Chapitre 16

Nombres premiers

Résumé -

Nous continuons notre plongée dans la reine des mathématiques : l'arithmétique. Euclide s'est particulièrement concentré sur l'ensemble des nombres premiers. C'est le but de ce chapitre.
Nous verrons que cet ensemble reste toujours le graal des mathématiciens.
Ces dernières années, les nombres premiers sont revenus au centre des mathématiques comme le coeur des applications numériques de codes secrets (internet...).
Cela nous permettra d'étudier l'énoncé et des applications du petit théorème de Fermat. Nous prendrons le temps de comprendre les idées du plus grand mathématicien toulousain !
Youtube (parodies ?) :

- *Panpan1963 - Petit théorème de Fermat - https ://www.youtube.com/watch ?v=Ei4PMxddm9Q*
- *ScienceEtonnante - Les nombres premiers - https ://www.youtube.com/watch ?v=R37JHiA-HOg*

Sommaire

1. Problèmes

? Problème 73 - Produit de premiers

Est-ce qu'on peut vraiment tout faire (multiplicativement) qu'avec des nombres premiers ?

? Problème 74 - Construction du cours

La notion de divisibilité est toujours première dans un cours d'arithmétique d'entiers.
Puis, ici nous avons choisi (selon le programme officielle) un cours sous la forme : PGCD (et PPCM) $\Longrightarrow$ Nombres premiers $\Longrightarrow$ congruence.
Dans son cours, GAUSS avait choisi : congruence $\Longrightarrow$ PGCD (et PPCM) $\Longrightarrow$ Nombres premiers. Quant à EUCLIDE, il commence par les nombres premiers.
Quel est le choix qui vous semble plus naturel ? Comment les démonstrations en sont-elles changées ?

? Problème 75 - Fonctions arithmétiques

Si une fonction $f : \mathbb{N} \to \mathbb{Z}$ est un morphisme : $f(ab) = f(a) \times f(b)$ ou $f(ab) = f(a) + f(b)$, que peut-on dire de f, en particulier concernant son image sur $\mathscr{P}$, l'ensemble des nombres premiers qui génèrent $\mathbb{N}$ par multiplication ?

2. Théorèmes d'Euclide

2.1. Définition

Il ne s'agit plus d'une notion relative comme précédemment (a et b sont premiers entre eux). Ici, il s'agit d'une notion absolue.

Définition - Nombre premier
Soit $p \in \mathbb{N}^*$.
On dit que p est (un nombre) premier
si $p \neq 1$ et si les seuls diviseurs de p dans $\mathbb{N}$ sont 1 et p.
On note souvent $\mathscr{P}$, l'ensemble des nombres premiers.

Le premier théorème d'Euclide est la version « nombre premier » du lemme de Gauss.

Pour aller plus loin - Nombres premiers
Dans un anneau euclidien (muni d'une division euclidienne), un nombre premier est un nombre qui n'est divisible que par des inversibles de l'anneau : si $p = a \times b$, alors a ou $b \in A^*$.
Ici $\mathbb{Z}^* = \{-1, 1\}$. Et pour les polynômes, un polynôme premier n'est divisible que par des constantes : $(\mathbb{K}[X])^* = \mathbb{K}$, c'est un polynôme irréductible.
Un autre anneau euclidien bien connu est $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, l'anneau des entiers de GAUSS.

2.2. Lemmes d'Euclide

On reconnait le lemme de Gauss et ses corollaires, mais associés à des nombres premiers.

Proposition - Premier théorème d'Euclide
Un nombre premier est premier avec tous les entiers qu'il ne divise pas.
Un nombre premier divise un produit si et seulement si il divise l'un des facteurs.

Démonstration

L'intérêt des nombres premiers est d'être des briques élémentaires multiplicatives de $\mathbb{Z}$, on ne peut la couper en deux.
La remarque suivante est un savoir-faire, puisqu'elle donne un truc de manipulation de nombres premiers. Mais c'est aussi un ATTENTION, car il y est associée une erreur fréquente, dans le cas de nombres non premiers.

