Leçon 121 - Nombres premiers. Applications.

Extrait du rapport de jury

Le sujet de cette leçon est très vaste. Elle doit donc être abordée en faisant des choix qui devront être clairement motivés. On attend une étude purement interne à l'arithmétique des entiers, avec des applications dans différents domaines : théorie des corps finis, théorie des groupes, arithmétique des polynômes, cryptographie, etc. On peut définir certaines fonctions importantes en arithmétique, les relier aux nombres premiers et illustrer leurs utilisations. Il est recommandé de s'intéresser aux aspects algorithmiques du sujet (tests de primalité). La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques simples. La répartition des nombres premiers doit être évoquée : certains résultats sont accessibles dans le cadre du programme du concours, d'autres peuvent être admis et cités pour leur importance culturelle.

Présentation de la leçon

Je vais vous présenter la leçon 121 intitulée : "Nombres premiers. Applications.". La décomposition en facteurs premiers des nombres pour la relation de divisibilité offre de nombreuses informations quant aux diviseurs et aux multiples d'un nombre. La connaissance des nombres premiers apporte donc beaucoup d'informations quant à la structure et au comportement des nombres et des objets construits sur eux, comme par exemple l'ordre d'un groupe ou encore la caractéristique d'un anneau. Cela motive donc la recherche d'informations sur leur répartition, et en particulier les nombreux résultats analytiques associés.
Dans une première partie, on s'intéresse aux nombres premiers ainsi qu'à l'arithmétique dans $\mathbb{Z}$. Tout d'abord on parle de nombres premiers et premiers entre eux en commençant par en rappeler les définitions ainsi que quelques exemples avant de passer à deux résultats très importants en arithmétique que sont l'identité de Bézout ainsi que le lemme de Gauss. On termine ce premier point avec quelques autres résultats sur les nombres premiers en termes de PGCD et PPCM. Dans un deuxième temps, on donne des propriétés plus poussées sur les nombres premiers en commençant par le théorème fondamental de l'arithmétique qui est (comme son nom l'indique !) fondamental pour la relation de divisibilité avant d'en venir à la valuation p-adique d'un nombre ainsi que les propriétés qui en découlent. On donne également quelques résultats de congruence, c'est-à-dire dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. On termine cette partie avec un dernier point concernant l'indicatrice d'Euler qui sert à déterminer le nombre de nombres qui sont premiers à un entier n donné. On donne deux formules pour calculer cette indicatrice avant de donner d'autres propriétés dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ notamment en termes de cyclicité.
Dans une deuxième partie on s'intéresse à la localisation des nombres premiers avec en premier lieu des résultats de répartition. On montre qu'il existe une infinité de nombres premiers et même qu'il existe une infinité de nombres premiers d'une certaine forme d'après le théorème de Dirichlet faible. On montre également que la série des inverses des nombres premiers diverge et l'on donne une application en probabilités avant de conclure par le théorème des nombres premiers et de Bertrand . Dans un deuxième point on donne quelques exemples de types de nombres premiers. On commence tout d'abord avec les nombres de Fermat, puis ensuite les nombres de Mersenne qui sont les plus grands connus et dont beaucoup de conjectures sont encore ouvertes à l'heure actuelle sur ces deux nombres. Enfin on termine par les nombres de Carmichaël qui vérifient la réciproque du théorème de Fermat (qui est fausse en général). On termine cette partie avec des tests de primalité. On commence tout d'abord avec des tests généraux tels que le crible d'Ératosthène où le théorème de Wilson avant de passer sur des tests plus spécifiques tels que les tests de Pépin et de Lucas pour détecter des nombres premiers de Fermat ou de Mersenne.
On termine cette leçon avec une dernière partie consacrée aux applications. On commence tout d'abord avec le cryptage `RSA` qui est utilisé de nos jours en finance et pour protéger nos données bancaires. Cette méthode repose sur le fait qu'il est

