Chapitre 4

NOMBRES PREMIERS

« Les problèmes posés par les nombres entiers nécessitent de tels travaux et de telles réflexions que, finalement, c'est de là que sortent à peu près la moitié des théories mathématiques... » Charles PISOT

Résumé Dans cette avant-dernière aventure, nous allons côtoyer quelques-uns des héros du passé les plus prestigieux : Euclide, Fermat, Gauss, Euler, Riemann, Tchebichev, Hadamard et beaucoup d'autres. Nous allons en même temps toucher du doigt des résultats encore brûlants issus des dernières recherches en mathématiques. Nous allons utiliser sans compter la puissance des logiciels de calcul formel, en l'occurrence Xcas. Nous allons mêler arithmétique, calcul algébrique, probabilité, géométrie, calcul intégral ... un vrai bonheur.

I - Nombres premiers

a. Nombres premiers - Nombres composés

Quoi de plus simple qu'un nombre premier :

Définition 4.1
Un entier naturel est dit premier s'il est supérieur (i.e. supérieur ou égal) à 2 et n'est divisible que par 1 et lui-même.

et pourtant, ils renferment tant de mystères que les plus grands esprits depuis des siècles n'ont toujours pas réussi à en percer tous les secrets et ce malgré les énormes progrès technologiques et les investissements colossaux consentis par les pouvoirs tant civils que militaires pour assurer ou percer la confidentialité des transmissions de toutes natures qui continuent de dépendre d'une meilleure connaissance des nombres premiers, ce que nous verrons un peu plus loin. Qui sont-ils ? Combien sont-ils ? Où sont-ils ? À quoi servent-ils ? Nous essaierons de donner quelques éléments de réponses à ces questions.

Mais tout d'abord, pourquoi jouent-ils un rôle si important ? Fondamentalement, il existe deux manières d'engendrer $\mathbb{N}$:

- si on veut engendrer $\mathbb{N}$ en utilisant l'addition, on s'aperçoit que le nombre 1 nous suffit : on « fabrique » 2 en additionnant 1 avec lui-même ; 3 en additionnant 1 avec 2, etc.
- si on veut engendrer $\mathbb{N}$ en utilisant la multiplication, là, les choses se compliquent. Pour « fabriquer » 2, il faut le créer ; même problème pour 3. On fabrique 4 en multipliant 2 avec lui-même, mais il faut créer 5. On fabrique 6 en multipliant 3 avec 2. On crée 7. On fabrique 8 à partir de 2. On fabrique 9 à partir de 3. On fabrique 10 à partir de 2 et 5, etc.

  Les nombres que l'on est obligés de créer sont les briques nécessaires à fabriquer tous les autres. C'est bien plus compliqué que l'addition me direz-vous, mais la multiplication est plus « puissante » et nous permet d'aller bien plus vite et plus loin.

Les nombres premiers sont donc ces éléments qui nous permettent de fabriquer tous les autres. Un des premiers problèmes étudiés à été de savoir s'ils peuvent tenir dans une boîte, comme les légos dans ma chambre. Euclide à répondu à cette question il y a vingt-trois siècles et la réponse est non.

Pour le prouver, nous aurons besoin d'un résultat intermédiaire :

Propriété 4.1
Tout entier naturel admet au moins un diviseur premier.

Si ce nombre, appelons-le n, est premier, tout va bien.
Sinon, l'ensemble de ses diviseurs étant non vide (n est dedans) et borné (par 1 et lui-même), il admet un plus petit élément $p \neq 1$. Ce nombre n'est pas divisible par un autre, sinon ce nombre plus petit que p divisant p diviserait n et alors p ne serait plus le plus petit diviseur de n. Le nombre p est donc premier et voilà.

Théorème 4.1
Il y a une infinité de nombres premiers.

Sa démonstration est classique et peut faire l'objet d'un ROC.
Raisonnons par l'absurde et supposons qu'il existe exactement n nombres premiers qu'on nommera p_1, p_2,$\cdots$, p_n et appelons N le nombre

$$\mathrm{N} = p_1 p_2 \cdots p_n + 1$$

Il est plus grand que tous les p_i, donc il n'est pas premier d'après notre hypothèse, donc il admet un diviseur premier p qui est donc un des p_i, puisqu'il n'y a qu'eux. Soit i_0 tel que $p = p_{i_0}$. Alors p divise $p_1 p_2 \cdots p_n$. Or il divise N, donc il divise leur différence $\mathrm{N} - p_1 p_2 \cdots p_n$, c'est à dire 1, donc $p = 1$ ce qui est absurde puisqu'il est premier. Ainsi, il n'existe pas de plus grand nombre premier.
Il y en a donc une infinité et l'aventure ne fait que commencer.

Comment vérifier qu'un nombre est premier ?

Sortons nos machines et observons les diviseurs de 1321 par exemple : si aucune des 1319 divisions ne « tombe juste », alors on pourra dire que 1321 premier. Et puis d'abord, il est impair, il ne semble pas être divisible par 3, alors pourquoi pas...

diviseur	2	3	4	5	6	7	8	9	10	11	12	13
quotient	660,5	440,3	330,3	264,2	220,2	188,7	165,1	146,8	132,1	120,1	110,1	101,6
diviseur	14	15	16	17	18	19	20	21	22	23	24	25
quotient	94,36	88,07	82,56	77,71	73,39	69,53	66,05	62,90	60,05	57,43	55,04	52,84
diviseur	26	27	28	29	30	31	32	33	34	35	36	37
quotient	50,81	48,93	47,18	45,55	44,03	42,61	41,28	40,03	38,85	37,74	36,69	35,70

Le tableau est incomplet : il reste encore à essayer les quotients de 38 à 1320, mais ça aurait pris trop de place sur la feuille , et quand on connaît le prix du papier. Mais bon, on s'égare.
Tout d'abord, nous n'avons pas trouvé de quotient entier en ce début d'enquête. Nous observons de plus que si la suite des diviseurs est croissante, celle des quotients est décroissante[a]. Vous avez sûrement remarqué qu'à partir de 37, les quotients sont inférieurs aux diviseurs. Donc nous pouvons nous arrêter là : si pour un diviseur supérieur à 37, on trouvait un quotient entier q, alors en divisant 1321 par q, qui est inférieur à 37 et donc devrait se trouver au début de notre liste de diviseurs, on devrait obtenir un entier. Le problème, c'est qu'aucune division par un entier inférieur à 37 n'a donné de quotient entier, donc on peut s'épargner les 1283 divisions restantes.

Mine de rien, nous venons de franchir un grand pas dans la théorie des nombres : pour tester si l'entier 1321 est premier, il nous a suffit d'effectuer 36 divisions[b]. Deux problèmes se posent maintenant : pourquoi 36 et pouvons-nous généraliser ce résultat aux autres entiers ?
Un petit Joker : $\sqrt{1321} \approx 36,3$.
Reprenons la propriété 4.1. Tout naturel n admet un plus petit diviseur p qui est premier. Écartons le cas où n est premier et donnons un nom aux nombres qui restent :

Définition 4.2
Un entier naturel *autre que 1* qui n'est pas premier est dit **composé**.

a On l'aurait deviné...
b Et encore, nous aurions pu faire mieux comme nous allons le voir tout de suite après.

