100.—

a) Montrer que $365 \equiv 1 \bmod 7$.

b) Montrer que $18 \equiv -17 \bmod 7$.

101. Déterminer si 17 est congru à 5 modulo 6 et si 24 et 14 sont congrus modulo 6.

Rép. $17 \equiv 5 \bmod 6$, $24 \not\equiv 14 \bmod 6$

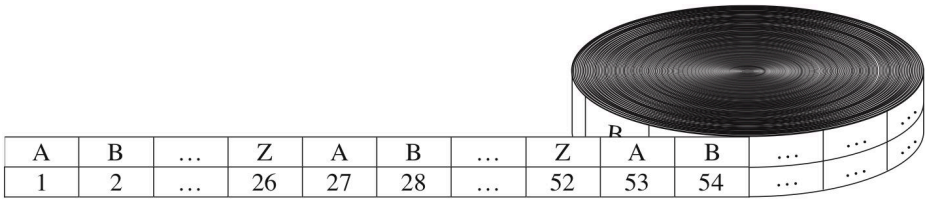
102. Calculer : a) $13 \bmod 3$ b) $155 \bmod 19$ c) $-97 \bmod 11$ d) $-221 \bmod 23$

Rép. 1 ; 3 ; 2 ; 9

103. Un élève qui aime bien les congés le jour de son anniversaire constate qu'en 2008, le 6 décembre tombait un samedi. Comment peut-il savoir, sans trop se fatiguer, si en 2009 puis en 2010 son anniversaire tombera sur un week-end ?

Rép. En 2009 : dimanche ; en 2010 : lundi

104. Imaginons une bande de papier infinie sur laquelle, on place les lettres de l'alphabet dans l'ordre alphabétique puis arrivé à Z, on recommence à A comme le suggère la figure ci-dessous :



A	B	…	Z	A	B	…	Z	A	B	…	…
1	2	…	26	27	28	…	52	53	54	…	…

a) Montrer qu'en 79e position, on retrouvera une lettre A.
b) Quelle sera la lettre située en 212e position ?
c) Quelles seront les positions des huit premières lettres F que nous rencontrerons en déroulant la bande ?

Rép. b) D c) 6, 32, 58, 84, 110, 136, 162, 188

105. Trouver le plus petit nombre supérieur ou égal à 0 qui est congru à a modulo m dans les cas suivants :

a) $a = 3'412,\ m = 4$
b) $a = 177,\ m = 9$
c) $a = 31,\ m = 31$
d) $a = 31,\ m = 25$
e) $a = 365,\ m = 5$
f) $a = -3122,\ m = 3$
g) $a = 31'458'687'312,\ m = 10$
h) $a = -259'874'629,\ m = 10$

Rép. a) 0 b) 6 c) 0 d) 6 e) 0 f) 1 g) 2 h) 1

106. Trouver tous les nombres compris entre 1950 et 2000 qui sont congrus à a modulo m dans les cas suivants :

a) $a = 1$, $m = 13$ b) $a = 1929$, $m = 15$ c) $a = 1776$, $m = 40$

Rép. a) 1951, 1964, 1977, 1990 b) 1959, 1974, 1989 c) 1976

107. Les propositions suivantes sont-elles vraies ?

a) L'égalité $914 = 19 \cdot 47 + 21$ permet de déduire les congruences :
$914 \equiv 21 \bmod 19$ et $914 \equiv 21 \bmod 47$.
b) Tout entier est congru modulo 4 à l'un des nombres 0, 1, 2 ou 3.
c) Si $a \equiv b \bmod n$ et si $b \equiv c \bmod n$ alors $a \equiv c \bmod n$.
d) Si $a \equiv b \bmod n$ et si $a \equiv c \bmod n$ alors $a^2 \equiv bc \bmod n$ et $2a \equiv b + c \bmod n$.

Rép. a) oui b) oui c) oui d) oui

108. Calculer, sans machine :

a) $(73 + 23'525) \bmod 5$ b) $(212 - 414) \bmod 5$
c) $(2342 \cdot 59) \bmod 5$ d) $(143 + 605) \bmod 7$

Rép. a) 3 b) 3 c) 3 d) 6

109. Montrer que si $a \equiv b \bmod n$, alors, pour tout $m \in \mathbb{N}$, $a^m \equiv b^m \bmod n$.

110. Calculer, sans machine :

a) $2^{12} \bmod 13$ b) $17^6 \bmod 5$
c) $8^{36} \bmod 10$ d) $5^{27} \bmod 3$

Rép. 1 ; 4 ; 6 ; 2

111. Montrer que, de trois nombres pairs consécutifs, l'un est un multiple de 3. Idem pour trois nombres impairs consécutifs. *Indication* : travailler modulo 3.

112.—

a) Vérifier que : $18^9 \equiv 9^{18} \bmod 7$.
b) Résoudre l'équation : $18^x \equiv 1 \bmod 7$ $(x \in \mathbb{N})$. *Indication* : travailler modulo 3.

