1. *Congruence*

E.24 On note $\overline{abcd}=1000\cdot a+100\cdot b+10\cdot c+d$ l'écriture d'un entier en base dix dont les chiffres sont a, b, c et d.

1 a Déterminer le reste de la division euclidienne de 100 par 11, puis de 1000 par 11.

b Montrer que si un nombre entier n vérifie :
$n \equiv 10 \pmod{11}$
alors on peut aussi écrire : $n \equiv -1 \pmod{11}$

c En déduire que si $\overline{abcd}$ est divisible par 11 alors $-a+b-c+d$ est aussi divisible par 11.

2 a Les entiers du type $\overline{abba}$ sont-ils divisibles par 11?

b Pour quelle valeur de a, l'entier $\overline{1a1}$ est-il divisible par 11?

c Pour quelle valeur de a, l'entier $\overline{9a9}$ est-il divisible par 11?

3 À quelles conditions les entiers du type $\overline{aab}$ sont-ils divisibles par 11?

E.20 Le but de cet exercice est de démontrer que, pour tout entier naturel n non nul, l'entier $A=n\cdot(n^2-1)$ est un multiple de 6.

1 Dans chacun des cas suivants, calculer A et déterminer le reste dans la division euclidienne de A par 6.

a $n=5$ b $n=16$ c $n=32$

2 On suppose maintenant que le reste de la division euclidienne de n par 6 est 5 ; on peut donc écrire :
$n \equiv 5 \pmod{6}$.

a Que peut-on en conclure pour $(n-1)$ et $(n+1)$?

b Quel est le reste de la division euclidienne de (n^2-1) par 6 ?

c Justifier alors que $n(n^2-1)$ est un multiple de 6.

3 Recopier et compléter le tableau :

Reste de la division de n par 6	Reste de la division de $(n-1)$ par 6	Reste de la division de $(n+1)$ par 6	Reste de la division de (n^2-1) par 6	Reste de la division de $n(n^2-1)$ par 6
0				
1				
2				
3	2	4	2	0
4				
5				

4 Conclure.

E.27

1 a Trouver les plus petits entiers naturels a, b, c vérifiant :
$100 \equiv a \pmod{4}$; $27 \equiv b \pmod{4}$; $95 \equiv c \pmod{4}$

b En déduire le reste de la division euclidienne 27×100 par 4.
Puis, le reste de 2 795 par 4.

2 a Calculer le reste de la division euclidienne de 10, 100, 1000 par 9.

b En déduire les plus petits entiers naturels a, b, c vérifiant :
$3\times1000 \equiv a \pmod{9}$; $7\times100 \equiv b \pmod{9}$; $8\times10 \equiv c \pmod{9}$

c Donner le reste de la division euclidienne de 3 785 par 9.

3 a En utilisant une méthode équivalente à celle de la question 2, donner les plus petits entiers naturels a et b vérifiant :
$318 \equiv a \pmod{9}$; $1\,203\,631 \equiv b \pmod{9}$

b En utilisant les propriétés de conservation de la congruence, montrer que le calcul ci-dessous est faux :
$3\,785\times318 = 1\,203\,631$

E.23 Le but de l'exercice est de prouver pour les entiers à quatre chiffres, le critère de divisibilité : "Un entier est divisible par 3 si et seulement si la somme de ses chiffres est elle-même divisible par 3".

1 Un exemple :

a Pour un entier naturel n, que signifie la phrase "n *est congru à 1 modulo 3*"?
Traduire à l'aide d'une congruence "n est divisible par 3".

b Pour chacun des entiers suivants, donner l'entier positif le plus petit auquel il est congru modulo 3 : 10, 100, 1000, 10^p où est un entier positif.

c Déterminer le plus petit entier, positif auquel est congru l'entier 4520 modulo 3. On remarquera que :
$4520 = 4\times1000 + 5\times100 + 2\times10$.

2 Quelques généralisations :
On considère un entier N à quatre chiffres, quatre entiers a, b, c et d entre 0 et 9 tels que $a\neq0$ et :
$N = 1000\cdot a + 100\cdot b + 10\cdot c + d$.
Le chiffre des unités est d, celui des dizaines est c, des centaines b et des milliers a.

a Montrer que : $N \equiv a+b+c+d$ modulo 3.

b Justifier, pour les entiers à quatre chiffres, le critère de divisibilité par 3, énoncé au début de l'exercice.

c Énoncer un critère analogue de divisibilité par 9 et le démontrer pour les entiers à quatre chiffres.

E.1851 Le code barre à 13 chiffres ou EAN 13 *(European Article Number)* est un code constitué de 13 chiffres compris entre 0 et 9, utilisé pour classifier les produits de la grande distribution :

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}$$

On calcule :

$$S = a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + a_{13}$$

Le code est accepté lorsque : $S \equiv 0 \pmod{10}$.
Il est refusé sinon.

1. En pratique.
   On considère le code $A = 9\,780\,130\,515\,186$.
   a. Vérifier que A est accepté.
   b. Au lieu du code A, on a saisi le code $B = 9\,770\,130\,515\,186$ en commettant une erreur sur le troisième chiffre. Montrer que le code B est refusé.
   c. Lors de la saisie du code A, deux chiffres voisins ont été permutés.
   Le code $C = 9\,780\,135\,015\,186$ est-il accepté ou refusé?
   Le code $D = 9\,780\,130\,155\,186$ est-il accepté ou refusé?
2. Effet d'une erreur de saisie sur le quatrième chiffre.
   a. On désigne par E le code $9\,78n\,130\,515\,186$ où n représente un chiffre. Si $n = 0$, on retrouve le code A donc E est accepté.
   Déterminer toutes les valeurs de n pour lesquelles E est accepté.
   b. En déduire qu'une erreur de saisie sur le quatrième chiffre du code A est toujours détectée.

E.11 Le célèbre tableau de DAVID : "Le sacre de Napoléon" immortalise l'événement du 2 décembre 1804.
Sur la période considérée, toutes les années dont le millésime est multiple de 4 sont bissextiles, sauf l'année 1900.

