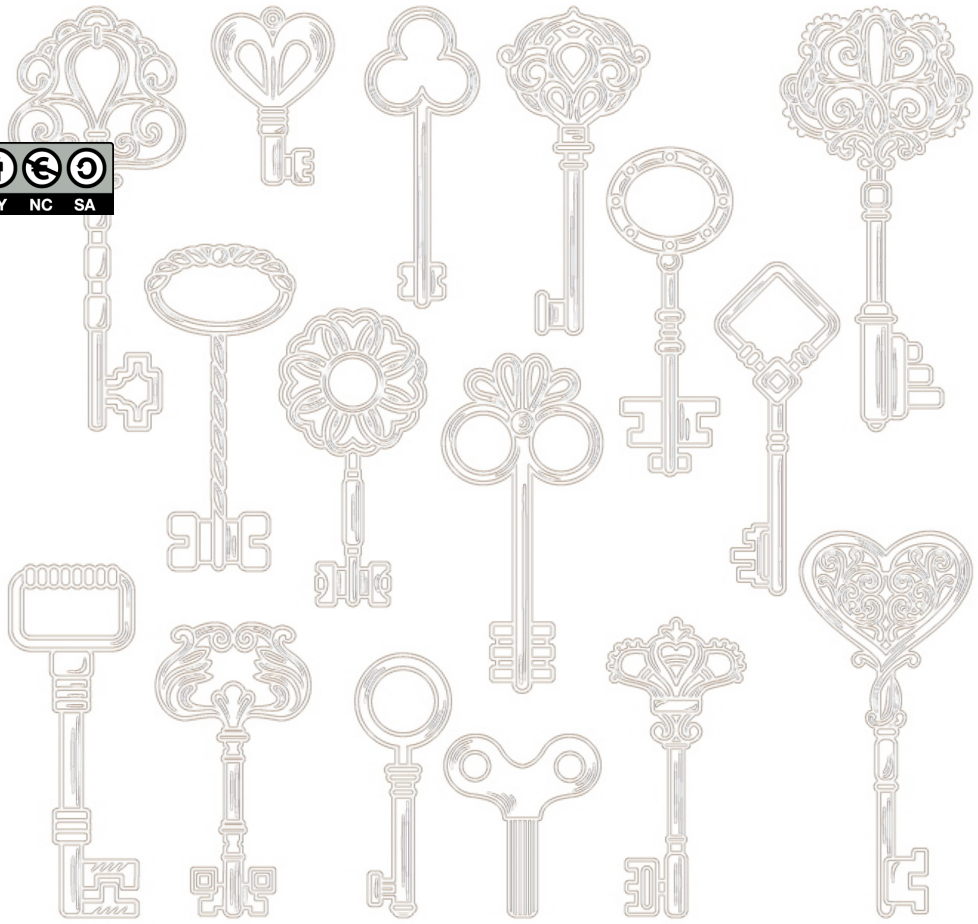
Arithmétique & Éléments de cryptanalyse Exercices

David Hébert
hebert.iut@gmail.com

2022



1. Arithmétique modulaire

Division euclidienne

Exercice 1

Parmi les opérations suivantes, lesquelles représentent une division euclidienne ?

1. $5 = 2 \times 3 - 1$
2. $5 = 1 \times 2 + 3$
3. $5 = 2 \times 2 + 1$

Exercice 2

Dans chacun des cas suivants, effectuer la division euclidienne de A par B.

1. $A = 101$, $B = 13$
2. $A = 111$, $B = 13$
3. $A = 164$, $B = 78$
4. $A = 2015$, $B = 98$
5. $A = 5678$, $B = 51$
6. $A = 8$, $B = 9$
7. $A = -321$, $B = 9$
8. $A = 0$, $B = 78$

Exercice 3

Parmi les propositions, lesquelles sont vraies.

1. 6 divise 2
2. 5 divise 2050
3. 16 est un multiple de 2
4. 123 est un multiple de 6
5. $4 \mid 6$
6. $8 \mid 54$
7. $3 \mid 444$
8. $1 \mid 6354$
9. 666 est un diviseur de 1998

Exercice 4

On a effectué la division euclidienne d'un entier a par 40. On a obtenu un quotient q et pour reste $3q^2$. Déterminer tous les entiers a.

Congruences

Exercice 5

Parmi les propositions, lesquelles sont vraies.

1. $15 \equiv_8 7$
2. $99 \equiv_2 -1$
3. $654 \equiv_3 0$
4. $3 \equiv_3 3$
5. $873 \equiv_5 555$
6. $8704 \equiv_{13} 791$
7. $-8 \equiv_9 1$
8. $-984 \equiv_{19} 17$

Exercice 6

Dans chacun des cas, déterminer x modulo n (donner un représentant dans $\mathbb{Z}/n\mathbb{Z}$).

1. $x = 555$, $n = 12$
2. $x = 983$, $n = 45$
3. $x = 3078$, $n = 487$
4. $x = 573$, $n = 159$

Exercice 7

Simplifier les expressions suivantes.

1. 123^{122} modulo 124
2. $2014 \times 2015 \times 2016$ modulo 2017
3. 2792^{217} modulo 5
4. 133^{39} modulo 10
5. 99^{100} modulo 42
6. 2^{1147} modulo 17

Exercice 8

Dessiner les tables d'addition et de multiplication de $\mathbb{Z}/7\mathbb{Z}$.

Exercice 9

Dessiner les tables d'addition et de multiplication de $\mathbb{Z}/8\mathbb{Z}$.

Congruences 2

Exercice 10

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

Exercice 11

Montrer que pour tout entier $n \in \mathbb{N}$, $6^n + 13^{n+1}$ est divisible par 7.

Exercice 12

1. Montrer que $34^{57} - 1$ est un multiple de 11.
2. Montrer que $9518^{42} - 4$ est divisible par 5.

Exercice 13

Montrer la propriété de transitivité de '|' : pour tout entier a, b et c $(a|b) \wedge (b|c) \Rightarrow (a|c)$

Exercice 14

Montrer que pour tout entier a, b, c et d $(a|b) \wedge (c|d) \Rightarrow (ac|bd)$

Exercice 15

Déterminer tous les entiers n tel que $n|n+7$.

Exercice 16

Soient a, b, c et n des entiers. Montrer la proposition suivante.

$$an^2 + bn + c = 0 \Rightarrow n|c$$

Exercice 17

Soient a et n des entiers tels que $a \geqslant 1$. Montrer que si $a|n+2$ et $a|n^2+n+5$ alors $a = 1$ ou $a = 7$.

Exercice 18

Soit $n \in \mathbb{N}_{>0}$.

1. Montrer que $3 \times 2^{2n-1} + 3^{2n}$ est divisible par 5.
2. Montrer que $7 \times 3^{2n-1} + 7^{2n}$ est divisible par 10.
3. Montrer que $11 \times 8^{2n-1} + 11^{2n}$ est divisible par 19.
4. Soient a et b des entiers. On note $X = a + b$. Montrer que $b \times a^{2n-1} + b^{2n}$ est divisible par X.

Exercice 19

Soit $n \in \mathbb{N}$. Montrer que si $n \equiv_3 0$ alors $7^n + 11^n \equiv_{19} 2$. Que dire de $7^n + 11^n$ si $n \not\equiv_3 0$?

Exercice 20

1. Calculer $1 + 2 + 3 + 4 + 5$ modulo 5.
2. Calculer $1 + 2 + 3 + 4 + 5 + 6 + 7$ modulo 7.
3. Calculer $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8$ modulo 8.
4. Déterminer, de façon générale, $1 + 2 + \cdots + (n-1) + n$ modulo n.

Exercice 21

(Olympiade de Mathématiques, Saint-Petersburg, 2004).
Déterminer tous les entiers n tels que $3^{n-1} + 5^{n-1}$ divise $3^n + 5^n$.
On pourra observer que $3(3^{n-1} + 5^{n-1}) < 3^n + 5^n < 5(3^{n-1} + 5^{n-1})$.

Cryptologie de César

Exercice 22

Crypter le mot *MATHEMATIQUES* par la méthode de César par paquet de 1 avec 19 comme clef.

Exercice 23

Crypter le mot *ZEBRE* par la méthode de César par paquet de 1 avec 25 comme clef.

Exercice 24

Crypter le message *VIVELACRYPTO* par la méthode de César par paquet de 3 avec 190091 comme clef.

Exercice 25

On a utilisé la méthode de César par paquet de 1 avec 25 comme clef pour obtenir *BDRSBGZTCBZAQTKD*. Quel était le message original ?

Exercice 26

On a utilisé la méthode de César par paquet de 3 avec 250025 comme clef pour obtenir *208907-107501-39318-48312-77499*. Quel était le message original ?

Exercice 27

Ce message a été codé par la méthode de César : *2138-523-1651-1650-712-1434-1834-2338-412-721-212-708*. Quel était le message original ?