Savoir faire - Trouver un facteur premier avec un nombre premier
Soit $p \in \mathscr{P}$ tel que $p|ab$ alors p divise a ou p divise b.
Ce n'est pas le cas de $p = 12$ qui divise 6×4 avec $a = 6$ et $b = 4$, par exemple

Théorème -
Tout entier naturel $n \geqslant 2$ possède au moins un diviseur premier.

Démonstration

Corollaire - Critère de primalité entre deux entiers
Soient $a, b \in \mathbb{Z}$.
Alors a et b sont premiers entre eux si et seulement s'ils n'ont aucun diviseur premier en commun.

Démonstration

Pour aller plus loin - Idéaux premiers
On retrouve aussi la même notion dans la définition des idéaux premiers d'un anneau intègre (vu en seconde année).
De même un groupe simple est un groupe qui ne peut se décomposer en produit de sous-groupes (distingués). La décomposition d'un groupe en produit de sous-groupe simple suit à la même philosophie…

2.3. Théorème fondamental

Puis le théorème fondamental de l'arithmétique :

Théorème - Décomposition en produit de facteurs premiers
Soit $n \in \mathbb{N}$, $n \geqslant 2$.
Alors il existe $r \in \mathbb{N}$, $p_1, p_2, \dots p_r$, r nombres premiers et $\alpha_1, \dots \alpha_r \in \mathbb{N}^*$ tel que

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

Cette écriture est unique.

Démonstration

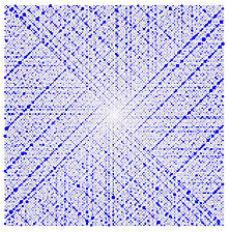
3. L'ensemble des nombres premiers

3.1. Ensemble infini

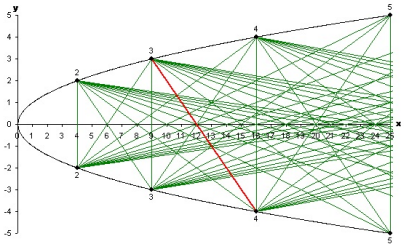
Proposition - Théorème d'Euclide
L'ensemble des nombres premiers, noté $\mathscr{P}$ (parfois $\mathbb{P}$) est infini.

Démonstration

Représentation - Deux visions de $\mathscr{P}$
Sans commentaires :
Spirale d'Ulam :



Crible de Matiyasevich



Cet ensemble mystérieux représente une sorte de graal du mathématicien.

Remarque - Ensemble dénombrable
Comme tout ensemble inclus dans $\mathbb{N}$ et infini, $\mathscr{P}$ est dénombrable, c'est-à-dire il existe une bijection de $\mathbb{N}$ dans $\mathscr{P}$. Et cela signifie qu'on peut donc écrire $\mathscr{P} = \{p_1, p_2, \dots p_r, \dots\}$, où $p_1 = 2$ est le premier des nombres premiers, $p_2 = 3$, $p_3 = 5\dots$, p_r est le r-ième nombre premier.

Proposition - Enumération des nombres premiers
Il existe une bijection $\rho : \mathbb{N}^* \to \mathscr{P}$, $i \mapsto p_i$, le i-ième nombre premier

Exercice
Que vaut p_{10} ?

Démonstration

3.2. Crible d'Eratosthène

Informatique - Crible d'Eratosthène
Pour obtenir la liste des nombres premiers, nous n'avons pas trouvé beaucoup mieux que le crible d'Eratosthène (3-ième siècle avant J-C).
Il s'agit d'écrire la liste des entiers de 1 à n. Puis d'enlever les multiples des nombres qui restent. Une fois terminée (deux boucles), il ne reste que la liste des nombres premiers plus petit que n.

```
def Eratosthene(n):
    """Crible d'Erathostene adapte"""
    L=[1]*n
    for k in range(2,n):
        if L[k]==1 :
            h=2*k
            while h<n :
                L[h]=0
                h=h+k
    P=[]
    for k in range(1,n):
        if L[k]==1 :
            P=P+[k]
    return(P)
```