Considérons le 2 décembre 1804 comme le jour de rang 1

1. a. Combien y a-t-il d'années dont le millésime est compris entre 1805 *(inclus)* et 2003 *(inclus)* ?
   b. Parmi ces années, montrer qu'il y a 48 années bissextiles
2. Prouver que le rang du 1er janvier 2004 est 72 714.
3. Déterminer l'entier a compris entre 0 et 6 inclus tel que :
   $72\,714 = a \pmod{7}$.
4. Sachant que le 1er janvier 2004 était un jeudi, recopier et compléter le tableau suivant où k désigne un nombre entier.

Rang du jour	$7k$	$7k+1$	$7k+2$	$7k+3$	$7k+4$	$7k+5$	$7k+6$
Jour de la semaine							

5. Quel jour de la semaine, Napoléon 1er a-t-il été sacré empereur?

E.19 Les questions 1 et 2 sont indépendantes.

1. On considère deux nombres entiers naturels a et b tel que :
   - a est congru à 10 modulo 23
   - b est congru à 15 modulo 23

   a. Déterminer le plus petit nombre entier naturel congru à $(a+b)$ modulo 23.
   b. Déterminer le plus petit nombre entier naturel congru à $a \cdot b$ modulo 23.
2. a. Déterminer le plus petit nombre entier naturel congru à 1000 modulo 111
   b. Montrer que pour tout nombre entier naturel n, $1000n$ est congru à n modulo 111.
   En déduire que le nombre 10^8+10^4+1 est divisible par 111.

E.2 Une horloge électronique a été programmée pour émettre un bip toutes les sept heures. Le premier bip est émis le 31 décembre à minuit.

1. a. À quelle heure est émis le dernier bip du 1er janvier 2005?
   b. À quelle heure est émis le premier bip du 2 janvier 2005?
   c. À quelle heure est émis le dernier bip du 2 janvier 2005?
   d. À quelle heure est émis le premier bip du 3 janvier 2005?

   Expliquer les réponses.
2. a. Montrer que : $24 \equiv 3 \pmod{7}$
   b. En déduire le reste de la division euclidienne de 2×24 par 7 et le reste de la division euclidienne de 3×24 par 7. Justifier les réponses. Reproduire sur la copie et compléter le tableau suivant :

n	1	2	3	4	5	6	7	8	9	10
Reste de la division euclidienne de $n\times24$ par 7				5	1	4	0	3	6	2

   c. Expliquer pourquoi l'horloge émet un bip à minuit tous les 7 jours et tous les 7 jours seulement.
3. On rappelle que l'année 2005 est une année non bissextile et comporte 365 jours.
   a. Déterminer le plus petit entier naturel a tel que :
   $365 \equiv a \pmod{7}$.
   b. À quelle date l'horloge émettra-t-elle un bip à minuit pour la dernière fois en 2005? Expliquer la réponse.

E.18 *Dans cet exercice, on étudie la divisibilité par 11 en exploitant la congruence modulo 11 des puissances de 10.*

1. a) Vérifier que : $100 \equiv 1 \pmod{11}$.
   En déduire que : $10^4 \equiv 1 \pmod{11}$
   b) Vérifier que : $10 \equiv -1 \pmod{11}$.
   En déduire que :
   - $10^3 \equiv -1 \pmod{11}$
   - $10^5 \equiv -1 \pmod{11}$

2. a) En utilisant l'égalité $3729 = 37\times100+29$ et les résultats précédents, montrer que 3729 est divisible par 11.
   b) En utilisant la méthode précédente, étudier la divisibilité de 9 240 par 11.

3. a) En utilisant l'égalité :
   $3729 = 3\times1000 + 7\times100 + 2\times10 + 9$
   et les résultats précédents, montrer que 3 729 est divisible par 11.
   b) En utilisant cette méthode, étudier la divisibilité de 9 240 par 11.

4. Étudier la divisibilité de 197 277 par 11.

E.10

1. Donner le reste de la division euclidienne de 5 par 8.
   Donner le reste de la division euclidienne de 5^2 par 8.

2. Donner le reste de la division euclidienne de 5^{86} par 8.
   Donner le reste de la division euclidienne de 5^{87} par 8.

3. Donner est le reste de la division euclidienne de 965^{87} par 8.

4. Soit n un entier naturel.
   Montrer que $5^{2n+1}+5^{2n}+2$ est un multiple de 8.

E.1 Le code d'identification d'un article est formé de sept chiffres compris entre 0 et 9. Les six premiers chiffres identifient l'article, le septième est une clé de contrôle destinée à déceler une erreur dans l'écriture des six premiers.

On notera $x_1x_2x_3x_4x_5x_6x_7$ un tel code. la clé de contrôle x_7 est le reste de la division euclidienne par 10 de la somme :
$N = (x_1+x_3+x_5)+7(x_2+x_4+x_6)$

1. a) Vérifier que le code suivant est correct : 2 3 4 1 5 4 7
   b) Calculer la clé du code suivant : 9 2 3 4 5 1 •
   c) Un des chiffres du code suivant a été effacé :
   1 1 2 • 7 7 4.
   Le calculer.

2. Dans cette question un des chiffres du code est erroné : au lieu de saisir $x_1x_2x_3x_4x_5x_6x_7$,le dactylographe a frappé $x_1x_2x_3yx_5x_6x_7$
   a) Écrire les sommes N_1 et N_2 associées respectivement aux deux codes précédents puis calculer la différence N_1-N_2
   b) Montrer que l'équation $7a = 0 \pmod{10}$ où a est un entier compris entre 0 et 9, a pour seule solution 0.
   c) L'erreur de frappe sera-t-elle détectée?

3. Dans cette question, deux des chiffres du code ont été intervertis : au lieu de saisir $x_1x_2x_3x_4x_5x_6x_7$, le dactylographe a frappé $x_1x_3x_2x_4x_5x_6x_7$.
   a) Écrire les sommes N_1 et N_2 associées à ces deux codes, puis calculer la différence N_1-N_2.
   b) Donner un exemple de valeurs de x_2 et x_3 pour lesquelles la clé de contrôle ne détecte pas l'erreur.

E.25 *Une année bissextile compte 366 jours et une année non bissextile 365 jours. Une année est bissextile si son "numéro" est divisible par 4 sauf s'il s'agit d'un siècle.*
Les siècles, années dont le "numéro" se termine par deux zéros, ne sont, en général, pas bissextiles sauf si leur "numéro" est divisible par 400.
Quelques exemples : 1996 était bissextile, 1997 ne l'était pas, 1900 non plus, mais 2400 le sera.