très difficile (à l'heure actuelle) de décomposer un très grand nombre en produit de deux nombres premiers. On donne une deuxième application avec l'anneau des entiers de Gauss où l'on donne des inversibles ainsi que le théorème des deux carrés et les éléments irréductibles de cet anneau. On donne une troisième application dans le cadre des anneaux principaux avec le théorème des restes chinois : on énonce le théorème et on donne des conséquences dans le cas de l'anneau $\mathbb{Z}$. On continue par une application en théorie des groupes avec les p-groupes (et notamment la classification des groupes d'ordre p^2) avant de passer aux théorèmes de Sylow ainsi que quelques applications et enfin la classification des groupes d'ordre $2p$. On continue avec une application avec des critères d'irréductibilité avec le critère d'Eisenstein et de réduction qui servent le plus souvent à montrer qu'un polynôme est irréductible dans $\mathbb{Q}[X]$. Finalement, on conclut cette leçon par une dernière sous-partie où l'on parle des corps finis : on introduit la notion de caractéristique et on montre qu'un corps fini a pour cardinal une puissance d'un nombre premier et on en donne un procédé de construction.

Plan général

Cours détaillé

I Nombres premiers et arithmétique dans $\mathbb{Z}$

I.1 Nombres premiers et premiers entre eux

Définition 1 : Nombre premier [Deschamps (1), p.837] :
On appelle **nombre premier** tout entier naturel différent de 1 n'admettant pour diviseurs positifs que 1 et lui-même.

Exemple 2 : [Deschamps (1), p.837]
∗ 2,3,5,7,11,...,65537,...,314159,...,2718281,... sont des nombres premiers.
∗ 15,42,100 et 512 ne sont pas des nombres premiers.

Définition 3 : Nombres premiers entre eux [Deschamps (1), p.832] :
Des entiers relatifs a et b sont dits **premiers entre eux** lorsque le seul diviseur positif commun à a et à b est 1.

Exemple 4 : [Deschamps (1), p.837]
Deux nombres premiers distincts sont premiers entre eux puisqu'aucun des deux ne divise l'autre.

Théorème 5 : Identité de Bézout [Deschamps (1), p.832] :
Deux entiers relatifs a et b sont premiers entre eux si, et seulement si, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Proposition 6 : [Deschamps (1), p.832]
Soient a et b deux entiers non tous les deux nuls et d leur PGCD.
Il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Lemme 7 : Lemme de Gauss [Deschamps (1), p.836] :
Soient a, b et c trois entiers relatifs.
Si a divise bc et si a est premiers avec b, alors a divise c.

Proposition 8 : [Deschamps (1), p.836] :
Soient a et b deux entiers naturels non nuls.
Si a et b sont premiers entre eux, alors on a $\mathrm{PGCD}(a,b) = 1$ et $\mathrm{PPCM}(a,b) = ab$.
Plus généralement, on a $\mathrm{PGCD}(a,b)\,\mathrm{PPCM}(a,b) = ab$.

Proposition 9 : [Deschamps (1), p.837]
Si $p \in \mathcal{P}$, alors p est premier avec tous les entiers qu'il ne divise pas.
En particulier, si p est un nombre premier, on a : $\forall k \in [\![1; p-1]\!]$, $\mathrm{PGCD}(k,p) = 1$.

Corollaire 10 : [Deschamps (1), p.838]
Un nombre premier divise un produit si, et seulement si, il divise l'un de ses facteurs.

Remarque 11 : [Deschamps (1), p.838]
Le résultat est faux sans l'hypothèse "premier". En effet, 6 divise $6 = 2 \times 3$ mais 6 ne divise ni 2 ni 3.

Proposition 12 : [Deschamps (1), p.838]
Tout entier naturel strictement supérieur à 1 admet un diviseur premier.

I.2 Propriétés

Proposition 13 : [Deschamps (1), p.838]
Soit n un entier naturel supérieur strictement à 1.
Si n n'est pas premier, alors il admet un diviseur premier inférieur ou égal à $\sqrt{n}$.