Remarque - Conjectures
L'ensemble $\mathscr{P}$ est infini, mais une question résiste : contient-il une infinité de nombres premiers jumeaux?
On dit que $(p, p+2)$ est un couple de nombres premiers jumeaux si ils sont tous les deux premiers. Par exemple $(3,5)$ ou $(11,13)$ sont des nombres premiers jumeaux.
Ben Green(1977-) et Terence Tao (1975-) ont démontré ce qui est désormais connu sous le nom de théorème de Green-Tao (pré-publié en 2004 et publié en 2008). Ce théorème établit qu'il existe des progressions arithmétiques de nombres premiers arbitrairement longues.
Un résultat culturel (mais pas nécessairement à retenir)

Histoire - Conjecture de Riemann
Parmi les problèmes qui résistent aux mathématiciens, ce trouve la fameuse conjecture de Riemann. Elle concerne directement les nombres premiers même si elle s'énonce avec des nombres complexes. L'esthétisme de cette conjecture réside en partie dans le lien miraculeux entre l'arithmétique à l'ensemble des fonctions de la variable complexe. L'énoncé est :
Les zéros non triviaux de la fonction

$$\begin{array}{rccc} \zeta : & \mathbb{C} & \to & \mathbb{C} \\ & s & \to & \displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^s} \end{array}$$

ont une partie réelle exactement égale à $\frac{1}{2}$.
Lire : la symphonie des nombres premiers de Marcus du Sautoy

Théorème - Hadamard - De la Vallée Poussin (1896)
Notons $\pi(n)$, le nombre de nombres premiers plus petit que n. Alors

$$\pi(n) \underset{n\to+\infty}{\sim} \frac{n}{\ln n}$$

Le livre Merveilleux nombres premiers de Jean-Paul Delahaye donne une foule d'informations et d'anecdotes concernant les nombres premiers (par exemple : l'histoire des jumeaux John et Michael qui voient les nombres premiers...).

Exercice
En exploitant le théorème de Hadamard-De la vallée Poussin, donner une valeur approchée du 1000 nombre premiers (i.e. de p_{1000})

4. Valuation (p-adique)

4.1. Fonction valuation (en base p)

Définition - Valuation p-adique
Soit p un nombre premier. Pour $n \in \mathbb{N}$, on appelle valuation p-adique de n le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n. On le note $v_p(n)$.
Donc pour p premier, $p|n \Leftrightarrow v_p(n) \geqslant 1$.

On a les caractérisations suivantes, qu'il faut savoir exploiter comme savoir-faire :

Savoir faire - Caractérisations de $v_p(a)$.

$$\begin{array}{ll} p^h|a & \Longleftrightarrow v_p(a) \geqslant h. \\ p^h q = a \text{ et } p \wedge q = 1 & \Longleftrightarrow v_p(a) = h. \end{array}$$

Démonstration

Exercice
Montrer que $v_p(pb) = 1 + v_p(b)$

Remarque - Réécriture du théorème fondamentale de l'arithmétique
Pour tout $n \in \mathbb{N}$,

$$n = \prod_{i=1}^{+\infty} p_i^{v_{p_i}}(n) = \prod_{p\in\mathscr{P}} p^{v_p}(n)$$

le produit en réalité, nécessairement (à support) fini puisqu'à partir d'un certain rang, $v_{p_k}(n) = 0$.

4.2. Morphisme (de monoïde)

Proposition - Valuation, fonction logarithmique
Pour tout $a, b \in \mathbb{Z}$ et $p \in \mathscr{P}$, $v_p(a \times b) = v_p(a) + v_p(b)$

Démonstration

4.3. Factorisation en produit de premiers

Proposition - Liste des diviseurs
Soient $a, b \in \mathbb{N}$ non nuls. Si

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \text{ et } b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

où les p_i sont des nombres premiers distincts deux à deux, $\alpha_i, \beta_i \in \mathbb{N}$ (éventuellement nuls), alors

$$a|b \iff \forall i \in [\![1, k]\!],\ \alpha_i \leqslant \beta_i$$

$$a \wedge b = PGCD(a, b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$$

$$a \vee b = PPCM(a, b) = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$$

Ce qui peut aussi s'écrire :

Corollaire - Liste des diviseurs, avec la valuation

$$a|b \iff \forall p \text{ premier}, v_p(a) \leqslant v_p(b)$$

$$\forall p \text{ premier}, v_p(a \wedge b) = \min(v_p(a), v_p(b)) \text{ et } v_p(a \vee b) = \max(v_p(a), v_p(b))$$

$$a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))} \qquad a \vee b = \prod_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))}$$

Cette dernière formule se généralisant sans difficulté au cas de k entiers distincts.

