Congruences

prérequis : toute l'arithmétique de $\mathbb{Z}$, c'est un anneau euclidien donc principal donc factoriel : notions de pgcd, ppcm, relation de Bezout.
Remarque : si on veut être stricte, il ne faut pas parler des corps finis sauf des $\mathbb{Z}/p\mathbb{Z}$; dans ce cas il est difficile d'en faire trop sur ce thème puisque le jury ne comprendrait pas pourquoi il devrait ce restreindre à ces seuls corps. Pour ouvrir le sujet, vous pourrez mentionner que la généralisation est l'étude des idéaux I d'un anneau A et donc des quotients A/I : par exemple lorsque A est l'anneau des entiers d'une extension finie K de $\mathbb{Q}$. La généralisation de l'unicité de la décomposition en facteurs premiers, est le fait que tout idéal de A s'écrit uniquement comme un produit d'idéaux premiers de A. A ce propos, en général, l'idéal pA n'est pas forcément premier.

Table des matières

1. Généralités 1
   1.1. Le groupe $\mathbb{Z}/n\mathbb{Z}$ 1
   1.2. L'anneau $\mathbb{Z}/n\mathbb{Z}$ 3
   1.3. Loi de réciprocité quadratique 4
2. Applications arithmétiques 6
   2.1. Critères de divisibilité 6
   2.2. Cryptographie 6
3. Applications aux nombres premiers 7
   3.1. Développement décimal de $1/p$ 7
   3.2. Théorème de Dirichlet 9
   3.3. Tests de primalité 11
   3.4. Méthodes de factorisation 12
4. Calculs modulaires 15
   4.1. Polygones de Newton 15
   4.2. Factorisation 22
   4.3. Principe de Hasse 24
5. Développements 26
6. Questions 27
7. Solutions 29
Références 33

1. Généralités

1.1. Le groupe $\mathbb{Z}/n\mathbb{Z}$. — Bien que l'on puisse admettre la notion de groupe quotient dans les prérequis, on pourra proposer de l'oublier temporairement.

Définition 1.1. — Pour $n \in \mathbb{Z}$, on munit $\mathbb{Z}$ de la relation d'équivalence suivante :

$$x \sim_n y \Leftrightarrow n|x-y$$

et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence. On notera $\bar{x}$ la classe associée à $x \in \mathbb{Z}$, i.e. $\bar{x} = \{x + kn : \ k \in \mathbb{Z}\}$, de sorte que $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$. Deux éléments x, y d'une même classe seront dits congrus modulo n et on le notera sous la forme $x \equiv y \mod n$.

Remarque : l'addition de $\mathbb{Z}$ muni l'ensemble $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe ; en effet soit $\bar{x}, \bar{y}$ deux classes d'équivalence, on définit alors $\bar{x} + \bar{y} = \overline{x_0 + y_0}$ où x_0 et y_0 sont des éléments quelconques de $\bar{x}$ et $\bar{y}$ respectivement. Le fait, trivial mais primordial, est que le résultat $\overline{x_0 + y_0}$ ne dépend pas du choix de x_0 et y_0. On notera

$$\psi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$$

la surjection dite canonique qui à un entier x associe sa classe d'équivalence $\bar{x}$.
Remarque : tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$; en effet soit $G =< g >$ et considérons le morphisme $f : \mathbb{Z} \to G$ qui à 1 associe g. Par définition le noyau de f est $n\mathbb{Z}$ de sorte que f induit un isomorphisme $\bar{f} : \mathbb{Z}/n\mathbb{Z} \simeq G$.

Proposition 1.2. — *Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de cardinal d où d est un diviseur de n. Réciproquement pour tout $d|n$, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ qui est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.*

Preuve : Le premier point est un cas particulier du théorème de Lagrange. Réciproquement soit H un sous-groupe de $G = \mathbb{Z}/n\mathbb{Z}$; considérons et $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow G/H$, où G/H est le groupe quotient de G par H. Le noyau de ϕ est un sous-groupe de $\mathbb{Z}$ donc de la forme $d\mathbb{Z}$, contenant $\operatorname{Ker}\psi = n\mathbb{Z}$, de sorte que d divise n. Ainsi H est cyclique, engendré par la classe de d ; son ordre est n/d. □

Corollaire 1.3. — *Le groupe engendré par un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est le groupe engendré par $\overline{k \wedge n}$; il est de cardinal $\frac{n}{n \wedge k}$.*

Preuve : Comme k est un multiple de $k \wedge n$, on a l'inclusion $(k) \subset (k \wedge n)$. Réciproquement on écrit une relation de Bezout $uk + vn = n \wedge k$ de sorte que modulo n, $n \wedge k$ appartient au groupe engendré par k et donc $(k \wedge n) \subset (k)$. On en déduit alors que l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ qui est par définition le cardinal du groupe engendré par k, est $\frac{n}{n \wedge k}$. □
Remarque : un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur si et seulement si $k \wedge n = 1$; on notera $\psi(n)$ le cardinal de l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$, et donc aussi le cardinal des $1 \leq k \leq n$ premiers avec n.

Corollaire 1.4. — *L'ensemble des éléments d'ordre $d|n$ (resp. d'ordre divisant d) dans $\mathbb{Z}/n\mathbb{Z}$ est de cardinal $\psi(d)$ (resp. d). Par ailleurs on a $n = \sum_{d|n} \psi(d)$.*

Preuve : Remarquons tout d'abord que si d ne divise pas n, il n'y a aucun élément d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. Si d divise n, tous les éléments d'ordre d appartiennent au groupe engendré par $(\frac{n}{d})$ qui est isomorphe, en tant que groupe cyclique d'ordre d, à $\mathbb{Z}/d\mathbb{Z}$. Ainsi les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre d de $\mathbb{Z}/d\mathbb{Z}$ qui sont en nombre $\psi(d)$.

Cherchons maintenant les éléments d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z}$ qui sont donc d'ordre divisant $d \wedge n$ et qui appartiennent au groupe engendré par $\frac{n}{n \wedge d}$ isomorphe à $\mathbb{Z}/(n \wedge d)\mathbb{Z}$. Ainsi, comme précédemment, les éléments d'ordre divisant d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre divisant $n \wedge d$ de $\mathbb{Z}/(n \wedge d)\mathbb{Z}$, qui sont en nombre $n \wedge d$.

La dernière égalité découle du dénombrement des éléments de $\mathbb{Z}/n\mathbb{Z}$ selon leur ordre. □

Corollaire 1.5. — *Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.*

Preuve : Soit donc G un sous-groupe fini du groupe multiplicatif d'un corps K (commutatif), et soit n le cardinal de G. Si $g \in G$, son ordre est un diviseur de n car le sous-groupe engendré par g est de cardinal son ordre, et le cardinal d'un sous-groupe divise le cardinal du groupe (cf. cours). Ainsi pour d divisant n, on note A_d (resp. H_d) l'ensemble des éléments de G d'ordre d (reps. divisant d) : en particulier on a $H_d = \{g \in G \ / \ g^d = 1\}$. Le corps K étant commutatif, on a $|H_d| \leq d$, car le polynôme $X^d - 1$ y a au plus d racines. En outre si $A_d \neq$, alors $|H_d| = d$ car tout élément de A_d engendre un sous-groupe d'ordre d dans lequel tout élément g est tel que $g^d = 1$. Or $A_d \subset H_d$ soit $|A_d| \leq \varphi(d)$, l'inégalité $|A_d| \geq \varphi(d)$ étant évidente. En résumé soit A_d est vide soit son cardinal est égal à $\varphi(d)$. En reprenant le comptage de la question précédente, $G = \coprod_{d|n} A_d$, on obtient

$$n = \sum_{d|n} \epsilon(d)\varphi(d)$$

où $\epsilon(d)$ est nul si A_d est vide, et égal à 1 sinon. En comparant cette égalité avec celle de (v), on en déduit que $\epsilon(d) = 1$ pour tout $d|n$, soit A_d non vide et en particulier A_n, d'où le résultat. □

Théorème 1.6. — ***(chinois)*** *Soient n et m des entiers premiers entre eux ; l'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ qui à un entier k associe sa classe modulo n et m, induit un isomorphisme*

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}.$$

Preuve : Considérons tout d'abord un élément k du noyau de sorte que n et m divise k et comme $n \wedge m = 1$, d'après le lemme de Gauss $nm|k$. Ainsi le noyau est contenu dans $nm\mathbb{Z}$, l'inclusion réciproque étant évidente de sorte que l'on a une injection de $\mathbb{Z}/nm\mathbb{Z} \hookrightarrow \mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}$ qui est un isomorphisme par égalité des cardinaux. □
Remarque : il peut être utile de savoir déterminer un antécédent d'un couple $(\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Pour cela on part d'une relation de Bézout $un + vm = 1$ et on pose $k = unb + vma$; on vérifie aisément que comme $un \equiv 1 \mod m$ et $vm \equiv 1 \mod n$, on a $k \equiv a \mod n$ et $k \equiv b \mod m$. Dans le cas où $n \wedge m = d$, le noyau est $n \vee m\mathbb{Z}$ et l'image

$$\{(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} : \ d|a - b\}.$$

Bien que les groupes cycliques paraissent particulièrement simples et isolés, notons que leur connaissance implique celle des groupes abéliens de type fini.

Théorème 1.7. — *Soit G un groupe abélien fini de cardinal n ; il existe alors des entiers $1 < a_1|a_2|\cdots|a_r$ tels que*

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/a_i\mathbb{Z}.$$

La suite a_i est uniquement déterminée avec $n = \prod_{i=1}^{r} a_i$.

Remarque : dans le cas où G est seulement supposé de type fini, il faut dans l'isomorphisme précédent rajouter une composante $\mathbb{Z}^s$ où s est appelé le rang de G.

1.2. L'anneau $\mathbb{Z}/n\mathbb{Z}$. — L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est aussi muni d'une structure d'anneau déduite de celle de $\mathbb{Z}$; on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$, i.e. l'ensemble des éléments inversibles muni de la multiplication.

Proposition 1.8. — *Un élément $k \in \mathbb{Z}/n\mathbb{Z}$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement s'il est un générateur additif de $\mathbb{Z}/n\mathbb{Z}$. En particulier $(\mathbb{Z}/n\mathbb{Z})^\times$ est de cardinal $\varphi(n)$.*

Preuve : Par définition k est inversible si et seulement s'il existe k' tel que $kk' \equiv 1 \mod n$, i.e. s'il existe $\lambda \in \mathbb{Z}$ tel que $kk' + \lambda n = 1$ ce qui est équivalent à $k \wedge n = 1$ et donc k est un générateur de $\mathbb{Z}/n\mathbb{Z}$. □
Remarque : comme $\mathbb{Z}/n\mathbb{Z}$ est monogène tout morphisme de source $\mathbb{Z}/n\mathbb{Z}$ est déterminé par l'image de $\bar{1}$ de sorte qu'en particulier le groupe $\mathrm{aut}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollaire 1.9. — *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n = p$ est premier auquel cas on le notera $\mathbb{F}_p$.*

Théorème 1.10. — ***(de Fermat)*** *Pour tout $n \in \mathbb{Z}$ et $k \wedge n = 1$, on a $k^{\varphi(n)} \equiv 1 \mod n$.*

Preuve : Nous avons vu que le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à $\varphi(n)$ et comme l'ordre d'un élément divise le cardinal du groupe, l'ordre de k divise $\varphi(n)$ et donc $k^{\varphi(n)} \equiv 1 \mod n$. □

Proposition 1.11. — *Pour $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, on a*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

Preuve : Le théorème chinois donne un isomorphisme

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times;$$

le résultat découle alors du fait que le cardinal des $1 \leq k \leq p^\alpha$ divisible par p est de cardinal $p^{\alpha-1}$ et donc $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. □
En ce qui concerne les $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, on a le résultat suivant.

Proposition 1.12. — *Pour p premier impair et $\alpha \geq 1$, $(\mathbb{Z}/p^a\mathbb{Z})^\times$ est cyclique et pour $p = 2$, on a*

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}).$$

1.3. Loi de réciprocité quadratique. — On dit qu'un élément $a \in \mathbb{F}_p$ est un carré s'il existe $b \in \mathbb{F}_p$ tel que $a = b^2$.