Rép. $S = \{3k \mid k \in \mathbb{N}\}$

113. Quel est le chiffre des unités de 4568^7 ? (sans machine) *Rép.* 2

114. Soient $a, b, d \in \mathbb{Z}$. Démontrer les propositions suivantes :

1. Si $d \mid a$, alors $d \mid ab$
2. Si $d \mid a$ et $d \mid b$, alors $d \mid a \pm b$
3. Si $d \mid a$ et $a \mid b$, alors $d \mid b$

115. Montrer que, pour tout $k \in \mathbb{N}$, $10^k \equiv (-1)^k \mod 11$.

116. Soient $n, a, b \in \mathbb{Z}$. Démontrer que si $n \mid a$ et $n \mid a+b$, alors $n \mid b$.

117. Déterminer le reste de la division de 35^{27} par 7 ; de 89^{35} par 11 ; de 77^{20} par 13.

Rép. 0 ; 1 ; 1

118. Etablir les congruences suivantes :

a) $\left(35^{228} + 84^{501}\right) \equiv 0 \mod 17$

b) $\left(2 \cdot 35^{2008} - 3 \cdot 84^{2010}\right) \equiv 16 \mod 17$

119. *(Critère d'Eratosthène)* Prouver le théorème suivant :

Un naturel $n > 1$ est premier s'il n'est divisible par aucun premier inférieur ou égal à $\sqrt{n}$.

120. 397 est-il un nombre premier ?

121. Trouver le plus grand diviseur commun (pgdc) de $a = 2^7 \cdot 3^2 \cdot 5^6$ et $b = 2^4 \cdot 3^5 \cdot 5^6 \cdot 7$.

Rép. 2'250'000

122. Décomposer a et b en un produit de facteurs premiers. En déduire le plus petit multiple commun m de a et b et leur plus grand diviseur commun d. Vérifier de plus que :

$$\boxed{md = ab}$$

1) $a = 600$; $b = 90$ 2) $a = 10647$; $b = 66885$ 3) $a = 66550$; $b = 7480$

Rép. 1) 1800, 30 2) 2'608'515, 273 3) 4'525'400, 110

123. On pose $A = 101! + 1$. Montrer que les 100 nombres consécutifs $A+1$, $A+2$, … , $A+100$ ne sont pas premiers.

124. Soient a, b, c trois entiers. Montrer que si a ne divise pas bc, alors a ne divise pas b.

125. Démontrer que, pour tout $n \in \mathbb{N}^*$, la fraction $\dfrac{n+1}{n}$ est irréductible.

126. Soit $k \in \mathbb{N}$. Remarquer que 10^k est congru à 1 modulo 3 (resp. 9). En déduire que tout nombre naturel est congru modulo 3 (resp. 9) à la somme des chiffres de son développement décimal.

127. Soit $n \in \mathbb{N}$. Montrer qu'aucun entier de la forme n^3+1 n'est premier, sauf 1^3+1.
Indication : se servir de l'identité $a^3+b^3=(a+b)\left(a^2-ab+b^2\right)$.

128. Démontrer que le produit de quatre nombres consécutifs est divisible par 8.

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
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

200. Chiffre de César, clé +3 :

a) Coder à la main le message suivant : TU QUOQUE MI FILI.
b) Décoder à la main le message suivant : DYHFDHVDUPRULWXULWHVDOXWDQW.

201. Chiffre de César, clé +3 :

a) Coder la phrase suivante : LE CRYPTAGE EST L'ART DE CODER UN MESSAGE.
b) Décrypter : LOHVWWHPSVGHSDVVHUDDXWUHFKRVH.

202. Chiffre de César :

a) Crypter avec la clé $k = 17$: AVE CAESAR MORITURI TE SALUTANT.
b) Sachant que la clé est $k = 12$, décrypter :
XQETAYYQEODAUQZFQZOQCGUXEPQEUDQZF

203. Trouver la clé de ce cryptogramme de César et le décrypter :

ARZDVIRZJDZVLOVKIVCVGIVDZVIUREJLEMZCCRXVHLVCVJVTFEURIFDV

(Utiliser maths-a.com/crypto/frequences.php)

204. Les messages en français ci-dessous ont été cryptés par deux chiffres de César différents. Déterminer le décalage et décryptez-les :

a) QJXXF SLQTY XQTSL XIJXA NTQTS XIJQF ZYTRS J.
b) IXBHC GHPDL QPDWL Q.

205. Combien y a-t-il de substitutions monoalphabétiques (= bijections = permutations) distinctes sur un alphabet de 26 symboles ? Et sur un alphabet de 256 symboles ?

Rép. $403291461126605635584000000$; $\sim 8{,}57817775342842654 \cdot 10^{506}$

206. Quelle est la fonction de chiffrement dans la substitution « Atbash » (cf. brochure p. 3) ? Et celle de déchiffrement ? [On travaille dans $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$.]

207. Décoder ce cryptogramme de César :
(disponible ici : maths-a.com/crypto/cryptogrammes.php, No. 1)

UXKMXMGZRXQGHQUXEMBBQXXQXMYQBAGDCGAUFKQZSMSQEFGFGBQGJQFDQ
NUQZBXGETQGDQGJAQEBDUFEGDEMDUHQDQSMDPQXMDNDQCGUTADEPGFQYBE
EQPDQEEQMGNADPPQOQOAGDMZFXQRXQGHQEQTMFQEMZEEMHAUDHQDEAGXM
DNDQQEFMZODQPMZEXQEAX

Utiliser maths-a.com/crypto/frequences.php.

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
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

208.—

a) Déterminer le chiffrement de Vigenère de MONPREMIERMESSAGE en se servant de la clé BO.
b) Idem pour MONDEUXIEMEMESSAGE et la clé BABAR.
c) Idem pour ETVOICILEDERNIER et la clé MACLEF.