Application - Algorithme de recherche du PGCD

Démonstration

Exercice
Soit $n \in \mathbb{N}^*$. Donner une expression de $\text{card}\mathscr{D}(n)$, utilisant les valuations $v_p(n)$

4.4. Formule de Legendre

On termine par un exercice
Exercice
Soit p un nombre premier.
Montrer que $v_p(n!) = \sum_{k=1}^{+\infty} \lfloor \frac{n}{p^k} \rfloor$ (la somme étant en réalité finie).
On pourra s'intéresser aux ensembles $N_a = \{k \in \mathbb{N}_n \mid p^a | k\}$.

5. Garantir que des nombres sont premiers

5.1. Motivations

Heuristique - Décomposable vs. décomposition

L'analyse de la primalité éventuelle d'un nombre n entier peut déboucher sur quatre questions de complexités différentes :

1. Prouver que n n'est pas premier
2. Si n n'est pas premier, le décomposer
3. Garantir, avec un risque d'erreur faible que n est premier
4. Certifier que n est premier

Cela semble comparable, mais le petit théorème de Fermat permet de répondre « aisément » aux questions 1 et 3. Les deux autres questions qui semblent équivalentes sont bien plus compliquées…

Remarque - Obtenir des nombres premiers

L'arithmétique et avec la géométrie la plus vieille branche des mathématiques. Pendant deux millénaires, on s'y intéresse « pour le plaisir ». Mais avec le renouveau de l'algorithmique et la développement exponentielle des ordinateurs, se sont développés deux branches :

— la cryptanalyse
— les codes correcteurs.

Dans ces disciplines, on a très largement besoin de grands nombres premiers. C'est le cas du codage RSA, grand consommateur de nombres premiers qui permet de coder et décoder les messages numérisés (internet, banque…). Il faut trouver des nombres premiers, savoir les reconnaitre. Peut-on faire mieux qu'avec le simple crible d'Eratosthène ?

Analyse - Et pour Fermat ?

Pour aller plus loin - Plus grand nombre premier connu (janvier 2016)
C'est un nombre de Mersenne : $2^{74\,207\,281} - 1$, *il contient plus de 22 millions de chiffres.*

5.2. Enoncé et applications

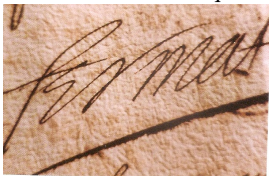
Théorème - Petit théorème de Fermat (1640)
Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$.
Si $n \wedge p = 1$ (i.e. p ne divise pas n) , alors $n^{p-1} \equiv 1[p]$

Histoire - Nombres parfaits
Depuis l'antiquité, de nombreux mathématiciens se sont intéressés aux nombres parfaits. Ce sont les nombres égaux à la somme de leurs diviseurs stricts (sans eux-mêmes).
Ainsi $6 = 1+2+3$ *est parfait. C'est aussi le cas de* 28 *ou* 496*...*

Savoir faire - Exploiter le petit théorème de Fermat
Il y a deux façons d'exploiter ce théorème pour un nombre N :
- Trouver une factorisation (plus exactement un facteur premier) du nombre N de la forme $a^n - 1$ (voir l'application qui suit)
- Montrer que le nombre N est probablement premier ; dans ce cas N joue le rôle de p (voir la remarque : nombre de Carmichaël)

Application - $2^{37} - 1$ est-il premier ?

Histoire - De la main de Fermat
« Tout nombre premier mesure infailliblement une des puissances -1 *de quelques progression que ce soit ; et l'exposant de la dite puissance est sous-multiplie du nombre premier donné* -1 *; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question »*



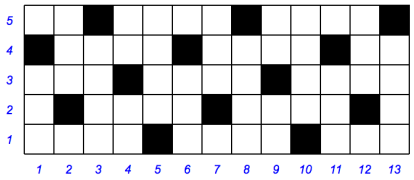
Remarque - Réciproque ? Nombre de Carmichaël
Malheureusement, la réciproque du théorème de Fermat est fausse.
Il existe des nombres non premiers P tels que $P|2^P-2$:

$$341|2^{341}-2$$

C'est le plus petit contre-exemple. On se restreint ici au cas $n=2$.
Mais il y a pire, des nombres p, non premiers qui vérifient : $\forall\ a\in\mathbb{N}$, $p|a^p-a$.
Ces nombres sont appelés les nombres de Carmichaël.
Le plus petit connu est $p=561=3\times11\times17$.
On sait depuis peu (1994) qu'il en existe une infinité.