2. PGCD

Diviseur

Exercice 1

Pour chacun des entiers a, déterminer $D(a)$ l'ensemble des diviseurs positifs de a.

1. $a = 99$
2. $a = 1069$
3. $a = 3742$
4. $a = 6725$
5. $a = 684$

Exercice 2

Dans chacun des cas suivant, appliquer l'algorithme d'Euclide pour déterminer le PGCD de A et B.

1. $A = 540$, $B = 256$
2. $A = 561$, $B = 187$
3. $A = 982$, $B = 1000$
4. $A = 998$, $B = 47$
5. $A = 5742$, $B = 1320$
6. $A = 5454$, $B = 8572$

Exercice 3

Dans chacun des cas, donner l'inverse de a modulo n lorsque cela est possible.

1. $a = 13$, $n = 7$
2. $a = 4$, $n = 17$
3. $a = 2$, $n = 8$
4. $a = 54$, $n = 17$
5. $a = 100$, $n = 101$
6. $a = 396$, $n = 111$
7. $a = 48$, $n = 619$
8. $a = 987$, $n = 1069$

Exercice 4

Dresser la table de multiplication de $\mathbb{Z}/8\mathbb{Z}$. En déduire $(\mathbb{Z}/8\mathbb{Z})^*$.

Équations

Exercice 5

Résoudre les équations diophantienne suivantes.

1. $3x + 2y = 1$
2. $15x + 22y = 1$
3. $100x + 19y = 2$
4. $6x + 10y = 2$
5. $8x - 12y = 3$
6. $5x^2 + y^2 = 1$

Exercice 6

Résoudre les systèmes suivants.

1. $\begin{cases} x \equiv_3 1 \\ x \equiv_2 0 \end{cases}$
2. $\begin{cases} x \equiv_{15} 5 \\ x \equiv_{22} 11 \end{cases}$
3. $\begin{cases} 5x \equiv_8 7 \\ x \equiv_{11} 0 \end{cases}$

Exercice 7

(BAC S - 2001 - Polynésie)

1. Déterminer un coupe d'entier (x, y) solution de $91x + 10y = 1$.
2. En déduire une solution particulière de $91x + 10y = 412$.
3. Résoudre $91x + 10y = 412$.
4. Démontrer que pour tout $n \in \mathbb{N}$, $A_n = 3^{2n} - 1$ est divisible par 8.
5. Résoudre l'équation $A_3x + A_2y = 3296$.

Diviseur 2

Exercice 8

Pour quelle valeur de l'entier n, n et $n + 2$ sont premiers entre eux ?

Exercice 9

Déterminer tous les entiers n tel que $n^2 - 1$ et $n^2 - 2n + 1$ soit premier entre eux.

Exercice 10

Soient x et y des entiers. Montrer la proposition suivante

$$2x + 1 | 8y \Rightarrow 2x + 1 | y$$

Exercice 11

(Olympiade Internationale de Mathématiques - 1959)

Montrer que pour tout entier n, la fraction $\dfrac{21n + 4}{14n + 3}$ est toujours irréductible.

Exercice 12

Soit $f : \mathbb{N} \to \mathbb{N}$ une fonction strictement croissante tel que

(i). $f(2) = 2$

(ii) $f(nm) = f(n)f(m)$ dès que n et m sont premiers entre eux.

1. Montrer que pour tout $n \in \mathbb{N}$, $f(n) \geqslant n$.
2. En partant de $15 < 18$ montrer que $f(3) = 3$.
3. Montrer que pour tout entier $n \in \mathbb{N}_{>0}$, $f(2^n + 1) = 2^n + 1$.
4. Montrer que $f(n) = n$ pour tout entier $n \in \mathbb{N}$.

Cryptologie affine

Exercice 13

Les couples suivants définissent-ils des clefs de cryptage affine par paquet de N

1. Pour $N = 1$: $(3, 2)$, $(13, 8)$, $(9, 0)$.
2. pour $N = 2$: $(7, 421)$, $(25, 11)$, $(421, 801)$
3. pour $N = 3$: $(2015, 1998)$, $(4567, 9002)$, $(4073, 88)$

Exercice 14

Pour chacune des clefs valides de l'exercice précédent, déterminer la fonction de déchiffrement.

Exercice 15

Crypter le message *CHOCOBO* par la méthode affine par paquet de 1 avec $(7, 7)$ comme clef.

Exercice 16

Crypter le message *VACANCES* par la méthode affine par paquet de 2 avec $(1999, 999)$ comme clef.

Exercice 17

On a utilisé le cryptosystème affine par paquet de 1 avec $(7, 1)$ comme clef pour obtenir *CBLXD*. Retrouver le message original.

Exercice 18

Décrypter ce message sachant que l'on a utilisé un cryptage affine et que le texte claire commence par *TOUT*.

OLZOJFENAFKNZOWNDEFWLXDLAHZXUFJLZEFUFOFDRFZG UFOFDRFZGKFSODENJDLZ-
PLANPFOSFPYEFFODFKLXONEFAKFSD

Exercice 19

On a utilisé le cryptosystème affine pour obtenir *50029-125229-237773-194389-55281-50645*. Retrouver le message original.

3. Vigénère et Kasiski

Vigénère

Exercice 1

Chiffrer ce message par la méthode de vigénère de clef **ASSIEGIONS** :

QUIMAIMEMESUIVE

Exercice 2

Chiffrer ce message par la méthode de vigénère de clef **RASSASIONS** :

LANEFROTTELANE

Exercice 3

Déchiffrer ce message par la méthode de vigénère de clef **CHIPES** :

EOIGMLGIQTRGTKWCRWGJWBQWPJMEEJUVQBIEG

Exercice 4

Déchiffrer ce message par la méthode de vigénère de clef **CRYPTASSE** :

NRAPEOEFMGVQIEAJEIWCRXFEVWPKDNJBSKSRV

Exercice 5

Vous trouverez un message chiffré par la méthode de vigénère. Vous ne connaissez pas la clef mais vous savez que le texte est en français et que, dans cette langue, la lettre la plus fréquente est le *E*.

Déterminer la clef de chiffrement utilisée.

Vous trouverez en annexe différentes analyses statistiques sur le cryptogramme. Lorsqu'une ligne indique $\mathsf{Freq}\ x\%n + i$ cela signifie que sur la ligne concernée la fréquence d'apparition des lettres est donnée tout les n caractères décalés de i.