209. BIENVU est la clé de ce cryptogramme de Vigenère :

OMQNIKVMDCVMMMWVOYBZWPMSQBSTMUQPMPV

Le déchiffrer.

210. On sait que le cryptogramme de Vigenère ci-dessous a une clé de 3 lettres. Trouver la clé et décrypter :
GIJNEEBPFOWCJRXNHVNZZJPFIWUZPRPXFHRVWIIXIEOQFIGFZYIYYEZPRIKLZYIHS
EJXFIIKJYKNYWASTVRKZXSGIDZULVRUNSEIICCILMIAZQVNSLQMVIWUZWAJYINE
EXMVIWVONVKPVPVVZXAZQVIZRDWRPZVIXDVYMVMJLYZHIDKSIOIUZGRYICVTR
MIZGECVJVPMCGIDJVKZ (disponible à la page maths-a.com/crypto/cryptogrammes.php, No. 20)

211. le cryptogramme de Vigenère ci-dessous a une clé de 4 lettres. Trouver la clé et décrypter :
SIKHEAMGUSUXFHLBWIKKWOTXKQQXMLMMDOBXJFMESHMKJSMMSWBBFTWKE
SMMNWLXAZGTNOQMVSAMWBMUJSATDOANJTIVWRMESPQFWSBEWGXKAHLXV
WMNKSUHMJIBLOCWWGANKRMLWOCQVWMNVWBJMSTTDIUBWFMLGWBXLZIEM
AQXJSNNLRQXMJQMIIMESZCFASZXWHIBLPWGFSMMVWMNKSXTJOTTDIUBWFMW
SJMVDSAMWBMUJSAWASCTHDMESZIEMAQXJSRHMFMMAZIIHSTTDSAMWBMUJSA
GMWBTABABAZGXMHCGKCQKWHQEQSCMMBUTLWVVWTCMDSXKWAQXJXWNJ
(disponible à la page maths-a.com/crypto/cryptogrammes.php, No. 21)

212. Réduire modulo 7 et 11 :

a) 11233456 b) 58473625 c) 100'000'000'000'000'001

Rép. a) 3 ; 3 b) 0 ; 1 c) 6 ; 0

213. Montrer que tout nombre premier différent de 2 et de 3 est de la forme $6q \pm 1$, avec q entier.
Indication : remarquer que presque tous les nombres congrus à 0, 2, 3 ou 4 modulo 6 sont composés.

214. Montrer que le carré de tout nombre impair est supérieur d'une unité à un multiple de 8.

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
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

215. Soit un texte de n caractères pris dans l'alphabet {A, B, C, … , Z} identifié à $\mathbb{Z}_{26}$. On prend deux caractères au hasard dans ce texte. Calculer la probabilité qu'ils soient identiques, connaissant le nombre n_i d'occurrences de chaque caractère dans le texte : n_i = nombre d'occurrences du caractère numéro i, $i \in \mathbb{Z}_{26}$.

Rép. $\displaystyle\sum_{i=0}^{25} \frac{n_i(n_i-1)}{n(n-1)}$

216. Montrer que, si le nombre de lettres n d'un texte est grand, l'indice de coïncidence $\mathrm{IC} = \displaystyle\sum_{i=0}^{25} \frac{n_i(n_i-1)}{n(n-1)}$ est proche de $\displaystyle\sum_{i=0}^{25} f_i^{\,2}$, où $f_i = n_i / n$ = fréquence de la lettre i.

217. Calculer « à la main » l'indice de coïncidence (IC) de la phrase suivante :

L'INDICE NE COÏNCIDE PAS

Calculer également $\displaystyle\sum_{i=0}^{25} f_i^{\,2}$. [$n$ = nombre de lettres du texte ; n_i = nombre d'occurrences de la lettre numéro i ; $f_i = n_i / n$ = fréquence de la lettre i]

Rép. 0,0842 ; 0,13

218. Calculer l'IC d'un long texte dont toutes les fréquences f_i, $i \in \mathbb{Z}_{26}$, sont égales. (C'est l'IC de la "langue aléatoire".)

Rép. $0{,}0385 \cong 4\,\%$

219. Calculer l'IC d'un long texte dont la moitié des lettres sont des A et dont toutes les autres lettres (B, C, D, … , Z) apparaissent le même nombre de fois.

Rép. 26 %

220. Soit un texte T et soit T' le cryptogramme obtenu en chiffrant T par un décalage de César $x \mapsto x+3$. Montrer que l'IC de T' est égal à l'IC de T.

[Ceci vaut aussi pour toute fonction de chiffrement bijective.]

