A01 : L'arithmétique, c'est toute une histoire !

Première partie : questions préliminaires

1) Dire si chacun des nombres proposés est divisible par 6, 12 ou 7. Seul le calcul mental est autorisé.

	Divisible par 6	Divisible par 12	Divisible par 7
69814			
341898			
553924			
6515796			

2) Énoncer les critères de divisibilité par 6 et par 12 utilisés dans la question précédente et indiquer sur quelle propriété d'arithmétique repose leur justification.

.....

.....

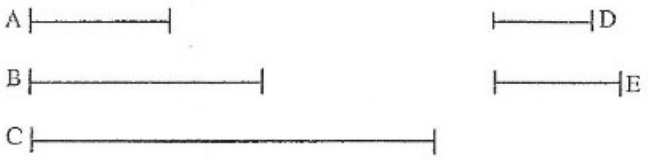
.....

.....

Deuxième partie :

- Étude de la proposition 30 du livre VII des Éléments d'Euclide.

Si deux nombres se multipliant l'un l'autre produisent un certain [nombre] et si un certain nombre premier mesure leur produit, il mesurera aussi l'un des nombres initiaux.



En effet, que deux nombres A, B, se multipliant l'un l'autre produisent C, et qu'un certain nombre premier D mesure C. Je dis que D mesure l'un des [nombres] A, B.

En effet, qu'il ne mesure pas A. Et D est premier; donc A, D sont premiers entre eux (VII. 29). Et qu'autant de fois que D mesure C, autant il y ait d'unités dans E. Or puisque D mesure C selon les unités dans E, le [nombre] D multipliant E a donc produit C. Mais A multipliant B a aussi produit C; donc le produit des D, E est égal au produit des A, B. Donc comme D est à A ainsi [est] B à E (VII. 19). Mais D, A sont premiers entre eux, et les premiers sont les plus petits (VII. 21), et les plus petits mesurent ceux qui ont le même rapport qu'eux autant de fois, le plus grand le plus grand, et le plus petit le plus petit (VII. 20), c'est-à-dire l'antécédent, l'antécédent, et le conséquent, le conséquent. Donc D mesure B.

Alors semblablement nous démontrerons que s'il ne mesure pas B, il mesurera A. Donc D mesure l'un des [nombres] A, B. Ce qu'il fallait démontrer.

Il s'agit **du lemme d'Euclide :**

Soient b et c deux entiers. Si un nombre premier p divise le produit bc alors p divise b ou c.

- Après avoir étudié la démonstration, l'exercice suivant a été proposé :

Reformuler le Corollaire du théorème de Gauss comme Euclide et le démontrer de la même façon.

Solutions :