Théorème 14 : Théorème de l'arithmétique [Deschamps (1), p.839] :
Soit n un entier naturel supérieur ou égal à 2.
Il existe $r \in \mathbb{N}^*$ ainsi que des nombres premiers $p_1 < p_2 < ... < p_r$ et des entiers naturels $\alpha_1, ..., \alpha_r$ non nuls tels que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$.
Les nombres premiers $p_1, p_2, ..., p_r$ sont appelés **facteurs premiers de** n.

Définition 15 : Valuation p-adique [Deschamps (1), p.840] :
On considère p un nombre premier.
Pour tout entier naturel n non nul, on appelle **valuation p-adique de** n (notée $v_p(n)$), le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n.

Exemple 16 : [Deschamps (1), p.841]
On a $7007 = 7 \times 7 \times 11 \times 13 = 7^2 \times 11^1 \times 13^1$ et donc $v_7(7007) = 2$, $v_{11}(7007) = 1$ et $v_{13}(7007) = 1$.

Proposition 17 : [Deschamps (1), p.841]
Soient p un nombre premier et a et b deux entiers naturels non nuls.
On a $v_p(ab) = v_p(a) + v_p(b)$.

Proposition 18 : [Deschamps (1), p.841]
Soient p un nombre premier et a et b deux entiers naturels non nuls.
* On a $v_p(a+b) \geq \min(v_p(a) + v_p(b))$.
* Si de plus $v_p(a) \neq v_p(b)$, alors $v_p(a+b) = \min(v_p(a) + v_p(b))$.

Proposition 19 : [Deschamps (1), p.841]
Soient a et b deux entiers naturels non nuls.
* b divise a si, et seulement si, pour tout $p \in \mathcal{P}$, $v_p(b) \leq v_p(a)$.
* Pour tout nombre premier p, on a $v_p(\text{PGCD}(a,b)) = \min(v_p(a), v_p(b))$ et $v_p(\text{PPCM}(a,b)) = \max(v_p(a), v_p(b))$.

Proposition 20 : [Deschamps (1), p.844]
Soit p un nombre premier.
* Pour tout $k \in [\![1; p-1]\!]$, le coefficient binomial $\binom{p}{k}$ est divisible par p.
* Pour tout $(a,b) \in \mathbb{Z}^2$, on a $(a+b)^p \equiv a^p + b^p \ [p]$.

Corollaire 21 : [Deschamps (1), p.844]
Pour tout nombre premier p et tout entier relatif n, on a $n^p \equiv n \ [p]$.

Proposition 22 : [Gourdon, p.11]
Soit n un entier naturel supérieur ou égal à 2.
L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est un nombre premier.

I.3 Indicatrice d'Euler

Définition 23 : Indicatrice d'Euler [Berhuy, p.156] :
Pour tout $n \geq 1$, on note $\varphi(n)$ le nombre d'entiers de l'ensemble $[\![1; n]\!]$ qui sont premiers avec n et on appelle **indicatrice d'Euler** la fonction $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$.

Proposition 24 : [Deschamps (2), p.13]
Si $n = \prod_{i=1}^{r} p_i^{k_i}$ (décomposition en facteurs premiers), alors on a :

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{k_i - 1} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Exemple 25 : [Rombaldi, p.283]
Si p est un nombre premier, alors $\varphi(p) = p - 1$.

Proposition 26 : [Deschamps (2), p.12]
Pour tout entier naturel $n \geq 1$, on a $n = \sum_{d|n} \varphi(d)$.

Proposition 27 : [Deschamps (2), p.27]
Pour tout $n \geq 1$, $\varphi(n)$ est égal :
* Au nombre d'inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
* Au nombre de générateurs de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
* Au nombre de racines n-ièmes qui sont primitives sur $\mathbb{C}$.

Théorème 28 : Théorème d'Euler [Rombaldi, p.283] :
Soit n un entier naturel non nul.
Pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1 \ [n]$.