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
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

230. le cryptogramme de Vigenère ci-dessous a une clé de 5 lettres. Trouver la clé et décrypter :
OEEZXXHVJZTRZKILXFLXXWKMEGMKVUNICRZTRKRKXVVMMXRKZPTPYFQFIUV
XHYKVPTTVZRXULZPLIUFRGIJFYLPVJSEIZCYGIXVRXVRKMHRJVROELEITYKIIOMV
EXXXCRXXVIVWNFJZWMIKFYCSLIWEIJFPXMCJIEIMVPXWFCIBPJVGHYTYIBPJFYIM
IVEIVVJPXPZVYWSLZPLICVZXHVESNZVRYEIMVRMWVUMKMXVZXVJCIFMUZXHYI
EIOIIJPXRFIHIYZJMEXFLVGIVEGHVVVXKIGIIGHCVWFIDVWVMITYBXJKSNWCVWY
PVLZXWMFRMECRQXVVKPTQVIRXWKGSBRKIIFTCZIBPJTSGXZEYXRKREEPVIZXVJ
CIEMVLSNMCJWXHZIMZIEKXHYKVWVLFJILWFEXXRKIEOEZCENHVCEWITVUNSEG
INXUZVXPFVMERVJIKEJJELMVGELHVMSBVVKPHVVZPEIEVWXPRJWXTRJHXRKVR
WVVTIJYZRIMITVWMGVHYBWVIEXXTVUNMJVWMJRZXVIJKGXULZWXJVIEBPEPEK
MVEHXRFLZXELJSNWCVWHPVZP
(disponible à la page maths-a.com/crypto/cryptogrammes.php, No. 22)

231. Décoder ce cryptogramme de Vigenère :
TLZDSOUMUEMDMWXOFQJIPLLGVNVVLPFJMLSJCMKPBSTSRDYMGTIVTAEGCWLX
FTWEQFLVYVBELDCTWTGXUVBJITCMFXFDMFXDFCULFVMFWFJTGRHJDGMMVAG
RFEBWREUIFWMVATSJJTGMOKIARTUMKLBCTSPJJDGMDZXDYTUMEMMCMSRTHC
WPBKZAWUVWHLFCQWTBJAWJBEBGQFSTSRDJCJPFCWFKGCMMZFEWAVWFQUMQ
CCKHFDQDPFRVKUVVASHPLKWJPCQWQVIUMVFJIJSNRVUIBCITVJJMVYTFQJPFMM
FXCRQKITVAKIJEAWXEVXDSJVMFGPIWDPFJMKKSRVVWWFQDITSMJGFJUGPMVU
WRUGIJPFJMSYYCMKWBLTWWGIQKWPEVSRUJXDIVIMFXTLZKSOVXSYMVAMVTF
VYVBELXVPEBJIWVCJWJEKDMOVVLPFJZGWFRCPPFJVWRVGPSVTWZGMTJMKWPL
XAVFEBSYUFCJHFCTWIMCMWZFZTDIQRZXSJJLSRTLVSYOVYMMEFZLUVVTIYFEQ
VHPLAWGIRXHIVEXWXJKNJMTJWFHBZTWYOTPSRUDGKXFIQWYYKWEFFUMKETK
ZWWEFZ
(disponible à la page maths-a.com/crypto/cryptogrammes.php, No. 6)

232. Décoder ce cryptogramme de Vigenère :
BIZRZCVVRRUOWRWSEWSXLDCRDFYEGCEVSXVNCVNBZFSARMSMFJIAREOVFHFX
ZCKBWENHILUREXWNUFGBROMFJZRKFUYNOAASMGMSAMWNGFBRCFYKPWZNA
YVOQRMSXROGGJDYETSRYSLTBBGSIMHVOFJGILSQRCCHVTDERHJCPBTNSHJPWF
XIZWMSRCGYETOHCFYWPBQBFYTVSVUZCJUCHCRYKPWRWHIZGWKNSNCBGVVD
FVNSACGIZT
(disponible à la page maths-a.com/crypto/cryptogrammes.php, No. 7)

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
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

233. Décoder ce cryptogramme de Vigenère :
NCQTAJMEAFTVKHMDHGWLNWJISBBJMFARLWOVUVIHMSNCWIZJWJIGGFMRABA
ZIICEWBKVFGWZJZMJKCVJWHTVKDIIXIUJLCCIFSVKVOVJDOQIVIAFAFDRDGMDWZ
IEUCTZIIMVLZIEYCCIWIFMWFBZYSKYSECVXZMLJGMMSDWIWOQEKWYLMBMEUS
VJGWZCWJQFDCVWJSUZLQWDESCEUCMLJECFFONWDWOVNOTJWAMCSBKFDWYL
WSBCSBOFMFMLPJMILWOVDSKZWZMJLHZZKHMVLPMRMQWDESCEYFIEVFMGGG
WZJZMMACTFFTZVEWBTGAUVMBKFWIZHMCVRXTTZYSCEUCMLJHMEVFMHMWP
RAHTVFSIELJIJLSMKFCQIDSKZWZMJLHZZKHMVLPMRMQWDESCEYFIEVFMGGGWZ
JZMJGZMZDGMJLBWPWRIEKGWEKOVXIIQJWTQXWIVTGSCILSVUJSYLAVIZLZMEW
OVKNOAKWSBEGWZUMDIJKSTLEWVVMLZVUIMZDZMKGIBMWGBZYSTVKCTVAZA
VKHVFQSLRFGAFFGIEYECZKSNZYSBFFGWLNSVZJSVDGWTLAHKFEAMLFCAKWBA
FAF
(disponible à la page maths-a.com/crypto/cryptogrammes.php, No. 5)

240. Soit $k \in \mathbb{N}$. Monter que 10^k est congru à ± 1 modulo 11. En déduire que tout nombre naturel est congru modulo 11 à la *somme alternée* des chiffres de sa figuration décimale. Plus précisément, si la figuration décimale de $x \in \mathbb{N}$ est $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, alors x est congru modulo 11 à $a_0 - a_1 + a_2 - a_3 + a_4 - \ldots$. Enoncer un critère de divisibilité par 11.