1. Trouver les deux entiers naturels a et b inférieurs ou égaux à 6 tels que :

$$365 \equiv a \pmod 7 \quad ; \quad 366 \equiv b \pmod 7.$$

2. a. En supposant que le premier janvier d'une année non bissextile soit un lundi, expliquer pourquoi le premier janvier de l'année suivante sera un mardi.
   b. Si le premier janvier d'une année bissextile est un lundi, quel jour de la semaine sera le premier janvier de l'année suivante?

3. Une période de quatre années consécutives compte :
$N = 3\times365 + 1\times366$.
Sans calculer N, justifier que $N \equiv 5 \pmod 7$.

4. En supposant que le premier janvier d'une année soit un lundi, quel jour de la semaine sera le premier janvier quatre ans plus tard? Expliquer la réponse.
Plus généralement, pour une date donnée, (par exemple le 1er janvier), chaque période de 4 années produit un décalage de cinq jours dans le cycle des jours de la semaine.

5. Compléter le tableau ci-dessous. Aucune justification n'est demandée.

Nombre de périodes de quatre années	J = nombre de jours de décalage dans le cycle des jours de la semaine	Reste de la division de J par 7
0	0	0
1	5	5
2	10	3
3		
4		
5		
6		
7		

6. a. Expliquer pourquoi l'année 2004 est bissextile.
   b. Sachant que le 29 février 2004 était un dimanche, quel jour de la semaine sera le 29 février 2008?
   c. Quelle sera la prochaine année où le 29 février sera un dimanche? Expliquer la réponse.

E.1770 Un entier naturel N s'écrit $\overline{cabc}$ dans e système de numération à base cinq où a, b, c sont non nuls, c'est-à-dire :

$$N = c\times5^3 + a\times5^2 + b\times5 + c$$

où a, b, c sont des entiers tels que :

$$0 < a < 5 \quad ; \quad 0 < b < 5 \quad ; \quad 0 < c < 5$$

Ce même nombre entier N s'écrit $\overline{aba}$ dans le système de numération à base huit.

1. Montrer que $N = 65\cdot a + 8\cdot b$ et en déduire que :
$40\cdot a = 126\cdot c - 3b\cdot$.

2. a. Justifier que $40\cdot a \equiv 0 \pmod 3$. En déduire la valeur de a.
   b. Montrer que $b \equiv 0 \pmod 2$. Déterminer les valeurs de b et c.
   c. Donner l'écriture de l'entier N dans les bases cinq, huit et dix.

E.1989 Le but de cet exercice est de montrer, par deux méthodes différentes, que pour tout nombre entier naturel n, le nombre $n^3+5\cdot n$ est divisible par 6.

Première méthode

1. Montrer que tout nombre entier naturel n est congru, modulo 6, à 0, 1, 2, 3, 4 ou 5.

2. Recopier et compléter le tableau suivant avec des nombres entiers naturels inférieurs ou égaux à 5.

$n \equiv \ldots \pmod 6$	0	1	2	3	4	5
$n^3 \equiv \ldots \pmod 6$						
$5n \equiv \ldots \pmod 6$						
$n^3 + 5n \equiv \ldots \pmod 6$						

3. En déduire que pour tout nombre entier naturel n, le nombre entier n^3+5n est divisible par 6.

Deuxième méthode

1. Montrer que pour tout nombre entier naturel n :

$n\cdot(n+1)$ est pair.

En déduire que pour tout nombre entier naturel n :

$3\cdot n\cdot(n+1)$ est divisible par 6.

2. On admet que :

$$(n+1)^3 + 5\cdot(n+1) = (n^3 + 5\cdot n) + 3\cdot n\cdot(n+1) + 6$$

Montrer que si pour un nombre entier naturel , $n^3+5\cdot n$ est divisible par 6, alors $(n+1)^3+5\cdot(n+1)$ est divisible par 6.

3. Que reste-t-il à vérifier, pour en déduire que $n^3+5\cdot n$ est divisible par 6, pour tout nombre entier naturel n?

2. Congruence et puissance

E.1849

1. a. Déterminer les restes de la division euclidienne par 7 des entiers 3^n pour $n \in \mathbb{N}$: $n \leqslant 6$.
   b. Recopier et compléter le tableau suivant :

Puissance de 3	3^0	3^1	3^2	3^3	3^4	3^5	3^6
Reste modulo 7							

c En déduire que, pour tout $k\in\mathbb{N}$, 3^{6k} est congru à 1 modulo 7.

2 a Déterminer le plus petit entier naturel congru à 1515 modulo 7.

b Après avoir remarqué que $2004=6\times334$, déduire du 1 le reste de la division euclidienne de 1515^{2004} par 7.

c Montrer que dans la division euclidienne de 1515^{2006} par 7 le reste est 2.

E.28

1 a Montrer que 1999 est congru à 4 modulo 7.

b Déterminer le plus petit nombre entier naturel congru à 2007 modulo 7.

2 Soit n un nombre entier naturel congru à 5 modulo 7.

a Déterminer un nombre entier naturel congru à n^3 modulo 7.

b En déduire que (n^3+1) est divisible par 7.

3 Montrer que si n est un nombre entier naturel congru à 4 modulo 7 alors (n^3-1) est divisible par 7.

4 On considère le nombre : $A=1999^3+2007^3$.
Sans calculer A, montrer en utilisant les résultats précédents que A est divisible par 7.

E.7 On considère les entiers :

$A = 8\,387\,592\,115$; $B = 9\,276\,312\,516$

1 a Montrer que 1 000 est divisible par 8.

b Montrer que A est congru à 3 modulo 8.

c Donner l'entier naturel b strictement inférieur à 8 tel que B soit congru à b modulo 8.

2 Déterminer les entiers naturels strictement inférieurs à 8 qui sont congrus respectivement à $A+B$ et à $A\cdot B$ modulo 8.

3 a Montrer que B^2 est divisible par 8.

b Montrer que A^2 n'est pas divisible par 8.

c Montrer que A^{100} n'est pas divisible par 8.