Définition 1.13. — Pour $p \geq 3$ premier, le symbole de Legendre $(\frac{n}{p})$ est défini par :

$$(\frac{n}{p}) = \begin{cases} 0 \text{ si } p \text{ divise n} \\ +1 \text{ si } n \text{ est un carré dans } \mathbb{F}_p \\ -1 \text{ sinon} \end{cases}$$

Remarque : l'application $x \in \mathbb{F}_p^\times \mapsto x^2 \in \mathbb{F}_p^\times$ est un morphisme de groupe multiplicatif, dont le noyau est $\{-1, 1\}$ et donc de cardinal 2 ; ainsi son image qui est l'ensemble $\mathbb{F}_p^{\times 2}$ des carrés de $\mathbb{F}_p^\times$ est de cardinal $(p-1)/2$. Rappelons par ailleurs que d'après le petit théorème de Fermat, pour tout $x \in \mathbb{F}_p^\times$, on a $x^{p-1} = 1$ et donc $x^{(p-1)/2} = \pm 1$. Ainsi si $x \in \mathbb{F}_p^{\times 2}$, x est une solution de l'équation $X^{(p-1)/2} = 1$ laquelle dans $\mathbb{F}_p$ possède au plus $(p-1)/2$ solutions. Ainsi d'après ce qui précède, $\mathbb{F}_p^{\times 2}$ est exactement égal à l'ensemble des racines de l'équation $X^{(p-1)/2} = 1$

dans $\mathbb{F}_p$ et que $(\frac{n}{p}) \equiv n^{(p-1)/2} \mod p$. On remarque en particulier que le symbole de Legendre est multiplicatif, i.e.

$$(\frac{nn'}{p}) = (\frac{n}{p})(\frac{n'}{p}).$$

Le calcul explicite des symboles de Legendre se fait au moyen du

Lemme 1.14. — ***(de Gauss)*** *Pour tout p premier impair on a $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.*

ainsi que de la loi de réciprocité quadratique :

Théorème 1.15. — *Pour tout p, q premiers impairs, on a*

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{(p-1)(q-1)/4}.$$

Il y a plus de 200 preuves différentes de ce résultat ; historiquement la première est due à Gauss via l'utilisation des sommes de Gauss. Une preuve particulièrement élémentaire est d'identifier le symbole de Legendre avec la signature de la permutation de $\mathbb{Z}/q\mathbb{Z}$ associée à la multiplication par p.

Preuve : L'idée est d'utiliser la relation

$$\mathrm{Res}(P, Q) = (-1)^{\deg P . \deg Q} \mathrm{Res}(Q, P)$$

et de choisir des polynômes P et Q de degré respectifs $\frac{p-1}{2}$ et $\frac{q-1}{2}$, où p et q sont des premiers impairs distincts, de sorte que

$$\mathrm{Res}(P, Q) = (\frac{p}{q}) \text{ et } \mathrm{Res}(Q, P) = (\frac{q}{p}).$$

Lemme 1.16. — *Pour tout p premier impair, il existe un polynôme $Q_p \in \mathbb{Z}[X]$ tel que*

$$X^{p-1} + X^{p-2} + \cdots + X + 1 = X^{(p-1)/2} Q_p(X + \frac{1}{X}).$$

Preuve : En posant $Y = X^{-1}$, le membre de gauche est égal à $X^{(p-1)/2} + \cdots + X + 1 + Y + \cdots + Y^{(p-1)/2}$, de sorte que d'après le théorème sur les polynômes symétriques, il existe $R \in \mathbb{Z}[X, Y]$ tel que le terme précédent est égal à $R(X + Y, XY)$, d'où le résultat en notant que $XY = 1$. □

Lemme 1.17. — *Pour $p \neq q$ des nombres premiers impairs, le résultant de Q_p et Q_q est égal à ± 1.*

Preuve : Raisonnons par l'absurde et considérons l premier divisant $\mathrm{Res}(Q_p, Q_q)$ de sorte que modulo l, $\bar{Q}_p$ et $\bar{Q}_q$ ont une racine commune $\beta \in \mathbb{F}_{l^n}$ pour $2n \leq \min\{p-1, q-1\}$. Soit alors $x \in \bar{\mathbb{F}}_l$ tel que $x^2 - \beta x + 1 = 0$ de sorte que

$$x^{p-1} + \cdots + x + 1 = x^{(p-1)/2} \bar{Q}_p(\beta) = 0.$$

En multipliant cette égalité par $x - 1$, on en déduit que $x^p = 1$ dans $\bar{\mathbb{F}}_l$. De la même façon on a aussi $x^q = 1$ et comme $p \wedge q = 1$, on en déduit $x = 1$ et donc $p \equiv q \equiv 0 \mod l$ ce qui n'est pas car $p \wedge q = 1$. □

Proposition 1.18. — *Pour $p \neq q$ des nombres premiers distincts, on a*

$$\mathrm{Res}(Q_p, Q_q) = (\frac{q}{p}).$$

Preuve : On raisonne modulo p de sorte que d'après le lemme précédent, il suffit de prouver que ce résultant est $\equiv q^{(p-1)/2} \mod p$:

$$X^{p-1}+\cdots+X+1 \equiv (X-1)^{p-1} \equiv (X^2-2X+1)^{(p-1)/2} \equiv X^{(p-1)/2}(X+\frac{1}{X}-2)^{(p-1)/2} \mod p,$$

de sorte que $Q_p(X+\frac{1}{X}) \equiv (X+\frac{1}{X}-2)^{(p-1)/2} \mod p$ et donc

$$Q_p(X) \equiv (X-2)^{(p-1)/2} \mod p.$$

Ainsi on en déduit que $\mathrm{Res}(Q_p, Q_q) \equiv Q_p(2)^{(p-1)/2} \equiv Q_q(1+\frac{1}{1})^{(p-1)/2} \equiv q^{(p-1)/2} \mod p$, d'où le résultat. □

□

2. Applications arithmétiques

2.1. Critères de divisibilité. — En utilisant que pour tout $k \geq 1$, $10^k \equiv 0$ modulo 2 et 5, on obtient qu'un nombre est divisible par 2 (resp. 5) si et seulement son dernier chiffre l'est. De même comme $10 \equiv 1 \mod 3$ ou 9, alors n est divisible par 3 (resp. 9) si et seulement si la somme de ses chiffres l'est. Enfin comme $10 \equiv -1 \mod 11$ alors n est divisible par 11 si et seulement si la somme alternée de ses chiffres l'est.

2.2. Cryptographie. — Il s'agit d'un système dit à clef publique, i.e. tout le monde connaît le procédé de cryptage mais seul une personne (le receveur) connaît la clef qui permet de déchiffrer. Concrètement on choisit deux nombres premiers p et q distincts impairs très grands (plus quelques autres contraintes) et on pose $n = pq$; on fixe aussi $0 \leq c < n$ un entier premier avec $\varphi(n)$. Sont publiques les entiers n et c ainsi que le procédé suivant. Si A veut envoyer un message à R, il le coupe d'abord en bouts et les transforme en des nombre m_i plus petit que n ; ensuite il envoie les m_i^c modulo n.

Le problème pour R ou pour B indiscret est de retrouver m connaissant n et c et sachant que $n = pq$ avec p, q premiers connus seulement de R. Pour R la méthode est assez simple, il lui suffit de connaître l'inverse e de c dans $(\mathbb{Z}/n\mathbb{Z})^\times$; en effet on a alors $(m^c)^e \equiv m \mod n$. Pour calculer e, R utilise le théorème chinois et calcule donc les inverses e_p et e_q de c dans respectivement $(\mathbb{Z}/p\mathbb{Z})^\times$ et $(\mathbb{Z}/q\mathbb{Z})^\times$ qui est d'après le petit théorème de Fermat égal à c^{p-2} et c^{q-2}. On construit alors facilement e en utilisant la version constructive du théorème chinois. Pour B, la situation est plus critique ; pour l'instant sa stratégie est de casser n, i.e. de trouver p ce qui est très long pourvu que R ait choisi p et q très grand convenablement. A ce propos signalons les précautions élémentaires à prendre :

- p et q doivent être pris tous deux grands, sinon l'algorithme ρ de Pollard pourrait très facilement trouver le petit facteur ;
- il faut que $|p-q|$ soit grand sinon pour $q = p+\delta$ avec δ beaucoup plus petit que p, on aurait pour $N = pq, \sqrt{N} = p\sqrt{1+\delta} \sim p + \delta/2$ et on pourra trouver p par un algorithme naïf en $O(\delta)$ étapes ;
- il faut que $p-1$ et $q-1$ ne soit pas trop friable au sens précédent, sinon l'algorithme $p-1$ de Pollard permettrait de le trouver rapidement ;
- il faut que l'exposant secret e ne soit pas trop petit ; trivialement si $e = O(\log N)$ alors en faisant $O(\log N)$ essais on trouvera e. En fait on peut montrer qu'il faut éviter $e << N^{1/4}$.

Il existe sûrement d'autres contraintes connues ou pas sur les choix de p, q, e. Signalons tout de même que la construction de grands nombres premiers ne posent pas de problèmes pratiques :

pour cela on part d'un entier impair k grand, on test en temps polynomial s'il est premier et sinon on teste $k+2$ et ainsi de suite. Le théorème des nombres premiers nous dit qu'en moyenne on devrait tomber sur un nombre premier au bout de $\ln k$ étapes. Si la conjecture sur la fonction trou, comme quoi $g(p_n) \leq K(\ln p_n)^2$ est vrai, on est assuré de trouver ainsi un nombre premier en temps polynomial.

3. Applications aux nombres premiers

Commençons par la curiosité suivante : d'après le théorème de Wilson, lequel affirme que p est premier si et seulement si $(p-1)! \equiv -1 \mod p$, la fonction

$$f(n) = 2 + 2(n!) \mod n+1$$

produit tous les nombres premiers exclusivement mais plusieurs fois.

3.1. Développement décimal de $1/p$. — Partons de quelques constatations amusantes :

$$\frac{1}{7} = 0,142\ 857\ 142\ 857\ 142\ 857\cdots$$

avec $7 \times 142857 = 999999$, $142 + 857 = 999$, $14 + 28 + 57 = 99$, $1+4+2+8+5+7 = 3 \times 9$ et encore

$$\frac{1}{7} = 0,142857\cdots, \quad \frac{2}{7} = 0,285714\cdots, \quad \frac{3}{7} = 0,428571\cdots$$
$$\frac{4}{7} = 0,571428\cdots, \quad \frac{5}{7} = 0,714285\cdots, \quad \frac{6}{7} = 0,857142\cdots$$

Sans calculs le 53-ème chiffre de $1/53$ est 0, le 52-ème étant 3 car $3 \times 3 = 9$. Essayons désormais d'ordonner toutes ces coïncidences.

Proposition 3.1. — *Le développement décimal de $\frac{1}{p}$ est périodique, après la virgule, de période l'ordre de* 10 *dans* $(\mathbb{Z}/p\mathbb{Z})^\times$.

Preuve : L'écriture s'obtient en effectuant la division euclidienne par p, puis en multipliant le reste par 10 et en effectuant la division euclidienne par p... Ainsi en notant r_k les restes et q_k les quotients qui sont donc les chiffres du développement décimal de $\frac{1}{p}$, on a :

$$\begin{aligned} r_0 &= 1 \\ r_1 &= 10r_0 - q_1 p \\ &\vdots \\ r_k &= 10r_{k-1} - q_k p. \end{aligned}$$

On a donc $r_k \equiv 10^k \mod p$ et si on note k_0 l'indice à partir duquel le développement est périodique de période T, on a $q_{k_0+T} = q_k$ avec $r_{k_0+T} = r_k$ et donc $10^{k_0+T} \equiv 10^{k_0} \mod p$ soit $10^T \equiv 1 \mod p$. On en déduit que $r_0 = r_T$ et donc $q_1 = q_{T+1}$, i.e. le développement est périodique dès le premier chiffre après la virgule. Notons alors $d|T$ l'ordre de 10 modulo p ; comme précédemment on a $r_{k+d} = r_k$ pour tout $k > 0$ et donc $q_{k+d} = q_k$ et donc $T|d$ d'où le résultat. □

Exemples $\frac{1}{13} = 0,076923\cdots$ et 10 est d'ordre 6 dans $(\mathbb{Z}/13\mathbb{Z})^\times$.

Remarque : le même raisonnement s'applique pour les $\frac{k}{p}$ avec $1 \leq k \leq p-1$.

Corollaire 3.2. — *Soit T la période du développement décimal de $\frac{1}{p} = 0, a_1 a_2 \cdots, a_T\ a_1 \cdots$ et notons $n = \sum_{i=1}^{d} a_i 10^{T-i}$. On a alors*

$$np = 10^T - 1.$$

Preuve : On a l'égalité

$$\frac{1}{p} = \sum_{i=1}^{+\infty} n 10^{-iT} = \frac{10^{-T} n}{1 - 10^{-T}} = \frac{n}{10^T - 1}$$

et donc $np = 10^T - 1$. □

Remarque : pour retrouver l'entier n associé à $p = 7$, on peut partir de l'égalité $999999 = 7n$ soit classiquement par division $999999 = 7 \times 100000 + 299999...$ soit au contraire en partant de droite : $999999 = 7 \times 7 + 999950...$ C'est comme cela par exemple que l'on trouve aisément le $p-1$-ème chiffre du développement décimal de $1/p$.