Théorème 29 : [Rombaldi, p.292]
Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Théorème 30 : [Rombaldi, p.292]
Si p est un nombre premier impair et α un entier supérieur ou égal à 2, alors le groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

Théorème 31 : [Rombaldi, p.294] [ADMIS]
Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si, $n = 2, 4, p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.

II Localisation des nombres premiers

II.1 Répartition

Proposition 32 : [Deschamps (1), p.838]
Il existe une infinité de nombres premiers.

Proposition 33 : [Deschamps (1), p.855]
Il existe des intervalles de $\mathbb{N}$ de longueur aussi grande que l'on veut qui ne contiennent aucun nombre premier.

Théorème 34 : Théorème de Dirichlet faible [Gourdon, p.99] :
Soit $n \in \mathbb{N}$.
Il existe une infinité de nombres premiers $p \in \mathcal{P}$ tels que $p \equiv 1\ [n]$.

Corollaire 35 : [Gourdon, p.14]
Il existe une infinité de nombres premiers de la forme $4k-1$ et $6k-1$ pour $k \in \mathbb{N}^*$.

Théorème 36 : Théorème de Dirichlet [Gourdon, p.14] [ADMIS] :
Soient a, b deux entiers naturels non nuls.
Si $\text{PGCD}(a, b) = 1$, alors il existe une infinité de nombres premiers de la forme $ak + b$ avec $k \in \mathbb{N}^*$.

Proposition 37 : [Rombaldi, p.314]
La série $\sum_{p\in\mathcal{P}} \frac{1}{p}$ est divergente.

Proposition 38 : [Gourdon, p.332]
Il n'existe pas de probabilité $\mathbb{P}$ sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que pour tout $n \in \mathbb{N}^*$, $\mathbb{P}(\{\text{Multiples de } n\}) = \frac{1}{n}$.

Théorème 39 : Théorème des nombres premiers [Rombaldi, p.308] [ADMIS] :
Soit n un entier naturel non nul.
Si l'on note $\mathcal{P}_n = \mathcal{P} \cap [1; n]$ et $\pi(n) = \text{Card}(\mathcal{P}_n)$, on a $\pi(n) \underset{n\to+\infty}{\sim} \frac{n}{\ln(n)}$.

Théorème 40 : Théorème de Bertrand [Rombaldi, p.325]
Pour tout entier naturel n, il existe des nombres premiers compris entre n et $2n$.

II.2 Listes de nombres premiers

Définition 41 : Nombre de Fermat [Deschamps (1), p.830] :
On appelle **nombre de Fermat** tout nombre de la forme $F_n = 2^{2^n} + 1$ avec $n \in \mathbb{N}$.

Remarque 42 : [Deschamps (1), p.856]
On considère $m \in \mathbb{N}^*$.
Si $2^m + 1$ est un nombre premier, alors m est de la forme 2^n avec $n \in \mathbb{N}$.

Proposition 43 : [Deschamps (1), p.856]
$*$ Pour tout $n \in \mathbb{N}$, on a $F_{n+1} - 2 = (F_n - 2)F_n$ et donc $F_n = 2 + \prod_{i=0}^{n-1} F_i$.
$*$ Pour tous $n, m \in \mathbb{N}$ distincts, on a $\text{PGCD}(F_n, F_m) = 1$.

Remarque 44 : [Gourdon, p.13]
F_0, F_1, F_2, F_3 et F_4 sont des nombres premiers. Cependant F_5 n'en est pas un et il en est de même jusqu'à F_{32} où la question est encore ouverte.

Définition 45 : Nombre de Mersenne [Deschamps (1), p.855] :
On appelle **nombre de Mersenne** tout nombre de la forme $M_n = 2^n - 1$ avec n un nombre premier.

Remarque 46 : [Deschamps (1), p.855]
On considère n un entier naturel supérieur ou égal à 2.
Si $2^n - 1$ est un nombre premier, alors n est premier. Cependant la réciproque est fausse. En effet, $2^{11} - 1 = 2047 = 23 \times 89$ n'est pas un nombre premier...