E.8 On considère le nombre entier $A=18^{2002}$.

1 A est divisible par 9? Par 4? *(justifier les réponses)*

2 On cherche à obtenir le reste de la division euclidienne de A par 7, en utilisant des congruences.

a Trouver l'entier r vérifiant : $\begin{cases}0\leqslant r<7\\18=r\pmod 7\end{cases}$

b Quel est le plus petit entier naturel non nul n tel que : $r^n=1\pmod 7$?

c Prouver que pour tout nombre entier naturel k, 4^{3k} est congru à 1 modulo 7.

d En déduire le reste de la division euclidienne de A par 7.

3 Montrer que 2002^{18} est divisible par 13.

E.1769 Pour tout entier $n\geqslant1$, on considère le nombre entier :

11^n+5^n-7

1 a Quel est le reste de 11 dans la division euclidienne par 10?

b Démontrer que, pour tout nombre entier $n\geqslant1$:

$11^n\equiv1\pmod{10}$.

2 Démontrer que, pour tout nombre entier $n\geqslant1$,

$5^n\equiv5\pmod{10}$.

(On pourra utiliser un raisonnement par récurrence ou s'appuyer sur des propriétés de divisibilité)

3 Quel est le chiffre des unités de l'entier $11^{2007}+5^{2007}-7$? Justifier la réponse donnée.

E.1848

1 Montrer que, pour tout $n\in\mathbb{N}$, on a :

$2^{3(n+1)}-1=8\cdot\left(2^{3n}-1\right)+7$.

2 Montrer, à l'aide d'un raisonnement par récurrence que la propriété suivante est vraie pour tout $n\in\mathbb{N}$:

$2^{3n}-1$ est divisible par 7.

E.35

1 Montrer la relation suivante pour $n\in\mathbb{N}$:

$9\cdot\left(9^n-2^n\right)+7\times2^n$

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

3. *Problème de clé de vérification*

E.15 Sur le catalogue d'une entreprise de vente par correspondance, la référence de chaque article d'un nombre à cinq chiffres $x\ y\ z\ t\ u$ *(le premier de ces chiffres x étant différent de zéro)*, suivi d'une lettre majuscule choisie antre A et N, à l'exception de la lettre I.
À cette lettre majuscule est associé un nombre appelé clé selon le tableau suivant :

Lettre	A	B	C	D	E	F	G	H	J	K	L	M	N
Clé	0	1	2	3	4	5	6	7	8	9	10	11	12

À des fins du contrôle, on impose, pour chaque référence, que la somme du nombre à cinq chiffres et de la clef obtenue grâce au tableau, soit un nombre divisible par 13.
Par exemple considérons un article dont la référence est 18 501M. Le nombre à cinq chiffres est 18 501. La clé associée à M est 11 :

$18501+11=18512=13\times1424$.

18512 est divisible par 13, donc cette référence est correcte.

1 Les deux références suivantes sont-elles correctes?

$13587M$; $45905A$

Les réponses doivent être justifiées.

2. On veut retrouver la lettre d'une référence dont il ne reste que le nombre à cinq chiffres 26014.

   a. Montrer que : $13\times2001<26014<13\times2002$.

   b. En déduire la lettre manquante.

3. On veut retrouver un chiffre illisible dans la référence d'un article. Cette référence est $85z29C$ *(z étant le chiffre illisible).*

   a. Montrer que le problème revient à trouver z tel que $0\leqslant z\leqslant 9$ et :
   $$8\times10^4+5\times10^3+z\times10^2+2\times10+9+2\equiv0 \pmod{13}$$
   Cette relation sera notée (E) dans toute la suite.

   b. Recopier et compléter le tableau suivant à l'aide d'entiers naturels compris entre 0 et 12.

   - $10^0\equiv\ldots \pmod{13}$ $\qquad$ $10^1\equiv\ldots \pmod{13}$
   - $10^2\equiv\ldots \pmod{13}$ $\qquad$ $10^3\equiv\ldots \pmod{13}$
   - $10^4\equiv\ldots \pmod{13}$

   c. En utilisant les propriétés des congruences et les résultats obtenus dans le tableau précédent, montrer que le problème revient à trouver z $(0\leqslant z\leqslant 9)$ tel que :
   $$11+9z\equiv \pmod{13}$$

   d. Déterminer le chiffre illisible de la référence. Écrire alors cette référence.

E.9 Dans une entreprise de vente par correspondance, les références des articles sont composées de 6 chiffres et d'une lettre de contrôle afin d'éviter les erreurs de saisie. La position de la lettre dans l'alphabet correspondant au reste de la division de la référence numérique par 26.

Exemple : la référence numérique $123\,456=4748\times26+8$ et la 8e lettre de l'alphabet est H donc la référence de l'article avec sa clé de contrôle est $123\,456\,H$.

1. La référence numérique d'un article est 784 503, déterminer la lettre de contrôle correspondant à cette référence.

2. On considère la référence $\ldots37\,254\,H$ où le premier chiffre a été effacé.

   a. On note n le chiffre manquant ; Vérifier que le nombre vérifie :
   $$n\cdot37\,254=n\times100\,000+37\,254$$

   b. Déterminer le reste de la division de 100 000 par 26, puis de 37 254 par 26.

   c. En déduire que : $4\cdot n+22=8 \pmod{26}$.

   d. Sachant que $1\leqslant n\leqslant9$, déterminer le chiffre manquant de la référence.

E.3 Le numéro I.N.S.E.E. est constitué de 15 chiffres. En lisant de gauche à droite :

- Le premier chiffre est 1 s'il s'agit d'un homme, 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 civil ;
- les deux derniers chiffres 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 clé)* du nombre $I.N.S.E.E.$ de Sophie sont 2 850 786 183 048. On note A ce nombre et r le reste de la division euclidienne de A par 97.

1. Donner le mois de l'année de naissance de Sophie.

2. a. Déterminer les deux entiers a et b tels que :
   $A=a\times10^6+b$ avec $0\leqslant b<10^6$.

   b. En utilisant le reste de 100 dans sa division euclidienne par 97 ; montrer que : $10^6\equiv27 \pmod{97}$

   c. En déduire le reste r de la division euclidienne de A par 97.