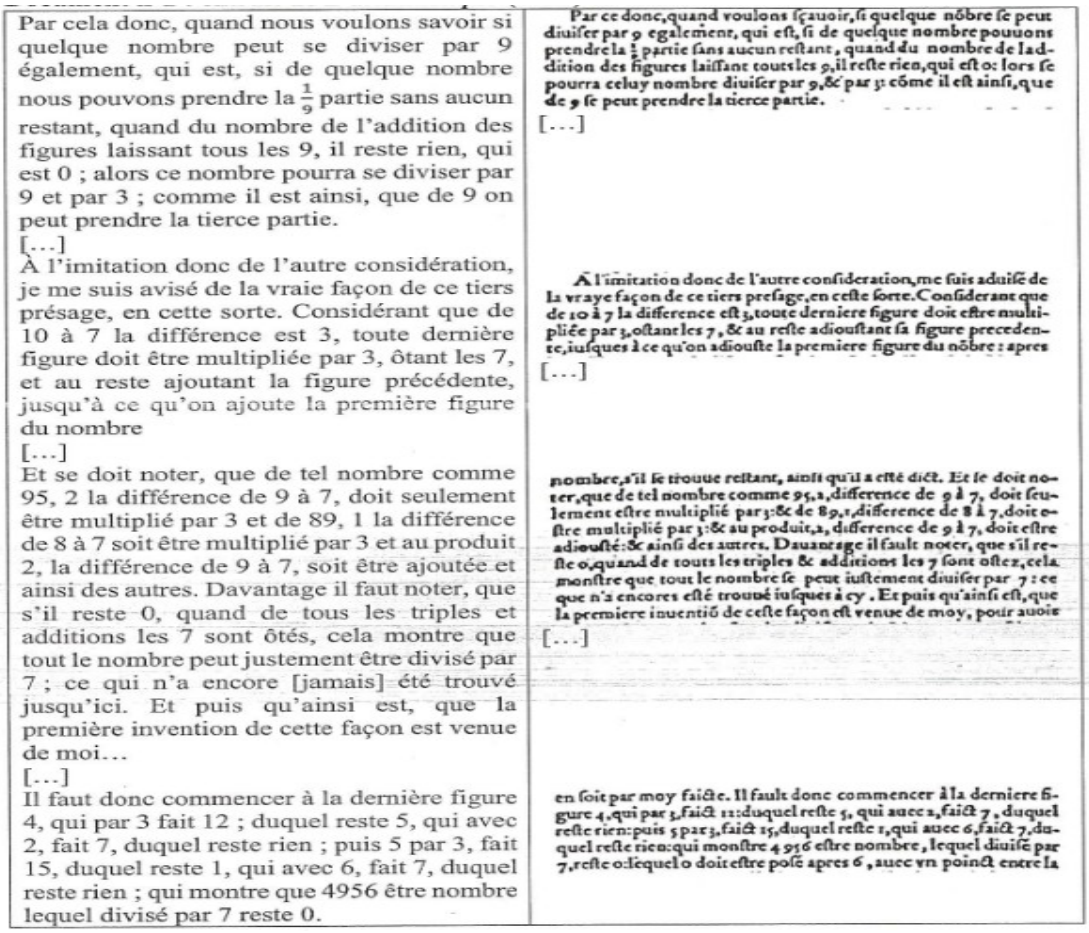
Énoncé : Si deux nombres premiers entre eux mesurent un nombre *a* alors leur produit mesure ce nombre.

Démonstration :
Soient *b* et c deux diviseurs de *a* premiers entre eux. Ils existent alors deux entiers *d* et *e* tels que $a = bd$ et $a = ce$. On a alors $bd = ce$ et $\frac{b}{c} = \frac{e}{d}$.
Comme *b* et *c* sont premiers entre eux, *b* et *c* sont alors les plus petits, il existe alors un entier *m* tel que $e = mb$ et $d = mc$.
Par conséquent $a = bmc$ donc *bc* divise *a*.

Troisième partie :

- Lecture de l'extrait de L'arithmétique de Pierre Forcadel, critère de divisibilité par 7.

Par cela donc, quand nous voulons savoir si quelque nombre peut se diviser par 9 également, qui est, si de quelque nombre nous pouvons prendre la $\frac{1}{9}$ partie sans aucun restant, quand du nombre de l'addition des figures laissant tous les 9, il reste rien, qui est 0 ; alors ce nombre pourra se diviser par 9 et par 3 ; comme il est ainsi, que de 9 on peut prendre la tierce partie.
[...]
À l'imitation donc de l'autre considération, je me suis avisé de la vraie façon de ce tiers présage, en cette sorte. Considérant que de 10 à 7 la différence est 3, toute dernière figure doit être multipliée par 3, ôtant les 7, et au reste ajoutant la figure précédente, jusqu'à ce qu'on ajoute la première figure du nombre
[...]
Et se doit noter, que de tel nombre comme 95, 2 la différence de 9 à 7, doit seulement être multiplié par 3 et de 89, 1 la différence de 8 à 7 soit être multiplié par 3 et au produit 2, la différence de 9 à 7, soit être ajoutée et ainsi des autres. Davantage il faut noter, que s'il reste 0, quand de tous les triples et additions les 7 sont ôtés, cela montre que tout le nombre peut justement être divisé par 7 ; ce qui n'a encore [jamais] été trouvé jusqu'ici. Et puis qu'ainsi est, que la première invention de cette façon est venue de moi...
[...]
Il faut donc commencer à la dernière figure 4, qui par 3 fait 12 ; duquel reste 5, qui avec 2, fait 7, duquel reste rien ; puis 5 par 3, fait 15, duquel reste 1, qui avec 6, fait 7, duquel reste rien ; qui montre que 4956 être nombre lequel divisé par 7 reste 0.