Remarque : comme $10^{p-1} - 1$ s'écrit avec un nombre pair de 9, l'entier pn est divisible par 99 et donc pour $p \neq 3, 11$, n est divisible par 99 ainsi donc que la somme de ses paquets de 2 chiffres ($100 \equiv 1 \mod 99$). Si $3|p-1$ alors n est divisible par 999 ainsi donc que la somme de ses paquets de 3 chiffres ($1000 \equiv 1 \mod 999$). Dans le même genre d'idée, on a le résultat suivant.

Proposition 3.3. — *Soit $d = 2e$ un multiple de l'ordre T de 10 dans $(\mathbb{Z}/p\mathbb{Z})^\times$ tel que e n'est pas un multiple de T. Pour*

$$A = \sum_{i=1}^{e} a_i 10^{e-i}, \qquad B = \sum_{i=1}^{e} a_{e+i} 10^{e-i}.$$

on a alors $A + B = 10^e - 1$.

Preuve : On a $n = 10^e A + B$ avec $0 \leq A, B < 10^e - 1$ car $p > 1$. Ainsi on a

$$\frac{10^{2e}}{p} = 10^e A + B + \frac{1}{p} \Rightarrow \frac{10^e + 1}{p} \times (10^e - 1) = 10^e A + B$$

. Or comme $(10^e)^2 \equiv 1 \mod p$ et que $10^e \not\equiv 1 \mod p$, on en déduit que $10^e + 1 \equiv 0 \mod p$ de sorte que $A + B \equiv 0 \mod 10^e - 1$ et le résultat découle de l'encadrement $1 \leq A + B < 2(10^e - 1)$. □

Remarque : dans le cas où T est divisible par r, le raisonnement précédent donne que la somme des paquets de T/r chiffres de n est de la forme $k(10^r - 1)$ avec $1 \leq k < r$.

Exemples $\frac{1}{19} = 0,052631578947368421 \cdots$ et on a

$052 + 631 + 578 + 947 + 368 + 421 = 3 \times 999 \quad 05 + 26 + 31 + 57 + 89 + 47 + 36 + 84 + 21 = 4 \times 99.$

Proposition 3.4. — *Soit p premier tel que la période de son développement décimal soit égale à $p - 1$; le nombre dn s'obtient alors à partir de n par permutation circulaire.*

Par exemple : pour $p = 7$, on a

$$\begin{aligned} 2 \times 142857 &= 285714 \\ 3 \times 142857 &= 428571 \\ 4 \times 142857 &= 571428 \\ 5 \times 142857 &= 714285 \\ 6 \times 142857 &= 857142 \end{aligned}$$

Preuve : On reprend les notations de la proposition 3.1 : comme $T = p-1$ on en déduit que $\{r_1, \cdots, r_{p-1}\} = \{1, \cdots, p-1\}$. En notant $1 \leq i_0 \leq p-1$ l'indice tel que $r_{i_0} = k$, on en déduit du calcul même du développement décimal que le i-ème chiffre b_i du développement décimal de k/p est égal à $i + i_0$, d'où le résultat. □

Remarque : une autre façon d'énoncer le résultat précédent est de dire que le n_k du développement décimal de k/p s'obtient par permutation circulaire de n en utilisant, avec les notations de la proposition 3.1 le premier reste $r_i = k$. Dans le cas général où la période est égale à T un diviseur quelconque de $p-1$, les restes des divisions euclidiennes des k/p pour k décrivant $\{1, \cdots, p-1\}$ se répartissent en $(p-1)/T$ sous-ensembles de sorte que les kn pour k décrivant $\{1, \ldots, p-1\}$, à permutations circulaires près, sont en nombre $(p-1)/T$.

Théorème 3.5. — *Soit $p > 11$ premier alors $a_{(p+1)/2} = 0$ si et seulement si $(\frac{10}{p}) = 1$ et sinon elle est égale à 9.*

Preuve : On écrit $A = \sum_{i=1}^{(p-1)/2} a_i 10^{(p-1)/2-i}$ et $B = \sum_{i=1}^{(p-1)/2} a_{(p-1)/2+i} 10^{(p-1)/2-i}$ de sorte que d'après 3.3 soit $A = B$ soit $A + B = 9 \cdots 9$. Dans le premier cas comme $a_1 = 0$, on en déduit que $a_{(p+1)/2} = 0$ et dans le deuxième on obtient 9. Il faut alors décider si $(p-1)/2$ est un multiple d'une période, i.e. si $10^{(p-1)/2} \equiv 1 \mod 2$ ce qui est équivalent à $(\frac{10}{p}) = 1$ d'où le résultat. □

Remarque : d'après la loi de réciprocité quadratique, le résultat ne dépend que de la congruence de p modulo 40. Dans le même ordre d'idée, on peut facilement déterminer le $(p-1)/2$-chiffres du développement décimal de $1/p$: en effet si $(p-1)/2$ est le multiple d'une période alors ce chiffre est le même que le $p-1$-ème que l'on détermine facilement comme expliqué ci-avant. Dans le cas où $(p-1)/2$ n'est pas une période comme avec les notations ci-dessus, $A + B = 9 \cdots 9$, on en déduit que le chiffre cherché est égal à 9 moins le $(p-1)$-ème chiffre.

Notons alors $\mathcal{P}(10)$ l'ensemble des premiers p tels que leur développement décimal est de période $p-1$: cet ensemble est-il infini et si oui quel est sa densité

$$d_{10}(x) = \frac{\sharp\{p \in \mathcal{P}(10),\ p \leq x\}}{\sharp\{p \in \mathcal{P},\ p \leq x\}}, \qquad \lim_{x \to +\infty} d_{10}(x).$$

On conjecture que cette limite est égale à

$$C_{Artin} = \prod_{p \in \mathcal{P}} \Big(1 - \frac{1}{p(p-1)}\Big) \simeq 0,3739558136 \cdots$$

Le choix de la base 10 ne semble pas intervenir dans le résultat, on conjecture que le résultat doit être vrai pour tout choix d'entier a en lieu et place de 10.

3.2. Théorème de Dirichlet. — L'ensemble $\mathcal{P}$ des nombres premiers est infini. Dirichlet améliore ce résultat, en affirmant que pour tout $a \wedge b = 1$, il existe une infinité de nombres premiers $p \equiv a \mod b$. En utilisant la loi de réciprocité quadratique, on peut montrer quelques cas simples.

Proposition 3.6. — *Il existe une infinité de nombres premiers p tels que*

(a) $p \equiv 3 \mod 4$; *(b)* $p \equiv 1 \mod 4$;
(c) $p \equiv 1 \mod 2^m$; *(d)* $p \equiv 5 \mod 6$;
(e) $p \equiv 5 \mod 8$; *(f)* $p \equiv 1 \mod 6$;
(g) $p \equiv -1 \mod 12$; *(h)* $p \equiv -1 \mod 10$.

Preuve : Le schéma de démonstration sera toujours le même : on raisonne par l'absurde en supposant la finitude de l'ensemble considéré et on construit un entier N qui permet d'aboutir à une contradiction. On note n le plus grand élément de l'ensemble supposé fini. Toute la difficulté revient donc à construire N en fonction de n et de l'ensemble considéré :

(a) $N = n! - 1$; si p divise N alors $p > n$ et donc $p \equiv 1 \mod 4$ de sorte que $N \equiv 1 \mod 4$ ce qui n'est pas.

(b) $N = (n!)^2 + 1$; si p premier divise N alors -1 est un carré modulo p soit $p \equiv 1 \mod 4$ et donc par hypothèse $p \leq n$ soit p divise $n!$ et donc $p|N - (n!)^2 = 1$ d'où la contradiction .

(c) si p divise $a^{2^{m-1}} + b^{2^{m-1}}$ avec p premier avec a, alors $\frac{a}{b}$ est d'ordre divisant 2^m et d'ordre distinct de 2^{m-1} ; il est donc d'ordre 2^m. Or l'ordre de tout élément divise le cardinal du groupe soit $p \equiv 1 \mod 2^m$. Soit alors $N = (n!)^{2^{m-1}} + 1$; tout diviseur p premier de N est congru à $1 \mod 2^n$ et supérieur à n d'où la contradiction.

(d) $p \equiv 5 \mod 6$ est équivalent à $p \equiv 1 \mod 2$ et $p \equiv 2 \mod 3$ soit $p > 2$ et $p \equiv 2 \mod 3$. Soit $N = n! - 1$; pour p premier divisant N, on a $p > n$ et donc $p \equiv 1 \mod 3$ de sorte que $N \equiv 1 \mod 3$ ce qui n'est pas.

(e) $N = 3^2 5^2 7^2 11^2 \cdots n^2 + 2^2$; N est visiblement impair. Soit alors p premier divisant N, p ne divise pas 4, de sorte que $p \equiv 1 \mod 4$, soit $p \equiv 1, 5 \mod 8$. À nouveau $p \equiv 5 \mod 8$ est exclu car sinon p diviserait $4 = N - 3^2 \cdots n^2$. On en déduit donc $N \equiv 1 \mod 8$. Or si p est premier impair on a $p \equiv 1, 3, 5, 7 \mod 8$ et on vérifie aisément que p^2 est alors congru à 1 modulo 8 et donc $N \equiv 5 \mod 8$, d'où la contradiction.

(f) $p \equiv 1 \mod 6$ est équivalent à $p > 2$ et $p \equiv 1 \mod 3$. Or si p divise $a^2 + 3b^2$ et p premier avec b, alors -3 est un carré modulo p et donc $(\frac{-3}{p}) = 1 = (-1)^{(p-1)(3-1)/4}(\frac{p}{3})(\frac{-1}{p}) = (\frac{p}{3})$ et donc -3 est un carré modulo p si et seulement si $p \equiv 1 \mod 3$. Soit alors $N = 3(n!)^2 + 1$; tout diviseur premier de N est alors congru à 1 modulo 3 et supérieur à n d'où la contradiction.

(g) si p divise $a^2 - 3b^2$ et p premier avec b alors 3 est un carré modulo p. Or on a $(\frac{3}{p}) = (\frac{p}{3})(-1)^{(p-1)/2}$ et donc 3 est un carré modulo p dans les deux situations suivantes :

- $(\frac{p}{3}) = (-1)^{(p-1)/2} = 1$ soit $p \equiv 1 \mod 3$ et $p \equiv 1 \mod 4$ soit $p \equiv 1 \mod 12$;
- $(\frac{p}{3}) = (-1)^{(p-1)/2} = -1$ soit $p \equiv -1 \mod 3$ et $p \equiv -1 \mod 4$ soit $p \equiv -1 \mod 12$;

Soit alors $N = 3(n!)^2 - 1$; tout diviseur premier p de N est alors congru à ± 1 modulo 12 et supérieur à n de sorte que par hypothèse, $p \equiv 1 \mod 12$. On en déduit alors que $N \equiv 1 \mod 12$ ce qui n'est pas car $N \equiv -1 \mod 12$.