0	U	G	A	T	X	S	J	W	V	E	A	W	J	K	M	D	M	U	G	K	V	C	Q	V	W
25	P	K	E	A	I	M	G	R	A	Q	W	E	D	Z	A	A	K	W	N	I	**P**	**Z**	**G**	**X**	**G**
50	**A**	**S**	**Q**	**G**	**F**	F	M	**P**	**Z**	**G**	**Y**	**T**	**I**	**M**	**U**	W	M	T	W	F	N	A	U	K	M
75	L	T	W	E	G	V	T	T	W	H	T	M	M	Q	W	J	O	I	T	Q	F	V	W	X	R
100	Q	F	L	G	U	P	A	V	W	G	B	P	W	M	J	C	C	T	I	F	L	S	C	E	R
125	S	A	G	X	U	K	Z	W	T	K	H	M	J	B	G	N	U	A	D	W	R	Z	E	U	A
150	W	T	P	O	T	D	S	P	L	A	Q	K	S	N	M	F	I	A	J	G	L	A	V	K	E
175	Q	V	P	I	Q	K	T	M	T	Z	G	**K**	**R**	**M**	**C**	**B**	A	N	**G**	**U**	**E**	**V**	**L**	D	C
200	K	H	W	K	W	N	I	P	T	M	K	G	B	O	V	F	S	P	B	E	N	M	L	N	I
225	L	M	F	L	G	C	R	I	N	W	E	T	A	Y	M	W	N	T	E	**T**	**S**	**H**	**T**	**W**	F
250	M	K	K	K	W	N	L	W	**H**	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**M**	**U**	**Z**	W	E	G	Z	G	M
275	S	V	W	U	O	Q	F	K	F	I	N	A	E	S	T	M	G	Q	G	F	F	C	M	W	F
300	V	G	C	N	M	D	W	P	B	E	C	J	I	W	Q	E	A	L	E	C	Q	N	B	W	F
325	C	V	T	L	A	X	H	Q	C	Q	D	W	C	K	R	W	A	J	G	U	A	Q	K	B	C
350	Q	D	M	M	P	U	W	U	D	W	F	K	Z	S	B	J	W	U	V	E	B	K	V	G	K
375	E	B	L	W	R	M	R	Q	G	V	G	Y	U	Q	U	G	P	N	I	Z	E	W	P	B	C
400	M	L	L	G	T	E	V	L	W	W	Z	S	I	F	K	C	C	C	C	F	V	Q	C	T	M
425	S	H	T	M	S	I	N	G	K	Z	**P**	**Z**	**G**	**Y**	**T**	**I**	**M**	**U**	W	H	G	V	D	I	F
450	L	V	Z	O	Q	K	S	P	A	J	M	M	K	W	V	E	L	A	K	E	C	S	A	A	G
475	P	I	V	M	U	S	X	I	N	E	A	B	P	O	A	I	J	V	G	V	Q	C	A	**W**	**V**
500	**I**	**I**	**B**	S	D	Q	Z	S	U	G	F	R	I	T	Z	G	F	C	C	C	M	F	L	T	M
525	D	M	E	S	V	P	E	U	S	L	K	Y	U	M	K	V	C	U	S	B	W	J	F	I	M
550	C	F	W	F	Q	S	K	M	K	U	Q	O	V	H	G	W	Z	L	I	I	M	G	T	L	M
575	B	W	N	C	I	Z	W	K	V	M	R	I	A	K	C	R	A	U	S	A	U	Z	E	K	G
600	F	P	I	I	A	K	S	P	B	L	I	I	M	G	A	T	Q	G	F	G	B	A	Q	L	I
625	W	M	E	B	S	F	V	A	I	U	M	D	V	I	N	M	E	W	P	B	S	C	H	H	Q
650	A	E	M	L	M	F	Q	E	Z	D	S	R	P	Y	A	A	I	W	M	T	P	W	G	T	Q
675	Q	C	W	S	N	C	N	Q	N	W	T	A	I	B	W	V	G	T	E	Q	V	W	P	M	T
700	B	J	G	W	D	A	V	L	D	G	A	D	M	M	P	C	K	T	Q	N	A	V	M	S	L
725	W	H	N	C	S	M	F	H	N	C	S	L	A	X	H	Q	C	Q	D	W	U	I	C	W	F
750	U	K	T	I	M	J	B	G	L	E	D	S	A	U	U	E	L	W	U	K	L	E	Z	K	G
775	K	B	A	I	J	J	G	B	E	Z	V	W	R	Z	O	O	J	S	O	U	E	Z	W	L	C
800	L	E	D	W	F	K	Z	U	V	N	W	T	Q	T	I	T	D	G	C	N	Z	W	**K**	**R**	**M**
825	**C**	**B**	S	T	N	M	T	P	W	G	T	Q	C	Q	W	F	F	M	L	I	H	Z	A	A	I
850	Y	M	W	U	W	I	B	S	S	E	P	E	D	W	J	O	M	S	M	L	M	F	M	S	L
875	W	H	J	G	S	Q	I	M	G	A	A	D	W	U	N	M	M	Q	F	A	O	C	M	L	W
900	X	H	W	R	B	W	L	C	L	E	D	W	F	K	Z	O	C	A	I	W	W	I	C	F	**H**
925	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**M**	**U**	**Z**	E	S	K	A	**E**	**B**	**S**	**A**	**V**	K	E	C	F	W	R
950	Z	O	N	W	K	U	Q	O	V	J	W	U	X	E	K	L	S	D	T	E	K	S	J	C	X
975	R	M	K	L	Q	C	T	Y	M	**W**	**V**	**I**	**I**	**B**	U	W	S	C	E	**T**	**S**	**H**	**T**	**W**	**G**
1000	**Z**	**S**	**E**	**O**	**I**	**T**	**Q**	**G**	**F**	Q	C	**E**	**B**	**S**	**A**	**V**	T	E	A	G	D	K	L	E	K
1025	Z	S	O	X	D	M	U	G	P	V	A	Q	K	K	C	V	C	M	K	I	W	Q	P	W	M
1050	N	C	Q	T	T	S	K	Q	C	T	M	F	A	T	K	O	U	E	W	W	V	E	L	A	K
1075	E	Q	P	T	A	F	G	Q	N	B	W	D	N	M	C	B	M	W	N	**T**	**E**	**U**	**W**	**F**	**V**
1100	Z	E	A	H	W	E	B	A	J	D	W	L	M	M	M	J	S	R	X	E	T	D	W	V	Z
1125	E	A	N	A	X	**M**	**M**	**M**	**F**	**L**	E	W	M	U	W	B	G	V	V	Q	S	A	O	M	S
1150	K	G	D	N	M	G	C	W	K	V	Z	A	D	S	A	N	T	A	V	L	K	W	Z	L	M
1175	E	S	V	M	R	Q	W	D	S	C	I	Q	F	L	G	Z	R	W	Y	W	U	A	U	Z	D
1200	W	W	Z	S	K	G	E	R	M	T	M	F	U	G	A	**P**	**Z**	**G**	**X**	**G**	**A**	**S**	**Q**	**G**	**F**
1225	P	M	L	T	W	K	R	W	U	D	S	A	G	V	T	I	M	E	Q	Q	N	A	E	W	V
1250	B	R	M	W	F	C	D	A	V	L	D	G	C	R	X	D	W	K	V	E	K	G	F	P	I

1275	I	A	K	S	P	K	E	L	W	K	V	C	B	M	K	S	X	Q	D	M	V	W	U	I	M
1300	X	D	A	H	Q	C	I	L	W	W	Z	S	M	L	L	Q	C	T	T	W	J	G	A	T	M
1325	S	D	Q	Z	S	Y	M	W	L	I	V	I	A	K	N	Q	M	X	J	W	U	A	I	W	F
1350	I	W	M	C	W	F	X	T	W	N	B	W	S	E	M	T	B	W	I	W	M	S	B	A	G
1375	P	R	E	V	S	M	T	I	I	A	J	A	G	V	E	C	S	J	G	X	O	V	V	J	G
1400	M	M	X	D	A	F	M	D	W	M	L	G	A	J	M	X	J	C	X	P	I	A	K	C	T
1425	A	X	G	J	V	M	D	C	T	M	T	M	A	C	V	W	Y	Q	J	V	Y	S	C	Z	D
1450	M	F	W	V	T	U	Q	V	W	O	I	N	L	S	A	U	A	I	R	W	H	Q	C	V	I
1475	A	K	N	C	I	X	S	J	N	M	R	Y	M	W	N	Y	U	M	K	A	P	A	T	I	F
1500	L	U	Y	U	I	F	V	L	M	Q	C	A	L	V	I	I	A	K	G	P	J	U	Z	W	S
1525	W	X	L	C	K	A	G	C	R	A	Z	W	W	Z	**E**	**A**	**H**	**D**	**W**	**A**	T	I	J	V	L
1550	M	T	I	A	K	W	V	E	I	M	L	T	M	P	M	J	K	Q	V	N	M	U	S	T	I
1575	P	Z	W	K	C	D	O	Q	J	H	C	B	I	M	E	E	G	V	T	M	U	G	W	B	E
1600	U	W	K	R	Z	O	J	D	W	O	M	S	M	L	V	K	B	D	I	U	U	Q	Z	D	I
1625	N	W	E	U	O	Q	I	M	K	T	N	G	S	N	C	Q	T	X	S	K	X	Z	A	Q	E
1650	**W**	**P**	**B**	**D**	**M**	V	A	U	K	I	X	D	A	P	M	D	M	D	S	R	Z	O	O	J	S
1675	O	U	A	B	A	G	P	Q	L	A	W	E	K	B	A	M	P	H	N	Q	Q	C	W	J	R
1700	W	S	M	E	W	P	B	Q	C	W	D	G	A	O	Z	V	A	P	I	T	M	M	J	U	I
1725	U	B	G	E	C	B	I	Y	M	W	U	M	T	**I**	**A**	**W**	**P**	**B**	L	I	H	G	W	Z	D
1750	C	J	W	T	Y	U	**M**	**F**	**G**	**W**	**A**	N	M	F	W	V	Q	O	V	K	I	W	I	U	L
1775	W	T	W	B	E	B	I	M	G	X	E	C	L	W	V	Z	E	R	W	K	G	Z	A	Q	K
1800	M	P	M	D	M	K	H	G	Z	S	W	F	F	G	A	A	X	H	W	N	M	E	A	S	X
1825	C	Q	R	M	V	W	N	I	**P**	**Z**	**G**	**Y**	**T**	**I**	**M**	**U**	S	L	K	W	N	C	F	W	F
1850	Q	S	K	A	H	N	Q	N	M	J	W	U	X	E	K	L	S	D	T	E	L	S	F	U	T
1875	E	A	S	F	P	M	E	A	S	N	G	V	I	Z	U	W	H	C	T	C	F	L	Q	C	R
1900	V	S	F	V	L	E	U	S	N	K	M	E	B	B	W	O	M	D	M	T	S	T	Z	A	A
1925	K	S	K	A	D	M	E	W	U	M	T	C	V	W	U	L	E	X	Z	Q	U	Q	Q	C	W
1950	K	N	M	P	T	M	K	T	I	P	Q	V	W	O	M	N	B	H	G	U	A	I	J	D	W
1975	W	V	E	L	W	K	O	W	R	I	D	W	U	L	E	K	W	L	V	M	H	Q	K	L	Q
2000	Q	R	M	W	K	V	J	I	M	F	K	W	Z	Q	C	W	F	Q	C	S	L	W	N	Q	V
2025	S	N	S	A	T	M	T	Z	W	K	C	B	T	M	F	L	K	W	N	T	G	J	U	Y	U
2050	**M**	**F**	**G**	**W**	**A**	D	W	F	F	Q	V	S	L	W	K	E	W	N	A	W	A	N	A	A	V
2075	G	K	E	I	D	M	L	K	R	I	R	N	G	A	U	Q	L	A	D	W	U	A	U	Q	N
2100	**W**	**P**	**B**	**D**	**M**	M	P	C	V	S	X	D	M	U	B	A	Z	V	W	P	R	E	U	W	E
2125	C	Z	I	I	A	K	G	B	L	I	U	W	T	M	M	W	F	A	G	P	O	T	D	S	P
2150	L	A	Q	K	W	F	C	M	I	J	A	C	O	E	L	W	E	C	V	D	I	F	L	S	C
2175	E	D	G	M	U	L	E	K	D	S	T	Q	E	H	N	G	V	Z	E	X	J	G	H	M	S
2200	A	A	G	P	R	E	L	W	U	N	I	R	I	A	K	S	C	E	R	W	L	C	Q	S	**X**
2225	**J**	**G**	**I**	**Z**	**A**	**U**	**E**	W	W	Z	M	I	A	K	N	M	S	I	M	L	Q	Z	I	B	W
2250	K	O	C	N	Q	U	A	R	I	L	M	K	V	G	T	A	D	A	D	N	M	D	I	E	K
2275	V	M	R	L	S	E	P	M	L	I	U	U	G	X	T	M	J	W	P	B	P	I	K	U	Q
2300	V	S	Q	V	W	T	I	N	B	I	M	W	V	E	B	W	D	N	M	**P**	**Z**	**G**	**X**	**G**	**A**
2325	**S**	**Q**	**G**	**F**	P	M	X	Q	K	L	C	Q	T	X	S	K	G	B	C	Z	G	Q	G	H	L
2350	M	G	M	P	W	N	A	G	M	U	T	E	B	A	L	T	M	**P**	**Z**	**G**	**X**	**G**	**A**	**S**	**Q**
2375	**G**	**F**	O	W	N	I	U	L	G	L	E	U	S	J	K	I	G	M	H	G	T	B	E	T	S
2400	E	G	V	T	Q	G	F	T	Q	D	Q	U	M	N	M	D	M	H	Z	A	A	I	K	A	W
2425	P	B	H	M	G	J	K	Y	U	M	N	G	K	T	A	X	G	M	T	T	A	T	W	F	V
2450	M	U	Z	S	N	G	K	L	I	I	M	G	T	L	M	B	S	K	D	U	**T**	**S**	**H**	**T**	**W**
2475	F	M	K	K	K	W	N	L	W	**H**	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**M**	**U**	**Z**	W	E	G	Z	G
2500	M	J	V	C	V	S	U	G	F	R	Z	O	X	J	W	R	I	Y	A	V	W	R	C	I	A