Par ce donc, quand voulons ſçauoir, ſi quelque nõbre ſe peut diuiſer par 9 egalement, qui eſt, ſi de quelque nombre pouuons prendre la $\frac{1}{9}$ partie ſans aucun reſtant, quand du nombre de laddition des figures laiſſant tous les 9, il reſte rien, qui eſt 0: lors ſe pourra celuy nombre diuiſer par 9, & par 3: cõme il eſt ainſi, que de 9 ſe peut prendre la tierce partie.
[...]

A l'imitation donc de l'autre conſideration, me ſuis aduiſé de la vraye façon de ce tiers preſage, en ceſte ſorte. Conſiderant que de 10 à 7 la difference eſt 3, toute derniere figure doit eſtre multipliée par 3, oſtant les 7, & au reſte adiouſtant la figure precedente, iuſques à ce qu'on adiouſte la premiere figure du nõbre: apres
[...]

nombre, s'il ſe trouue reſtant, ainſi qu'il a eſté dict. Et ſe doit noter, que de tel nombre comme 95, 2, difference de 9 à 7, doit ſeulement eſtre multiplié par 3: & de 89, 1, difference de 8 à 7, doit eſtre multiplié par 3: & au produit, 2, difference de 9 à 7, doit eſtre adiouſté: & ainſi des autres. Dauantage il fault noter, que s'il reſte 0, quand de tous les triples & additions les 7 ſont oſtez, cela monſtre que tout le nombre ſe peut iuſtement diuiſer par 7: ce que n'a encores eſté trouué iuſques à cy. Et puis qu'ainſi eſt, que la premiere inuentiõ de ceſte façon eſt venue de moy, pour auoir
[...]

en ſoit par moy faicte. Il fault donc commencer à la derniere figure 4, qui par 3, faict 12: duquel reſte 5, qui auec 2, faict 7, duquel reſte rien: puis 5 par 3, faict 15, duquel reſte 1, qui auec 6, faict 7, duquel reſte rien: qui monſtre 4956 eſtre nombre, lequel diuiſé par 7, reſte 0: lequel 0 doit eſtre poſé apres 6, auec vn poinct entre la

- Application du critère de divisibilité avec le nombre 4**9**56 :
  dernière figure : 4
  $4\times3=12$
  $12-7=5$
  9 $= 7 + 2$ et $5+2=7$
  $7 - 7 = 0$
  $0\times3=0$
  $0 + 5 = 5$
  $5\times3=15$
  $15-14=1$
  $1 + 6 = 7$ donc 4956 est divisible par 7

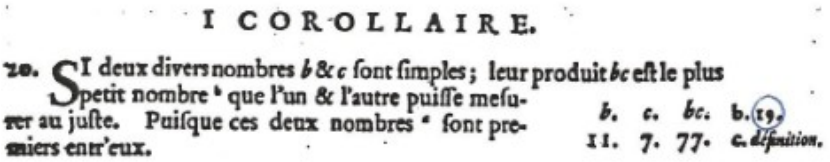
  Application du critère de divisibilité avec le nombre 6**9**814 :
  dernière figure : 6
  $6\times3=18$
  $18-14=4$
  9 $= 7 + 2$ et $4+2=6$
  $6\times3=18$
  $18-14=4$
  $8 = 7 + 1$ et $1 + 4 = 5$
  $5\times3=15$
  $15-14=1$
  $1 + 1 = 2$
  $2\times3=6$
  $6 + 4 = 10$ donc 69814 n'est pas divisible par 7

- Éléments de justifications de ce critère de divisibilité:

  Complément à 10 : 3
  Soient *a, b, c* et *d* quatre entiers.
  $a+10b+100c+1000d=a+10(b+10(c+10d))$
  $a+10b+100c+1000d\equiv a+3(b+3(c+3\mathrm{d}))(7)$

Quatrième partie :

Lecture des extraits des Nouveaux éléments des mathématiques ou principes généraux de toutes les sciences qui ont les grandeurs pour objet (1695), premier volume de Jean Prestet.



I COROLLAIRE.

20. SI deux divers nombres *b* & *c* ſont ſimples ; leur produit *bc* eſt le plus petit nombre [b] que l'un & l'autre puiſſe meſurer au juſte. Puiſque ces deux nombres [c] ſont premiers entr'eux.

b. c. bc. b. 19. 11. 7. 77. c. définition.

I : si deux nombres *b* et *c* sont premiers, leur produit *bc* est le plus petit nombre divisible par l'un et l'autre puisque ces deux nombres sont premiers entre eux.