241. Soient $a, b, c \in \mathbb{Z}$.

a) Montrer que si a et b sont impairs, $a^2 + b^2 \equiv 2 \bmod 4$.

b) En déduire que l'égalité $a^2 + b^2 = c^2$ est impossible si a et b sont tous deux impairs.
Indication : examiner les 4 possibilités modulo 4 pour c.

242. Si n est un nombre entier dont le carré est pair, montrer que n est pair.

243. Supposons a impair. Est-il vrai que si $ab \equiv ac \bmod 8$, alors $b \equiv c \bmod 8$?
Indication : que vaut a^2 modulo 8 ?

244. Montrer que $5^k + 6^k \equiv 0 \bmod 11$ pour tout entier impair k.

245. Montrer qu'il est impossible d'écrire $\sqrt{2} = \frac{a}{b}$, avec $a \in \mathbb{N}$, $b \in \mathbb{N}^*$, la fraction $\frac{a}{b}$ étant simplifiée. (On en déduit que $\sqrt{2} \notin \mathbb{Q}$.)

246. Montrer que $6 \cdot 4^n \equiv 6 \bmod 9$ pour tout $n \geq 0$. (Distinguer les cas $n = 0, 1, 2 \bmod 3$.)

300. Calculer à l'aide de l'algorithme d'Euclide le pgcd des nombres a et b :

1) $a = 9999,\ b = 1233$ 2) $a = 12345,\ b = 54321$

Rép. 1) 9 2) 3

301.—

a) Montrer que $\text{pgcd}(a + kb,\ b) = \text{pgcd}(a,\ b)$.

b) Prouver que si $x \equiv y \bmod m$, alors $\text{pgcd}(x, m) = \text{pgcd}(y, m)$.

302. Calculer $\text{pgcd}(486, 249)$ à l'aide de la factorisation première, puis à l'aide de l'algorithme d'Euclide. [*Rép.* 3]

303. Montrer que $\text{pgcd}(n, 0) = n$, quel que soit l'entier naturel n.

304. Déterminer :

a) $\text{pgcd}(72, 39)$ b) $\text{pgcd}(39, 52)$ c) $\text{pgcd}(48, 54)$ d) $\text{pgcd}(60, 45)$

Rép. a) 3 b) 13 c) 6 d) 15

305. Les nombres suivants sont-ils premiers entre eux ?

a) 122 et 49 b) 352 et 33 c) 455 et 186 d) 66542 et 20787

Rép. a) oui b) non c) oui d) oui

306. Calculer :

a) le pgcd de 4539 et 1958 b) le pgcd de 1365 et 558

Rép. a) 89 b) 3

307. Montrer que, pour tout nombre naturel n, les nombres n et $n^2 + 1$ sont premiers entre eux.

308. Si $\text{pgcd}(a, b) = p^3$, où p est premier, que dire de $\text{pgcd}\left(a^2,\ b^2\right)$?

309. Au moyen de l'algorithme d'Euclide étendu, déterminer $d = \text{pgcd}(a, b)$ ainsi que deux entiers α et β tels que $\alpha a + \beta b = d$:

1) $a = 4298,\ b = 847$ 2) $a = 24718,\ b = 4879$

Rép. 1) $d = 7,\ \alpha = 27,\ \beta = -137$ 2) $d = 17,\ \alpha = 136,\ \beta = -689$

310. Calculer au moyen de l'algorithme d'Euclide étendu des nombres α et β tels que $\alpha a + \beta b = \text{pgcd}(a, b)$:

1) $a = 72,\ b = 39$ 2) $a = 1008,\ b = 25$
3) $a = 1993,\ b = 210$ 4) $a = 1995,\ b = 323$

Rép. 1) $6a - 11b = 3$ 2) $-3a + 121b = 1$ 3) $-53a + 503b = 1$ 4) $6a - 37b = 19$

311.—

a) En utilisant l'algorithme d'Euclide, déterminer des entiers u et v tels que $383u + 127v = 1$.
b) Qu'en est-il des valeurs $u = 64$ et $v = -193$? et de $u = -317$ et $v = 956$? Qu'en déduisez-vous ?

Rép. a) $(u, v) = (-63, 190)$

312.

a) Trouver des entiers u et v vérifiant $73u + 17v = 1$; en déduire une solution dans $\mathbb{Z}^2$ de l'équation $73x + 17y = 3$.
b) Idem pour $62u + 43v = 1$ et $62x + 43y = 5$.

Rép. a) $(x, y) = (21, -90)$ b) $(x, y) = (-45, 65)$

313. Démontrer à partir du théorème de Bézout que, quels que soient $a, b \in \mathbb{Z}$ et quel que soit le nombre premier p,

si *p* divise *ab*, alors *p* divise *a* ou *p* divise *b*

314. Au moyen du théorème de Bézout, montrer que, quels que soient $a,\ b \in \mathbb{Z}$,

tout diviseur commun de *a* et *b* divise le pgcd de *a* et *b*

315. Montrer que les équations suivantes sont impossibles dans $\mathbb{Z}^2$:

a) $6x + 9y = 17$ b) $42x - 35y = 27$
c) $-832x + 3159y = 92$ d) $23ax - 46by = 23c + 1\ \ (a, b, c \in \mathbb{Z})$