(h) pour p premier $p \equiv -1 \mod 10$ si et seulement si $p \equiv -1 \mod 5$. Or si p divise $a^2 - 5b^2$ avec p premier avec b alors $(\frac{5}{p}) = 1 = (\frac{p}{5})$ et donc $p \equiv \pm 1 \mod 5$. Soit alors $N = 5(n!)^2 - 1$; tout diviseur premier p de N est strictement supérieur à n et congru à $\pm 1 \mod 5$. Par hypothèse il est donc congru à 1 modulo 5 et donc N aussi ce qui n'est pas. □

Cas $a = 1$: soit $L = Dec_{\mathbb{F}_p}(X^n - 1)$. Le corps L est isomorphe à $\mathbb{F}_{p^r}$ pour un certain r et $\mathrm{Gal}(L/\mathbb{F}_p) \simeq \mathbb{Z}/r\mathbb{Z}$ engendré par Fr_p. En outre on a $L = \mathbb{F}_p[\chi]$ pour $\chi \in L$ une racine primitive n-ième de l'unité. Ainsi un élément $\sigma \in \mathrm{Gal}(L/\mathbb{F}_p)$ est déterminé par $\sigma(\chi)$ qui doit être une racine primitive n-ième de l'unité et donc de la forme χ^k pour $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. On obtient ainsi une application injective naturelle

$$\sigma \in \mathrm{Gal}(L/\mathbb{F}_p) \longmapsto k \in (\mathbb{Z}/n\mathbb{Z})^\times$$

l'image étant le groupe engendré par la classe de p. Ainsi r est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Soit $\bar{\Phi}_n(X) = P_1 \cdots P_s$ la décomposition en irréductibles de la réduction modulo p de Φ_n. Soit χ une racine de P_1 de sorte que $L = \mathbb{F}_p[\chi]$ et donc P_1 est le polynôme minimal de χ sur

$\mathbb{F}_p$ et donc $\deg P_1 = [L : \mathbb{F}_p]$. En conclusion tous les P_i sont de même degré $[L : \mathbb{F}_p]$ et donc $s = \frac{\psi(n)}{[L:\mathbb{F}_p]}$ où l'on rappelle que $[L : \mathbb{F}_p]$ est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ainsi $p \equiv 1 \mod n$ est équivalent à demander que $\bar{\Phi}_n$ est totalement décomposé sur $\mathbb{F}_p$ ce qui on vient de le voir, est équivalent à demander que $\bar{\Phi}_n$ a une racine dans $\mathbb{F}_p$. Soit donc p premier divisant $\Phi_n(N!) \equiv 1 \mod N!$ soit $p > N$ et $p \equiv 1 \mod n$ car $\bar{\Phi}_n$ a pour racine $\bar{N}!$. On vient donc de montrer une version faible du théorème de progression arithmétique dont l'énoncé fort est que pour tout a premier avec n, il existe une infinité de premiers congrus à a modulo n, ceux-ci se répartissant de manière uniforme en un sens que l'on ne précise pas ici, sur les $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Remarque : en 2005 Benjamin Green et Terence Tao généralise encore le théorème de Dirichlet en prouvant que pour tout entier k, il existe une infinité de suites de k nombres premiers en progression arithmétique, i.e. il existe a et b tels que

$$a,\ a+b,\ a+2b,\ \cdots, a+(k-1)b \in \mathcal{P}$$

Par exemple pour $k = 10$ le plus petit a est 199 avec $b = 210$ ce qui donne

$$199,\ 409,\ 619,\ 1039,\ 1249,\ 1459,\ 1669,\ 1879,\ 2089.$$

Étant donné k on peut noter a_k et b_k les plus petits entiers tels que $a_k + ib_k$ soient premiers pour tout $i = 0, \cdots, k-1$; Green et Tao donne une majoration de la taille de $a_k + (k-1)b_k$ en fonction de k.

3.3. Tests de primalité. — - Si p divise $F_n = 2^{2^n} + 1$ alors $p \equiv 1 \mod 2^{n+1}$; de même si q est un diviseur de M_p alors l'ordre de la classe de 2 dans $\mathbb{Z}/q\mathbb{Z}$ est égale à p qui doit diviser $q-1$ et donc $q \equiv 1 \mod p$ (on a aussi $q \equiv 1 \mod 2p$). On en déduit aussi que 2 est un carré modulo q et donc $q \equiv \pm 1 \mod 8$.

- *Critère de Lehmer* : il s'agit d'un test effectif dans le cas où la factorisation de $n-1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est connue. En effet n est premier si et seulement si pour tout $i = 1, \cdots, k$, il existe $a_i \in \mathbb{Z}$ tel que

$$a_i^{n-1} \equiv 1 \mod n \text{ et } a_i^{\frac{n-1}{p_i}} \wedge n = 1.$$

Preuve : Si n est premier et si g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ alors il suffit de poser $a_i = g$ pour tout $i = 1, \cdots, k$. Réciproquement soit p un diviseur premier de n alors pour tout $i = 1, \cdots, k$, comme $a_i^{(n-1)/p_i} \not\equiv 1 \mod p$, on en déduit que $p_i^{\alpha_i}$ divise $p-1$ et donc finalement $p - 1 \geq n - 1$ soit $n = p$. □

En particulier pour les nombres premiers de Fermat, on obtient le *critère de Pépin* : $p = F_n$ est premier si et seulement si $3^{(p-1)/2} \equiv -1 \mod p$.

- *Solovay-Strassen* : un entier $n \in \mathbb{N}^*$ est dit pseudo-premier de base b si $b^{n-1} \equiv 1 \mod n$. Par exemple $n = 105 = 3.5.7$ est pseudo-premier de base 13 : en effet on a $13^{104} = (13^2)^{52} \equiv 1 \mod 3$, $13^{104} = (13^4)^{26} \equiv 1 \mod 5$ et $13^{104} = (13^6)^{17} \times 13^2 \equiv 1 \mod 7$, de sorte que d'après le lemme chinois on a $13^{104} \equiv 1 \mod 105$. En revanche on a $2^{104} = (2^6)^{17} \times 2^2 \equiv 4 \mod 7$ de sorte que 105 n'est pas pseudo-premier de base 2. Le petit théorème de Fermat dit qu'un nombre premier p est pseudo-premier de base b pour tout b premier à p.

Ce test serait « bon » dans le sens où calculer a^{N-1} requiert, en utilisant l'exponentiation rapide, $O(\log N)$ multiplications ; cependant il est « mauvais » à cause des nombres de Carmichael qui vérifient le test sans être premier : le plus petit de ces nombres est $561 = 3.11.17$ et on sait que l'ensemble de ces nombres est infini. Une amélioration de ce test est donné par

le test de *Solovay-Strassen* qui consiste à vérifier les congruences $a^{\frac{N-1}{2}} \equiv (\frac{a}{N}) \mod N$ dont la véracité est assurée par la proposition suivante.

Proposition 3.7. — *Soit* $H = \{a \in (\mathbb{Z}/N\mathbb{Z})^\times : a^{\frac{N-1}{2}} \equiv (\frac{a}{N}) \mod N\}$ *; alors* $H = (\mathbb{Z}/N\mathbb{Z})^\times$ *si et seulement si* N *est premier.*

Preuve : On a déjà vu que si N est premier alors $H = (\mathbb{Z}/N\mathbb{Z})^\times$. Réciproquement si p^2 divise N, il existe alors un élément $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ d'ordre $p(p-1)$ et comme p ne divise pas $N-1$, $a^{N-1} \not\equiv 1 \mod N$. Si $N = pp_2 \cdots p_r$ sans facteurs carrés ; par le lemme chinois soit $a \equiv 1 \mod p_2 \cdots p_r$ et a non carré modulo p de sorte que $(\frac{a}{N}) = -1$ mais $a^{(N-1)/2} \equiv 1 \mod p_2 \cdots p_r$ et donc $a^{(N-1)/2} \not\equiv 1 \mod N$. □

Remarque : on obtient ainsi un premier *test de primalité probabiliste* : si N est composé alors comme $[(\mathbb{Z}/N\mathbb{Z})^\times : H] \geq 2$, en prenant a aléatoirement on a au moins une chance sur deux d'avoir $a \notin H$ de sorte que si N passe successsivement k tests, on peut dire qu'il est premier avec une probabilité $\geq 1 - 2^{-k}$. Sous GRH, ce test est même déterministe, en effet l'hypothèse de Riemann généralisée implique que si N est composé, il existe $a \leq 2(\log N)^2$ qui ne passera pas le test de Solovay-Strassen

- *Test probabiliste de Rabin-Miller* : un entier $n = 1 + 2^k q$ impair, q impair, est dit fortement pseudo-premier de base b si l'une des conditions suivantes est vérifiée :

$$b^q \equiv 1 \mod n \qquad \exists 0 \leq j < k,\ b^{2^j q} \equiv -1 \mod n$$

Si n est premier alors il est fortement pseudo-premier de base b pour tout $1 \leq b < n$: en effet $b^{2^k q} \equiv 1 \mod n$ et soit donc $0 \leq i \leq k$ le plus petit entier tel que $b^{2^i q} \equiv 1 \mod n$. Si $i = 0$, on a $b^q \equiv 1 \mod n$ et si $i > 0$ alors $b^{2^{i-1} q} \equiv -1 \mod n$ car dans un corps $x^2 = 1$ entraine $x = \pm 1$.

Remarque : si n est fortement pseudo-premier de base b alors il est pseudo-premier de base b : en effet il existe $0 \leq i \leq k$ tel que $b^{2^i q} \equiv 1 \mod n$; or $2^i q$ divise $n-1$ de sorte que $b^{n-1} \equiv 1 \mod n$.

Exemple : $n = 561$ est pseudo-premier de base 13 mais il n'est pas fortement pseudo-premier de base 2 : en effet $n - 1 = 2^4 35$ et $2^{352^3} \equiv 1 \mod 561$ mais $2^{352^2} \equiv 67 \mod 561$.

Théorème 3.8. — *(Rabin) Pour* n *impair soit*

$$B_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ n \text{ est fortement pseudo-premier de base } x\}.$$

Alors si n *est non premier alors* $\frac{|B_n|}{\phi(n)} \leq 1/4$ *sauf pour* $n = 9$.

Remarque : autrement dit si $|B_n| \geq \phi(n)/4$ alors n est premier. Ainsi si n est fortement pseudo-premier dans m bases tirées au hasard, on peut présumer, avec une probabilité d'erreur inférieure à $1/4^m$, qu'il est premier. Par exemple pour $n = 561$, on obtient $|B_{561}| = 10$ de sorte qu'outre ± 1, il ne reste plus que 8 entiers qui font croire que 561 est premier et le rapport $\frac{|B_{561}|}{\varphi(561)} = 1/32$ est relativement faible. Ce critère est particulièrement adapté à la méthode RSA.

3.4. Méthodes de factorisation. — Une des idées pour factoriser de grands nombres n est de considérer des paires d'entiers (x, y) telles que $x^2 \equiv y^2 \mod n$ de sorte que n divise $(x-y)(x+y)$ et que « moralement » il y a une chance sur 2 pour que les facteurs premiers de n se répartissent sur les deux facteurs $(x-y)$ et $(x+y)$. Ainsi le pgcd $(x-y) \wedge (x+y)$ a de bonnes chances de donner un diviseur non trivial de n.

En 1931, D. H. Lehmer et R. E. Powers ont montré comment construire de telles paires systématiquement en utilisant les fractions continues. L'idée est la suivante : si t est petit avec $x^2 \equiv t \mod n$, alors $x = t + kd^2n$ et donc $(x/d)^2 - kn = t/d^2$ est petit, autrement dit x/d est une bonne approximation de $\sqrt{kn}$. Or on sait que les fractions continues sont de bonnes approximations rationnelles : ainsi on calcule via les fractions continues de bonnes approximations P/Q de $\sqrt{kn}$ pour divers k et on essaie de factoriser $t = P^2 - Q^2kn$ via des petits nombres premiers $\leq 10^4$ par exemple. Une fois que l'on a obtenu quelques (x_i, t_i) ainsi on essaie de construire une égalité du type

$$a^2 = \prod_i a_i \equiv \prod_j b_j = b^2 \mod N$$

Concrètement on construit un nombre de tels couples supérieur à nombre de premiers considérés, ici $\leq 10^4$ soit 1229. On représente alors une telle factorisation $p_1^{r_1} \cdots p_{1229}^{r_{1229}}$ par le vecteur $v(a) = (r_1, \cdots, r_{1229})$. Si toutes les coordonnées de $v(a)$ sont paires alors $a^2 - n$ est un carré ce qui donne une factorisation de n. Dans le cas contraire comme on a plus de vecteurs que de coordonnées, on en déduit qu'il existe une somme de $v(a)$ dont toutes les coordonnées sont paires : pour obtenir cette somme, on pose $w(a) = (s_1, \cdots, s_{1229})$ avec $s_i = 0$ si r_i est paire et $s_i = 1$ sinon. L'algorithme de Gauss sur les vecteurs $w(a)$ de $(\mathbb{Z}/2\mathbb{Z})^{1229}$, très rapide dans cette situation, fournit alors la somme à considérer.

En remarquant que si N n'est pas premier, il y a dans $(\mathbb{Z}/N\mathbb{Z})^\times$ au moins 4 racines carrés de 1, on en déduit qu'il y a au moins une chance sur deux pour que $\pm b$ soit distinct de a. On a alors une chance sur deux en étudiant $(a-b \wedge N)$ et $(a+b \wedge N)$ d'obtenir une factorisation non triviale de N. Cet algorithme a en fait une complexité $L(1/2, N) = \exp(C(\log N)^{1/2}(\log\log N)^{1/2})$ ce qui est déjà remarquable même si insuffisant pour factoriser de très grands nombres.
Remarque : la version optimale de cette idée est donné par Pomerance en 1981 et s'appelle *le crible quadratique*.

3.9 — Algorithme ρ de Pollard : cet algorithme construit en 1975 est le plus efficace pour trouver des petits facteurs par exemple d'ordre 10^7. En pratique, on commence par l'utiliser systématiquement pour tester s'il y a des diviseurs d'ordre 10^5 et dans la négative, on passe à des algorithmes plus efficaces comme le crible quadratique.