2525	D	G	T	A	J	I	A	N	W	C	N	M	H	D	W	A	G	Z	S	F	F	M	P	I	J
2550	L	K	M	D	C	E	G	P	L	E	M	L	E	Q	V	I	U	H	J	G	A	S	Q	G	F
2575	I	M	N	M	J	S	N	M	E	A	L	I	W	M	D	I	F	K	N	M	S	I	M	L	T
2600	M	S	X	S	Q	U	I	V	M	U	I	W	M	L	Y	M	W	U	L	E	K	S	D	C	O
2625	E	A	V	W	F	I	T	M	K	D	G	U	O	L	W	D	G	L	E	K	J	G	K	A	S
2650	I	F	U	G	I	E	B	W	W	P	O	R	I	F	V	G	X	A	Z	L	A	G	T	E	U
2675	W	E	G	T	A	Q	K	K	G	H	M	W	A	W	U	A	A	G	W	J	F	M	D	M	U
2700	J	K	Z	E	T	S	K	K	B	U	I	L	A	Q	V	D	I	F	K	E	M	S	R	G	M
2725	T	A	A	V	U	A	G	V	S	I	N	W	E	C	N	X	W	M	R	T	U	A	V	W	F
2750	M	T	I	A	D	F	I	N	A	D	W	U	X	O	Q	J	I	W	M	C	M	D	S	P	W
2775	U	A	V	G	P	V	E	C	F	W	O	M	I	T	D	W	W	Z	E	K	G	E	R	Z	E
2800	P	W	F	U	Q	O	V	V	W	N	I	S	Q	L	M	C	B	I	W	F	S	W	R	O	C
2825	J	V	J	C	I	M	F	H	Q	C	R	A	M	A	X	I	N	B	F	G	V	Z	E	I	F
2850	S	N	G	S	M	F	G	W	A	V	M	J	J	Q	V	S	K	G	E	O	M	T	I	F	L
2875	F	M	M	I	D	W	P	B	E	V	V	M	U	I	P	Z	G	H	Q	A	D	M	D	S	X
2900	M	R	Q	L	S	D	T	E	V	S	L	W	Z	E	L	W	D	C	K	T	Q	N	A	V	M
2925	D	M	H	J	Q	O	R	I	E	E	C	B	I	W	F	H	G	C	V	M	F	L	T	M	M
2950	W	F	L	G	Z	A	K	W	H	C	A	S	M	E	S	K	V	T	M	F	S	P	B	L	W
2975	A	F	V	I	I	V	D	W	U	X	R	M	E	A	G	Z	S	W	J	V	K	V	A	B	W
3000	M	T	A	E	T	W	U	V	Z	O	V	A	I	W	M	S	I	M	L	Q	U	A	B	A	I
3025	W	M	S	M	L	S	K	M	N	B	L	G	W	A	D	M	K	E	C	K	H	Q	F	W	U
3050	C	N	Q	I	M	G	A	E	V	M	F	U	M	U	T	W	P	G	U	P	T	S	A	T	M
3075	E	B	A	D	U	M	T	I	A	W	P	B	T	W	M	K	U	Q	T	C	W	K	F	I	N
3100	A	M	F	G	V	V	Q	J	G	P	V	E	U	W	F	V	Q	M	X	J	W	I	V	E	L
3125	W	D	C	U	B	Q	S	F	E	M	E	V	L	Z	Q	C	S	Q	S	K	O	I	N	B	W
3150	V	W	V	L	I	T	G	T	I	T	W	A	J	G	M	X	X	W	J	K	U	E	V	L	S
3175	N	Y	U	I	F	V	N	Q	D	M	W	V	G	T	O	Z	V	A	P	I	T	M	M	J	C
3200	C	T	W	E	S	V	Q	Q	C	W	S	R	X	A	Z	M	L	U	I	R	M	S	D	K	A
3225	A	B	A	G	P	N	U	B	M	F	H	W	R	U	A	V	C	J	L	M	V	W	H	Q	P
3250	W	M	J	N	I	T	M	U	Z	P	W	L	W	Y	A	G	M	L	M	U	L	T	W	N	Q
3275	I	M	G	L	I	A	H	G	P	Q	B	T	W	S	N	M	P	W	I	M	G	M	T	C	F
3300	W	E	P	O	A	W	W	U	B	C	M	J	L	C	Q	N	M	F	G	W	A	N	M	H	G
3325	W	D	O	V	K	H	C	A	N	Q	W	J	N	M	C	W	M	J	C	O	E	L	W	K	G
3350	Y	U	Q	H	W	U	Y	U	Q	V	W	E	Q	D	M	J	W	P	B	D	M	K	W	N	I
3375	N	K	W	J	F	I	N	A	D	S	E	W	N	A	L	J	W	K	T	Q	G	F	F	C	N
3400	M	I	M	K	X	E	U	W	F	V	I	U	A	K	A	H	I	N	B	S	K	V	Q	Q	C
3425	W	U	C	Z	C	M	L	S	K	B	D	M	K	W	S	C	I	X	W	E	G	V	T	A	X
3450	S	P	B	A	A	L	A	S	C	E	A	J	W	V	Z	O	A	H	W	E	B	I	D	W	E
3475	G	V	T	W	F	H	G	C	T	A	W	M	N	M	M	M	F	L	U	M	M	M	J	N	G
3500	Q	L	T	W	J	S	C	E	K	W	K	R	Z	E	U	A	W	T	M	S	U	S	U	J	Q
3525	N	M	K	S	K	M	N	B	K	W	W	T	E	U	W	F	V	N	O	V	U	L	K	W	N
3550	V	W	V	W	U	O	Q	F	K	R	I	R	N	G	A	U	T	A	B	S	U	J	M	E	K
3575	J	S	U	I	N	B	W	W	V	I	I	B	V	W	O	M	T	B	J	W	G	B	D	M	U
3600	G	P	A	E	Z	N	W	T	K	E	A	E	S	E	P	I	V	W	K	G	V	E	B	S	L
3625	F	M	F	W	F	U	V	Q	O	V	F	W	O	M	N	B	D	S	R	Z	E	W	U	U	W
3650	X	A	B	A	G	P	M	N	D	W	J	U	T	E	A	S	K	R	M	C	B	K	E	C	B
3675	E	Z	A	W	N	A	D	C	U	S	N	K	U	T	S	M	V	W	M	I	L	A	S	C	E
3700	A	W	J	G	N	L	M	L	W	V	W	U	R	G	M	T	A	D	I	F	K	N	M	S	V
3725	G	E	U	L	E	A	H	D	W	A	V	Q	W	A	N	T	E	A	K	G	E	Q	E	B	W
3750	K	U	K	I	M	F	L	K	N	I	Y	M	W	U	L	U	A	W	U	V	M	U	Z	U	G