3. Déterminer la clé K du numéro I.N.S.E.E. de Sophie.

4. Sophie, à qui l'on demande les **treize** premiers chiffres de son numéro I.N.S.E.E., inverse les deux derniers chiffres et répond 2 850 786 183 084 à la place de 2 850 786 183 048.

   On note B la réponse de Sophie.

   a. Calculer la différence $B-A$ et en déduire que le reste de la division euclidienne de B par 97 est égal à 21.

   b. L'erreur faite par Sophie peut-elle être détectée ?

E.1850 Tous les ouvrages publiés sont identifiés par un numéro ISBN *(International Standard Book Number)* qui indique la langue de publication, l'éditeur et la référence de l'ouvrage chez cet éditeur. Un numéro ISBN est constitué de neuf chiffres *(c'est-à-dire neuf entiers compris entre 0 et 9)* suivis d'une espace et d'une clé. Cette clé est un chiffre ou la lettre X *(le 10 en numérotation romaine)*.

Pour déterminer la clé d'un numéro ISBN dont les neuf premiers chiffres sont $abcdefghi$, on calcule l'entier :

$N = a+2\cdot b+3\cdot c+4\cdot d+5\cdot e+6f\cdot+7\cdot g+8\cdot h+9\cdot i$

puis on déterminer l'entier r compris entre 0 et 10 qui est congru à N modulo 11. Si l'entier r est strictement inférieur à 10, la clé est égale à r ; si l'entier r est égal à 10, la clé est X.

1. Vérifier que la clé du numéro ISBN 190190340 0 est correcte.
2. Calculer la clé du numéro ISBN dont les 9 premiers chiffres sont : 103 241 052.
3. Le quatrième chiffre du numéro ISBN d'un ouvrage est illisible. On le note d.
   La clé de ce numéro est 4 et le numéro se présente ainsi :
   329 d12 560 4.
   a. Montrer que : $4\cdot d \equiv 2 \pmod{11}$.
   b. En déduire le chiffre d.
4. Le premier chiffre et le neuvième chiffre du numéro ISBN d'un ouvrage sont illisibles. On les note a et i. La clé de ce numéro est 9 et le numéro se présente ainsi :
   a32 100 50i.
   a. Montrer que : $a \equiv 2-9\cdot i \pmod{11}$.
   b. Donner deux valeurs possibles du couple $(a\,;i)$.

4. *Codage*

E.21 Les codes secrets des cartes bancaires sont formés de quatre chiffres pris de 0 à 9.

Pierre n'a pas noté celui de sa carte bancaire dans son agenda, mais comme il a peur de l'oublier, il a quand même noté la forme "*cryptée*" de son code secret de façon que son code secret ne soit pas découvert si son agenda était perdu.

Pierre réalise toujours son cryptage de la façon suivante :

- Il choisit deux chiffres a et b, appelés "*clés du cryptage*", qui vont lui servir à tout le cryptage.
- Il remplace chaque chiffre n de son code secret par le chiffre p, appelée forme cryptée de n, qu'il calcule à l'aide de la formule suivante :
  $p \equiv a\times n + b \pmod{10}$

L'objectif de la partie **A** est de retrouver le code secret de la carte bancaire de Pierre, connaissant les clés de cryptage.

L'objectif de la partie **B** est de retrouver les clés de cryptage.

Les parties **A** et **B** sont donc indépendantes.

Partie A

Pierre a choisi ici : $a = 3$; $b = 7$

Alors : $p \equiv 3\times n + 7 \pmod{10}$

Par exemple, la forme cryptée du chiffre 5 sera le chiffre 2.
Car : $3\times 5 + 7 = 22$; $22 \equiv 2 \pmod{10}$

1. Reproduire et compléter la table de cryptage ci-dessous correspondant à la formule de Pierre.

n	0	1	2	3	4	5	6	7	8	9
p				6	9	2			1	

2. Pierre a inscrit 8 5 0 3 dans son agenda qui est la forme cryptée de son code secret, quel est son véritable code secret?

Partie B

Pierre a fait des émules.

Quentin utilise la même formule que Pierre :

$p \equiv a\times n + b \pmod{10}$

Mais en prenant deux autres valeurs de a et b parmi les chiffres de 0 à 9.

Pierre prétend pouvoir déterminer la formule de Quentin *(c'est-à-dire trouver les nombres a et b)*, car ce dernier lui a avoué les formes cryptées de deux chiffres :

- La forme cryptée du chiffre 3 est le chiffre 3.
- La forme cryptée du chiffre 4 est le chiffre 2.

1. Établir que découvrir a et b revient à résoudre le système d'inconnue $(a\,;b)$:

$$\begin{cases} 3a + b \equiv 3 \pmod{10} \\ 4a + b \equiv 2 \pmod{10} \end{cases}$$

où a et b sont des chiffres de 0 à 9.

2. Pierre prétend que le couple $(9\,;6)$ est une solution de ce système. Montrer qu'il a raison

E.17 Les parties I et II sont indépendantes.

Partie I

Nathalie communique avec une amie en fabriquant des messages codés. Chaque lettre de l'alphabet est repérée par son rang x, $1 \leqslant x \leqslant 26$: 1 pour A, 2 pour B, etc...

La lettre de rang x est codée par la lettre de rang y tel que :

$$1 \leqslant y \leqslant 26 \quad ; \quad y \equiv x + 10 \pmod{26}$$

Exemples :

La lettre V a pour rang $x = 22$; on a :

$1 \leqslant y \leqslant 26$; $y \equiv 32 \pmod{26}$

donc $y = 6$. La lettre V est codée par la lettre F.

1. Recopier et dresser le tableau ci-dessous pour toutes les lettres de l'alphabet.

Lettre	A	.....	V	.....
x	1		22	
y	11		6	
Codage	K		F	

2. Retrouver le codage du mot "*ARITHMETIQUE*".
3. Décoder le mot "*OEBY*".

Partie II

1. Remarquant que $999 = 27 \times 37$, démontrer que :

$$10^3 \equiv 1 \pmod{37} \quad ; \quad 10^{30} \equiv 1 \pmod{37}$$

2. Démontrer que, pour tout entier naturel n, on a :

$$10^{3n} \equiv 1 \pmod{37}.$$

3. En déduire que l'entier $N = 10^{10} + 10^{20} + 10^{30}$ est un multiple de 37.
(On pourra remarquer que $10^{10} = 10^9 \times 10$).