On choisit a_0 entre 1 et N et on considère la suite $a_{i+1} = f(a_i)$ avec $f(a) = a^2 + 1 \mod N$. On suppose que la suite des a_i modulo p est suffisamment aléatoire, ce qui est assez bien vérifié par l'expérience et la pratique. Ainsi la probabilité pour que r nombres pris au hasard modulo p soient tous distincts est

$$P_r = (1 - \frac{1}{p})(1 - \frac{2}{p}) \cdots (1 - \frac{r-1}{p}) \leq \exp(-\frac{r(r-1)}{2p})$$

Prenons r de l'ordre de $\sqrt{p}$ et disons $r > 2\sqrt{p}$ de sorte que $P_r \leq \exp(-r(r-1)/(2p)) \leq \exp(-2 + 1/\sqrt{p}) < 1/2$. On a ainsi une bonne chance qu'il existe $1 < i < j < r$ tels que $a_i \equiv a_j \mod p$ ce qui implique $a_{i+m} \equiv a_{j+m} \mod p$ pour tout $m \geq 0$. Ainsi pour $m = j - 2i$ et $k = j - i$ on aura $a_k \equiv a_{2k} \mod p$. En résumé on a au moins une chance sur deux qu'il existe k d'ordre $O(\sqrt{p})$ tel que $(a_{2k} - a_k) \wedge n$ soit distinct de 1, ce qui fournit un algorithme qui avec une bonne probabilité donne une factorisation de N en temps $O(\sqrt[4]{N})$.

3.10 — Algorithme $p-1$ de Pollard : supposons que n possède un facteur premier p tel que les facteurs premiers de $p-1$ soient petits, i.e. plus petit que 10^4. Supposons en fait que $p-1$ divise 10000!. Comme l'exponentiation modulo n est très rapide, on calcule $m = 2^{10000!} \mod n$. Comme $p-1$ divise 10000!, $m \equiv 1 \mod p$ et donc p divise $m-1$ et comme par

ailleurs il y a de bonnes chances que n ne divise pas 10000!, $g = (m-1) \wedge n$ devrait être un facteur non trivial de n. Dans la pratique on teste $(2^{k!} - 1) \wedge n$, s'il est égal à 1 on passe à $k+1$ et s'il est égal à n alors on peut essayer de remplacer 2 par une autre valeur c, ou alors essayer un autre algorithme.

3.11 — Méthode de factorisation de Lenstra : soit Y un entier ; on dit qu'un nombre est *Y-friable* (resp. *Y-puissance friable*) si tous ses diviseurs premiers sont inférieurs à Y (resp. si toute puissance d'un premier le divisant est inférieure à Y). Soit N le nombre à factoriser et p un diviseur de N ; si $p-1$ est Y-puissance friable pour Y de taille raisonnable, alors $p-1$ divise $m(Y) = ppcm(2, 3, \cdots, Y)$. Si donc $a \wedge N = 1$, alors $a^{m(Y)} \equiv 1 \mod p$ et donc

$$(a^{m(Y)} - 1) \wedge N \neq 1.$$

La méthode sera donc efficace si N possède un facteur premier Y-puissance friable pour Y pas trop grand : le problème est que les grands nombres premiers tels que $p-1$ soit Y-friable sont assez rares. L'idée clef de l'algorithme de Lenstra est que l'on est en train de raisonner dans $(\mathbb{Z}/p\mathbb{Z})^\times$ qui est cyclique de cardinal $p-1$ (cf. ci dessus l'algorithme $p-1$ de Pollard). Ainsi plus généralement soient n un entier à factoriser et G un groupe tel que :

- l'ensemble sous-jacent à G est un sous-ensemble de $(\mathbb{Z}/n\mathbb{Z})^r$ pour un certain entier r ;
- la loi de G est définie en termes d'opérations arithmétiques modulo n.

Pour $d|n$, on note $G|d$ le groupe obtenu à partir de G en réduisant les coordonnées modulo d.

Proposition 3.12. *— Soient n et G comme ci-dessus.*
(1) Test de primalité : s'il existe un $x \in G$ et un entier m satisfaisant les conditions suivantes, alors n est premier :

- *m est plus grand que l'ordre de $G|q$ pour tout éventuel diviseur q de n inférieur à $\sqrt{n}$;*
- *$x^m = e$ l'élément identité de G ;*
- *pour tout premier p divisant m, une coordonnée de $x^{m/p} - e$ est première à n.*

(2) Factorisation : soit p premier divisant n, si l'ordre de $G|p$ divise $k!$ et si n ne divise pas la i-ème coordonnées de $x^{k!} - e$ alors le pgcd de celle-ci avec n fournit un diviseur non trivial de n.

Preuve : (1) Si n n'est pas premier soit alors q un diviseur plus petit que $\sqrt{n}$. Soit alors x et m vérifiant les deux dernières propriétés de l'énoncé. On en déduit alors que l'image de x dans $G|q$ est égale à m ce qui contredit la première hypothèse.

(2) Le résultat découle du fait que p divise toutes les coordonnées de $x^{k!} - e$. □

Remarque : l'algorithme $p-1$ de Pollard correspond à l'application de cette proposition pour le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi pour trouver un diviseur q de n, il faut que $q-1$ divise $k!$ pour un entier $k \ll$ petit $\gg$. Pour appliquer pleinement la proposition précédente, il faut disposer de nombreux exemples de groupes G comme ci-dessus. Les courbes elliptiques $E(a,b) : \{[x,y,z] \in \mathbb{P}^2(\mathbb{C}) : zy^2 = x^3 + axz^2 + bz^3\}$ que l'on regarde modulo n fournissent de tels exemples. Citons sans démonstration les résultats suivants.

Théorème 3.13. *—*

- *(Hasse) L'ordre de $E(a,b)|p$ appartient à l'intervalle $I(p) =]p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}[$.*
- *(Waterhouse) Étant donné un premier $p \geq 3$ et $n \in I(p)$, il existe a et b tels que le cardinal de $E(a,b)|p = n$.*

– *(conjecture de Sato-Tate prouvée en 2006 par M. Harris et R. Taylor) On écrit*

$$-\frac{1}{2\sqrt{p}}(|E(a,b)|p-p-1)=\cos(\theta_{a,b}),$$

alors la mesure de probabilité de θ *est* $\frac{2}{\pi}\sin\theta^2 d\theta$*.*

Ainsi pour factoriser n, il suffit de trouver un entier un entier dans un intervalle $I(p)$ qui divise $k!$ ce qui est bien plus souple que la méthode $p-1$ de Pollard. Cependant il n'est pas simple de calculer l'ordre de $E(a,b)|p$, ni étant donné $n\in I(p)$ de trouver a et b tels que $E(a,b)|p$ soit de cardinal n. Le procédé consiste alors, d'après Sato-Tate, à prendre des courbes elliptiques « au hasard ».
Remarque : on peut montrer que la complexité de cet algorithme est $\exp\sqrt{2\log p\log\log p}$ où p est le plus petit facteur premier divisant N. Par ailleurs cet algorithme est peu gourmand en mémoire puisque l'on doit stocker un nombre de données polynomial en $\log N$.
Remarque : il existe un autre algorithme moins élémentaire appelé *le crible algébrique* dont la complexité est de l'ordre de $L(1/3)$ qui est donc plus efficace que celui de Lenstra pour les N ne possédant pas de facteurs premiers de taille moyenne, ce qui est typiquement le cas pour RSA. Enfin en 1997, Shor a montré que le problème de la factorisation pouvait être résolu en temps polynomial à l'aide d'un ordinateur quantique dont un premier exemplaire vient juste d'être construit.

4. Calculs modulaires

Le critère d'Eisenstein est un moyen simple de construire un polynôme irréductible de degré n donné. Pour cela on prend $a_0\equiv a_1\equiv\cdots\equiv a_{n-1}\equiv 0 \mod p$ et a_n, a_0/p non divisible par p de sorte que $P(X)=a_nX^n+\cdots+a_0$ est irréductible sur $\mathbb{Z}$: c'est un cas particulier du théorème de Lucas.
Remarque : une façon de le démontrer est de considérer la réduction modulo p de $P(X)$. Plus généralement si la réduction modulo p d'un polynôme $Q(X)$ est irréductible alors $Q(X)$ l'est aussi sur $\mathbb{Z}$: malheureusement cette technique n'est pas très efficace. En effet si n est tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique, alors la réduction modulo p du polynôme irréductible Φ_n dit cyclotomique, n'est pas irréductible car le degré d'un quelconque de ses facteurs irréductibles est égal à l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$ qui ne peut donc jamais égaler $\psi(n)$.

Le but de ce paragraphe est de donner divers test d'irréductibilité d'un polynôme ainsi qu'un algorithme de factorisation. Contrairement à la factorisation des entiers, le problème de factorisation d'un polynôme de $\mathbb{Z}[X]$ se fait en temps polynomial.

4.1. Polygones de Newton. — Soient p un nombre premier et ρ un réel quelconque. On définit la *valuation penchée* p-adique de pente ρ la fonction

$$v_{p,\rho}:f=\sum_i a_it^i\in\mathbb{Q}[t]\mapsto v_{p,\rho}(f)=\min\{v_p(a_i)-\rho i:\ a_i\neq 0\}\in\mathbb{R}\cup\{\infty\}$$

où v_p désigne la valuation p-adique, i.e. $n=p^{v_p(n)}m$ avec $m\wedge p=1$. On pose par ailleurs $v_{p,\rho}(0)=\infty$. Visuellement on trace dans le plan $\mathbb{R}^2$ l'ensemble des couples $(i,v_p(a_i))$ alors $v_{p,\rho}(g)$ est la plus grande ordonnée z telle que tous ces points soient au dessus de la droite d'équation $x\mapsto\rho x+z$.
Exemples : $v_{p,\rho}(t^i)=-\rho i$ et pour $f(t)=1+t+pt^2+pt^3$ on a $v_{p,\rho}(f)=0$ si $\rho\leq 0$, vaut $-\rho$ si $0\leq\rho\leq 1/2$ et $1-3\rho$ si $\rho\geq 1/2$, cf. la figure 1

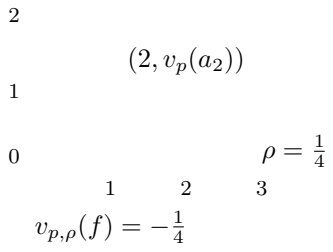

FIGURE 1. Pentes p-adiques de $f(t) = 1 + t + pt^2 + pt^3$

Définition 4.1. — Pour tout $f = \sum_i a_i t^i$, on note $m_{p,\rho}(f)$ (resp. $M_{p,\rho}(f)$) le plus petit (resp. le plus grand) entier i tel que $v_p(a_i) = \rho i + v_{p,\rho}(f)$. *Une pente du polygone de Newton* (p-adique) est un réel ρ tel que *la largeur* $\Delta_{p,\rho}(f) = M_{p,\rho}(f) - m_{p,\rho}(f)$ de la pente ρ est strictement positive.

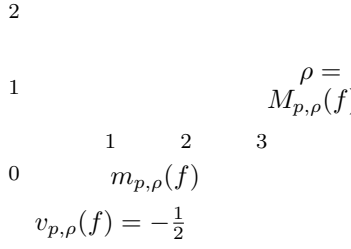

FIGURE 2. Largeurs p-adiques de $f(t) = 1 + t + pt^2 + pt^3$

Remarque : les pentes sont forcément rationnelles car pour ρ irrationnel toute droite d'équation $y = \rho x + z$ ne peut rencontrer qu'au plus un point $(i, v_p(a_i))$. L'ensemble des pentes est fini. *Exemple* : les pentes p-adique du polygone de Newton de $f(t) = 1 + t + pt^2 + pt^3$ sont $\rho = 0$ avec $M_{p,0}(f) = 1$, $m_{p,0}(f) = 0$, et $\rho = 1/2$ avec $M_{p,1/2}(f) = 3$, $m_{p,1/2}(f) = 1$.

Proposition 4.2. — *La fonction $v_{p,\rho}$ est une valuation sur $\mathbb{Q}[t]$, i.e.*
(i) $v_{p,\rho}(f) = \infty$ si et seulement si $f = 0$;
(ii) $v_{p,\rho}(fg) = v_{p,\rho}(f) + v_{p,\rho}(g)$ avec la convention $a + \infty = \infty$;
(iii) $v_{p,\rho}(f + g) \geq \min\{v_{p,\rho}(f), v_{p,\rho}(g)\}$ avec la convention $\infty \geq a$.
En outre pour tous $f, g \in \mathbb{Q}[t]$ non nuls, on a $M_{p,\rho}(fg) = M_{p,\rho}(f) + M_{p,\rho}(g)$ et $m_{p,\rho}(fg) = m_{p,\rho}(f) + m_{p,\rho}(g)$.