L'entier n étant composé, il s'écrit donc $n = pq$, avec q un entier supérieur à p (car p est le plus petit diviseur). Ainsi

$$p \leqslant q \text{ et donc } p^2 \leqslant pq = n \text{ c'est à dire } p \leqslant \sqrt{n}$$

Nous pouvons donc généraliser l'observation précédente

Propriété 4.2
Si un entier est composé, alors il admet un diviseur premier inférieur à sa racine carrée.

b. Tests et cribles

La théorie des nombres[c] est actuellement intimement liée à l'informatique. Même à notre petit niveau, nous ne pouvons donc pas passer à côté...

Premier or not premier ?

Commençons par le problème crucial de tester si un nombre est premier :

```
test1(n):={
local k;
L:=[]; //on crée une liste vide au départ pour y placer les diviseurs de n
for(k:=2;k*k<=n;k++){ //pour travailler sans approximation
if (n mod k==0) {return n+''␣n'est␣pas␣premier'' //si k divise n, n n'est pas premier
 }
return n+" est premier." // sinon n est premier
}:;
```

Ce qui donne

```
>> test1(123) ;
"123 n'est pas premier"
>> test1(97) ;
"97 est premier."
```

mais

```
  >> test1(101!+1) ;
"Aborted"
```

Ce test a des limites et nécessitera de nombreuses améliorations. Sachez cependant que XCAS a un test très efficace mais dont le principe est hors de notre portée

```
  >> isprime(101!+1) ;
false
```

Crible d'Ératosthène

Autre problème crucial[d] : comment obtenir une liste des entiers inférieurs à un *petit* nombre donné n ?
Le principe est ancien puisqu'il est attribué au grec Ératosthène[e]
On écrit les entiers de 2 à n puis on barre les multiples des nombres premiers inférieurs à $\sqrt{n}$. Les entiers restant sont premiers.

```
Erato(n):={
local x,j,k,m,q,P;
x:=[seq(1,j=1..n+1)] // on crée une liste de n+1 nombres valant tous 1 au départ
x[1]:=0; // 0 et 1 ne sont pas premiers donc on les "raye" en leur associant 0
for(k:=2;k*k<=n;k++){ // on teste les entiers de 2 à racine carrée de n
   if (x[k]==1) { // si le keme nombre n'est pas barré
            for(m:=2;m<=floor(n/k);m++){
                x[k*m]:=0; // on barre tous ses multiples
```

c la partie des mathématiques qui étudie les nombres premiers
d et toujours pas résolu à ce jour...
e Né 276 années avant JiCé, directeur de la Bibilothèque d'Alexandrie, on lui doit aussi une approximation du diamètre de la Terre. Devenu aveugle, il s'est laissé mourir de faim...

```
  }}}
P:=[]; // on crée une liste vide
for(q:=2;q<=n;q++){
  if (x[q]==1) { // si q n'est pas barré
      P:=append(P,q); // on ajoute q à la liste des premiers
  }
}
return P
}:;
```

Par exemple :

```
>> Erato(100) ;
[2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97]
```

c. Décomposition des entiers en produit de nombres premiers

Avant d'aller plus loin dans notre exploration, nous avons dit en introduction que les nombres premiers étaient les briques qui nous permettaient de construire tous les autres : il serait bon de le vérifier.

Propriété 4.3
Tout entier n supérieur à 2 se décompose en produit fini de nombres premiers.

La démonstration la plus simple (mais pas la plus intéressante) consiste à raisonner par récurrence sur n.
Nous savons que 2 est premier.
Supposons que tout entier inférieur ou égal à n se décompose en produit de facteurs premiers.
L'entier suivant $n+1$ admet au moins un diviseur premier p d'après la propriété 4.1 page 2.
Soit q le quotient de $n+1$ par p.
Si $q=1$, alors $n+1=p$ et donc $n+1$ est premier.
Si $q>1$, nous appliquons l'hypothèse de récurrence à q : q se décompose en produit fini de nombres premiers, et par suite $n+1$ aussi, car $n+1=p\times q$.

Par exemple, $50=2\times5^2$: les facteurs premiers ne sont pas forcément distincts. On a donc l'habitude d'écrire la décomposition sous la forme

$$n=p_1^{\alpha_1}\times p_2^{\alpha_2}\times\cdots\times p_r^{\alpha_r}$$

Une petite chose reste à vérifier : cette décomposition est-elle unique ? Elle a l'air de l'être...c'est pourquoi la démonstration de ce résultat est **admis** en Terminale. C'est dommage car elle offre une utilisation originale du théorème de Gauss.

Théorème 4.2
Tout entier n supérieur à 2 admet une et une seule (à l'ordre près des termes) décomposition en produit fini de nombres premiers

Décomposition informatique

Nous allons utiliser la procédure Erato mise au point précédemment

```
decompo(n):={
local L,D,N,k;
D:=[]; //liste des diviseurs premiers, vide au départ
L:=Erato(n); // on utilise la procédure précédente
N:=n; // N est l'entier mobile dont on cherche les diviseurs
while (contains(L,N)==0){ // tant que N n'est pas premier
for(k:=0;k<length(L);k++){// length(L)=nombre d'éléments de L
if (N mod L[k]==0){ D:=append(D,L[k]); // si le keme premier divise N, on le rajoute à D
N:=iquo(N,L[k]); // on divise N par ce nombre premier
break; // on recommence la boucle au cas où le keme premier divise encore n
}
}
}
```

```
D:=append(D,N); // on n'oublie pas n au cas où il est premier
 }:;
```

Alors par exemple

```
>> decompo(500) ;
[2,2,5,5,5]
```

Pour être honnête, il existe la fonction ifactor qui donne directement la décomposition en produit de facteurs premiers.

```
>> ifactor(500) ;
2^2*5^3
```

II - Le théorème des nombres premiers

Cette section peut être passée en première lecture car elle déborde du programme, mais comment ne pas parler des nombres premiers sans évoquer cette épique aventure intellectuelle...

a. Approche expériementale

Nous venons de voir qu'il y a une infinité de nombres premiers : le problème n'est donc pas de déterminer combien il y a de nombres premiers, mais plutôt de savoir combien sont inférieurs à un nombre donné x.

Cette dernière question a hanté tant d'esprits qu'on a fini par lui donner un nom : on appelle $\pi(x)$ le nombre d'entiers premiers inférieurs à x.

Nous n'avons peut-être pas le cerveau de Gauss ou d'Euler, mais nous avons un ordinateur...