3775	O	U	E	T	S	K	U	W	C	Q	S	L	K	W	N	X	G	M	T	T	O	C	L	A	N
3800	T	A	O	W	A	P	N	O	Z	E	S	V	Q	Q	C	W	S	U	A	O	K	A	S	V	Q
3825	O	V	X	G	T	K	O	U	H	M	V	Q	N	O	E	S	E	P	I	V	W	J	A	I	C
3850	U	G	M	N	I	S	W	U	A	G	B	E	J	J	A	V	I	N	V	A	I	W	M	D	M
3875	D	G	T	L	I	V	S	L	G	C	R	J	J	A	V	Q	S	P	U	G	O	X	U	B	W
3900	J	U	W	C	Q	W	L	A	L	E	A	F	G	O	A	F	I	A	K	C	V	T	L	A	J
3925	G	K	T	M	E	W	P	B	R	M	X	W	T	M	N	K	W	S	N	M	Q	C	A	H	G
3950	U	E	V	L	E	C	B	E	Z	A	W	N	M	T	T	W	H	C	C	V	Z	W	H	T	W
3975	G	Z	S	E	O	M	U	Z	W	L	D	Q	E	V	S	D	C	D	E	Z	A	L	G	W	N
4000	T	W	J	G	U	A	Z	I	M	C	Q	T	I	H	W	K	V	E	L	S	T	Q	Z	D	T
4025	W	K	R	Z	E	U	A	W	T	M	S	U	S	U	J	Q	N	M	K	W	V	I	I	M	F
4050	L	U	Q	M	I	K	K	K	D	E	A	I	M	G	T	L	M	K	W	V	I	I	M	F	L
4075	R	Z	A	B	A	I	W	M	M	M	F	L	K	U	P	W	K	K	K	J	L	M	K	S	F
4100	M	P	T	S	U	G	Z	E	B	V	W	R	T	U	A	W	D	N	M	S	L	W	E	C	V
4125	D	I	A	W	P	B	U	V	W	E	C	Q	N	B	W	F	C	V	C	M	K	A	E	W	N
4150	A	A	V	G	Z	A	J	D	W	S	C	I	T	W	K	V	V	A	B	M	J	G	T	Q	C
4175	W	D	G	V	D	Z	G	A	V	W	U	T	W	K	I	M	N	A	W	K	U	I	Y	I	A
4200	W	P	B	D	M	D	W	U	C	T	Q	D	A	U	M	R	M	L	S	K	B	L	M	D	S
4225	D	W	R	I	L	G	K	Z	E	U	W	E	G	W	U	M	D	D	G	A	A	D	S	A	G
4250	V	T	M	L	W	O	Q	S	M	K	S	W	X	O	Q	F	L	F	M	U	F	A	W	O	M
4275	M	M	F	L	U	W	N	B	J	S	X	I	I	T	S	H	G	C	P	Z	W	K	K	V	V
4300	Q	K	A	D	T	E	M	L	S	K	B	S	I	F	K	R	Z	E	A	L	A	I	M	V	W
4325	M	K	R	W	U	D	A	W	B	U	O	V	L	J	G	Z	L	I	E	S	E	P	I	V	W
4350	S	W	F	V	Q	K	A	V	M	U	Z	K	W	V	K	E	B	S	A	V	X	L	C	K	K
4375	R	M	C	B	S	U	W	T	A	Q	J	W	F	M	P	T	M	K	K	M	U	Z	K	G	T
4400	L	R	M	K	V	G	O	R	I	F	V	G	C	R	Y	M	W	S	C	E	T	I	M	G	A
4425	F	M	M	A	N	T	E	A	V	W	N	Q	S	B	A	F	I	U	A	Q	K	D	G	X	L
4450	C	K	A	O	X	O	Z	L	S	P	B	D	M	L	G	W	B	E	B	S	A	V	Y	U	M
4475	D	W	R	Z	O	O	J	S	O	U	E	C	J	D	W	Q	M	M	E	W	C	D	A	Q	L
4500	M	P	M	O	X	A	F	K	W	N	B	J	W	U	U	O	L	W	K	V	M	D	M	K	G
4525	P	B	R	I	N	S	K	T	T	W	M	L	G	T	A	A	A	Y	P	Q	F	Q	U	S	V
4550	Q	O	V	V	W	U	W	N	B	J	S	X	I	I	T	N	W	P	I	I	B	V	W	N	M
4575	X	Q	K	L	G	V	C	M	V	W	E	M	T	B	W	H	T	W	D	Q	Y	A	G	C	S
4600	M	E	S	E	P	I	V	W	H	C	Z	C	M	I	M	G	K	E	B	L	W	O	I	C	P
4625	A	F	G	M	T	I	A	L	W	V	I	Y	M	W	K	T	N	M	K	S	X	I	I	B	I
4650	M	G	B	R	W	H	T	K	M	N	Y	M	W	U	M	S	X	J	G	I	Z	A	U	E	W
4675	U	V	A	D	S	A	G	V	T	Y	M	M	P	M	P	W	J	L	G	M	L	W	U	S	N
4700	M	E	B	S	M	U	A	I	X	M	A	U	Y	U	Q	D	W	V	I	I	B	T	A	G	V
4725	E	D	A	V	G	V	T	Y	M	W	E	M	T	B	W	E	C	K	H	Q	F	W	C	C	R
4750	I	A	L	W	V	E	L	M	J	G	M	D	M	N	A	G	T	I	U	A	L	G	M	I	T
4775	K	S	X	I	I	B	I	M	G	B	R	M	K	H	G	C	D	M	K	G	P	B	R	I	N
4800	S	K	T	A	C	J	S	K	B	U	V	W	N	C	T	E	C	J	V	W	Z	A	J	D	W
4825	H	Q	N	I	D	W	O	M	N	B	A	D	A	I	U	V	S	M	V	Z	E	I	K	H	G
4850	K	T	L	W	K	E	Q	R	K	G	F	U	B	A	V	U	W	U	Y	U	Q	S	N	C	Q
4875	T	C	F	W	K	V	F	T	M	W	P	K	E	X	J	G	H	W	N	L	W	K	W	Z	L
4900	I	L	L	K	B	U	L	W	V	W	X	R	W	Y	J	C	U	M	M	M	J	G	V	V	M
4925	J	K	U	W	N	B	J	S	X	I	I	T	V	M	P	K	O	B	W	W	P	X	L	C	K
4950	V	G	B	R	M	H	W	W	N	I	I	T	D	G	A	A	U	S	U	J	Q	N	M	W	L
4975	C	Q	T	P	S	T	K	B	U	M	D	D	G	U	E	V	L	L	T	W	P	T	W	F	V
5000	M	E	B	K	S	O	M	M	W	A	J	G	B	R	W	H	H	G	B	I	B	W	A	N	M