Preuve : Les conditions (i) et (iii) sont immédiates d'après la définition en utilisant que v_p est une valuation. Montrons donc (ii) : pour $f = \sum_i a_i t^i$ et $g = \sum_i b_i t^i$ on a $h = fg = \sum_i c_i t^i$ avec $c_i = \sum_{j=0}^{i} a_j b_{i-j}$. Comme $v_p(c_i) \geq \min\{v_p(a_j) + v_p(b_{i-j} : \ j)+, \cdots, i\}$, on a également

$$v_p(c_i) - \rho i \geq \min\{\Big(v_p(a_j) - \rho j\Big) + \Big(v_p(b_{i-j}) - \rho(i-j)\Big) : \ j = 0, \cdots, i\},$$

ce qui prouve $v_{p,\rho}(h) \geq v_{p,\rho}(f) + v_{p,\rho}(g)$. Montrons alors l'inégalité inverse : on pose $r = m_{p,\rho}(f)$ et $s = m_{p,\rho}(g)$ de sorte que dans la somme $c_{r+s} = \sum_{j=0}^{r+s} a_j b_{r+s-j}$, le terme pour lequel $j = r$ est alors de valuation p-adique $\rho(r+s) + v_{p,\rho}(f) + v_{p,\rho}(g)$ et tous les autres termes sont de valuation p-adique strictement supérieure. On en déduit alors que $v_p(c_{r+s}) = \rho(r+s) + v_{p,\rho}(f) + v_{p,\rho}(g)$ et donc $v_{p,\rho}(h) \leq v_{p,\rho}(f) + v_{p,\rho}(g)$.

Par ailleurs si $i < r+s$ alors chaque terme de $\sum_{j=0}^{i} a_j b_{i-j}$ est de valuation strictement supérieure à $\rho i + v_{p,\rho}(f) + v_{p,\rho}(g)$ et donc $m_{p,\rho}(h) = r+s$. L'égalité sur $M_{p,\rho}$ se montre de manière strictement similaire. □

Corollaire 4.3. — *Pour tout p premier fixé et ρ réel ρ, on a $\Delta_{p,\rho}(fg) = \Delta_{p,\rho}(f) + \Delta_{p,\rho}(g)$.*

Remarque : on utilise ce corollaire pour obtenir des renseignements sur les degrés des facteurs irréductibles d'un polynôme h. Par exemple si h n'admet qu'une seule pente de largeur 1 alors il est irréductible. Si vous essayez quelques exemples numériques vous vous apercevrez du fait suivant : le dénominateur réduit d'une pente $\rho \in \mathbb{Q}$ est le plus petit entier naturel non nul q tel que $\rho q \in \mathbb{Z}$: si z, i, j sont des entiers tels que $\rho i + z$ et $\rho j + z$ soient entiers alors ces deux entiers sont distincts d'au moins ce dénominateur réduit. L'entier $\Delta_{p,\rho}(f)/q$ est appelé *le degré* de ρ.

Lemme 4.4. — *Soit $\rho \in \mathbb{Q}$ de dénominateur réduit q alors la valuation $v_{p,\rho}$ définit sur $\mathbb{Q}[t]\backslash\{0\}$ a pour image $\frac{1}{q}\mathbb{Z}$.*

Preuve : Pour $f \in \mathbb{Q}[t]$ non nul, on a clairement $v_{p,\rho}(f) \in \frac{1}{q}\mathbb{Z}$. Réciproquement tout élément de $\frac{1}{q}\mathbb{Z}$ peut s'écrire $a + \rho b$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}$; $p^a t^b$ a alors la valuation voulue. □

Corollaire 4.5. — ***(critère de Dumas)*** *: si $h \in \mathbb{Q}[t]$ avec $h(0) \neq 0$ a, pour un certain premier p, une pente ρ dont la largeur est* $\deg h$ *et égale au dénominateur réduit de ρ, alors h est irréductible.*

FIGURE 3. Le critère de Dumas.

Remarque : dans l'énoncé ci-dessus, demander que la largeur $\deg h$ soit égale au dénominateur réduit de ρ est équivalent à demander que la droite $y = \rho x + v_{p,\rho}(h)$ ne rencontre pas d'autres points de $\mathbb{Z}^2$ entre celui d'abscisse $m_{p,\rho}(h) = 0$ et celui d'abscisse $M_{p,\rho}(h) = \deg h$.

Preuve : Comme $m_{p,\rho}(h) = 0$ et $M_{p,\rho}(h) = \deg h$, pour $h = fg$ du corollaire précédent on en déduit que $m_{p,\rho}(f) = m_{p,\rho}(g) = 0$, $M_{p,\rho}(f) = \deg f$ et $M_{p,\rho}(g) = \deg g$. Ceci impose alors que $\deg f$ et $\deg g$ sont des multiples du dénominateur réduit de ρ supposé égal à $\deg h$. Ainsi de l'égalité $\deg h = \deg f + \deg g$, on en déduit que $\deg f.\deg g = 0$ i.e la factorisation $h = fg$ était triviale. □

Corollaire 4.6. — ***(critère d'Eisenstein)*** *: si $h = \sum_i a_i t^i \in \mathbb{Q}[t]$ est tel que pour un premier p, $v_p(a_0) = 1$, $v_p(a_{\deg h}) = 0$ et pour tout $0 < i < d$, $v_p(a_i) \geq 1$, alors h est irréductible.*

FIGURE 4. Le critère d'Eisenstein

Preuve : Pour $\rho = -1/\deg h$, les hypothèses assurent qu'il y a exactement deux points $(i, v_p(a_i))$ sur la droite $y = \rho x$ tous les autres étant strictement au dessus : ces deux points on pour abscisse $m_{p,\rho}(h) = 0$ et $M_{p,\rho}(h) = d$, i.e ρ est une pente de largeur maximale $\deg h$ égal à son dénominateur réduit. Comme $h(0) \neq 0$, le résultat découle du corollaire précédent. □

Définition 4.7. — Le polygone de Newton p-adique de $f(t) = \sum_i a_i t^i$ est la région du plan $\mathbb{R}^2$ constituée des points (ζ, z) tels que $\mathrm{val} f \leq \zeta \deg f$ avec $z \geq \rho\zeta + v_{p,\rho}(f)$ pour tout $\rho \in \mathbb{R}$.

Proposition 4.8. — *Le polygone de Newton p-adique de f est l'épigraphe $\mathcal{C}_p(f)$ de la fonction continue convexe et affine par morceaux $\mathcal{N}$ entre les abscisses* $\mathrm{val} f$ *et* $\deg f$ *qui a les pentes ρ sur l'intervalle $[m_{p,\rho}(f), M_{p,\rho}(f)]$ avec $\mathcal{N}(\mathrm{ord} f) = v_p(a_{\mathrm{val} f})$ et $\mathcal{N}(\deg f) = v_p(a_{\deg f})$. C'est aussi l'enveloppe convexe supérieure de l'ensemble des points $(i, v_p(a_i))$.*

Preuve : Il y a un certain nombre de sous-entendu dans cette proposition, il s'agit en fait de montrer que pour ρ croissant les segments $[A_\rho, B_\rho]$ de $\mathbb{R}^2$ où $A_\rho = (m_{p,\rho}(f), \rho m_{p,\rho}(f) + v_{p,\rho}(f))$ et $B_\rho = (M_{p,\rho}(f), \rho M_{p,\rho}(f) + v_{p,\rho}(f))$, forment une ligne polygonale.

Lemme 4.9. — *Soient $\rho < \varsigma$ deux réels :*
(i) si $\zeta \leq M_{p,\rho}(f)$ alors $\rho\zeta + v_{p,\rho}(f) \geq \varsigma\zeta + v_{p,\varsigma}(f)$ avec inégalité stricte si $\zeta < M_{p,\rho}(f)$;
(ii) si $\zeta \geq m_{p,\varsigma}(f)$ alors $\rho\zeta + v_{p,\rho}(f) \leq \varsigma\zeta + v_{p,\varsigma}(f)$ avec inégalité stricte si $\zeta > m_{p,\varsigma}(f)$.

FIGURE 5. Le polygone de Newton 2-adique de $12 + \frac{1}{7}X + 4X^2 + \frac{1}{2}X^4 + X^5 + \frac{4}{5}X^6 + 4X^7$.

Preuve : Pour $f = \sum_i a_i t$ı, notons $r = M_{p,\rho}(f)$ de sorte que $v_{p,\rho}(f) = v_p(a_r) - \rho r$. Si $\zeta \leq r$ alors

$$\rho\zeta + v_{p,\rho}(f) = \rho(\zeta - r) + v_p(a_r) \geq \varsigma(\zeta - r) + v_p(a_r) \geq \varsigma\zeta + v_{p,\varsigma}(f)$$

et si $\zeta < r$ alors la première inégalité est stricte ce qui prouve (i). La preuve de (ii) est strictement similaire. □

Lemme 4.10. — *Soient $f(t) = \sum_i a_i t^i$, p premier et $\rho \in \mathbb{R}$: on note $r = M_{p,\rho}(f)$. Si $\varsigma \geq \rho$ est suffisamment proche de ρ alors pour tout $j > r$ tel que $a_j \neq 0$, on a $v_p(a_j) - \varsigma j > v_p(a_r) - \varsigma r$ et $M_{p,\varsigma}(f) = r$.*

Preuve : Comme r est le plus grand entier réalisant le minimum de $v_p(a_i) - \rho i$, si $j > r$ on a $v_p(a_j) - \rho j > v_p(a_r) - \rho r$ de sorte que si $\varsigma \geq \rho$ est suffisamment proche de ρ, on a $v_p(a_j) - \varsigma j > v_p(a_r) - \varsigma r$. Pour un tel ς il est alors vrai que le plus grand j pour lequel $v_p(a_j) - \varsigma j$ atteint son minimum est $j = r$ i.e. $M_{p,\varsigma}(f) = r$. □

Lemme 4.11. — *Soient $f \in \mathbb{Q}[t]$ non nul et p un premier fixé, alors :*

(i) pour $\rho < \varsigma$, on a $v_{p,\rho}(f) \geq v_{p,\varsigma}(f)$ et $m_{p,\rho}(f) \leq m_{p,\varsigma}(f)$;

(ii) pour $\rho \in \mathbb{R}$ fixé, si $\varsigma > \rho$ est suffisamment proche de ρ alors $M_{p,\rho}(f) = m_{p,\varsigma}(f) = M_{p,\varsigma}(f)$;

(iii) pour tout réel val$f < \zeta < \deg f$*, il existe un unique ρ tel que $m_{p,\rho}(f) \leq \zeta < M_{p,\rho}(f)$.*

Preuve : (i) D'après le lemme 4.9 appliqué à $\zeta = 0 \leq M_{p,\rho}(f)$, on a $v_{p,\rho}(f) \geq v_{p,\varsigma}(f)$; en outre si $j < M_{p,\rho}(f)$ alors $v_p(a_j) \geq \rho j + v_{p,\rho}(f) > \varsigma j + v_{p,\varsigma}(f)$ et donc $m_{p,\varsigma}(f) \geq M_{p,\rho}(f)$.

(ii) D'après le lemme 4.10 on a $M_{p,\rho}(f) = M_{p,\varsigma}(f)$; or d'après (i) on a aussi $M_{p,\rho}(f) \leq m_{p,\varsigma}(f) \leq M_{p,\varsigma}(f)$ de sorte que toutes ces inégalités sont des égalités.

(iii) Pour ζ fixé, la fonction

$$\phi : \rho \mapsto (\rho\zeta + v_{p,\rho}(f)) = \min\{\rho(\zeta - i) + v_p(a_i) : \ a_i \neq 0\}$$

est continue car c'est le minimum d'un ensemble fini de fonctions continues. Lorsque $\rho \to +\infty$, l'hypothèse $\zeta < \deg f$ implique qu'il existe au moins un i tel que $a_i \neq 0$ et $\zeta_i < 0$ de sorte que ϕ tend vers $-\infty$ en $+\infty$. De même ϕ tend vers $-\infty$ en $-\infty$. Soit alors ρ tel que $\phi(\rho)$ atteigne son maximum : si on avait $\zeta > M_{p,\rho}(f)$ alors pour $\varsigma > \rho$ suffisamment proche de ρ, (ii) implique que $\zeta > m_{p,\varsigma}(f)$ de sorte que d'après 4.9 on aurait $\phi(\rho) < \phi(\varsigma)$ contredisant la définition de ρ. Un raisonnement similaire montre que $\zeta \geq m_{p,\rho}(f)$. Ainsi pour tout val$f < \zeta < \deg f$ il existe

un ρ tel que $m_{p,\rho}(f) \leq \zeta < M_{p,\rho}(f)$: en particulier si $\zeta \notin \mathbb{Z}$ alors $m_{p,\rho}(f) \leq \zeta < M_{p,\rho}(f)$. Si ζ est entier on applique ce qui précède à $\zeta + 1/2$ qui vérifie encore $\mathrm{val} f < \zeta + 1/2 < \deg f$ ce qui montre bien l'existence.