Le programme suivant utilise encore la procédure Erato

```
  >> length(Erato(100)) ;
25
>> length(Erato(1000000)) ;
78498
```

Il faut malgré tout remarquer qu'il a fallu 23 secondes pour calculer length(Erato(100 000)) et 27 minutes pour length(Erato(1 000 000)) : nous commençons à entrevoir les difficultés d'aller vers les grands nombres premiers. Dernièrement, Xavier Gourdon a calculé $\pi(10^{22})$[f] en mettant en commun les ressources de plusieurs ordinateurs personnels à travers le réseau internet.

Jusqu'ici, nous nous étions débrouillés seuls. À mesure que les calculs se compliquent, nous allons introduire des fonctions de Xcas bien pratiques. Par exemple, isprime(n) teste si n est un nombre premier[g]. Le programme suivant permet alors d'aller beaucoup plus vite

```
pii(n):={
  if (n<2){ return 0; }
  if (is_prime(n)){ return pii(n-1)+1; }
  return pii(n-1);
} :;
```

Il faut prendre soin de régler la configuration du CAS pour pouvoir obtenir au moins 1000 comme niveau de récursion.

```
>> pii(1000) ;
168
```

est obtenu en 48 centièmes de seconde.

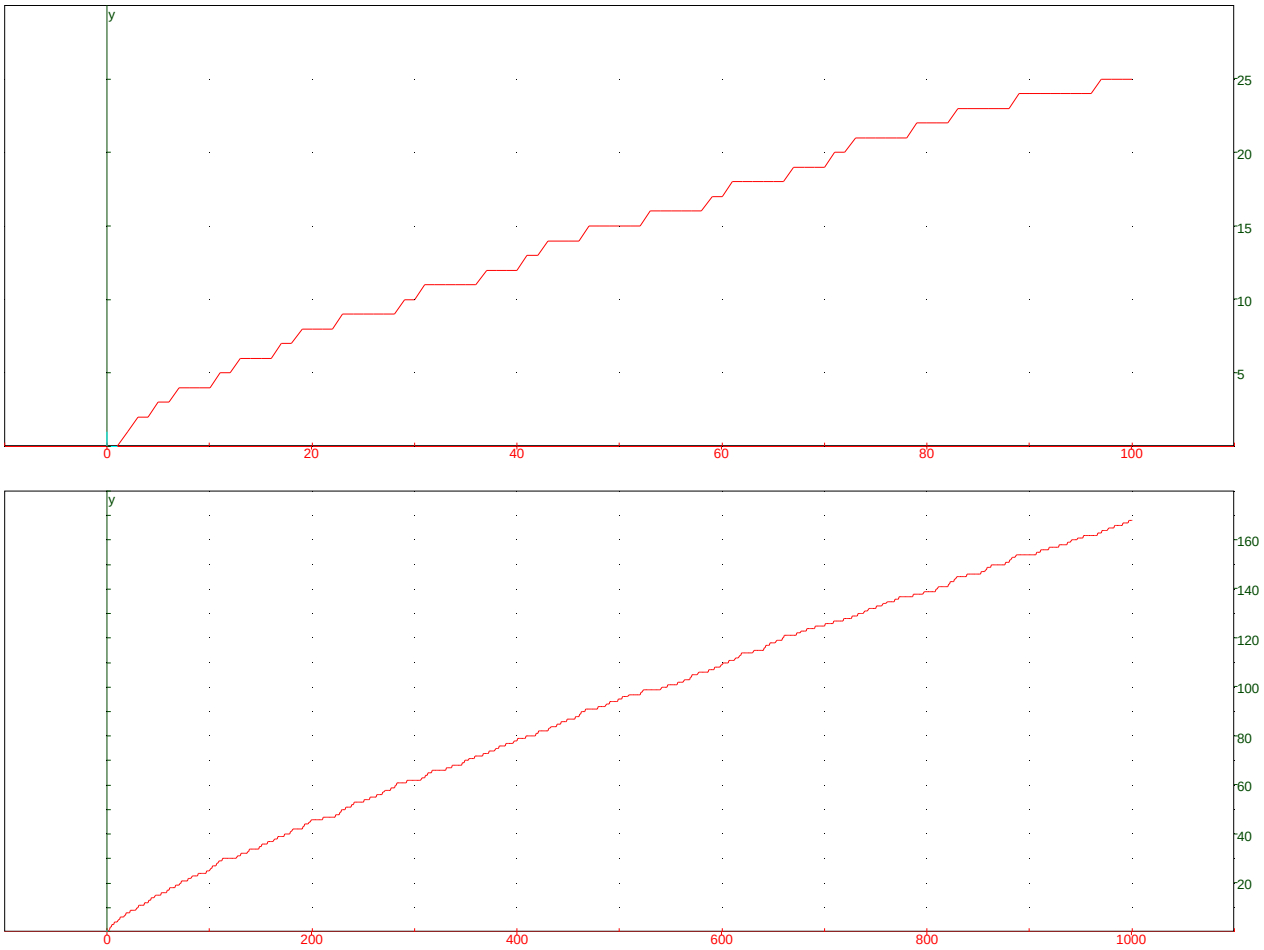
Cela va également nous permettre de tracer la courbe représentative de π

en rentrant

```
polygone_ouvert(seq(point([k,pii(k)]),k=0..100))
```

f 201 467 286 689 315 906 290

g Nous verrons plus loin avec quel degré de certitude



Même si l'allure de la courbe est un peu chaotique sur $[0,100]$, on sent qu'il y a comme une tendance régulière si on regarde de plus haut, par exemple sur $[0,1\,000]$ (attention, le repère n'est pas orthonormé).
Existerait-il une loi régissant la fonction π ?

À la fin du XVIII$^{\text{ème}}$ siècle, Gauss conjecture que, lorsque x tend vers l'infini, $\pi(x)$ est équivalent à $\text{Li}(x) = \displaystyle\int_2^x \frac{dt}{\ln t}$. À la même époque, Legendre pense que $\pi(x)$ est équivalent à $\dfrac{x}{\ln x}$.

Notez bien que dire que $a(x)$ et $b(x)$ sont équivalents au voisinage de l'infini signifie que $\lim\limits_{x\to+\infty} \dfrac{a(x)}{b(x)} = 1$. Mais attention, cela ne veut pas dire que $a(x) - b(x)$ est petit. Par exemple $\lim\limits_{x\to+\infty} \dfrac{x^2+x}{x^2} = 1$, mais leur différence $x^2 + x - x^2 = x$ tend vers l'infini.
Cela veut juste dire que $\ln x / x$ et $\text{Li}(x)$ seraient des approximations de $\pi(x)$ au voisinage de $+\infty$.
En fait, on peut employer n'importe quelle expression du type $\dfrac{x}{\ln x - a}$ avec a une constante arbitraire et on obtient le même résultat.