Exercice
Montrer que $341|2^{341}-2$ sans que 341 soit premier.

Représentation - Illustration de la démonstration
Dans le cas de $p=13$ et $n=31$.
On a alors $n\equiv 5[13]$ et donc $kn\equiv r_k$ se voit sur le carrelage $(a=p=13,b=5)$.
On remarque alors que tous les restes sont obtenus, et une et une seule fois



5.3. Démonstrations

Nous ferons plusieurs démonstrations. Chacune apporte un résultat mathématique différent.

Démonstration

Voici la première démonstration historique d'Euler et probablement de Leibniz :
Exercice
Considérons p un nombre premier.

1. Montrer que $\forall k\in[\![1,p-1]\!],\ p|\binom{p}{k}$
2. $\forall(a,b)\in\mathbb{Z}^2,(a+b)^p\equiv a^p+b^p[p]$
3. En déduire le petit théorème de Fermat

Pour aller plus loin - Fécondité d'un théorème
On peut choisir de mesurer l'intérêt d'un résultat mathématique aux domaines touchés.
Le petit théorème de FERMAT *dont la plupart des démonstrations datent d'*EULER *est assurément un théorème fécond. Chacune des démonstrations présentés ici exploite une partie différente des mathématiques : la structure du groupe $(\frac{\mathbb{Z}}{p\mathbb{Z}},\times)$ pour la première, le morphisme de* FROEBENIUS *: $a\mapsto a^p$ dans le groupe $(\frac{\mathbb{Z}}{p\mathbb{Z}},+)$ pour la seconde. La troisième démonstration assez proche de la première exploite un raisonnement de type combinatoire. La quatrième fait le lien entre la première et la troisième. Elle montre mieux : le petit théorème d'*EULER*, $n^{\varphi(p)}=1[p]$.*

Remarque - Morphisme de Fröbenius
Si p est premier, alors $(a+b)^p=a^p+b^p[p]$ et $(ab)^p=a^pb^p$.

Donc $x \mapsto x^p$ est un morphisme de corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$. C'est un morphisme de corps, a priori non trivial (différent de l'identité). Il s'appelle le morphisme de Frö-benius.
Autre méthode, par double dénombrement :

Exercice

Soit p un nombre premier et n, un entier quelconque.
Considérons un alphabet de n lettres.

1. Combien y a-t-il de mots (possibles) de p lettres avec au moins deux lettres distinctes ? On notera N ce nombre.
2. On note $\mathscr{R}$, la relation d'équivalence sur l'ensemble des mots de p lettres $A = a_1 a_2 \dots a_p$:
$$A \mathscr{R} B \iff \exists\, h \mid B = a_{h+1} a_{h+2} \dots a_p a_1 \dots a_h$$
(Il existe une permutation circulaire des lettres pour passer des mots A à B.
On peut aussi noter que $A = A_1 A_2$ et $B = A_2 A_1$ avec A_1 premier sous-mot de A de longueur h et A_2 de longueur $p-h$.) Montrer qu'il s'agit bien d'une relation d'équivalence.
3. Combien existe-t-il de mots différents dans chaque classe d'équivalence ?
4. On note H le nombre de classe d'équivalence avec au moins deux mots.
Quelle relation existe-t-il entre H, p et N ?
5. En déduire le petit théorème de Fermat.

La seconde démonstration d'Euler exploite (sans le savoir) un théorème dû par la suite à Lagrange.
Cet exercice est un bilan algébrique de l'exercice précédent et de la première démonstration.

Exercice

Soit p premier. Soit $n \in \mathbb{Z}$, supposons que p ne divise pas n.
Notons r le reste de la division euclidienne de n par p.