Remarque 47 : [Gourdon, p.13]
Les plus grands nombres premiers connus sont des nombres de Mersenne. Les nombres de Mersenne premiers sont pourtant rares : seulement 51 sont connus début 2022. On ne sait même pas s'il en existe une infinité.

Définition 48 : Nombre de Carmichaël [Rombaldi, p.329] :
On appelle **nombre de Carmichaël** tout entier naturel $n \geq 3$ non premier tel que $a^{n-1} \equiv 1\ [n]$ pour tout entier a premier avec n.

Remarque 49 : [Rombaldi, p.329]
La réciproque du théorème de Fermat est fausse en générale, cependant les nombres de Carmichaël vérifient le théorème sans pour autant être des nombres premiers (c'est par exemple le cas de 561 divisible par 3, 11 et 17).

Lemme 50 : [Rombaldi, p.329]
Un nombre de Carmichaël est impair et sans facteur carré.

Théorème 51 : Théorème de Korselt [Rombaldi, p.330]
Soit $n \geq 3$ un entier naturel.
Les assertions suivantes sont équivalentes :
$*$ Il existe un entier $r \geq 3$ et des nombres premiers impairs $p_1 < ... < p_r$ tels que $n = \prod_{i=1}^{r} p_i$ et pour tout $i \in [\![1; r]\!]$, $p_i - 1$ divise $n - 1$.
$*$ n est non premier et pour tout $a \in \mathbb{Z}/n\mathbb{Z}$, on a $a^n = a$.
$*$ n est un nombre de Carmichaël.

II.3 Test de primalité

Remarque 52 : [Deschamps (1), p.838]
Le premier test de primalité possible pour trouver une liste de nombres premiers inférieur à un nombre donné est le crible d'Ératosthène qui consiste à rayer au fur et à mesure les multiples des nombres précédents et le premier nombre non barré est alors premier et ainsi de suite.

Théorème 53 : Théorème de Wilson [Gourdon, p.11] :
Un entier $p \geq 2$ est un nombre premier si, et seulement si, $(p-1)! \equiv -1$ $[p]$.

Proposition 54 : Test de Pépin [Gourdon, p.50]
Soit $k \in \mathbb{N}$.
F_k est un nombre premier si, et seulement si, $3^{\frac{F_k-1}{2}} \equiv -1$ $[F_k]$.

Proposition 55 : Test de Lucas [Gourdon, p.13]
On considère la suite réelle $(Y_n)_{n\in\mathbb{N}}$ définie par $Y_0 = 2$ et $Y_{n+1} = 2Y_n^2 - 1$.
Pour $n \geq 3$, $2^n - 1$ est premier si, et seulement si, $2^n - 1$ divise Y_{n-2}.

Remarque 56 : [Gourdon, p.13]
Ce test est donc tout a fait adapté pour vérifier la primalité des nombres de Mersenne. Ce test a permis de trouver le plus grand nombre premier connu en 2020 : $2^{82589933} - 1$ (nombre qui comporte un peu moins de 25 millions de chiffres).

III Applications

III.1 Cryptage RSA

Proposition 57 : [Gourdon, p.36]
Soient p et q deux nombres premiers distincts, $n = pq$ et c et d deux entiers tels que $cd \equiv 1$ $[\varphi(n)]$.
Pour tout $t \in \mathbb{Z}$, on a $t^{cd} \equiv t$ $[n]$.

Remarque 58 : [Gourdon, p.37]
Le couple (n, c) est appelé **clef publique** et l'entier d est appelé **clef secrète**.

La sécurité de ce système repose sur le fait que connaissant la clef publique, il est très difficile de déterminer d : un moyen consiste par exemple à factoriser n pour trouver p et q, ce qui est encore impossible à réaliser lorsque p et q sont grands, typiquement (pour l'année 2020) de l'ordre de 150 à 200 chiffres.