5025	T	I	A	L	C	T	E	B	J	G	K	B	A	T	G	J	U	Y	U	M	V	W	N	I	U
5050	B	J	W	U	W	N	K	G	V	G	L	I	V	K	L	T	C	C	B	A	G	P	M	N	O
5075	W	F	G	Z	A	T	H	D	W	B	O	B	K	A	P	O	U	T	A	W	T	T	A	Q	K
5100	K	C	Q	T	T	W	U	J	I	M	X	D	A	D	Z	E	I	M	P	E	W	N	A	L	J
5125	W	K	T	Q	G	F	U	T	**E**	**A**	**H**	**D**	**W**	**A**	I	V	S	L	V	M	N	L	M	W	U
5150	M	T	I	U	W	V	B	E	M	H	G	S	C	E	J	W	S	W	K	O	C	H	V	G	X
5175	R	W	Y	J	C	U	M	M	M	J	U	I	S	B	M	U	K	M	U	F	J	W	V	Q	R
5200	**I**	**A**	**W**	**P**	**B**	U	V	W	A	O	U	E	V	K	W	U	I	T	Q	K	X	C	K	T	Q
5225	G	F	K	V	T	M	D	D	G	K	T	C	W	D	N	M	D	M	K	S	U	B	U	K	W
5250	K	K	V	G	M	F	A	G	C	S	M	K	Y	T	I	C	M	S	M	Z	Y	U	M	D	D
5275	G	A	I	T	K	H	C	Z	V	M	F	S	K	M	N	B	S	X	C	Q	R	M	L	W	P
5300	Q	R	T	A	E	R	W	S	A	A	T	N	M	D	I	F	K	N	M	C	I	V	J	G	K
5325	O	V	L	J	C	Q	G	V	S	F	V	L	E	T	W	M	T	M	Q	C	A	H	**G**	**U**	**E**
5350	**V**	**L**	V	G	C	X	W	H	A	P	Q	O	V	K	U	Q	V	C	M	J	F	C	V	T	**T**
5375	**S**	**H**	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**I**	**T**	**Q**	**G**	**F**	F	I	T	M	F	L	F	M	C	M	L
5400	L	G	M	P	W	I	M	G	R	E	T	W	K	O	M	N	B	A	G	P	V	E	A	A	E
5425	R	**T**	**E**	**U**	**W**	**F**	**V**	R	Y	Z	W	N	K	M	N	L	J	S	K	A	T	W	M	L	C
5450	T	H	M	M	J	G	T	U	V	**W**	**W**	**V**	**I**	**I**	**B**	**I**	**M**	W	V	**P**	**Z**	**G**	**Y**	**T**	**I**
5475	**M**	**U**	W	M	T	D	R	I	A	E	G	V	T	K	G	E	R	M	T	M	F	L	F	M	V
5500	I	A	L	G	B	R	M	S	E	C	B	E	C	J	V	G	V	I	O	E	W	U	M	T	L
5525	S	K	V	C	C	M	K	D	C	C	T	Z	**W**	**W**	**V**	**I**	**I**	**B**	**I**	**M**	G	T	A	**X**	**J**
5550	**G**	**I**	**Z**	**A**	**U**	**E**	**S**	**V**	**Q**	**O**	**V**	F	**W**	**V**	**I**	**I**	**B**	J	A	G	V	D	M	H	D
5575	W	A	Q	C	W	D	Q	X	T	Q	E	A	U	**I**	**T**	**Q**	**G**	**F**	F	C	P	Z	G	U	G
5600	A	S	C	K	V	G	K	A	T	U	M	N	L	A	V	K	M	P	A	E	V	K	G	W	L
5625	A	V	K	D	C	C	T	Z	W	U	G	B	T	M	V	W	T	V	I	M	J	W	Q	X	I
5650	V	A	G	P	M	T	I	A	L	N	M	R	M	K	M	N	B	A	B	V	W	U	K	I	Z
5675	U	G	P	A	T	I	F	U	G	A	F	Z	W	I	W	M	N	B	W	K	Q	C	L	M	I
5700	M	K	X	**E**	**U**	**W**	**F**	**V**	L	I	A	H	G	P	Q	B	T	**W**	**W**	**V**	**I**	**I**	**B**	N	W
5725	T	Q	T	I	T	D	**G**	**U**	**E**	**V**	**L**	L	T	M	S	K	G	F	V	Z	A	Q	Y	F	C
5750	V	T	M	L	D	Q	V	R	M	F	U	Q	V	T	Z	S	A	V	A	O	C	N	W	P	B
5775	L	M	K	H	G	Z	A	V	U	W	P	I	I	D	W	I	W	C	N	M	X	G	K	A	Q
5800	C	W	V	G	A	M	I	U	Z	K	V	**E**	**A**	**H**	**D**	**W**	**A**	P	C	A	K	U	I	N	B
5825	W	K	U	M	R	**I**	**A**	**W**	**P**	**B**	D	Q	K	H	Q	V	I	J	D	W	U	T	A	**X**	**J**
5850	**G**	**I**	**Z**	**A**	**U**	**E**	**S**	**V**	**Q**	**O**	**V**	F	W	U	M	R	I	A	L	R	T	U	A	M	F
5875	R	Z	O	J	D	W	O	M	P	C	A	K	S	C	A	K	W	E	Q	U	E	V	L	D	C
5900	T	E	N	X	G	T	B	P	W	M	J	R	W	U	A	K	W	T	T	A	**U**	**S**	**U**	**J**	**Q**
5925	**N**	**M**	S	D	C	T	I	U	A	L	G	L	E	A	W	K	E	I	P	I	U	A	V	M	S
5950	V	W	K	G	Z	A	Q	L	H	N	C	S	V	W	U	G	A	S	I	A	J	G	M	T	K
5975	W	L	C	Q	T	J	A	W	P	T	A	B	G	M	V	K	E	M	F	I	W	W	I	**T**	**S**
6000	**H**	**T**	**W**	**G**	**Z**	**S**	**E**	**O**	**I**	**T**	**Q**	**G**	**F**	E	W	N	A	A	K	V	I	I	B	F	G
6025	P	U	A	Q	K	S	W	K	O	C	J	K	F	M	S	L	W	U	G	V	N	Q	W	K	U
6050	C	I	D	S	F	V	M	S	Y	M	W	N	Y	U	M	U	Z	Q	A	E	L	W	U	Q	U
6075	P	T	W	L	**G**	**U**	**E**	**V**	**L**	V	K	N	F	M	J	W	P	B	A	Z	J	A	X	I	D
6100	M	K	E	C	K	H	Q	F	W	U	X	L	C	K	H	W	Q	S	A	S	F	V	M	S	I
6125	H	H	C	Z	U	Z	W	F	V	X	A	A	K	W	W	**T**	**E**	**U**	**W**	**F**	**V**	X	L	C	K
6150	H	W	Q	S	A	S	F	V	M	S	L	M	F	Q	Z	D	Z	W	V	G	U	A	O	F	A
6175	V	C	D	M	E	S	K	A	P	T	M	K	R	C	I	A	K	S	P	B	E	A	V	W	R
6200	T	U	A	A	W	W	Z	S	W	J	V	T	M	S	L	W	E	C	O	N	Q	L	M	F	M
6225	M	I	A	K	C	C	L	Q	W	M	F	M	N	W	M	K	T	M	T	Z	G	M	X	M	R

Cara	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq x%3 + 0	7.4	0.4	1.6	5	10	3.7	3.8	2.4	4.7	2.9	4.5	5.6	4.6	4.6	2.5	2.1	0.9	2.6	7.9	5	4.8	2.6	8.9	0.7	0.5	0.3
Freq x%3 + 1	3.9	4.4	6.7	1.2	1.4	1.6	7.9	0.6	5	0.9	4.9	2.1	8.5	3.4	2.3	4.3	6.4	2.3	0.6	6.1	6	7.2	6.1	2.1	0.7	3.2
Freq x%3 + 2	7.9	3.8	3.6	2.6	1.5	4.2	3.1	1.6	5.5	3.5	5.9	4.1	11.6	1.3	0.4	0.5	4	0.4	4.6	3.1	3.4	5.4	11.2	1.8	1.1	4

Cara	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq x%4 + 0	7.5	5.6	3.8	2.2	1.3	2.4	2.3	1.7	6	2	4.7	4.3	12.9	0.8	0.4	0.5	5.8	0.6	3.1	4	3.5	6.6	10	2	1.1	4.9
Freq x%4 + 1	5.7	0.3	3.8	3.5	7.3	3.8	6.8	1.4	3.3	2.4	5.3	3.4	3.7	5.5	2.9	4.1	1.6	2.8	5.6	6.1	6.5	4.1	8.4	0.7	0.5	0.1
Freq x%4 + 2	6.7	5.4	4.5	2.6	1.6	2	2.1	1.2	7.2	2.6	5.6	4.9	13.7	1	0.6	0.8	5.7	0.3	2.4	3.6	3.4	5	8.4	2.7	1.2	4.8
Freq x%4 + 3	5.8	0.2	3.6	3.5	7	4.4	8.5	1.9	3.8	2.7	4.9	3.1	2.5	5.1	2.9	3.8	2	3.3	6.2	5.3	5.4	4.6	8.1	0.8	0.3	0.2