316. On considère l'équation diophantienne $ax + by = c\ \ (a, b, c \in \mathbb{Z}\,;\ a \text{ ou } b \neq 0)$. Démontrer que si $(x_0,\ y_0) \in \mathbb{Z}^2$ est une solution de cette équation et si d est le pgcd de a et b, l'ensemble des solutions est :

$$\left\{ (x, y) \in \mathbb{Z}^2 \;\middle|\; \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + k \begin{pmatrix} b/d \\ -a/d \end{pmatrix},\ k \in \mathbb{Z} \right\}$$

317. Résoudre les équations diophantiennes suivantes :

1) $8x+6y=10$ 2) $8x+6y=9$
3) $226x+51y=1$ 4) $60x+126y=6$

Rép. 1) $\begin{cases} x=2+3k \\ y=-1-4k \end{cases}$ 2) impossible 3) $\begin{cases} x=7+51k \\ y=-31-226k \end{cases}$ 4) $\begin{cases} x=-2+21k \\ y=1-10k \end{cases}$

318. De combien de manières peut-on peser 25 kg de marchandises à l'aide de poids de 2 et de 3 kg ? [*Rép.* de 4 manières]

319. Dans $\mathbb{Z}_{13}$, trouver les inverses de 2, 4, 5 et 7.

Rép. 7, 10, 8, 2

320. Dans $\mathbb{Z}_{25}$, trouver les inverses de 3, 11 et 23.

Rép. 17, 16, 12

321.—

a) Dans $\mathbb{Z}_{12}$, trouver les éléments qui ont un inverse et, pour chacun des éléments trouvés, calculer l'inverse.
b) Idem pour $\mathbb{Z}_{14}$.
c) Idem pour $\mathbb{Z}_{20}$.

Rép. a) $1^{-1}=1$, $5^{-1}=5$, $7^{-1}=7$, $11^{-1}=11$
b) $1^{-1}=1$, $3^{-1}=5$, $5^{-1}=3$, $9^{-1}=11$, $11^{-1}=9$, $13^{-1}=13$
c) $1^{-1}=1$, $3^{-1}=7$, $7^{-1}=3$, $9^{-1}=9$, $11^{-1}=11$, $13^{-1}=17$, $17^{-1}=13$, $19^{-1}=19$

322. Les pièces de 1 franc ont un diamètre de 23 mm, celles de 50 centimes un diamètre de 18 mm. En alignant de telles pièces, peut-on obtenir une longueur de 1 m ? Si oui, quelle la solution la plus économique ?

Rép. 2 p. de 1 fr. et 53 p. de 50 c. / 20 p. de 1 fr. et 30 p. de 50 c. / 38 p. de 1 fr. et 7 p. de 50 c. ; la première solution est la plus économique

323. Résoudre dans $\mathbb{Z}$ les équations suivantes :

a) $12x \equiv 5 \bmod 25$ b) $12x \equiv 5 \bmod 36$ c) $12x \equiv 5 \bmod 47$
d) $12x \equiv 5 \bmod 24$ e) $313x \equiv 1 \bmod 543$ f) $7x \equiv 1 \bmod 215$

Rép. a) $x=15+25k$ b) impossible c) $x=20+47k$
d) impossible e) $x=229+543k$ f) $x=123+215k$

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
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

324.—

a) Crypter le message LE ROI EST MORT à l'aide de la fonction affine $f : x \mapsto 3x + 5$.
b) Idem pour le message ALEA JACTA EST et fonction affine $f : x \mapsto 7x + 3$.

Rép. a) MREVDRHKPVEK b) DCFDODRGDFZG

325.—

a) Crypter la phrase "C'est un trou de verdure où chante une rivière" avec la clé affine $(7 ; 9)$.
b) Quelle est la clé de déchiffrement ?

Rép. a) XLFMTWMYDTELALYETYLDTXGJWMLTWLYNANLYL b) $(15 ; 21)$

326. On considère le cryptage affine $y = 11x + 22$. Déterminer la clé de décryptage.

Rép. $(19 ; 24)$

327. Montrer que le choix $a = 13$ dans un codage $y = ax + b$ induit que toutes les lettres ayant un équivalent numérique pair sont codées de la même façon. Idem si l'équivalent numérique est impair.

328. *(Des vaches et des cochons)* A farmer bought a number of cows at $ 80 each, and a number of pigs at $ 50 each. His bill was $ 810. How many cows and how many pigs did he buy ?

Rép. 7 cows and 5 pigs or 2 cows and 13 pigs

329. Dans un chiffrement affine, on sait que ES est codé BH. Trouver les deux clés $(a ; b)$ possibles. Quel est le défaut de l'une des clés ?