En ce qui concerne l'unicité soient $\rho < \varsigma$ tels que $m_{p,\rho}(f), m_{p,\varsigma}(f) \leq \zeta < M_{p,\rho}(f), M_{p,\varsigma}(f)$ alors $M_{p,\rho}(f) > m_{p,\rho}(f)$ ce qui contredit (i). □

On a donc prouvé que :

- la fonction $\rho \mapsto v_{p,\rho}(f)$ est continue décroissante ;
- la fonction $\rho \mapsto m_{p,\rho}(f)$ (resp. $\rho \mapsto M_{p,\rho}(f)$) est croissante et continue à gauche (resp. à droite) ; par ailleurs ces deux fonctions ne différent qu'en un nombre fini de points à savoir les pentes du polygone de Newton p-adique de f.

On a donc justifié la définition de polygone de Newton telle que donnée plus haut. Montrons alors la dernière affirmation : la convexité est claire car le polygone de Newton est défini comme une intersection de demi-plans. La stabilité par translation vers le haut est évidente ainsi que le fait qu'il contient les points $(i, v_p(a_i))$. Soit alors un convexe C stable par translation vers le haut contenant les points $(i, v_p(a_i))$ et limité par les abscisses $\mathrm{val} f$ et $\deg f$. En particulier pour tout $\rho \in \mathbb{R}$, C doit contenir les points A_ρ et B_ρ et donc par convexité le segment $[A_\rho, B_\rho]$ ainsi que tout translaté vers le haut de ce segment. Comme par ailleurs pour tout ζ de $]\mathrm{val} f, \deg f[$, il existe ρ tel que $m_{p,\rho}(f) \leq \zeta \leq M_{p,\rho}(f)$, on obtient bien que C contient le polygone de Newton de f d'où le résultat. □

Remarque : les points A_ρ, B_ρ sont appelés les sommets du polygone de Newton et $\mathcal{N}$ s'appelle la fonction du polygone de Newton de f. La proposition 4.2 se traduit alors comme suit sur le polygone de Newton.

Corollaire 4.12. — *Soient f, g deux polynômes de $\mathbb{Q}[t]$ et p un premier fixé alors*

$$\mathcal{C}_p(fg) = \mathcal{C}_p(f) + \mathcal{C}_p(g) = \{u \in \mathbb{R}^2 : \ \exists v \in \mathcal{C}_p(f),\ w \in \mathcal{C}_p(g) \text{ tels que } u = v + w\}.$$

Exemples :

- le critère d'Eisenstein appliqué à $p = 3$ montre que $t^3 + 9t + 6 \in \mathbb{Q}[t]$ est irréductible ;
- le critère de Dumas appliqué à $p = 2$ montre que $t^3 + 2t^2 + 4 \in \mathbb{Q}[t]$ est irréductible : sa seule pente est $-\frac{2}{3}$ de largeur 3 ;
- si le polynôme $h(t) = t^n + pt + bp^2$ avec $b \wedge p = 1$ n'a pas de racines dans $\mathbb{Z}$ alors il est irréductible dans $\mathbb{Q}$: en effet son polygone de Newton p-adique a pour pente -1 et $-\frac{1}{n-1}$ de largeur respectives 1 et $n-1$ de sorte que si $h = fg$ est une factorisation non triviale alors $\deg f = 1$ et $\deg g = n - 1$;
- le polynôme $h(t) = 2t^4 + 2t^3 + 3t^2 + 6 \in \mathbb{Q}[t]$ est irréductible : en effet son polygone de Newton 2-adique a les pentes $\pm\frac{1}{2}$ de largeurs 2 de sorte que si h n'est pas irréductible il est le produit de deux polynômes irréductibles de degré 2, un de pente $\frac{1}{2}$ et de largeur 2 et l'autre de pente $-\frac{1}{2}$ et de largeur 2. Son polygone 3-adique a les pentes $-\frac{1}{3}$ et 0 de largeurs respectives 3 et 1 de sorte que si h n'est pas irréductible il est le produit de deux polynômes irréductibles de degré 3 et 1 de pentes respectives $-\frac{1}{3}$ et 0 avec pour largeurs respectives 3 et 1. La confrontation de ces deux faits montre bien que h est irréductible.

4.13 — Réduction modulo une pente : considérons l'exemple $h(t) = t^4 + 2t^2 + 4$ dont le polygone de Newton 2-adique possède une unique pente $-\frac{1}{2}$ de largeur 4. On en déduit alors que soit h est irréductible soit le produit de deux polynômes irréductibles de degré 2, avec pour pente $-\frac{1}{2}$ et largeur 2. A ce stade il ne nous est pas possible d'aller plus loin.

Définition 4.14. — Soient p un premier fixé et $\rho \in \mathbb{Q}$ de dénominateur réduit $q \in \mathbb{N}$. Pour tout $f = \sum_i a_i t^i \in \mathbb{Q}[t]$ tel que $v_{p,\rho}(f) > 0$, on appelle réduction de f modulo p et suivant la pente ρ, le polynôme $\tilde{f} = \sum_i \tilde{a}_i t^i \in \mathbb{F}_p[t]$ où pour tout i, $\tilde{a}_i$ est la réduction modulo p de $p^{-qi\rho} a_{qi}$.

Remarque : comme $v_p(p^{-qi\rho} a_{qi}) = v_p(a_{qi}) - qi\rho \geq v_{p,\rho}(f) \geq 0$, cela a bien un sens de considérer la réduction modulo l de $p^{-qi\rho} a_{qi}$. Par ailleurs si i n'est pas un multiple de q alors $v_p(a_i) - i\rho \geq v_{p,\rho}(f) \geq 0$ mais comme $v(a_i) - i\rho$ n'est pas un entier, car $i\rho \notin \mathbb{Z}$, cette inégalité est stricte et il est donc naturel de ne considérer dans la définition de $\tilde{f}$ que les coefficients a_{qi}.

Proposition 4.15. — *Soient p premier fixé et $\rho \in \mathbb{Q}$. Si $f, g \in \mathbb{Q}[t]$ vérifient tous deux $v_{p,\rho} \geq 0$ alors en réduisant modulo p suivant la pente ρ, on a*

$$\widetilde{f+g} = \tilde{f} + \tilde{g}, \qquad \widetilde{fg} = \tilde{f}\tilde{g}.$$

Preuve : Notons q le dénominateur réduit de ρ et écrivons $f = \sum_i a_i t^i$ et $g = \sum_i b_i t^i$. La première égalité ne pose aucune difficulté puisque $c_i = a_i + b_i$ est le coefficient de degré i de $f + g$ alors $p^{-qi\rho} c_{qi} = p^{-qi\rho}(a_{qi} + b_{qi})$ se réduit modulo p en $\tilde{a}_i + \tilde{b}_i$.

Pour ce qui est de la deuxième formule soit $c_i = \sum_{k=0}^{i} a_k b_{i-k}$ le coefficient de degré i de fg. On a $v_p(a_k) \geq \rho k$ et cette égalité est stricte si k n'est pas un multiple de q car alors ρk n'est pas un entier ; de même on a $v_p(b_{i-k} \geq \rho(i-k)$ avec inégalité stricte si $i - k$ n'est pas un multiple de q. Posons $i = qj$: dans l'écriture de c_{qj} tous les termes $a_k b_{qj-k}$ ont alors une valuation p-adique au moins égale à ρqj et ceux pour lesquels k n'est pas un multiple de q ont une valuation strictement plus grande que ρqj. Par conséquent dans la somme $p^{-qj\rho} c_{qj} = \sum_{k=0}^{qj} p^{-qj\rho} a_k b_{qj-k}$, tous les termes ont une valuation positive et ceux pour lesquels k n'est pas un multiple de q ont une valuation strictement positive de sorte qu'après réduction modulo p on peut ne conserver que les termes où $k = qm$ c'est à dire les $p^{-qm\rho} a_{qm} . P^{-q(j-m)\rho} b_{q(j-m)}$ ce qui donne $\tilde{c}_j = \sum_{m=0}^{j} \tilde{a}_m \tilde{b}_{j-m}$. □

Corollaire 4.16. — *Soit $h \in \mathbb{Q}[t]$ avec $h(0) \neq 0$ et supposons qu'il existe un premier p tel que le polygone de Newton p-adique de h n'ait qu'une seule pente ρ et que, en notant $v = v_{p,\rho}(h)$, la réduction de $p^{-v} h$ modulo p et suivant la pente ρ, est irréductible, alors h est irréductible.*

Preuve : Comme il n'y a qu'une seule pente sa largeur est $M_{p,\rho}(f) = \deg h$ avec $m_{p,\rho}(f) = 0$. Quitte à multiplier h par p^{-v} on peut supposer $v = 0$. Soit alors $h = fg$; on peut de même supposer $v_{\rho,p}(f) = 0$ ce qui impose alors $v_{p,\rho}(g) = 0$ (on rappelle que $v_{p,\rho}$ est une valuation sur $\mathbb{Q}[t] \backslash \{0\}$). On a aussi $M_{p,\rho}(f) = \deg f$, $M_{p,\rho}(g) = \deg g$ et $m_{p,\rho}(f) = m_{p,\rho}(g) = 0$. D'après la proposition précédente on a $\tilde{h} = \tilde{f}\tilde{g}$ et comme il est supposé irréductible, on a $\deg \tilde{f} = 0$ ou $\deg \tilde{g} = 0$. Le résultat découle alors du fait que $\deg \tilde{f} = \frac{1}{q} \deg f$ et $\deg \tilde{g} = \frac{1}{q} \deg g$. □

Remarque : le critère de Dumas correspond au cas particulier où $\tilde{h}$ est de degré 1.
Exemples :

- reprenons le polynôme $h(t) = t^4 + 2t^2 + 4$ qui a pour unique pente $-\frac{1}{2}$ dans son polygone de Newton 2-adique ; on multiplie par $\frac{1}{4}$ pour avoir $v_{2,-\frac{1}{2}}(h) = 0$ et on réduit modulo 2 suivant la pente $-\frac{1}{2}$ ce qui donne $\tilde{h}(t) = t^2 + t^1 \in \mathbb{F}_2[t]$ qui est irréductible sur $\mathbb{F}_2$ de sorte que h est irréductible sur $\mathbb{Q}$;
- le polynôme $h(t) = t^4 + 3t^3 - 9t^2 + 9$ a pour unique pente $-\frac{1}{2}$ avec largeur 4 dans son polygone de Newton 3-adique. On multiplie par $\frac{1}{9}$ et on réduit modulo 3 selon la pente

$-\frac{1}{2}$ ce qui donne t^2+1 qui est irréductible sur $\mathbb{F}_3$ de sorte que $h(t)$ est irréductible sur $\mathbb{Q}$.

4.2. Factorisation. — Nous allons dans ce paragraphe présenter une stratégie, i.e. un algorithme, pour factoriser les polynômes à coefficients dans $\mathbb{Q}$. Notons tout d'abord que factoriser $A \in \mathbb{Z}[X]$ dans $\mathbb{Q}$ revient à le factoriser dans $\mathbb{Z}[X]$: explicitement si $A = \prod_i A_i$ où les A_i sont des polynômes irréductibles de $\mathbb{Q}[X]$, alors après multiplication par un certain entier d, on a $dA = \prod_i (d_i A_i)$ où les $d_i A_i \in \mathbb{Z}[X]$ sont primitifs de sorte que d'après le lemme de Gauss, $d = \pm 1$.

Exemples de factorisation par réduction modulo p :

- le polynôme X^2+X+1 est irréductible sur $\mathbb{F}_2$, il l'est donc sur $\mathbb{Z}$ et $\mathbb{Q}$;
- le polynôme X^4-X^2+2X+1 est irréductible sur $\mathbb{Z}$: en effet nous allons voir que les décompositions en facteurs irréductibles modulo 2 et 3 sont incompatibles. Modulo 2 il se factorise en $(X^2+X+1)^2$ avec X^2+X+1 irréductible sur $\mathbb{F}_2$; modulo 3 il se factorise en $(X-1)(X^3+X^2-1)$ avec X^3+X^2-1 irréductible sur $\mathbb{F}_3$;
- le polynôme X^4+1 est irréductible car c'est le polynôme cyclotomique Φ_8 or ses factorisations modulo p sont compatibles : en effet modulo 2, on a $X^4+1=(X+1)^4$ et pour $p \equiv 1 \mod 8$ (resp. $p \equiv 3,5,7 \mod 8$) ses facteurs irréductibles sont tous de degré 1 (resp. de degré 2) car les racines primitives 8-ièmes de l'unité appartiennent toutes à $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^2} \backslash \mathbb{F}_p$) ;

4.17 — Algorithme de Berlekamp :

4.18 — Majoration des coefficients des facteurs irréductibles de A : les résultats qui suivent sont pour l'essentiel dus à Mignotte, on pourra en trouver une présentation dans [**?**].