Cara	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq x%5 + 0	5.7	2.7	3.5	3	4.8	4	4.2	1.8	4.6	2.8	4.6	3.4	8.6	2.7	2.5	2.3	3.8	1.8	4.2	4.4	5	5.8	8.7	2	0.8	2.3
Freq x%5 + 1	6.7	3.1	3.7	3.4	4.5	2.9	5.7	1.8	5.5	2.2	5.5	3.6	7.3	3	1.4	1.9	4.1	2	5.5	4.9	4.5	4.2	8.2	1.1	0.6	2.6
Freq x%5 + 2	7.6	3.3	3.7	2.6	3.9	2.9	4.6	1.4	4.4	2.4	5.2	4.6	9.2	2.9	1.2	2.4	3.8	2.1	3.6	4.9	4.6	5.1	8.6	1.6	1.3	2.2
Freq x%5 + 3	5.9	3.4	4.3	3.4	3.9	2.5	5.2	1.8	5.5	2.4	5.4	4.6	7.4	3	2	2.2	2.7	1.4	4	5.1	4.6	5	9.2	1.5	0.8	2.6
Freq x%5 + 4	6.2	1.8	4.6	2.3	4.5	3.5	5	0.8	5.4	2.3	4.9	3.5	8.6	3.9	1.6	2.7	4.4	1.5	4.5	4.5	4.9	5.2	9	1.4	0.3	2.7

Cara	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq x%6 + 0	7.1	0.5	0	4.6	4.3	6.3	6.2	4.1	1.7	5.4	9	7.3	5.8	1.2	0	0.5	0.3	0	8.3	0.6	3.2	3.6	17.8	1.1	0.6	0.6
Freq x%6 + 1	0.5	0.1	8	0.8	2.8	3	15.6	1.1	0.9	0.8	6.9	0.4	0	6.1	3.7	8.1	3.8	3.9	1.2	7	8.1	8.1	7.8	1.2	0.1	0.1
Freq x%6 + 2	6.8	7.3	7.1	0.9	0	0.1	0.2	0.2	8.8	0.4	3.4	2.7	17.2	0.9	0.9	1	7.9	0.8	0	5.6	3.3	7.3	5.4	3.1	1.5	7.6
Freq x%6 + 3	7.8	0.4	3.3	5.4	15.6	1.1	1.4	0.8	7.7	0.4	0	3.8	3.4	8	5.1	3.7	1.4	5.3	7.4	9.5	6.3	1.5	0	0.4	0.4	0
Freq x%6 + 4	7.4	8.7	5.4	1.7	0.1	0.2	0.2	0.1	9.2	1.1	3	3.7	17	0.7	0.8	0.6	9	0.6	0	5.2	3.9	6.4	4.4	2.9	1.3	6.3
Freq x%6 + 5	8.9	0.3	0	4.4	3.1	8.3	6	3.1	2.1	6.5	8.5	5.6	6	1.8	0	0.1	0.1	0	9.1	0.7	3.5	3.5	17	0.6	0.7	0.4

Cara	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq x%7 + 0	6.3	2.7	3.6	2.8	4.7	3.2	5.5	1.9	5.8	2.1	5.3	3.8	8	3.4	1.5	2.8	4	1.5	3.6	5.5	4.5	4.7	9.4	1.3	0.6	1.7
Freq x%7 + 1	6	2.9	4.5	3.1	3.8	3.2	5.3	1.7	6.9	2.5	4	4.6	8.6	2.6	1.7	2.1	3.6	1.2	4	4.5	4.7	6.8	7.5	1.1	0.7	2.2
Freq x%7 + 2	6.4	2.8	4.8	3.2	4.1	3	4.5	1.3	3.9	2.4	5.8	4.6	8.6	2.9	1.8	1.8	3.2	1.5	4.1	4.9	4.9	5.4	9.9	1.2	0.6	2.2
Freq x%7 + 3	6.2	2.6	3.1	1.9	4.6	2.8	4.8	1.2	5.6	1.7	6.3	3.7	7.7	3.1	1.6	1.7	4	2.7	4.8	4.9	5.2	4.4	9.7	2.1	1.1	2.5
Freq x%7 + 4	7.8	2.6	3.8	3.7	4	2.4	4.8	1.7	4.5	2.8	4.1	3.8	8.5	3.8	1	2.7	3.5	1.8	4.7	3.9	4.9	4.8	7.3	2.1	1.2	3.7
Freq x%7 + 5	6	3.7	4	2.2	4.7	3.9	5.4	1.7	3.2	2.5	5.4	3.8	8.3	2.9	1.9	2.1	4.5	1.8	4.5	4.3	4	4.5	9.6	1.6	0.6	2.9
Freq x%7 + 6	6.2	2.9	3.8	3.7	4.3	3.5	4.4	1.3	5.5	3	4.9	3.1	7.7	3	2.8	3	3.5	1.9	4.7	5.3	4.7	4.9	7.6	1.2	0.7	2.2

4. Substitution

La substitution

Exercice 1

Dans $\mathfrak{S}_5$, simplifier lorsque c'est possible les permutations suivantes (par exemple : $(1\ 2)(3\ 2) = (1\ 2\ 3)$).

1. $(1\ 2\ 3)(1\ 4)(1\ 3)$
2. $(4\ 5)(4\ 3)$
3. $(5\ 4)(3\ 2)(1\ 5)$
4. $(1\ 2)(4\ 5)(1\ 2)$
5. $(3\ 5)(4\ 5)(3\ 4\ 5)$
6. $(2\ 1)(3\ 4\ 5)$
7. $(3\ 5)(1\ 3\ 5)(2\ 1)$
8. $(1\ 2\ 3\ 4)(1\ 2\ 3)(1\ 2)$
9. $(1\ 2)(1\ 3)(1\ 4)(1\ 5)$

Exercice 2

Décrypter le texte suivant dans lequel on a appliqué une substitution.

P'TQAOS ALHDS TJ GDHOT A LA KAQITKAQOFWT.

QTKGS SHKZDT ! TJYAJQ TKW RW YDOSSHJ GHTQOFWT,

GAWXDT HOSTAW FWO ITWDQAOS RW EDAJT KTS ZADDTAWV,

HJ KT LOXDAOQ QHWQ XOY AWV EIOYYDTS, JHODS ZHWDDTAWV ;

HJ KT YAOSAOQ RT YHDET OJUWDUOQTD L'ALUTZDT ;

HJ KT LOAOQ AW YHJR R'WJ ZHOSZTDQDAJR YWJTZDT.

HJ KT QHDRAOQ RTGWOS LTS AOLTS PWSFW'AW ZTE,

SWD L'AYYDTWV EITXALTQ RTS V TQ RTS B ;

ITLAS, HJ KT YHWDDAOQ SHWS LTS HS KAVOLLAODTS

LT QITHDTKT HDJT RT QHWS STS EHDHLLAODTS ;

TQ PT KT RTZAQQAOS, LWUWZDT GAQOTJQ

RW ROXOSTWD GDTQAJQ KAOJ-YHDQT AW FWHQOTJQ.

Pour simplifier voici les occurrences des lettres apparaissant dans ce message.

Caractère	A	B	C	D	E	F	G	H	I	J	K	L	M
Apparition	38	1	0	35	6	5	7	28	6	21	15	18	0

Caractère	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Apparition	0	33	3	31	14	32	63	4	6	33	5	13	10

5. Matrice modulaire

Matrices

Exercice 1

Soient $A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 1 \\ 5 & 0 \end{pmatrix}$ et $C = \begin{pmatrix} 6 & 3 \\ 3 & 1 \end{pmatrix}$ des matrices de $\mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$.

1. Calculer $A + B$, $A \times C$ et $B \times C$.
2. Comparer $(A + B) \times C$ et $A \times C + B \times C$
3. Comparer le résultat précédent avec $C \times (A + B)$

Exercice 2

Calculer le déterminant de chacune des matrices suivantes. Identifier les matrices de $\mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$.

1. $A = \begin{pmatrix} 11 & 3 \\ 2 & 5 \end{pmatrix}$
2. $B = \begin{pmatrix} 3 & 1 \\ 4 & 6 \end{pmatrix}$
3. $C = \begin{pmatrix} 1 & -5 \\ -1 & 8 \end{pmatrix}$
4. $D = \begin{pmatrix} 1 & -5 \\ 1 & 8 \end{pmatrix}$
5. $E = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$
6. $F = \begin{pmatrix} 12 & 13 \\ 11 & 10 \end{pmatrix}$
7. $G = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$
8. $H = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$
9. $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Exercice 3

Pour chacune des matrices de $\mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$ de l'exercice précédent, donner la matrice inverse (modulairement).

Hill

Exercice 4

Parmis les matrices suivantes, lesquelles sont des clefs du cryptosystème de Hill de dimension 2 par paquet de n ?

1. $n = 1$ et $A = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}$
2. $n = 1$ et $B = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}$
3. $n = 2$ et $C = \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}$
4. $n = 2$ et $D = \begin{pmatrix} 1 & 100 \\ 1001 & 1 \end{pmatrix}$
5. $n = 3$ et $E = \begin{pmatrix} 1 & 13 \\ 2 & 1 \end{pmatrix}$

Exercice 5

En utilisant un chiffrement de Hill de dimension 2 par paquet de 1, chiffrer le mot *MATH* avec $= \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$ comme clef.