1. On note $G = (\llbracket 1, p-1 \rrbracket, \times)$. Montrer que $(G, \times)$ est un groupe
2. Montrer qu'il existe $k \in \mathbb{N}$ tel que $r^k \equiv 1[p]$. On note $k_0 = \min\{k \in \mathbb{N} \mid r^k \equiv 1[p]\}$
3. Montrer que $\mathscr{R}$: $a \mathscr{R} b$ ssi $\exists\, k \in \mathbb{Z}$ tel que $a = r^k b$
est une relation d'équivalence.
4. Quelle est la taille de chacune des classe d'équivalence ?
5. On note H le nombre de classe d'équivalence. Montrer que $p - 1 = k_0 \times h$.
En déduire r^{p-1}, puis le théorème de Fermat

Pour aller plus loin - Théorème d'Euler
En affinant ce dernier exercice, on montre que : pour $t > 0$, n tel que $n \wedge t = 1$, alors $n^{\varphi(t)} \equiv n[t]$, avec $\varphi(a)$ est le nombre de diviseur de a.
Pour cela on considère le groupe des $\varphi(t)$ éléments de $\llbracket 1, t-1 \rrbracket$ inversible (i.e. premier avec t).
On notera que si p est premier : $\varphi(p) = p - 1$.

6. Bilan

Synthèse

- ⇝ Les nombres entiers relatifs sont les premiers objets reconnus comme mathématiques rencontrés. Ils sont donc comme à la base du sentiment mathématique de tout apprenti mathématicien.
- ⇝ Plus généralement, au lieu d'étudier des nombres premiers relativement à a, on peut étudier les nombres premiers relativement à tous les nombres. Ce sont les nombres premiers, atomes minimaux des multiplications/divisions d'entiers.
- ⇝ Gauss a eu la merveilleuse idée de plonger $\mathbb{Z}$ dans des sous-ensemble modulo le nombre a qui nous intéresse. Cela marche bien car la structure d'anneau est conservée, mais cela peut être encore plus fort si a est premier, car on crée une structure de corps ! Avec cette façon de penser, beaucoup de théorèmes devient faciles à démontrer voire à comprendre : c'est le cas du petit théorème de Fermat.
Nous re-investirons ce point de vue lors de l'étude des polynômes

⇝ Nous terminons par l'étude hors-programme de quelques fonctions arithmétiques. La motivation est la même que celle pour les séries génératrices. Il est souvent mathématiquement plus simple d'étudier directement toute la suite (u_n) plutôt qu'un seul de ces éléments u_n...

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Trouver un facteur premier, avec un nombre premier.
— Savoir-faire - Caractérisations de $v_p(a)$.
— Savoir-faire - Exploiter le petit théorème de Fermat

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\mathscr{P}_a$	Ensemble des nombres premiers avec a	$b \in \mathscr{P}_a \iff a \wedge b = 1$	Equivalent à $a \in \mathscr{P}_b$ (symétrie)
$\mathscr{P}$	Ensemble des nombres premiers	$\mathscr{D}(p) = \{1,-1,p,-p\}$ et $p \in \mathbb{N}$, $p \geqslant 2$	$p \in \mathscr{P} \Leftrightarrow \forall\ k \in [\![2, p-1]\!]$, $k \in \mathscr{P}_p$
$v_p(a)$	Valuation p-adique de a	$v_p(a) = r \Leftrightarrow a = p^r q$ avec $p \wedge q = 1$	On raisonne plutôt par double inégalité

Retour sur les problèmes

72. En effet, en simplifiant par $(n-1)!$, premier avec n (si n est premier), on trouve $k^{n-1} \equiv 1[n]$

73. Par exemple si l'on commence par les nombres premiers, le lemme de Gauss s'applique avec le théorème 1 d'Euclide...
Nous ne faisons pas ici tous les 6(=3 !) cas possibles

74. $f(p_1 p_2) = f(p_1) \times f(p_2)$ et il suffit de connaître $f(p)$, pour tout $p \in \mathbb{N}$:
$f(\prod_{i=1}^{r} p_i^{r_i}) = \prod_{i=1}^{r} f(p_i)^{r_i}$.