II COROLLAIRE.

21. SI deux nombres *b* & *c* meſurent au juſte l'un & l'autre un même nombre *a*; le moindre comme *z* que chacun des deux *b* & *c* puiſſe meſurer au juſte, peut auſſi meſurer cet autre *a* ſans reſte. Car *z* ne peut ſurpaſſer *a* par la ſuppoſition. Et ſi *z* & *a* ſont égaux; le nombre *z* ou *a* ſe meſure [b] luy-même. Et ſi *z* eſt moindre que le nombre *a*; les deux *b* & *c*, qui meſurent *a* l'un & l'autre au juſte, meſurent auſſi tous les nombres enſemble [c] qu'on pourra prendre en *a*, & encore le [d] reſte *e* s'il s'en peut trouver un. Et ainſi le nombre *z*, plus grand que le reſte *e*, n'eſt pas le moindre que chacun des deux *b* & *c* puiſſe meſurer au juſte. Ce qui repugne à la ſuppoſition. Le reſte *e* eſt donc [e] nul, & *z* meſure [f] au juſte le nombre *a*.

b. z. a. c. e.
12. 84. 168. 7. 0.

[b. 1.] [c. 9.] [d. 15.] [e. 16. 1.]

III COROLLAIRE.

22. SI un nombre *d* meſure au juſte un produit *bc* de deux nombres *b* & *c*, & que *c* & *d* ſoient premiers entr'eux; le nombre *d* eſt un diviſeur de l'autre nombre *b*. Car *c* & *d* étant premiers entr'eux, & chacun meſurant au juſte le produit *bc*; leur produit *cd*, qui eſt le moindre nombre [b] que l'un & l'autre puiſſe meſurer au juſte, eſt [c] un diviſeur de *bc*. Si donc *e* eſt l'expoſant entier de la diviſion de *bc* par *cd*; le nombre *bc* eſt égal [d] au produit *cde* du diviſeur *cd* par l'expoſant *e*. Et ſi on diviſe l'un & l'autre par *c*; les expoſans *b* & *de* ſont [e] égaux, ou ne ſont qu'un même nombre. Mais ſi on diviſe *de* par *d*, on aura l'expoſant entier *e*. Et ainſi *d* eſt un diviſeur du nombre *de* ou *b*.

d. bc. b. c. cd. e.
4. 84. 12. 7. 28. 3.
cde. de.

[b. 19.] [c. 21.] [d. 18. 2.] [e. 27. 3.]

II : Si deux nombres *b* et *c* divisent un même nombre a, le plus petit nombre *z* divisible par *b* et *c* est aussi divisible par *a*. Car *z* ne peut pas être supérieur à *a*...

III : Théorème de Gauss
Soit *a, b* et *c* des entiers. Si *a* divise le produit *bc* et si *a* est premier avec *b* alors *a* divise *c*.

Théorème **19** : Si *b* et *c* sont premiers entre eux alors PPCM(*b ; c*) = *bc*.

Document n°4 : extrait de la section première des *Recherches arithmétiques* (1801) de Carl Friedrich Gauss (dans la traduction de A. C. M. Poullet-Delisle)

Si un nombre *a* divise la différence des nombres *b* et *c*, *b* et *c* sont dits congrus suivant *a*, sinon incongrus. *a* s'appellera le module ; chacun des nombres *b* et *c*, résidus de l'autre dans le premier cas et non résidus dans le second.

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire sans aucun signe.

Ainsi −9 et +16 sont congrus par rapport au module 5 ; −7 est résidu de 15 par rapport au module 11 ; et non résidu par rapport au module 3.

Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque. […]

Nous désignerons dorénavant la congruence de deux nombres par ce signe ≡, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses ; ainsi, $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$.

[…]

Chaque nombre aura un résidu, tant dans la suite 0, 1, 2, …, $(m-1)$, que dans celle-ci 0, −1, −2, …, $-(m-1)$; nous les appellerons résidus minima ; et il est clair que qu'à moins que 0 ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif.