Exercice 6

En utilisant un chiffrement de Hill de dimension 2 par paquet de 1, chiffrer le mot *KAAMELOT* avec $= \begin{pmatrix} 11 & 1 \\ 0 & 19 \end{pmatrix}$

comme clef

Exercice 7

On a utilisé un chiffrement de Hill de dimension 2 par paquet de 1 avec $= \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}$ comme clef pour obtenir *QMPPEXZVIKUL*. Quel était le message clair ?

Exercice 8

On a utilisé un chiffrement de Hill de dimension 3 par paquet de 1 avec $= \begin{pmatrix} 8 & 3 & 0 \\ 1 & 1 & 11 \\ 0 & 8 & 7 \end{pmatrix}$ comme clef pour obtenir *YHHKJJUPPLQQGEE*. Quel était le message clair ?

6. Nombres premiers

Nombres premiers

Exercice 1

Appliquer la méthode du crible d'Eratosthène et entourer les nombres premiers de la liste suivante.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Exercice 2

Parmi les nombres suivants identifier ceux qui sont des nombres premiers.

1. 103
2. 247
3. 367
4. 539
5. 587
6. 597
7. 683
8. 693
9. 701
10. 787
11. 809
12. 909
13. 989
14. 991
15. 997
16. 1009
17. 1211
18. 1311
19. 1319
20. 1321

Exercice 3

Calculer.

1. $v_3(15)$
2. $v_7(120)$
3. $v_5(625)$
4. $v_2(18)$
5. $v_{11}(121)$
6. $v_3(18^{2017})$

Nombres premiers 2

Exercice 4

Soit $p \in \mathcal{P}$ tel que $p > 2$. Montrer qu'il existe $k \in \mathbb{N}$ tel que soit $p = 4k+1$ soit $p = 4k-1$.

Exercice 5

Trouver tous les nombres premiers p tel que $4p+1$ et $7p-4$ soient également premiers. On pourra regarder modulo 3.

Exercice 6

1. Montrer que 13 divise $2^{70} + 3^{70}$.
2. Montrer que 11 divise $2^{129} + 3^{118}$.
3. Montrer que $2^{281} + 3^{193}$ est un multiple de 7.

Exercice 7

Pour quelle valeur de n, $5^{6n} + 5^n + 2$ est-il divisible par 7.

Exercice 8

Déterminer les entiers n tel que $72n^5 - 95n^3 + 3n$ est divisible par 5.

Exercice 9

Soit $p \in \mathcal{P}$ tel que $p > 2$. Montrer que s'il existe $k \in \mathbb{N}$ tel que $k^2 \equiv_p -1$ alors $p \equiv_4 1$.

Exercice 10

Calculer $v_2(2^{100} + 2^{200})$.

Exercice 11

Calculer $v_7(100!)$.

Exercice 12

Déterminer le nombre de 0 à droite dans l'écriture décimale de $10!$. Même question avec $100!$

Exercice 13

Soient $a \in \mathbb{N}_{>0}$ et $p \in \mathcal{P}$. Montrer la propriété suivante : $p|a^2 \Rightarrow p|a$

Exercice 14

Soient a et b des entiers non nul. Montrer la proposition suivante : $a^2|b^2 \Rightarrow a|b$

Exercice 15

Montrer que pour tout entier $n \in \mathbb{N}_{>0}$, $v_2(n!) \leqslant n$.

Exercice 16

Soient 111 nombres relatifs de somme nulle. Montrer que la somme de leur puissance 37-ième est divisible par 399.

Bases

Exercice 17

Convertir en décimal.

1. $(10110)_2$
2. $(1201)_3$
3. $(3021)_4$
4. $(444)_5$
5. $(555)_6$
6. $(666)_7$
7. $(765)_8$
8. $(45A0D)_{16}$

Exercice 18

Convertir les entiers n en base b.

1. $n = 12$, $b = 2$
2. $n = 12$, $b = 8$
3. $n = 12$, $b = 16$
4. $n = 987$, $b = 7$
5. $n = 150$, $b = 150$
6. $n = (A8)_{16}$, $b = 11$
7. $n = (754)_8$, $b = 16$
8. $n = (94E)_{16}$, $b = 8$

Exercice 19

Déterminer tous les entiers $b \in \mathbb{N}_{>0}$, tel que $((11)_b)^2 - (111_b) = 5$.

Exercice 20

On a $341 = (2331)_a$. Déterminer a.

Exercice 21

Déterminer les entiers x, y et z tels que $(xyz)_7 = (zyx)_{11}$

Exercice 22

Déterminer la base a du système de numération dans laquelle on a l'égalité $(46)_a + (53)_a = (132)_a$.

Exercice 23

Déterminer la base a du système de numération dans laquelle on a l'égalité $(31)_a \times (13)_a = (443)_a$.

Exercice 24

Déterminer a et b pour que le nombre qui s'écrit $(aabb)_{10}$ soit un carré.

Exercice 25

1. Vérifier que 123448 est divisible par 13. Si on fait passer le premier chiffre en dernière position, on obtient le nombre 234481. Vérifier que ce nombre est divisible par 13.
2. De manière générale, prouver qu'en déplaçant le premier chiffre en dernière position dans l'écriture décimal d'un nombre à 6 chiffres divisible par 13, on obtient un nombre également divisible par 13.

Exercice 26

Soit $a \geqslant 2$. On considère les nombres $N = 2(a-1)$ et $P = (a-1)^2$. Montrer que N et P s'écrivent avec les mêmes chiffres dans l'ordre inverse en base a.

Exercice 27

(Olympiade de mathématiques - Ibéroamérique - 1994)

Un entier $n > 0$ est dit *Brésilien* s'il existe une base $b < n-1$ tel que n s'écrit en base b avec le même symbole. Montrer que 1994 est brésilien mais pas 1993.

Exercice 28

Existe-t-il deux puissances de 2 distinct tel que leur écriture en base 10 soient composé des mêmes chiffres (avec le même nombre de répétition). On pourra regarder modulo 9.

Exercice 29

(Crux Mathematicorum)

Déterminer tous les nombres premiers p tel qu'il existe une base $b > 1$ dans laquelle l'écriture de p utilise une et une seule fois tous les chiffres (le 0 pouvant être à gauche). On pourra regarder p modulo $b-1$ si b est paire et p modulo $\dfrac{b-1}{2}$ sinon ; on rappel que la somme des entiers entre 0 et $b-1$ vaut $\dfrac{b(b-1)}{2}$.

RSA

Exercice 30

Appliquer la méthode du crible d'Eratosthène et entourer les nombres premiers de la liste suivante.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Exercice 31

Compléter le tableau suivant sachant que $p < q$ sont deux nombres premiers, $n = pq$, $\varphi = (p-1)(q-1)$ et e et d sont des nombres premiers à φ inverse l'un de l'autre.

p	q	n	φ	e	d
3	13			11	
7	41			13	
139	101				43
2		202			19
		77		47	
		437			23
			32	7	
			16		5
		3599	3480	1001	
		1341517	1339200		433

Exercice 32

Calculer les nombres suivants.

1. 71^{21} modulo 65
2. 33^{19} modulo 130
3. 123^{43} modulo 98
4. 301^{17} modulo 59
5. 1000^{55} modulo 99
6. 2^{666} modulo 2015

Exercice 33

On considère dans le système RSA, la clef publique $(1763, 929)$.

1. Déterminer deux entiers p et q tel que $p < q$ et $1763 = pq$.
2. Justifier que $(1763, 929)$ est une clef publique valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 929 en binaire.
   (b) Calculer 18^{929} modulo 1763.
   (c) Quel est le message chiffré de $M = 18$.
4. Déterminer la clef privé associée à la clef publique $(1763, 929)$.

5. Déchiffrer le message $M' = 884$

Exercice 34

On considère dans le système RSA, la clef publique $(1189, 1031)$.

1. Déterminer deux entiers p et q tel que $p < q$ et $1189 = pq$.
2. Justifier que $(1189, 1031)$ est une clef publique valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 1031 en binaire.
   (b) Calculer 44^{1031} modulo 1189.
   (c) Quel est le message chiffré de $M = 44$.
4. Déterminer la clef privé associée à la clef publique $(1189, 1031)$.
5. Déchiffrer le message $M' = 583$

Exercice 35

Chiffrer le message suivant en RSA par la clef publique $(4559, 1705)$: CHIFFREMENTRSA.

Exercice 36

Déchiffrer le message suivant chiffrer en RSA de clef publique $(2047, 1931)$ et de clef privée inconnue :
$1141 - 2 - 1878 - 425 - 128 - 64 - 64 - 2 - 1434 - 1516 - 64 - 19 - 128 - 64$.

Exercice 37

Déchiffrer le message suivant chiffrer en RSA de clef publique $(444931, 97919)$ et de clef privée inconnue :
$32755 - 394934 - 234962 - 412077 - 169502 - 187788 - 83769$