Le tableau suivant nous permet de nous faire une idée sur des petits (eh oui) nombres premiers

x	$\pi(x)$	$\text{Li}(x)$	$\frac{x}{\ln x}$	$\frac{x}{\ln x - 1}$
1 000	168	178	172	169
10 000	1 229	1 246	1 231	1 218
1 000 000	78 498	78 628	78 534	78 030
10 000 000 000	455 052 511	455 055 614	455 743 004	454 011 971

III - Être ou ne pas être premier

a. Fermat et son petit théorème

Nous avons mis au point avec le modèle du crible d'Eratosthène une méthode permettant de tester si un entier est premier ou non. Cela marche assez bien pour des petits nombres, mais cette méthode devient impraticable s'il s'agit de tester un entier d'une centaine de chiffres. Nous allons nous occuper dans cette section de deux problèmes imbriqués : d'une part trouver des méthodes permettant de vérifier rapidement si un nombre est premier et d'autre part réfléchir à d'éventuelles méthodes permettant de « fabriquer » des nombres premiers aussi grands que l'on veut.

« *A thing of beauty is a joy for ever. Its loveliness increases ; it will never Pass into nothingness* » écrivait John Keats 217 ans après la naissance de Pierre de Fermat, dont le Petit Théorème demeure un joyau de la théorie des nombres, malgré les innombrables découvertes effectuées depuis dans ce domaine. [h]
Au contraire de son grand frère, notre petit théorème, bien moins « médiatique » et à la démonstration abordable, a eu de très nombreuses et importantes conséquences : nous allons en étudier quelques-unes.

Mais tout d'abord, comment l'idée de son théorème est venu à l'esprit de l'ami Pierre ?
Au cours de ses nombreuses recherches, Fermat s'est intéressé aux nombres de Mersenne qui sont les nombres de la forme $M_n = 2^n - 1$, avec n un entier premier. On savait déjà que M_{11} était composé

$$2^{11} - 1 = 2047 = 23 \times 89 \ (i)$$

Mais c'est Fermat qui remarqua que

$$2^{23} - 1 = 8388607 = 47 \times 178841 \ (ii)$$

Il sauta aux yeux de Fermat qui vivait parmi les entiers, que $47 = 2 \times 23 + 1$ en observant (ii) ce qui lui mit la puce à l'oreille pour observer que $23 = 2 \times 11 + 1$ dans (i). Qu'en dire ? Que le plus petit diviseur premier d'un nombre composé $2^p - 1$ est de la forme $2p + 1$?
Le problème, c'est que $2^{29} - 1 = 536870911 = 233 \times 1103 \times 2089$, et donc, ça ne marche pas. D'ailleurs, ce n'est pas ce qui attira l'attention de Fermat. Il remarqua en effet que dans (i), non seulement $23 = 2 \times 11 + 1$ mais aussi $89 = 8 \times 11 + 1$. De même dans (ii), $47 = 2 \times 23 + 1$ et $178481 = 7760 \times 23 + 1$. Il conjectura donc que tout diviseur premier de $2^p - 1$ est congru à 1 modulo p.
Mais l'ami Pierre ne s'arrêta pas là. On a $2^{11} \equiv 1[23]$, mais on a le même résultat avec 2^{22}, 2^{33}, etc. De même, 2^{11}, 2^{22},...,2^{88}, etc. sont tous congrus à 1 modulo 89. Et puis 2^{23}, 2^{46}, etc. sont congrus à 1 modulo 47 et enfin 2^{23},...,2^{178480}, etc. sont aussi tous congrus à 1 modulo 178481.
Oui, et alors. Et bien, pour ces quatre nombres premiers, on a $2^m \equiv 1[p]$, mais surtout, dans chaque cas, l'un de ces m est $p - 1$.
En bref, pour les nombres premiers 23, 89, 47 et 178481, on a $2^{p-1} \equiv 1[p]$. Est-ce vrai pour *tous* les entiers premiers ?
Pour résoudre ce problème, occupons-nous du théorème énoncé pour la première fois par Fermat en 1640 dans une lettre adressée au fameux Frère Marin Mersenne.

Théorème 1

Soit p un nombre premier et a un entier non divisible par p. Alors $a^{p-1} - 1$ est divisible par p, ou, en d'autres termes

$$a^{p-1} \equiv 1[p]$$

Comme d'habitude, Fermat affirma avoir la démonstration mais ne pas avoir la place de l'écrire à son correspondant[i]
Il existe de très nombreuses démonstrations de ce théorème. Nous en verrons deux : une maintenant et une comme cas particulier d'un théorème plus général, le théorème d'Euler.

h S'il est qualifié de petit, c'est qu'une conjecture célèbre du même Fermat, restée indémontrée pendant des siècles, s'est accaparée le titre de *Grand Théorème de Fermat*.

$$x^n + y^n = z^n \quad \text{n'a pas de solution dans } \mathbb{N}^3 \quad \text{pour } n > 2$$

Dans la marge d'un manuscrit, Fermat prétendait en avoir trouvé la démonstration mais manquer de place pour l'écrire. Il a pourtant fallu attendre 1995 pour qu'Andrew Wiles le démontre en utilisant des outils surpuissants : l'entêtement d'une multitude de chercheurs a abouti à la démonstration de ce théorème, mais surtout a permis de développer d'importants outils en théorie des nombres. Quant à lui trouver des applications, le problème reste ouvert.

i Fermat était-il malhonnête ou avare de son encre ?

La plus rapide consiste à montrer que $a^{p-1}(p-1)! = a\times 2a\times 3a\times\cdots\times(p-1)a$ est congru à $(p-1)!$ modulo p puis d'en déduire le résultat. Nous aurons besoin d'établir deux petites propriétés[j].

Propriété1
Soit p un nombre premier et a un entier, alors p divise a OU p et a sont premiers entre eux.

Propriété2
Soit p un nombre premier et a et b deux entiers. Si p divise ab, alors p divise a ou p divise b.

Considérons donc les multiples successifs de a jusqu'à $(p-1)a$ et appelons r_k le reste de la division de ka par p.

- Montrons d'abord qu'aucun r_k n'est nul : en effet, si p divisait ka, alors il diviserait a ou k, or il ne divise pas a par hypothèse et il ne divise pas k car $k \leqslant p-1$.
- Montrons maintenant que ces restes sont deux à deux distincts : s'il existe deux entiers k et k' tels que $r_k = r_{k'}$, alors $ka \equiv k'a[p]$, puis $a(k-k') \equiv 0[p]$, ce qui veut dire que p divise $a(k-k')$. On peut donc conclure comme tout à l'heure.
- On obtient donc que $a^{p-1}(p-1)! = a\times 2a\times 3a\times\cdots\times(p-1)a \equiv r_1\times r_2\times\cdots\times r_{p-1}[p]$. Or les r_k sont $p-1$ entiers distincts compris entre 1 et $p-1$: il s'agit donc exactement des entiers de 1 à $p-1$ à l'ordre près, donc leur produit est égal à $(p-1)!$
  On obtient donc que $a^{p-1}(p-1)! \equiv (p-1)![p]$
- Pour conclure, on montre facilement que p est premier avec $(p-1)!$. Or p est premier avec $(a^{p-1}-1)\big((p-1)!\big)$ et on utilise une troisième fois le théorème de Gauss pour conclure que p divise $a^{p-1}-1$.