E.22 "*La lutte incessante entre concepteurs et briseurs de codes a permis une série de remarquables percées scientifiques. Les concepteurs ont cherché à élaborer des codes toujours plus sophistiqués pour protéger les communications, alors que les décrypteurs imaginaient perpétuellement des méthodes plus performantes pour les attaquer... Leur travail a accéléré le développement technologique, notamment dans le cas de l'ordinateur....*
L'art de communication secrète, aussi appelé cryptographie, fournira à l'âge de l'information ses verrous et ses clefs".

Histoire des codes secrets - **Simon Singh**

Le code ASCII *(American Standard Code for Information Interchange)* en informatique, permet d'associer à chaque caractère *(lettre, signe de ponctuation, chiffre,...)* un nombre entier n, compris entre 0 et 255.

Le tableau ci-dessous donne les codes attribués aux lettres de l'alphabet :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Code ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Code ASCII	78	79	80	81	82	83	84	85	86	87	88	89	90

1 "Chiffrement" à clé utilisant l'arithmétique

Le procédé suivant permet de masquer le mot initial : à chaque nombre n, du Code ASCII correspondant à une lettre donnée, on associe le reste de la division de $7n$ par 256.

Exemple : Codage de la lettre **B**
Code ASCII de la lettre **B** : 66.
Calcul du nouveau code de la lettre **B** :
$7 \times 66 = 462$; $462 = 256 \times 1 + 206$.
Nouveau code de la lettre **B** : 206
Ainsi le mot BONJOUR sera codé :

Mot	B	O	N	J	O	U	R
Code ASCII	66	79	78	74	79	85	82
Nouveau codage	206	41	34	6	41	83	62

Codage du mot CLE

a. Code ASCII de C : 67 ; $7 \times 67 = 469$
Déterminer le reste de la division euclidienne de 469 par 256, en déduire le nouveau code de la lettre C.

b. De la même façon, déterminer le nouveau code de la lettre L, puis de la lettre E, puis de la lettre F, en déduire le codage du mot CLEF.

2 "Déchiffrement" :

Soit x le nouveau code de la lettre à découvrir et n son code ASCII.

a. Justifier que : $x = 7 \cdot n \pmod{256}$

b. En déduire que : $193 \cdot x = n \pmod{256}$.
On admet que n est le reste de la division euclidienne de $183 \cdot x$ par 256.

c. Vérifier que pour $x = 206$, on a bien $n = 66$ qui correspond à la lettre B.

d. Décoder le mot suivant :

206	199	213

E.4 Arthur et Wilson sont deux jumeaux qui ont l'habitude de communiquer à l'aide de messages codés. Ils réalisent toujours leur cryptage de la façon suivante :
Chaque lettre de l'alphabet munie de son numéro d'ordre n est remplacée par la lettre de l'alphabet munie du numéro d'ordre p $(1 \leqslant p \leqslant 26)$ obtenue à l'aide de la formule :

$$p = 3\times n + 7 \pmod{26}$$

Par exemple la forme cryptée de L est Q car :
$3\times 12+7 = 43$ et $43 = 17 \pmod{26}$.

1. Reproduire et compléter la table de cryptage ci-dessous *(aucune justification n'est demandée)*.

lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
p												17		
forme cryptée	J											Q		

lettre	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	15	16	17	18	19	20	21	22	23	24	25	26
p										1		
forme cryptée										A		

2. Arthur a envoyé le message suivant à Wilson : $MIJUZ\ CZRI\ OJ\ IVRLLHOV$.
Retrouver la forme décryptée du message.

3. Wilson désire lui répondre : $MERCI$.
Donner la forme cryptée de ce message.

5. Propriété du pgcd et ppcm

E.3865 Indiquer si la proposition suivante est vraie ou fausse et donner une démonstration de la réponse choisie.

"Il existe un seul couple $(a\,;b)$ de nombres entiers naturels, tel que :
$a<b$; $PPCM(a\,;b)-PGCD(a\,;b)=1$"

E.3866 Indiquer si la proposition suivante est vraie ou fausse et donner une démonstration de la réponse choisie.

"On considère l'équation : (E) : $x^2-52x+480=0$
où x est un entier naturel.
Il existe deux entiers naturels non nuls dont le PGCD et le PPCM sont solutions de l'équation (E)."

E.4118 Soit (U_n) la suite numérique définie par :

$$\begin{cases} U_0 = 0 \\ U_{n+1} = 2\cdot U_n + 1 \quad \text{pour tout } n \in \mathbb{N} \end{cases}$$

1. Montrer que, pour tout entier naturel n, U_{n+1} et U_n sont premiers entre eux.

2. Montrer que pour tout entier naturel n :
$U_n = 2^n - 1$

3. Montrer que, pour tous entiers naturels n et p non nuls tels que $n \geqslant p$:
$U_n = U_p\cdot(U_{n-p}+1) + U_{n-p}$

La notation $\text{pgcd}(a\,;b)$ est utilisée, dans la suite, pour désigner le plus grand diviseur commun à deux entiers naturels a et b.

4. Montrer pour $n \geqslant p$ l'égalité :
$\text{pgcd}(U_n\,;U_p) = \text{pgcd}(U_p\,;U_{n-p})$

5. Soit n et p deux entiers naturels non nuls, montrer que :
$\text{pgcd}(U_n\,;U_p) = U_{\text{pgcd}(n\,;p)}$

Déterminer l'entier : $\text{pgcd}(U_{2005}\,;U_{15})$.

6. Petit théorème de Fermat

E.3192 Le but de l'exercice est d'étudier certaines propriétés de divisibilité de l'entier $4^n - 1$, lorsque n est un entier naturel.

On rappelle la propriété connue sous le nom de petit théorème de Fermat : "*Si p est un nombre entier premier et a un entier naturel premier avec p, alors $a^{p-1}-1\equiv 0 \pmod{p}$*"

Partie A. Quelques exemples.