Ainsi, tout le monde peut chiffrer mais seuls ceux connaissant la clef secrète peuvent déchiffrer. Ce système de chiffrement est apparu en 1976, il est appelé RSA (du nom des inventeurs Rivest, Shamir et Adleman) et est couramment utilisé aujourd'hui car il est extrêmement robuste. Son apparition explique l'intérêt que l'on porte aujourd'hui aux algorithmes de factorisation et de primalité.

III.2 Anneau des entiers de Gauss

Dans toute cette sous-partie, on pose $\Sigma = \{n \in \mathbb{N} \text{ tq } n = a^2 + b^2,\ a, b \in \mathbb{N}\}$, $\mathcal{P}$ l'ensemble des nombres premiers (au sens usuel) et une application (qui est multiplicative) $N : a + ib \longmapsto a^2 + b^2$ définie de $\mathbb{Z}[i]$ dans $\mathbb{N}$.

Définition 59 : L'anneau $\mathbb{Z}[i]$ [Perrin, p.56] :
On appelle **anneau** $\mathbb{Z}[i]$ l'anneau $\mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$ muni de l'addition et de la multiplication usuelles.

Proposition 60 : [Perrin, p.56]
$\mathbb{Z}[i]^\times = \{-1; 1; -i; i\}$.

Proposition 61 : [Perrin, p.56]
L'ensemble Σ est stable par multiplication.

Proposition 62 : [Perrin, p.57]
L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N.

Lemme 63 : [Perrin, p.57]
Soit $p \in \mathcal{P}$.
Les assertions suivantes sont équivalentes :
$*$ $p \in \Sigma$. $*$ L'élément p n'est pas irréductible dans $\mathbb{Z}[i]$.
$*$ On a $p = 2$ ou $p \equiv 1$ $[4]$

Théorème 64 : Théorème des deux carrés [Perrin, p.58] :
Soit $n = \prod_{p\in\mathcal{P}} p^{v_p(n)} \in \mathbb{N}$.
$n \in \Sigma$ si, et seulement si, pour tout $p \in \mathcal{P}$ vérifiant $p \equiv 3$ $[4]$, l'entier $v_p(n)$ est pair.

Proposition 65 : [Perrin, p.58]
Les irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près :
$*$ Les entiers premiers $p \in \mathbb{N}$ tels que $p \equiv 3$ [4].
$*$ Les entiers de Gauss $a+ib$ dont la norme est un nombre premier.

III.3 Théorème des restes chinois

Dans toute cette sous-partie, on considère un anneau $(A, +, \times)$ principal.

Développement 1 : [cf. ROMBALDI]

Lemme 66 : [Rombaldi, p.249]
Soient $a_1, ..., a_r$ des éléments deux à deux premiers entre eux de A.
Si l'on pose pour tout $j \in [\![1; r]\!]$, $b_j = \prod_{\substack{i=1 \\ i \neq j}}^{r} a_j$, alors les b_j sont premiers entre eux dans leur ensemble.

Théorème 67 : Théorème des restes chinois [Rombaldi, p.249] :
Soient $a_1, ..., a_r$ des éléments de A deux à deux premiers entre eux.
L'application :

$$\varphi : \left| \begin{array}{ccc} A & \longrightarrow & \prod_{i=1}^{r} A/(a_i) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array} \right.$$

est un morphisme d'anneaux surjectif de noyau $\left(\prod_{i=1}^{r} a_i\right)$.

On a donc en particulier :

$$A\Big/\left(\prod_{i=1}^{r} a_i\right) = \prod_{i=1}^{r} A/(a_i)$$

Exemple 68 : [Rombaldi, p.291]
Le système d'équations diophantiennes :

$$(S) \begin{cases} k \equiv 2 & [4] \\ k \equiv 3 & [5] \\ k \equiv 1 & [9] \end{cases}$$

possède pour solution particulière $k_0 = 118$ et l'ensemble des solutions à ce système d'équations diophantiennes est $\{118 + 180n,\ n \in \mathbb{Z}\}$.