IV - ÉNONCÉS DES EXERCICES

Exercice 1 Petit théorème de Fermat

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 et a un entier naturel premier avec p, alors $a^{p-1}-1 \equiv 0 \mod p$ ».

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, le nombre $4^{4k}-1$ est divisible par 17.

4. Pour quels entiers naturels n le nombre 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 nombre premier
Soit p un nombre premier différent de 2.

1. Démontrer qu'il existe un entier $n \geqslant 1$ tel que $4^n \equiv 1 \mod p$.

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

a) Démontrer que $4^r \equiv 1 \mod p$. 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 $p-1$.

[j] Un petit exercice d'entraînement consiste à les démontrer

Exercice 2 Tiens, le petit théorème de Fermat

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

1. Soit p un nombre premier impair.

a) Montrer qu'il existe un entier naturel k, non nul, tel que $2^k \equiv 1 \quad [p]$.

b) Soit k un entier naturel non nul tel que $2^k \equiv 1 \quad [p]$ et soit n un entier naturel. Montrer que, si k divise n, alors $2^n \equiv 1 \quad [p]$.

c) Soit b tel que $2^b \equiv 1 \quad [p]$, b étant le plus petit entier non nul vérifiant cette propriété.
Montrer, en utilisant la division euclidienne de n par b, que si $2^n \equiv 1 \quad [p]$, alors b divise n.

2. Soit q un nombre premier impair et le nombre $A = 2^q - 1$.
On prend pour p un facteur premier de A.

a) Justifier que : $2^q \equiv 1 \quad [p]$.

b) Montrer que p est impair.

c) Soit b tel que $2^b \equiv 1 \quad [p]$, 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 $p \equiv 1 \quad [2q]$.

3. Soit $A_1 = 2^{17} - 1$. Voici la liste des nombres 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.

Exercice 3 Oh ! Le petit théorème de Fermat

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 de 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 nombre 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 $g[f(0)] = 0$.
On rappelle le résultat suivant appelé petit théorème de Fermat :
Si p est un nombre premier et a un entier non divisible par p alors $a^{p-1} \equiv 1$ modulo p.

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

c) En utilisant **1. b.**, en déduire que, quel que soit l'entier non nul a de A. $g[f(a)] = a$.
Que peut-on dire de $f[(g(a)] = a$?

Exercice 4 Fichtre ! Le petit théorème de Fermat

On rappelle le (petit) théorème de Fermat : si p est un nombre premier qui ne divise pas l'entier naturel a, alors on a la congruence

$$a^{p-1} \equiv 1 \mod p$$

Partie A

1. a) Prouver que 29 est un nombre premier.

b) Soit $x \in \mathbb{N}$ et n un entier naturel tel que $n \equiv 1 \mod 28$.
En utilisant le théorème de Fermat, prouver que $x^n \equiv x \mod 29$.

2. On considère l'équation (E) : $17x - 28y = 1$ où $(x,\ y) \in \mathbb{Z}^2$.

a) Quel théorème permet d'affirmer que l'équation (E) admet au moins un couple solution d'entiers relatifs ?

b) En utilisant l'algorithme d'Euclide, trouver un tel couple solution.

Partie B

Soit A = $\{x \in \mathbb{N},\ x < 29\} = \{0,\ 1,\ 2,\ \ldots,\ 28\}$.
Pour $x \in$ A, on note $f(x)$ le reste de la division euclidienne de x^{17} par 29 et $g(x)$ le reste de la division euclidienne de x^5 par 29.

3. a) Prouver que $f(x) \in$ A et $x^{17} \equiv f(x) \mod 29$.
On admettra (la démonstration est analogue) que $g(x) \in$ A et $x^5 \equiv g(x) \mod 29$.

b) Pour $x \in$ A, prouver que $g\left[f(x)\right] = x$.

4. Applications : On attribue à chaque lettre de l'aphabet et aux deux signes + et − , l'entier donné par le tableau ci-dessous :

a	b	c	d	e	f	g	h	i	j	k	l	m	n
1	2	3	4	5	6	7	8	9	10	11	12	13	14
o	p	q	r	s	t	u	v	w	x	y	z	+	−
15	16	17	18	19	20	21	22	23	24	25	26	27	28

a) Bob code le mot « GAUSS » à l'aide de la fonction f et envoie le message codé à Alice.
Voici le codage des deux premières lettres « G » et « A » :

Message initial	G	A
Entier associé	7	1
Utilisation de f	$7^{17} \equiv 24 \mod 29$	$1^{17} \equiv 1 \mod 29$
Message codé	X	A

Compléter son message.

b) Alice reçoit le message suivant, codé par Bob, à l'aide de la fonction f :

J	I	L	L	R

Décrypter ce message à la place d'Alice.

Exercice 5 Le théorème d'Euler

1. On appelle indicateur d'Euler de n et on note $\varphi(n)$ le nombre d'entiers inférieurs à n et premiers avec n.

a) Calculez $\varphi(1), \ldots, \varphi(10)$.

b) On suppose que p est premier : calculez $\varphi(p)$ et $\varphi(p^2)$.

c) Soient p et q deux entiers premiers distincts : calculez $\varphi(pq)$.

2. On rappelle qu'un élément a de $[\![0, n-1]\!]$ est inversible modulo n s'il existe un élément a' de $[\![0, n-1]\!]$ tel que $aa' \equiv 1[n]$
Montrez que le nombre d'entiers inversibles modulo n de $[\![0, n-1]\!]$ est égal à $\varphi(n)$.

3. Soit n un entier non nul et a un entier premier avec n.

a) Soit $y \in [\![0, n-1]\!]$. Montrez qu'il existe un unique entier x de $[\![0, n-1]\!]$ tel que $ax \equiv y[n]$

b) Montrez que x est inversible modulo n si et seulement si ax l'est aussi.

c) Soit $I = \{x_1, ..., x_m\}$ l'ensemble des entiers de $[\![0, n-1]\!]$ inversibles modulo n, ces entiers étant tous distincts. Montrez que

$$x_1 \cdot x_2 \cdots x_m \equiv (ax_1) \cdot (ax_2) \cdots (ax_m)\,[n]$$

d) Déduisez-en le **théorème d'Euler** : si a et n sont premiers entre eux, alors $a^{\varphi(n)} \equiv 1[n]$.

e) Quel cas particulier de ce théorème est bien connu ?

V - Quelques exercices de Bac

Exercice 6

1. Démonstration de cours.
Démontrer qu'il existe une infinité de nombres premiers.

2. Soit p un nombre premier strictement plus grand que 2. Démontrer que p est congru à 1 ou à -1 modulo 4. Donner deux exemples de chacun de ces cas.
Le but de ce qui suit est de répondre à la question suivante : « *Les nombres premiers p congrus à -1 modulo 4 sont-ils en nombre fini ?* »
Supposons que ce soit le cas : soit n le nombre des nombres premiers congrus à -1 modulo 4 ; notons $A = p_1 p_2 \cdots p_n$ le produit de ces nombres et $B = 4A - 1$.

