 = 2901$. Que dire ?

Exercice 13 Trouver un critère de divisibilité par 11.
Application : montrer que 12221 est divisible par 11.
Indication : On peut remarquer que $10 \equiv -1$ modulo 11.

Exercice 14 Le but de l'exercice est d'étudier le chiffrement affine. On code chaque lettre de l'alphabet à l'aide du tableau suivant :

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
0	1	2	3	4	5	6	7	8	9	10	11	12
N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
13	14	15	16	17	18	19	20	21	22	23	24	25

1) On suppose que la fonction de codage est $f(x) = 11x + 8$ modulo 26.

a) Coder la lettre W.

b) Montrer que pour tous nombres entiers relatifs x et j on a

$$11x = j \quad \text{modulo } 26 \quad \Leftrightarrow \quad x = 19j \quad \text{modulo } 26.$$

c) En déduire que la fonction de décodage est $f^{-1}(y) = 19y + 4$ modulo 26.

d) Décoder la lettre L.

2) On suppose que la fonction de codage est $f(x) = 2x + 1$ modulo 26.

a) Coder quelques lettres à l'aide de cette fonction. Que peut-on remarquer ?

b) Plus généralement, on considère une fonction de codage de la forme $f(x) = ax + b$ modulo 26. Que doivent vérifier a et b pour que f soit une bonne fonction de codage ?

Exercice 15 Dans les années 60, un des premiers générateurs de nombres aléatoires entre 0 et 1, noté $RANDU$, était conçu de la façon suivante :

- on part d'une graine g_0, un entier sur 31 bits (entre 1 et $2^{31} - 1$),
- pour $n \geq 0$, on définit $g_{n+1} = (2^{16} + 3)g_n \mod 2^{31}$,
- on renvoie alors $u_{n+1} = g_{n+1}/2^{31}$.

1) On choisit $g_0 = 1$. Calculer g_1, g_2 et g_3.

2) Montrer que pour tout $n \geq 0$ on a la relation $g_{n+2} = 6g_{n+1} - 9g_n \mod 2^{31}$.

3) En déduire que ce générateur est très mauvais.

Exercice 16 Le numéro INSEE est constitué de 15 chiffres. Quand on le lit de gauche à droite :

- le premier chiffre est 1 s'il s'agit d'un homme et 2 s'il s'agit d'une femme ;
- les deux chiffres suivants désignent les deux derniers chiffres de l'année de naissance ;
- les deux chiffres suivants désignent le mois de naissance ;
- les deux chiffres suivants désignent le département de naissance ;
- les trois chiffres suivants désignent la commune de naissance ;
- les trois chiffres suivants désignent le numéro d'inscription sur le registre d'état-civil ;
- les deux chiffres suivants désignent la clé K, calculée de la manière suivante :
- soit A le nombre entier constitué par les 13 chiffres de gauche ;
- soit r le reste de la division euclidienne de A par 97 ; alors $K = 97 - r$.

Les 13 premiers chiffres (sans la clé) du numéro INSEE de Sophie sont : 2 85 07 86 183 048.

1) À l'aide d'un ordinateur ou d'une calculatrice, calculer le reste de la division euclidienne de

$$2\,85\,07\,86\,183\,048$$

par 97. En déduire la clé de Sophie.
Indication : Sur Scilab on peut utiliser la commande `modulo(n,m)`. On obtient $2\,85\,07\,86\,183\,048 \equiv 82$ modulo 97.

2) Sophie, à qui l'on demande les treize premiers chiffres de son numéro INSEE, inverse les deux derniers chiffres et répond 2 85 07 86 183 084 au lieu de 2 85 07 86 183 048. Peut-on détecter l'erreur de Sophie ?
Indication : Sur Scilab on peut utiliser la commande `modulo(n,m)`. On obtient $2\,85\,07\,86\,183\,084 \equiv 21$ modulo 97.

3) Montrer que si l'on additionne la clé aux 13 premiers chiffres du numéro INSEE, on obtient un nombre divisible par 97.

4) Dans la construction de la clé, pourquoi prend-on le reste modulo 97 et non pas par 3 ou 9 par exemple ?

5) Vérifier la clé de votre numéro INSEE.

Exercice 17 On suppose qu'Alice et Bob utilisent l'algorithme RSA avec un module n trop grand pour être factorisé. Alice code chaque lettre par un entier (A $\leftrightarrow$ 0, B $\leftrightarrow$ 1, etc) et chiffre les lettres les unes après les autres. Montrer comment un attaquant peut déchiffrer le message envoyé.

Exercice 18 Alice utilise le système RSA avec $p = 3$ et $q = 7$.

1) Calculer $n = pq$ et $\varphi(n)$.

2) Alice choisit comme clé d'encryptage $e = 5$. Vérifier que cette valeur est possible.

3) Calculer l'exposant d associé à e.

4) Bob veut envoyer le message $m = 10$ à Alice. Calculer le message chiffré x, avec la clé publique d'Alice.

5) Vérifier qu'Alice sait déchiffrer le message.