Rép. $(6 ; 3)$ ou $(19 ; 3)$

330. Déchiffrer cette épitaphe célèbre : (cryptage affine)

RKIIKXFIUCIEYFUAHYKCLYRUIYBMURPKXFYEYIOCYDOCYIZYLIFLKEYIRKLCXYA
KMXIKZKXFYZUXFFYVKMLYEUXXKMFLYKOCYDKSYMDYIFAULFBYIJUCLIKIIYNX
UAHLYCTOCYDCMEUARFKDYIULFDYIMTMYAYAKLOCKDYFYARIBYIUXYXVKXEY
DYBUCNMYAYVCFRLMIRKLIUXKBUDYIEYXEYBYIIYRFRKLFIBYIKZMYCXYYXEUL
YIYEUCDKRCMIIYFKXFAKLMYIKVYAAYDCMBUXXKEMXOKXIKRLYICXVMDIOCM
BCBYIFMXIYZYLYLYECFBYJUCLIPYDKIBYCTVUMIAUMXIOCYIUXRYLYBYOCKFLY
KXIBKXIDYIRDYCLIEYDCMEMICLZYECFBMIFCIKMIEUARFYLKOCYDKSYMDAUCL
CF (Cryptogramme No. 30, disponible ici : maths-a.com/crypto/cryptogrammes.php)

331. Donner les valeurs de $\varphi(n)$ pour $1 \leq n \leq 12$.

Rép. $1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4$

332. Calculer $\varphi(n)$ dans les cas suivants :

a) $n = 16,\ n = 32$
b) $n = 3,\ n = 9,\ n = 27,\ n = 81$
c) $n = 75,\ n = 4027$
d) $n = 4087$

Rép. a) $8, 16$ b) $2, 6, 18, 54$ c) $40, 4026$ d) 3960

333. *(Des chiens et des rats)* Un petit boutiquier de Canton achète un certain nombre de petits chiots bien gras et un nombre de paires de rats égal à la moitié du nombre de chiots. Il paie deux francs pour un chiot et le même prix pour un couple de rats. Puis il vend les animaux dix pour cent plus cher. Quand le marchand chinois les a tous vendus, sauf sept, il s'aperçoit qu'il a récupéré une somme d'argent égale à celle qu'il avait dépensée pour acheter les animaux. Combien lui reste-t-il de chiots et de rats ?

Rép. 5 chiots et 2 rats

334. On sait que Roméo a envoyé à Juliette le message crypté suivant :

ZXTHAWBNJQBDQIEZMBJOHADRDQIIZB

Habituellement, Roméo se sert de la langue anglaise et du chiffrement affine $y = 19x + 3$.
Déchiffrer le message.

335. Résoudre dans $\mathbb{Z}$ le système :

$$\begin{cases} x \equiv 5 \bmod 8 \\ x \equiv 3 \bmod 7 \end{cases}$$

Rép. $x = 45 + 56k$

336. Déterminer : a) $\varphi(100)$ b) $\varphi(1001)$ c) $\varphi(10!)$

Rép. $40, 720, 829440$

337. Montrer que pour tout entier positif n, $\varphi(2n) = \begin{cases} \varphi(n) \text{ si } n \text{ est impair} \\ 2\varphi(n) \text{ si } n \text{ est pair} \end{cases}$.

338. Pour quelles valeurs de b est-il vrai que si $ab \equiv 10b \bmod 25$, alors $a \equiv 10 \bmod 25$?

Rép. $b \neq 5k$

400. *(Exponentiation rapide)* Si n est un nombre naturel, la n-ième puissance d'un nombre a est, par définition, le produit de n facteurs égaux à a. Ainsi, d'après cette définition, le calcul de a^n nécessite $n-1$ multiplications. On peut cependant obtenir le même résultat en effectuant moins d'opérations. Voici à titre d'exemple l'évaluation de a^{35} :

• On écrit l'exposant n comme une somme de puissance de 2. Ici, $35 = 32 + 2 + 1$;

• on calcule ensuite les puissances paires de a : $a^2 = aa$, $a^4 = a^2a^2$, $a^8 = a^4a^4$, $a^{16} = a^8a^8$, $a^{32} = a^{16}a^{16}$;

• on multiplie pour terminer les « bons » carrés : $a^{35} = a^{32}a^2a^1$. Le nombre de multiplications nécessaires est dans ce cas de 7, au lieu de 34.

a) Combien de multiplications nécessite cet algorithme pour calculer a^{10} ? a^{61} ?

b) Calculer $835^{25} \bmod 1073$, en 6 multiplications.

Rép. a) 4 ; 9 b) 136

401. Calculer : a) $5^{18} \bmod 7$ b) $68^{105} \bmod 13$ c) $6^{47} \bmod 12$

Rép. a) 1 b) 1 c) 0

402. Chiffrer et déchiffrer le message $m = 8$ à l'aide du système RSA, avec $p = 7$, $q = 11$ et $e = 17$.

Rép. $c = 57$

403. Connaissant la clef publique (n, e) d'un individu, déterminer la clef privée d dans les cas suivants :

a) $(n, e) = (1073, 115)$ b) $(n, e) = (1073, 117)$ c) $(n, e) = (111, 31)$

d) $(n, e) = (117, 17)$ e) $(n, e) = (105, 13)$ f) $(n, e) = (10001, 187)$

Rép. a) 859 b) $\varnothing$ c) 7 f) $\varnothing$

d) $e^{-1} \equiv 17 \bmod \varphi(n)$, mais 117 n'est pas le produit de deux premiers

e) $e^{-1} \equiv 37 \bmod \varphi(n)$, mais 105 n'est pas le produit de deux premiers

404. Votre professeur envoie votre moyenne au secrétariat via un courriel crypté en RSA. La clé publique du secrétariat est $(n, e) = (55, 7)$ et le message crypté envoyé est 25. Quelle est votre moyenne ? [*Rép.* 5]

405.—

a) Crypter lettre par lettre le message OUI (= 14 20 08) avec la clé RSA $(n, e) = (253, 3)$.

b) Trouver la clé de déchiffrement d et déchiffrer le cryptogramme obtenu en a).