3. Montrer que B est congru à -1 modulo 4.

4. Soit q un diviseur premier de B. Montrer que q est distinct de chacun des nombres $p_1,\ p_2,\ \cdots,\ p_n$ précédents.
Montrer que parmi les diviseurs premiers de B, l'un au moins est congru à -1 modulo 4.

5. Quelle réponse apporter à la question posée ?

Exercice 7 Rep-units première version

Les nombres 1 ; 11 ; 111 ; 1111 etc. sont des nombres que l'on appelle rep-units (répétition de l'unité). Ils ne s'écrivent qu'avec des chiffres 1. Ces nombres possèdent de nombreuses propriétés : nous allons en découvrir quelques-unes.
Pour k un entier strictement positif, on note N_k le rep-unit qui s'écrit avec k chiffres 1.

1. Citez deux nombres premiers inférieurs à 10 n'apparaissant jamais dans la décomposition d'un rep-unit. Justifiez rapidement votre réponse.

2. À quelle condition sur k le nombre 3 apparaît-il dans la décomposition du rep-unit N_k ? Justifiez brièvement votre réponse.

3. Pour $k \geqslant 1$, $N_k = \sum_{i=0}^{k-1} 10^i = 1 + 10^1 + 10^2 + \cdots + 10^{k-1}$ Justifiez l'égalité suivante pour tout $k \geqslant 1$

$$9N_k = 10^k - 1$$

4. Le tableau ci-dessous donne les restes de la division par 7 de 10^k, pour $k \in [\![1, 8]\!]$

k	1	2	3	4	5	6	7	8
Reste de la division de 10^k par 7	3	2	6	4	5	1	3	2

Soit k un entier strictement positif. Démontrez que

$$10^k \equiv 1[7] \iff k \text{ est un multiple de 6}$$

Déduisez-en que 7 divise N_k si et seulement si 6 divise k.

Exercice 8 Autre formulation

Les nombres 1 ; 11 ; 111 ; 1111 etc. sont des nombres que l'on appelle rep-units (répétition de l'unité). Ils ne s'écrivent qu'avec des chiffres 1. Ces nombres possèdent de nombreuses propriétés : nous allons en découvrir quelques-unes.
Pour k un entier strictement positif, on note N_k le rep-unit qui s'écrit avec k chiffres 1.

1. Citez deux nombres premiers inférieurs à 10 n'apparaissant jamais dans la décomposition d'un rep-unit. Justifiez rapidement votre réponse.

2. Donnez la décomposition en facteurs premiers de N_3, N_4 et N_5.

3. Soit n un entier strictement supérieur à 1. On suppose que l'écriture décimale de n^2 se termine par le chiffre 1.

a) Montrez que, dans son écriture décimale, n se termine lui-même par 1 ou par 9.

b) Montrez qu'il existe un entier m tel que n s'écrive sous la forme $10m+1$ ou $10m-1$.

c) Déduisez-en que $n^2 \equiv 1[20]$.

4. a) Soit $k \geqslant 2$. Quel est le reste de la division de N_k par 20 ?

b) Déduisez-en qu'un rep-unit distinct de 1 n'est pas un carré.

Exercice 9 Rep-units : épisode III

On se propose dans cet exercice d'étudier le problème suivant :
« *Les nombres dont l'écriture décimale n'utilise que le seul chiffre* 1 *peuvent-ils être premiers* ? »
Pour tout entier naturel $p \geqslant 2$, on pose $N_p = 1\ldots1$ où 1 apparaît p fois.
On rappelle dès lors que $N_p = 10^{p-1} + 10^{p-2} + \cdots + 10^0$.

1. Les nombres $N_2 = 11$, $N_3 = 111$, $N_4 = 1111$ sont-ils premiers ?

2. Prouver que $N_p = \dfrac{10^p - 1}{9}$. Peut-on être certain que $10^p - 1$ est divisible par 9 ?

3. On se propose de démontrer que si p n'est pas premier, alors N_p n'est pas premier.
On rappelle que pour tout nombre réel x et tout entier naturel n non nul,

$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right).$$

a) On suppose que p est pair et on pose $p = 2q$, où q est un entier naturel plus grand que 1.
Montrer que N_p est divisible par $N_2 = 11$.

b) On suppose que p est multiple de 3 et on pose $p = 3q$, où q est un entier naturel plus grand que 1.
Montrer que N_p est divisible par $N_3 = 111$.

c) On suppose p non premier et on pose $p = kq$ où k et q sont des entiers naturels plus grands que 1.
En déduire que N_p est divisible par N_k.

4. Énoncer une condition nécessaire pour que N_p soit premier.
Cette condition est-elle suffisante ?

Exercice 10 Dernière formulation pas encore tombée au Bac

1. Montrez que $N_k = \dfrac{10^k - 1}{9}$

2. Démontrez que, lorsque k est pair, 11 divise N_k.

3. Démontrez que $\dfrac{b^{mr} - 1}{b-1} = \dfrac{b^m - 1}{b-1} \displaystyle\sum_{i=0}^{r-1} (b^m)^i$

4. Démontrez que si p divise k, alors N_p divise N_k.

5. Déduisez-en que si N_k est premier, alors k l'est aussi. La réciproque est-elle vraie ?

6. a) Démontrez pour $b \neq 1$ et $k \geqslant k'$ l'égalité

$$\frac{b^k-1}{b-1} = b^{k-k'}\left(\frac{b^{k'}-1}{b-1}\right) + \frac{b^{k-k'}-1}{b-1}$$

b) déduisez-en que les diviseurs communs de N_k et $N_{k'}$ sont les diviseurs communs de $N_{k'}$ et $N_{k-k'}$.

c) démontrez par récurrence que si k et k' sont premiers entre eux, alors N_k et $N_{k'}$ le sont aussi.

Exercice 11 Un problème sur les nombres premiers appartenant à une suite.

La suite (u_n) est définie par $u_1 = 1$, $u_2 = 2$ et $u_{n+2} = u_{n+1} + u_n + 1 \quad (i)$.
Le but du problème est de rechercher tous les nombres premiers de cette suite.
(W_n) est la suite définie pour tout n de $\mathbb{N}^*$ par $w_n = u_n + 1$.