Exemple 69 : [Berhuy, p.471]
L'inverse de l'isomorphisme $\varphi : \mathbb{Z}/48\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ est :

$$\varphi^{-1} : \left| \begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \longrightarrow & \mathbb{Z}/48\mathbb{Z} \\ (\widehat{a_1}, \dot{a_2}, \widetilde{a_3}) & \longmapsto & \overline{28a_1 + 21a_2 + 36a_3} \end{array} \right.$$

Théorème 70 : [Berhuy, p.485]
Soient $m_1, ..., m_r$ des entiers naturels non nuls premiers entre eux deux à deux.
Le morphisme des projections $f : \mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$ est surjectif et de noyau $(m_1...m_r)$.
En particulier, on a l'isomorphisme $\mathbb{Z}/m_1...m_r\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$.

Corollaire 71 : [Berhuy, p.485]
Soit n un entier naturel supérieur ou égal à 2.
Si $n = \prod_{i=1}^{r} p_i^{m_i}$ (décomposition en facteur premiers), alors on a l'isomorphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_r^{m_r}\mathbb{Z}$.

III.4 Théorie des groupes et de Sylow

Dans toute cette sous-partie, on considère $(G, *)$ un groupe de cardinal fini noté n et p un nombre premier.

Proposition 72 : [Berhuy, p.155]
Soit p un nombre premier.
Si G est d'ordre p, alors G est cyclique et $G \cong \mathbb{Z}/p\mathbb{Z}$.

Lemme 73 : [Berhuy, p.194]
Le centre d'un p-groupe non trivial est non trivial.

Développement 2 : [cf. BERHUY]

Proposition 74 : [Berhuy, p.194]
Soit p un nombre premier.
Si G est d'ordre p^2, alors $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Définition 75 : p-sous-groupe de G [Berhuy, p.311] :
On appelle **p-sous-groupe de G** tout sous-groupe de G de cardinal une puissance de p.

Désormais, on écrit $\text{Card}(G) = n = p^m q$ où $p \nmid q$ et $m \in \mathbb{N}^*$.

Définition 76 : p-sous-groupe de Sylow de G [Berhuy, p.311] :
On appelle **p-sous-groupe de Sylow de G** (ou plus simplement p-Sylow) tout sous-groupe de G d'ordre p^m.

Exemple 77 :
$*$ $\mathbb{Z}/6\mathbb{Z}$ contient un 2-Sylow et un 3-Sylow (respectivement $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$).
$*$ $\mathbb{Z}/56\mathbb{Z}$ contient un 2-Sylow et un 7-Sylow (respectivement $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$).

Théorème 78 : Théorème de Sylow [Berhuy, p.313] :
∗ Il existe des p-sous-groupes de Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow.
∗ Le conjugué d'un p-Sylow est un p-Sylow et tous les p-Sylow de G sont conjugués entre eux. En particulier, si S est un p-Sylow de G, alors S est distingué dans G si, et seulement si, S est l'unique p-Sylow de G.
∗ Si n_p désigne le nombre de p-Sylow de G, alors $n_p \equiv 1\ [p]$ et $n_p | q$.

Exemple 79 : [Berhuy, p.315 + 328]
Tout groupe d'ordre 63 ou 255 n'est pas simple.

Corollaire 80 :
Tout groupe d'ordre pq avec $p < q$ qui sont deux nombres premiers n'est pas simple.

Corollaire 81 : [Berhuy, p.315]
Tout groupe d'ordre 33 cyclique.

Théorème 82 : Théorème de Cauchy [Berhuy, p.179] :
G possède au moins un élément d'ordre p.

Développement 3 : [cf. BERHUY]

Proposition 83 : [Berhuy, p. 310]
Soit p un nombre premier supérieur ou égal à 3.
Si G est d'ordre $2p$, alors G est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou à D_{2p}.

III.5 Critères d'irréductibilité

Dans toute cette sous-partie, on considère A un anneau factoriel.