Rép. a) 214 157 006 b) $d = 147$

406. Un ennemi intercepte le message chiffré $c = 10$, dont le destinataire possède la clef publique $(n, e) = (35, 5)$. Quel est le texte clair m ?

Rép. $m = 5$

407. Démontrer le petit théorème de Fermat : si p est premier et si a est non nul modulo p, alors $a^{p-1} \equiv 1 \mod p$.

408. Calculer $1001^{1290} \mod 1291$.

409. Calculer $2^{1728} \mod 1729$.

410. Calculer :

a) $5^{51} \mod 97$ b) $11^{22} \mod 167$ c) $123456789^{987654} \mod 11$

Rép. a) 69 b) 7 c) 9

411. Un système RSA a pour paramètres $p = 97$ et $q = 109$. Parmi les nombres ci-dessous, lesquels peuvent-ils être choisis comme clé publique d'encryptage ?

a) $e = 123$ b) $e = 865$ c) $e = 169$

Rép. 865 et 169

412. Déterminer la représentation décimale des entiers suivants :

a) $(5, 21, 3)_{26}$ b) $(6, 0, 5)_7$ c) $(1, 0, 0, 1, 1)_2$ d) $(1, 0, 25, 12)_{26}$
e) $(1, 1, 1, 1, 1, 1)_2$ f) $(25, 25, 25)_{26}$ g) $(255, 255, 255)_{256}$ h) $(1, 14, 15, 0)_{16}$

Rép. a) 3929 b) 299 c) 19 d) 18238 e) 63 f) 17575 g) 16777215 h) 7920

413. Déterminer la représentation en base b de l'entier x :

a) $x = 8436$; $b = 16$ b) $x = 73463$; $b = 26$
c) $x = 141$; $b = 2$ d) $x = 5489$; $b = 26$

Rép. a) $(2, 0, 15, 4)_{16}$ b) $(4, 4, 17, 13)_{26}$ c) $(1, 0, 0, 0, 1, 1, 0, 1)_2$ d) $(8, 3, 3)_{26}$

414. Déterminer le nombre de chiffres décimaux du plus grand nombre binaire de 256 bits. Qu'en est-il pour des nombres binaires de 512 bits, 1024 bits et 2048 bits ?

Rép. 78, 155, 309, 617

415. A partir d'un alphabet de 26 lettres, combien peut-on former de digrammes ? Et combien de trigrammes, de tétragrammes, de k-grammes ?

Rép. $676, 17'576, 456'976, 26^k$

416. Représenter les k-grammes suivants en base 26, puis en base 10 :
[*Exemple* : CRY $\leftrightarrow (2, 17, 8)_{26} \leftrightarrow 2 \cdot 26^2 + 17 \cdot 26 + 8 = 1802$.]

a) OH b) JIM c) ZAZA d) BEAUTE

Rép. $371, 6304, 440'050, 13'723'298$

417. Convertir les entiers suivants en base 26, puis en k-grammes :
[*Exemple* : $784 \leftrightarrow (1, 4, 4)_{26} \leftrightarrow$ BEE.]

a) $207'198$ $(k = 4)$ b) $56'459'810$ $(k = 6)$ c) $5'171'601$ $(k = 5)$ d) $783'114$ $(k = 6)$

Rép. LUNE, ETOILE, LIGHT, ABSOLU

418. On utilise le code alphabétique standard et le système RSA de clé publique $(n, e) = (46'927, 39'423)$.

a) Vérifier que l'on peut chiffrer des messages par trigrammes.
b) Montrer que le message YES est chiffré en BFIC.
c) A partir de BFIC, retrouver YES.

419.—

a) Coder le message JETAIME selon la clé publique $(n, e) = (2077, 19)$.
[Comme $26^2 < 2077 < 26^3$, il faut crypter par blocs de deux lettres.]
b) Retrouver la clé privée d puis contrôler que le déchiffrement redonne JETAIME.

Rép. a) CAZ CIF ATO CVP b) $d = 1459$

420. Dans un système RSA où $n = 77'075'627$, de quelle longueur faut-il choisir les blocs à encrypter si l'on utilise le code alphabétique standard ?

Rép. blocs de longueur 5

421. Dans un système RSA on connaît $p = 97$, $q = 167$ et $e = 797$. On a reçu le message chiffré HCE. Déchiffrez-le. (Le code alphabétique est le code standard.)

Rép. NO

422. Le cryptogramme BOTDTICBYJ est reçu par une personne dont la clé publique RSA est $(n, e) = (10'765'283, 11)$.

a) Montrer que $d = 1'956'131$. On donne la factorisation première de n : $3203 \cdot 3361$.
b) Déchiffrer le message.
c) Déchiffrer le message EGSIOXEWXGDPXMA.

Rép. b) FINISHED c) GIVE ME A BREAK

423. Soit $m = 1234\ 5678\ 9098\ 7654$ le numéro d'une carte de crédit.

a) Crypter m avec la clé RSA $(n, e) = (51'201'345'568'138'081'747, 158'792'633)$.
b) Vérifier que la clé $d = 39'115'303'732'664'896'793$ permet de retrouver le numéro m.

Rép. a) $c = 29'702'459'841'482'412'081$

424. Le numéro d'une carte de crédit a été crypté 02136084940035301413 via la clé publique $(n, e) = (10231, 167)$. Retrouver le numéro.

Rép. 2324 7444 8756 0003