[…]

Plusieurs théorèmes que l'on a coutume d'exposer dans les traités d'arithmétique, s'appuient sur ceux que nous avons présentés ; par exemple, la règle pour connaître si un nombre est divisible par 9, 11 ou tout autre nombre. Suivant le module toutes les puissances de 10 sont congrues à l'unité ; donc si le nombre est de la forme $a + 10b + 100c + 1000d + etc.$ il aura, suivant le module 9 le même résidu minimum que $a + b + c + d + etc.$ Il est clair d'après cela, que si l'on ajoute les figures du nombre, sans avoir égard au rang qu'elles occupent, la somme que l'on obtiendra, et le nombre proposé auront les mêmes résidus minima ; si donc ce dernier est divisible par 9, la somme des chiffres le sera aussi, et seulement dans ce cas.

Cinquième partie :

Extrait de la section seconde des Recherches arithmétiques de Carl Friedrich Gauss.

13. Théorème. *Le produit de deux nombres positifs plus petits qu'un nombre premier donné, ne peut être divisé par ce nombre premier.*

Soit p le nombre premier et $a < p$ et > 0; je dis qu'on ne pourra trouver aucun nombre positif b, plus petit que p, qui rende

$$ab \equiv 0 \text{ (module } p\text{)}.$$

En effet, s'il peut y en avoir, supposons que ce soient les nombres $b, c, d,$ etc, tous plus petits que p, ensorte qu'on ait $ab \equiv 0$, $ac \equiv 0$, etc., (mod. p), soit b le plus petit de tous, desorte qu'on n'en puisse supposer un plus petit que b, on aura évidemment $b > 1$; car si $b = 1$, on aurait $ab = a < p$ et partant non divisible par p. Or p comme nombre premier ne peut être divisé par b, mais tombera entre deux multiples de b, mb et $(m+1)b$. Soit $p - mb = b'$, b' sera positif et $< b$. Or nous avons supposé $ab \equiv 0$ (mod. p), on aura donc $mab \equiv 0$; et retranchant de $ap \equiv 0$, on aura $a(p - mb) = ab' \equiv 0$; donc b' devrait être mis au rang des nombres $b, c, d,$ etc., et serait plus petit que le plus petit de tous, ce qui est contre la supposition.

14. *Si aucun des deux nombres* a *et* b *n'est divisible par un nombre premier* p, *le produit* ab *ne le sera pas non plus.*

Soient α et β les résidus *minima* positifs des nombres a et b, suivant le module p, aucun d'eux ne sera nul par hypothèse. Or si l'on avait $ab \equiv 0$, comme $ab \equiv \alpha\beta$, on aurait $\alpha\beta \equiv 0$, ce qui serait contraire au théorème précédent.

La démonstration de ce théorème a déjà été donnée par Euclide, *El.* VII, 32. Nous n'avons pas cependant voulu l'omettre, tant parceque plusieurs auteurs modernes ont présenté des raisonnemens vagues au lieu de démonstration, ou bien ont négligé ce théorème; que dans le but de faire mieux saisir, par ce cas très-simple, l'esprit de la méthode que nous appliquerons par la suite à des points bien difficiles.

[...]

19. *Si les nombres* a, b, c, etc. *sont premiers avec* k, *leur produit l'est aussi.*

En effet, puisqu'aucun des nombres $a, b, c,$ etc. n'a de facteurs premiers communs avec k, et que le produit de ces nombres ne peut avoir de facteurs premiers qui n'appartiennent à quelqu'un d'entr'eux, ce produit n'aura non plus aucun facteur premier commun avec k.

Si les nombres a, b, c, *etc. sont premiers entr'eux, et que* k *soit divisible par chacun d'eux, il le sera aussi par leur produit.*

C'est une suite des nos 17 et 18. Soit en effet p un diviseur premier quelconque du produit abc etc. et qu'il ait l'exposant π, quelqu'un des nombres $a, b, c,$ etc. sera divisible par p^π, parconséquent k, qui est divisible par ce nombre, le sera aussi par p^π : il en sera de même des autres diviseurs du produit.

Donc, *si deux nombres* m, n *sont congrus suivant plusieurs modules* a, b, c, etc. *premiers entr'eux, ils le seront aussi suivant leur produit.* En effet, puisque $m - n$ est divisible par chacun des nombres $a, b, c,$ etc., il le sera aussi par leur produit.

Enfin, *si* a *est premier avec* b, *et que* ak *soit divisible par* b, k *sera aussi divisible par* b. En effet, puisque ak est divisible par a et par b, il le sera par leur produit; donc $\frac{ak}{ab} = \frac{k}{b}$ sera un entier.