Proposition 84 : Critère d'irréductibilité d'Eisenstein [Perrin, p.76] :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$.
S'il existe un élément irréductible p tel que :
∗ p ne divise pas a_n. ∗ Pour tout $i \in [\![0; n-1]\!]$, p divise a_i.
∗ p^2 ne divise pas a_0.
alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 85 :
Les polynômes $X^n - 2$ et $X^4 - 6X^3 + 3X^2 - 12X + 3$ sont irréductibles dans $\mathbb{Q}[X]$.

Proposition 86 : Critère de réduction [Perrin, p.77] :
Soient I un idéal premier de A et $P \in A[X]$ unitaire.
Si $\overline{a}_n \neq 0$ dans A/I et si $\overline{P}$ est irréductible sur A/I ou $\mathrm{Frac}(A/I)$, alors le polynôme P est irréductible sur $\mathrm{Frac}(A)$.

Exemple 87 : [Perrin, p.77]
Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Q}[X]$ par le critère de réduction.

III.6 Corps finis

Dans toute cette sous-partie, on considère $\mathbb{K}$ un corps commutatif quelconque.

Définition 88 : Sous-corps premier [Perrin, p.72] :
On appelle **sous-corps premier de** $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$ (contenant l'élément $1_{\mathbb{K}}$).

On considère le morphisme d'anneaux :

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ n & \longmapsto & n \cdot 1_{\mathbb{K}} \end{array} \right.$$

Le noyau de φ est un idéal de $\mathbb{Z}$ et par le premier théorème d'isomorphisme, on a $\mathbb{Z}/\mathrm{Ker}(\varphi) \cong \mathrm{Ima}(\varphi) \subseteq \mathbb{K}$, donc $\mathrm{Ker}(\varphi)$ est un idéal premier de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ avec $p \in \mathcal{P} \cup \{0\}$.

Définition 89 : Caractéristique d'un corps [Perrin, p.72] :
On appelle **caractéristique de** $\mathbb{K}$ le nombre $p \in \mathcal{P} \cup \{0\}$ qui est le générateur de $\mathrm{Ker}(\varphi)$ et on le note $\mathrm{car}(\mathbb{K})$.

Proposition 90 : [Perrin, p.72]
∗ $\mathrm{car}(\mathbb{K}) = 0$ si, et seulement si, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$.
∗ $\mathrm{car}(\mathbb{K}) > 0$ si, et seulement si, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 91 : [Perrin, p.72]
Soient p un nombre premier et $\mathbb{K}$ un corps fini.
Si $\mathbb{K}$ est de caractéristique p, alors $\mathbb{K}$ a pour cardinal une puissance de p.

Exemple 92 :
Il n'existe pas de corps de cardinal 6 mais de cardinal 7 oui (par exemple $\mathbb{Z}/7\mathbb{Z}$).

Théorème 93 : [Perrin, p.73]
Soient p un nombre premier et $n \in \mathbb{N}^*$.
Si l'on pose $q = p^n$, alors il existe un corps commutatif $\mathbb{K}$ à q éléments (c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$).
En particulier, $\mathbb{K}$ est unique à isomorphisme près et on le note $\mathbb{F}_q$.

Exemple 94 :
On peut construire un corps à 4 éléments de deux manières :
∗ En tant que corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$.
∗ Grâce à l'isomorphisme $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1)$.

Remarques sur la leçon

— Connaître le chiffrement RSA (notamment les clefs).

— On peut également parler des corps finis, des carrés dans les corps finis ainsi que du symbole de Legendre et de la loi de réciprocité quadratique.

Liste des développements possibles

— Théorème des deux carrés.

— Théorème des restes chinois + application.

— Classification des groupes d'ordre p^2 et $2p$.

Bibliographie

— Claude Deschamps, *Tout-en-un MPSI*.

— Xavier Gourdon, *Les maths en tête, Algèbre et Probabilités*.

— Grégory Berhuy, *Algèbre : le grand combat*.

— Claude Deschamps, *Tout-en-un MP/MP**.

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.

— Daniel Perrin, *Cours d'algèbre*.