1. Vérifiez que (w_n) est la suite de Fibonacci, i.e. $w_{n+2} = w_{n+1} + w_n$.

2. Démontrez par récurrence que

$$w_{2n}^2 = w_{2n-1}w_{2n+1} - 1 \quad (ii) \qquad \text{et} \qquad w_{2n+1}^2 = w_{2n}w_{2n+2} + 1 \quad (iii)$$

3. a) Déduisez des relations (ii) et (i) la relation

$$(u_{2n+1} - u_{2n-1})^2 = u_{2n-1}u_{2n+1} + u_{2n-1} + u_{2n+1}$$

b) Démontrez que

$$(u_{2n+1} + u_{2n-1})^2 = 5u_{2n-1}u_{2n+1} + u_{2n-1} + u_{2n+1}$$

c) Déduisez-en que

$$5u_{2n-1}u_{2n+1} = (u_{2n+1} + u_{2n-1})(u_{2n+1} + u_{2n-1} - 1) \quad (iv)$$

4. Démontrez que si u_{2n-1} est premier, il divise soit u_{2n+1}, soit $u_{2n+1} - 1$.

5. *Étude du cas $u_{2n+1} = ku_{2n-1}$ avec k entier.*

a) Expliquez pourquoi $k > 1$.

b) Démontrez en utilisant (iv) que

$$(k^2 - 3k + 1)u_{2n-1} = 1 + k$$

c) Démontrez que $k = 2$ ou $k > 4$ conduit à des valeurs de u_{2n-1} impossibles.

d) Démontrez que pour les valeurs restantes de k, les valeurs de u_{2n-1} ne sont pas des nombres premiers.

6. *Étude du cas $u_{2n+1} - 1 = ku_{2n-1}$ avec k entier.*

a) Expliquez pourquoi $k > 1$ et montrez en utilisant (iv) que

$$4 - k = (k^2 - 3k + 1)u_{2n-1}$$

b) Montrez que $k = 2$ ou $k > 3$ donne pour u_{2n-1} une valeur qui n'est pas entière positive.

c) la possibilité $k = 3$ donne-t-elle un nombre premier ?

d) Conclusion ?

7. a) Utilisez (iii) pour montrer que

$$((u_{2n+2} + 1) + (u_{2n} + 1))^2 = 5(u_{2n} + 1)(u_{2n+2} + 1) + 1$$

b) Déduisez-en la relation v

$$5u_{2n}u_{2n+2} = (u_{2n} + u_{2n+2} - 2)(u_{2n} + u_{2n+2} + 1) \quad (v)$$

8. a) Démontrez que si u_{2n} est premier, il divise $u_{2n+2} - 2$ ou $u_{2n+2} + 1$.

b) Expliquez pourquoi le « ou » est nécessairement exclusif.

9. *Étude du cas où $u_{2n+2} - 2 = ku_{2n}$ avec k un entier*

a) Justifiez que $k > 1$.

b) Utilisez (v) pour montrer que l'on aurait alors

$$7 - 3k = (k^2 - 3k + 1)\,u_{2n}$$

c) Montrez que $k = 2$ ou $k > 2$ ne donne pas une valeur entière positive à u_{2n}

10. *Étude du cas $u_{2n+2} + 1 = ku_{2n}$ avec k entier*

a) Justifiez que $k > 1$ et utilisez (v) pour montrer que

$$3k - 2 = (k^2 - 3k + 1)\,u_{2n}$$

b) Montrez que $k = 2$ ou $k > 5$ conduit à une impossibilité pour u_{2n}

c) Quels sont les seuls termes de la suite qui sont des entiers premiers ?

Exercice 12

Soit l'équation (1) d'inconnue rationnelle x :

$$78x^3 + ux^2 + vx - 14 = 0.$$

où u et v sont des entiers relatifs.

1. On suppose dans cette question que $\dfrac{14}{39}$ est solution de l'équation (1).

a) Prouver que les entiers relatifs u et v sont liés par la relation $14x + 39y = 1$.

b) Utiliser l'algorithme d'Euclide, en détaillant les diverses étapes du calcul, pour trouver un couple $(x\,;\,y)$ d'entiers relatifs vérifiant l'équation $14x + 39y = 1$.
Vérifier que le couple $(-25\,;\,9)$ est solution de cette équation.

c) En déduire un couple $(u_0\,;\,v_0)$ solution particulière de l'équation $14u + 39v = 1$.
Donner la solution générale de cette équation c'est-à-dire l'ensemble des couples $(u\,;\,v)$ d'entiers relatifs qui la vérifient.

d) Déterminer, parmi les couples $(u\,;\,v)$ précédents, celui pour lequel le nombre u est l'entier naturel le plus petit possible.

2. a) Décomposer 78 et 14 en facteurs premiers.
En déduire, dans $\mathbb{N}$, l'ensemble des diviseurs de 78 et l'ensemble des diviseurs de 14.

b) Soit $\dfrac{P}{Q}$ une solution rationnelle de l'équation (1) d'inconnue x :

$$78x^3 + ux^2 + vx - 14 = 0 \quad \text{où} \quad u \quad \text{et} \quad y \quad \text{sont des entiers relatifs.}$$

Montrer que si P et Q sont des entiers relatifs premiers entre eux, alors P divise 14 et Q divise 78.

c) En déduire le nombre de rationnels, non entiers, pouvant être solutions de l'équation (1) et écrire, parmi ces rationnels, l'ensemble de ceux qui sont positifs.

Exercice 13

On désigne par p un nombre entier premier supérieur ou égal à 7.
Le but de l'exercice est de démontrer que l'entier naturel $n = p^4 - 1$ est divisible par 240, puis d'appliquer ce résultat.

1. Montrer que p est congru à -1 ou à 1 modulo 3. En déduire que n est divisible par 3.

2. En remarquant que p est impair, prouver qu'il existe un entier naturel k tel que $p^2 - 1 = 4k(k+1)$, puis que n est divisible par 16.

3. En considérant tous les restes possibles de la division euclidienne de p par 5, démontrer que 5 divise n.

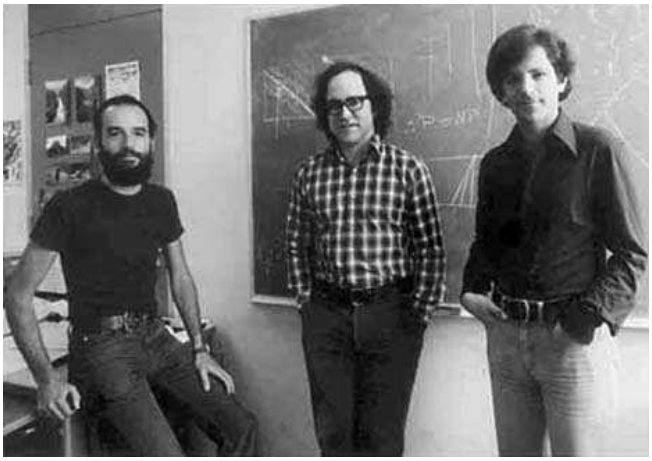
4. a) Soient a, b et c trois entiers naturels.
Démontrer que si a divise c et b divise c, avec a et b premiers entre eux, alors ab divise c.

b) Déduire de ce qui précède que 240 divise n.