1. Démontrer que, pour tout entier naturel n, 4^n est congru à 1 modulo 3.

2. Prouver à l'aide du petit théorème de Fermat, que $4^{28}-1$ est divisible par 29.

3. Pour $1 \leqslant n \leqslant 4$, déterminer le reste de la division de 4^n par 17. En déduire que, pour tout entier k, l'entier $4^{4k}-1$ est divisible par 17.

4. Pour quels entiers naturels n l'entier 4^n-1 est-il divisible par 5?

5. À l'aide des questions précédentes, déterminer quatre diviseurs premiers de $4^{28}-1$.

Partie B. Divisibilité par un entier premier

Soit p un entier premier différent de 2.

1. Démontrer qu'il existe un entier $n \geqslant 1$ tel que :
$4^n \equiv 1 \pmod{p}$.

(2) Soit $n \geqslant 1$ un entier naturel tel que $4^n \equiv 1 \pmod{p}$. On note b le plus petit entier strictement positif tel que $4^b \equiv 1 \pmod{p}$ et r le reste de la division euclidienne de n par b :

(a) Démontrer que $4^r \equiv 1 \pmod{p}$. En déduire que $r = 0$.

(b) Prouver l'équivalence : $4^n - 1$ est divisible par p si, et seulement si, n est multiple de b.

(c) En déduire que b divise $p-1$.

E.4275 On rappelle la propriété connue sous le nom de petit théorème de Fermat :

"*Si p est un entier premier et q un entier naturel premier avec p, alors $q^{p-1} \equiv 1 \pmod{p}$.*"

On considère la suite (u_n) définie pour tout entier naturel n non nul par :

$$u_n = 2^n + 3^n + 6^n - 1$$

Soit p un entier premier strictement supérieur à 3.

(1) Montrer que :

$$6 \times 2^{p-2} \equiv 3 \pmod{p} \quad ; \quad 6 \times 3^{p-2} \equiv 2 \pmod{p}$$

(2) En déduire que : $6 \cdot u_{p-2} \equiv 0 \pmod{p}$.

E.3252

(1) On considère l'équation (E) : $109x - 226y = 1$

où x et y sont des entiers relatifs.

(a) Déterminer le *pgcd* de 109 et 226. Que peut-on en conclure pour l'équation (E) ?

(b) Montrer que l'ensemble des solutions de (E) est l'ensemble des couples de la forme $(141+226k\,;68+109k)$, où k appartient à $\mathbb{Z}$.

En déduire qu'il existe un unique entier naturel non nul d inférieur ou égal à 226 et un unique entier naturel non nul e tels que : $109d = 1 + 226e$.

(On précisera les valeurs des entiers d et e)

(2) Démontrer que 227 est un entier premier.

(3) On note A l'ensemble des 227 entiers naturels a tels que : $a \leqslant 226$.

On considère les deux fonctions f et g de A dans A définies de la manière suivante :

- à tout entier de A, f associe le reste de la division euclidienne de a^{109} par 227 ;
- à tout entier de A, g associe le reste de la division euclidienne de a^{141} par 227.

(a) Vérifier que : $g\big[f(0)\big] = 0$.

On rappelle le résultat suivant appelé petit théorème de Fermat :

Si p est un entier premier et a un entier non divisible par p alors $a^{p-1} \equiv 1 \pmod{p}$

(b) Montrer que, quel que soit l'entier non nul a de A : $a^{226} \equiv 1 \pmod{227}$.

(c) En utilisant (1)(b), en déduire que, quel que soit l'entier non nul a de A : $g\big[f(a)\big] = a$.

Que peut-on dire de : $f\big[g(a)\big] = a$?

E.3625

(1) On considère l'ensemble : $A_7 = \{1\,;2\,;3\,;4\,;5\,;6\}$

(a) Pour tout élément de A_7 écrire dans le tableau figurant en annexe l'unique élément y de A_7 tel que :

$$a \cdot y \equiv 1 \pmod{7}.$$

(b) Pour x entier relatif, démontrer que :

l'équation $3x \equiv 5 \pmod{7}$ équivaut à $x \equiv 4 \pmod{7}$.

(c) Pour x entier relatif, montrer que les seuls entiers relatifs x solutions de l'équation $a \cdot x \equiv 0 \pmod{7}$ sont les multiples de 7.

(2) Dans toute cette question, p est un entier premier supérieur ou égal à 3. On considère l'ensemble $A_p = \{1\,;2\,;\ldots\,;p-1\}$ des entiers naturels non nuls et strictement inférieurs à p. Soit a un élément de A_p.

(a) Vérifier que a^{p-2} est une solution de l'équation :

$$a \cdot x \equiv 1 \pmod{p}.$$

(b) On note r le reste dans la division euclidienne de a^{p-2} par p. Démontrer que r est l'unique solution x dans A_p, de l'équation $a \cdot x \equiv 1 \pmod{p}$.

(c) Soient x et y deux entiers relatifs. Démontrer que $x \cdot y \equiv 0 \pmod{p}$ si, et seulement, si x est un multiple de p où y est un multiple de p.

(d) Application : $p = 31$. Résoudre dans A_{31} les équations :

$$2x \equiv 1 \pmod{31} \quad \text{et} \quad 3x \equiv 1 \pmod{31}.$$

À l'aide des résultats précédents, résoudre dans $\mathbb{Z}$ l'équation :

$$6x^2 - 5x + 1 \equiv 0 \pmod{31}$$

E.3867 On rappelle la propriété, connue sous le nom de petit théorème de Fermat : "*soit p un entier premier et a un entier naturel premier avec p ; alors $a^{p-1} - 1$ est divisible par p*".

(1) Soit p un entier premier impair.

(a) Montrer qu'il existe un entier naturel k, non nul, tel que :

$$2^k \equiv 1 \pmod{p}.$$

(b) Soit k un entier naturel non nul tel que $2^k \equiv 1 \pmod{p}$ et soit n un entier naturel. Montrer que, si k divise n, alors :

$$2^n \equiv 1 \pmod{p}.$$

(c) Soit b tel que $2^b \equiv 1 \pmod{p}$, b étant le plus petit entier non nul vérifiant cette propriété.

Montrer, en utilisant la division euclidienne de n par b, que :

si $2^n \equiv 1 \pmod{p}$ alors b divise n.

(2) Soit q un entier premier impair et l'entier $A = 2^q - 1$.

On prend pour p un facteur premier de A.

(a) Justifier que : $2^q \equiv 1 \pmod{p}$

(b) Montrer que p est impair.

(c) Soit b tel que $2^b \equiv 1 \pmod{p}$, b étant le plus petit entier non nul vérifiant cette propriété.

Montrer, en utilisant (1), que b divise q. En déduire que $b = q$.

(d) Montrer que q divise $p-1$, puis montrer que $p \equiv 1 \pmod{2q}$.

(3) Soit $A_1 = 2^{17} - 1$. Voici la liste des entiers premiers inférieurs à 400 et qui sont de la forme $34m+1$, avec m entier non nul : 103, 137, 239, 307. En déduire que A_1 est premier.

E.3868 Pour tout entier naturel n supérieur ou égal à 2, on pose :
$A(n) = n^4 + 1$

L'objet de l'exercice est l'étude des diviseurs premiers de $A(n)$.

1. Quelques résultats :
   - a) Étudier la parité de l'entier $A(11)$.
   - b) Montrer que, quel que soit l'entier n, $A(n)$ n'est pas un multiple de 3.
   - c) Montrer que tout entier d diviseur de $A(n)$ est premier avec n.
   - d) Montrer que, pour tout entier d diviseur de $A(n)$:
     $n^8 \equiv 1 \pmod{d}$
2. Recherche de critères :

   Soit d un diviseur de $A(n)$. On note s le plus petit des entiers naturels non nuls k tels que :
   $n^k \equiv 1 \pmod{d}$
   - a) Soit k un tel entier. En utilisant la division euclidienne de k par s, montrer que s divise k.
   - b) En déduire que s est un diviseur de 8.
   - c) Montrer que si, de plus, d est premier, alors s est un diviseur de $d-1$. On pourra utiliser le petit théorème de Fermat.
3. Recherche des diviseurs premiers de $A(n)$ dans le cas où n est un entier pair.
   Soit p un diviseur premier de $A(n)$. En examinant successivement les cas :
   $s = 1$; $s = 2$; $s = 4$
   conclure que p est congru à 1 modulo 8.
4. **Indication :** *dans cette question toute trace de recherche, même incomplète, sera en compte dans l'évaluation.*

   Appliquer ce qui précède à la recherche des diviseurs premiers de $A(12)$.

   Indication : la liste des entiers premiers congrus à 1 modulo 8 débute par 17, 41, 73, 89, 97, 113, 137....

E.4327 On rappelle la propriété, connue sous le nom de petit théorème de Fermat : *Si p est un entier premier et a est un entier naturel non divisible par p, alors $a^{p-1} \equiv 1 \pmod{p}$.*

On considère la suite (u_n) d'entiers naturels définie par :
$u_0 = 1$; $u_{n+1} = 10 \cdot u_n + 21$ pour tout entier $n \in \mathbb{N}$

1. Calculer u_1, u_2 et u_3.
2. a) Démontrer par récurrence que, pour tout entier naturel n :
   $3 \cdot u_n = 10^{n+1} - 7$
   b) En déduire, pour tout entier naturel n, l'écriture décimale de u_n.
3. Montrer que u_2 est un entier premier.

On se propose maintenant d'étudier la divisibilité des termes de la suite (u_n) par certains entiers premiers.

4. Démontrer que, pour tout entier naturel n, u_n n'est pas divisible ni par 2, ni par 3, ni par 5.
5. a) Démontrer que, pour tout entier naturel n :
   $3 \cdot u_n \equiv 4 - (-1)^n \pmod{11}$
   b) En déduire que, pour tout entier naturel n, u_n n'est pas divisible par 11.
6. a) Démontrer l'égalité : $10^{16} \equiv 1 \pmod{17}$.
   b) En déduire que, pour tout entier naturel k, u_{16k+8} est divisible par 17.

E.8701 Déterminer l'ensemble des couples $(p\,;q)$ d'entiers premiers vérifiant tels que $p \leqslant q$ et que le produit $p \times q$ divise la somme $2^p + 2^q$

7. PPCM

E.3863 Dans tout l'exercice x et y désignent des entiers naturels non nuls vérifiant $x < y$. S est l'ensemble des couples $(x\,;y)$ tels que : $PGCD(x\,;y) = y - x$

1. a) Calculer le $PGCD(363\,;484)$.
   b) Le couple $(363\,;484)$ appartient-il à S?
2. Soit n un entier naturel non nul ; le couple $(n\,;n+1)$ appartient-il à S
   Justifier votre réponse.
3. a) Montrer que $(x\,;y)$ appartient à S si, et seulement si, il existe un entier naturel k non nul tel que :
   $x = k \cdot (y - x)$; $y = (k+1)(y-x)$
   b) En déduire que pour tout couple $(x\,;y)$ de S, on a :
   $PPCM(x\,;y) = k \cdot (k+1) \cdot (y-x)$
4. a) Déterminer l'ensemble des entiers naturels diviseurs de 228.
   b) En déduire l'ensemble des couples $(x\,;y)$ de S tels que :
   $PPCM(x\,;y) = 228$

E.4280 On considère l'équation (F) : $x^2 - 52 \cdot x + 480 = 0$ où x est un entier naturel.

Montrer qu'il n'existe pas deux entiers naturels non nuls dont le $PGCD$ et le $PPCM$ sont solutions de l'équation (F).

E.3864

1. Soient a et b des entiers naturels non nuls tels que :
$$PGCD(a+b\,;\,a{\cdot}b) = p$$
où p est un entier premier.

   a. Démontrer que p divise a^2.
   (On remarquera que $a^2 = a(a+b) - a{\cdot}b$)

   b. En déduire que p divise a.
   On constate donc, de même, que p divise b.

   c. Démontrer que $PGCD(a\,;\,b) = p$.

2. On désigne par a et b des entiers naturels tels que $a \leqslant b$.

   a. Résoudre le système :
$$\begin{cases} PGCD(a\,;\,b) = 5 \\ PPCM(a\,;\,b) = 170 \end{cases}$$

   b. En déduire les solutions du système :
$$\begin{cases} PGCD(a+b\,;\,a{\cdot}b) = 5 \\ PPCM(a\,;\,b) = 170 \end{cases}$$