5. Existe-t-il quinze nombres premiers p_1, p_2,..., p_{15} supérieurs ou égaux à 7 tels que l'entier A = $p_1^4 + p_2^4 + ... + p_{15}^4$ soit un nombre premier ?

VI - Système RSA

a. Systèmes à clé publique



Voici nos amis Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman avant que les mathématiques les rendent riches et célèbres. Ces braves chercheurs mirent au point en 1977 un système de codage alors qu'ils essayaient au départ de montrer que ce qu'ils allaient développer étaient une impossibilité logique : aah, la beauté de la recherche...Et savez-vous quel est la base du système ? Je vous le donne en mille : le petit théorème de Fermat ! Mais replaçons dans son contexte les résultats de R, S et A. Jusqu'il y a une trentaine d'années, la cryptographie était l'apanage des militaires et des diplomates. Depuis, les banquiers, les mega business men et women, les consommateurs internautes, les barons de la drogue et j'en passe ont de plus en plus recours aux messages codés. Oui, et alors ? Le problème, c'est que jusqu'ici, l'envoyeur et le destinataire partageait une même clé secrète qu'il fallait faire voyager à l'insu de tous : les états et l'armée ont la valise diplomatique, mais les autres ?
C'est ici que Whitfield Diffie et Martin Hellman apparaissent avec leur idée de principe qu'on peut résumer ainsi : votre amie Josette veut recevoir de vous une lettre d'amour mais elle a peur que le facteur l'intercepte et la lise. Elle fabrique donc dans son petit atelier une clé et un cadenas. Elle vous envoie le cadenas, ouvert mais sans la clé, par la poste, donc à la merci du facteur : le cadenas est appelé *clé publique*. Vous recevez le cadenas et l'utilisez pour fermer une boîte contenant votre lettre : le facteur ne peut pas l'ouvrir car il n'a pas la clé. Josette reçoit donc la boîte fermée : elle utilise sa clé, qu'elle seule possède, pour ouvrir la boîte et se pâmer devant vos élans epistolaires.

En termes plus mathématiques, cela donne : je fabrique une fonction π définie sur $\mathbb{N}$ qui possède une réciproque σ. On suppose qu'on peut fabriquer de telles fonctions mais que si l'on ne connaît que π, il est (quasiment) impossible de retrouver σ. La fonction ${}_p i$ est donc la clé publique : vous envoyez π(message) à Josette. Celle-ci calcule $\sigma\big(\pi(\text{message})\big) = \text{message}$. Josette est la seule à pouvoir décoder car elle seule connaît σ.
Tout ceci était très beau en théorie, mais Diffie et Hellman n'arrivèrent pas à proposer de telles fonctions. Mais voici qu'arrivent Ronald, Adi et Leonard...

Je vais vous présenter la méthode en effectuant les calculs grâce à Xcas. Il ne vous restera plus qu'à prouver mathématiquement que tout ceci fonctionne de manière cohérente...

Voici comment quelqu'un peut m'envoyer un message crypté en utilisant le protocole RSA, que personne ne peut comprendre sauf moi, puis comment je vais décrypter ce message.
Avant de m'envoyer un message, on doit connaître ma *clé publique*, connue de tous et constituée d'un couple de nombres (n, e).
Et avant de connaître cette clé, il faut que je la fabrique - secrètement - de la manière suivante :

▷ je commence par fabriquer un nombre premier quelconque mais suffisamment grand

```
>>  p:=nextprime(4578465795689568795678456845684567879065780) ;
4578465795689568795678456845684567879065841
```

▷ puis un autre

```
>> q:=nextprime(907689576834535362345135535467569745645734576) ;
907689576834535362345135535467569745645734587
```

Ces deux nombres ne sont connus que de moi !

▷ je forme le produit de ces deux nombres

```
>> n:=p*q ;
4155825680640858939562812705134419974961298878181518872770399803455388286242591783942667
```

Ce nombre n est mon module public. Il reste à former le nombre e qui est ma puissance de cryptage publique. Là encore, cela se fait par étapes.

- je commence par former le nombre phi_n (tiens, tiens...) de la manière suivante

```
>> phi_n:=(p-1)*(q-1) ;
4155825680640858939562812705134419974961297965913476242545468662641395972988278259142240
```

- c'est là qu'il faut jouer avec la chance : je dois choisir un nombre f premier avec phi_n. En pratique, je choisis un grand nombre premier au hasard :

```
>> f:=nextprime(85434678565724658567586345678968 97) ;
8543467856572465856758634567896901
```

Vérifions quand même que e et phi_n sont premiers entre eux

```
>> gcd(f,phi_n) ;
1
```

Ouf !...[k]

- il me reste à calculer ma puissance de décryptage secrète : je l'obtiens en cherchant l'inverse de e modulo phi_n, c'est à dire, comme vous commencez à le savoir puisque nous l'avons vu plusieurs fois, en déterminant un coefficient de Bézout grâce à l'algorithme d'Euclide étendu.

  Le problème, c'est que nos nombres sont un peu grands pour faire l'algorithme à la main, mais...heureusement, il y a Xcas. Il existe en effet une fonction inv(x%y) qui renvoie l'inverse de x modulo y.

```
>> d:= inv(f%phi_n) ;
-3414987797179866265176149416818690937234903531057159987469061279458935163489 5
      2729281779 % 4155825680640858939562812705134419974961297965913476242545 4
      6866264139597298827825914224 0
```

Bof : Xcas nous donne le résultat modulo phi_n. On le « transforme » en un entier « tout court », c'est à dire modulo 0.

```
>> D:=d%0 ;
-341498779717986626517614941681869093723490353105715998746906127945893516348952729281779
```

Je suis maintenant prêt à recevoir des messages cryptés selon le protocole RSA et vous êtes prêt(e) à m'en envoyer car j'ai rendu publique ma clé (e,n).

- d'abord vous « numérisez » votre message en prenant soin d'écrire en majuscule pour avoir des codes ASCII de deux chiffres : en fait, on transforme chaque lettre en son code ASCII.

```
>> text_num:=expr(cat(asc("LE LUNDI AU SOLEIL"))) ;
76693276857868733265853283797669737 6
```

- On applique le codage grâce à la clé publique

```
>> crypte:=powmod(text_num,f,n) ;
37346907654183423958441372457068261986812349914527863692150903018850278014961867155194 39
```

- On décode sous forme numérique grâce à notre clé secrète D

```
>> decrypt:=powmod(crypte,D,n) ;
76693276857868733265853283797669737 6
```

- On crée une procédure qui prend les chiffres de l'entier décrypté deux par deux et associe la lettre associée par le codage ASCII

[k] Pouvait-on en être sûr ?

```
>> alph(n):={
>> local l,L;
>> L:=[];l:=cat(n);
>> for (k:=0;k<size(l);k:=k+2){
>> L:=concat(L,expr(mid(l,k,2)))
>> }
>> return char(L);
>> };;
```

▷ et on traduit

```
>> alph(decrypt) ;
"LE LUNDI AU SOLEIL"
```

Ça marche !