Théorème 4.19*. — Pour $P(X) = \sum_{i=0}^n p_i X^i \in \mathbb{C}[X]$, on note $|P| = (\sum_i |p_i|^2)^{1/2}$. Soit $A = \sum i = 0^m a_i X^i$ et $B = \sum_{i=0}^n b_i X^i$ des polynômes à coefficients entiers tels que B divise A. Alors pour tout $0 \le j \le n$, on a*

$$|b_j| \le \binom{n-1}{j} |A| + \binom{n-1}{j-1} |a_m|$$

Preuve : Soient $\alpha \in \mathbb{C}$, $G(X) = (X-\alpha)A(X)$ et $H(X) = (\bar{\alpha}X - 1)A(X)$. On a alors

$$\begin{aligned} |G|^2 &= \sum |a_{i-1} - \alpha a_i|^2 = \sum (|a_{i-1}|^2 + |\alpha a_i|^2 - 2Re(\alpha a_i \bar{a}_{i-1})) \\ &= \sum (|\alpha a_{i-1}|^2 + |a_i|^2 - 2Re(\alpha a_i \bar{a}_{i-1})) \\ &= \sum |\bar{\alpha} a_{i-1} - a_i|^2 = |H|^2 \end{aligned}$$

Soit alors $A(X) = a_m \prod (X - \alpha_j)$ et posons

$$C(X) = a_m \prod_{|\alpha_j| \ge 1} (X - \alpha_j) \prod_{|\alpha_j| < 1} (\bar{\alpha}_j X - 1)$$

de sorte que $|C| = |A|$. Ainsi en considérant seulement le coefficient de X^m et le terme constant, on en déduit :

$$|A|^2 = |C^2| \ge |a_m|^2 \Big(M(A)^2 + m(A)^2 \Big)$$

où $M(A) = \prod_{|\alpha_j|>1} |\alpha_j|$ et $m(A) = \prod_{-\alpha_j|<1} |\alpha_j|$. En particulier, on a $M(A) \le |A|/|a_m|$ et

$$|a_j| = |a_m| \Big| \sum \alpha_{i_1} \cdots \alpha_{i_{m-j}} \Big| \le |a_m| \sum \beta_{i_1} \cdots \beta_{i_{m-j}},$$

où $\beta_i = \max\{1, |\alpha_i|\}$.

Lemme 4.20. — *Si $1 \leq x_1 \leq x_m$ sont des réels dont le produit est égal à M alors les fonctions symétriques $\sigma_{m,k} = \sum x_{i_1} \cdots x_{i_k}$ vérifient*

$$\sigma_{m,k} \leq \binom{m-1}{k-1} + \binom{m-1}{k}$$

Preuve : Si on change la paire (x_{m-1}, x_m) par $(1, x_{m-1}x_m)$, toutes les contraintes sont encore satisfaites quitte a réordonner et $\sigma_{m,k}$ augmente de

$$\sigma_{m-2,k-1}(x_{m-1} - 1)(x_m - 1)$$

Ainsi si $x_{m-1} > 1$, le point $(x_1, \cdots, x_m)$ ne réalise pas un maximum. Le maximum est donc atteint pour $x_{m-1} = 1$ ce qui implique $x_i = 1$ pour tout $i < m$ de sorte que $x_m = M$. Le reste du calcul est alors élémentaire : le terme $\binom{m-1}{k-1}$ correspond aux k-uplets contenant x_m et $\binom{m-1}{k}$ à ceux qui ne le contienne pas. □

Comme le produit des β_i est par définition $M(A)$ on en déduit que pour tout j,

$$\begin{aligned} |a_j| &\leq |a_m|\Big(\tbinom{m-1}{m-j-1}M(A) + \tbinom{m-1}{m-j}\Big) \\ &\leq |a_m|\Big(\tbinom{m-1}{j}M(A) + \tbinom{m-1}{j-1}\Big) \end{aligned}$$

Ainsi on a $|b_j| \leq |b_n|(\binom{n-1}{j}M(B) + \binom{n-1}{j-1})$ et donc $|b_j| \leq |a_m|(\binom{n-1}{j}M(A) + \binom{n-1}{j-1})$ car comme B divise A, on a $M(B) \leq M(A)$ et $|b_n| \leq |a_m|$. Le résultat découle alors de l'inégalité $M(A) \leq |A|/|a_m|$. □

Plutôt que de donner une description abstraite d'un algorithme utilisant le théorème de Mignotte, nous allons traiter un cas particulier, celui de $A(X) = X^6 - 6X^4 - 2X^3 - 7X^2 + 6X + 1$. Supposons que A n'est pas irréductible de sorte qu'il possède un facteur irréductible de degré ≤ 3 avec $|b_j| \leq 23$ d'après le théorème précédent. On choisit alors $p \geq 2.23$ et tel que A modulo p est sans facteur carré, par exemple $p = 47$. En appliquant l'algorithme de Berlekamp on trouve la factorisation :

$$A(X) = (X - 22)(X - 13)(X - 12)(X + 12)(X^2 - 12X - 4) \mod 47.$$

Montrons alors que A n'a pas de facteurs irréductibles de degré 1 ou 2 : le terme constant de A étant égal à 1, on en déduit que les termes constants de ses facteurs irréductibles sont égaux à ± 1. Par ailleurs les coefficients de ces facteurs appartiennent à $\{-23, \cdots, 23\}$ de sorte que leur réduction modulo 47 doit être des facteurs de degré 1 écrit dans la factorisation de A modulo 47 dont les coefficients constants sont égaux à ± 1 : il n'y en a pas. De même pour les facteurs de degré 2, on a modulo 47, $12.22 = -18$, $12.13 = 15$, $12.12 = 3$ et $12.22 = 4$; on ne trouve donc pas ± 1 d'où le résultat.

En reprenant le même raisonnement pour les facteurs de degré 3, on obtient qu'un facteur irréductible de degré 3 de A est soit $X^3 + 23X^2 - X + 1$ soit $X^3 - 7X - 1$. La première possibilité est exclue car $b_2 \leq 12$ d'après les majorations du théorème précédent. On teste alors la divisibilité du deuxième cas et on trouve

$$A(X) = (X^3 - 7X - 1)(X^3 + X + 1).$$

4.21 — Lemme de Hensel : en général la borne donnée par le théorème précédent est très grande ; plutôt que de raisonner avec un p grand on raisonne modulo p^e pour e assez grand en relevant de proche en proche les solutions : c'est le lemme de Hensel suivant.

Théorème 4.22. — *Soient p premier et C, A_e, B_e, U, V des polynômes à coefficients entiers tels que*

$$C(X) \equiv A_e(X)B_e(X) \mod p^2 \qquad U(X)A_e(X) + V(X)B_e(X) \equiv 1 \mod p$$

On suppose $e \geq 1$, A_e unitaire, $\deg U < \deg B_e$, $\deg V < \deg B_e$. Alors il existe des polynômes A_{e+1} et B_{e+1} vérifiant les mêmes conditions en remplaçant e par $e+1$ et tels que

$$A_{e+1}(X) \equiv A_e(X) \mod p^e \qquad B_{e+1}(X) \equiv B_e(X) \mod p^e$$

En outre ces polynômes sont uniques modulo p^{e+1}.

Preuve : Posons $D = (C - A_eB_e)/p^e \in \mathbb{Z}[X]$. On cherche $A_{e+1} = A_e + p^eS$ et $B_{e+1} = B_e + p^eT$ avec $S, T \in \mathbb{Z}[X]$. La condition $C(X) \equiv A_{e+1}(X)B_{e+1}(X) \mod p^{e+1}$ est équivalent, comme $2e \geq e+1$, à $A_eT + B_eS \equiv D \mod p$. La solution générale est alors $S \equiv VD + WA_e \mod p$ et $T \equiv UD - WB_e \mod p$ pour un polynôme W. La condition sur le degré impose que S et T sont uniques modulo p et donc A_{e+1} et B_{e+1} sont uniques modulo p^{e+1}. □

Ainsi pour factoriser un polynôme $A \in \mathbb{Z}[X]$, on choisit p tel que A modulo p soit sans facteur carré : i.e. p ne divise pas le discriminant de A. On factorise alors A modulo p via l'algorithme de Berlekamp. Avec le lemme de Hensel on remonte la factorisation modulo p^e pour e assez grand tel que p^e soit supérieur à deux fois la borne trouvée dans le théorème 4.19. On essaie alors les différentes combinaisons possibles de factorisation comme dans l'exemple donné plus haut.

Remarque : sur $\mathbb{F}_p$, on ne connait pas d'algorithme de factorisation en temps polynomial sauf à supposer GRH. En particulier l'algorithme ci-dessus est au pire en temps exponentiel, cependant en moyenne il s'avère que cet algorithme, probabiliste puisqu'il dépend d'un choix de p, aboutit en temps polynomial. De manière surprenante, sur $\mathbb{Z}$, Lenstra a trouvé un algorithme en temps polynomial qui en pratique, cependant, se révèle moins bon que celui présenté ci-dessus.

4.3. Principe de Hasse. — Une équation diophantienne vérifie le principe de Hasse si l'existence de solutions rationnelles « globales », i.e. sur $\mathbb{Q}$, découle de l'existence de solutions dans $\mathbb{Q}_p$ pour tout p premier ainsi que dans $\mathbb{R}$. L'exemple standard du à Selmer d'une équation diophantienne ne vérifiant pas le principe de Hasse est $3x^3 + 4y^3 + 5z^3 = 0$. Au contraire les formes quadratiques non dégénérées vérifient le principe de Hasse, c'est le fameux théorème de Hasse-Minkowski, cf. [**7**] p.73 : dans le cas particulier des formes ternaires le résultat est du à Legendre, cf. loc. ci. ou [**3**] chapitre 17 §3. Quitte à effectuer un changement de variable, on se ramène à étudier

$$ax^2 + by^2 + cz^2 = 0$$

avec $a, b, c \in \mathbb{Z}$ sans facteurs carrés, premiers entre eux deux à deux. L'existence d'une solution réelle est équivalente au fait que a, b, c ne soient pas tous du même signe ce que nous supposerons désormais. Par ailleurs quitte à multiplier a et b par c, et à faire le changement de variable $z' = cz$, on se ramène à étudier $z^2 = ax^2 + by^2$.

Proposition 4.23. — *Soient a, b des entiers positifs sans facteurs carrés alors*

$$ax^2 + by^2 = z^2$$

possède une solution non triviale si et seulement si les trois conditions suivantes sont vérifiées :

(i) a est un carré modulo b ;

(ii) b est un carré modulo a ;

(iii) $-\frac{ab}{(a\wedge b)^2}$ *est un carré modulo* $a\wedge b$.

Preuve : Notons déjà que si l'équation possède une solution non triviale alors les trois conditions de l'énoncé sont vérifiées : pour (i) et (ii) c'est immédiat et pour (iii), on a $-\frac{a}{a\wedge b}x^2 \equiv \frac{b}{a\wedge b}y^2 \mod a\wedge b$ car $a\wedge b$ divise z, et donc $-\frac{ab}{(a\wedge b)^2}$ est un carré modulo $a\wedge b$.

Réciproquement si $a=1$ la proposition est immédiate car $(x,0,x)$ est une solution non triviale et les conditions de l'énoncé sont vérifiées. Si $a=b$ alors d'après (iii), -1 est un carré modulo b, i.e. il existe r,s tel que $b=r^2+s^2$; $x=r$, $y=s$ et $z=r^2+s^2$ est alors une solution non triviale de l'équation.

Quitte à échanger les rôles de x et y, supposons donc $a>b$. L'idée est alors de construire une nouvelle forme $Ax^2+by^2=z^2$ avec $0<A<a$ satisfaisant les mêmes hypothèses que dans l'énoncé, i.e. A est sans facteurs carrés et les conditions (i), (ii), (iii) sont vérifiées, et telle que si elle possède une solution alors l'équation de l'énoncé aussi. Après un nombre fini d'étapes, en échangeant A et b si $A<b$, on arrive soit à $A=b$ soit à $A=1$ cas déjà traités.

En détail : d'après (ii) il existe T et c tels que $c^2-b=aT=aAm^2$ avec A sans facteurs carrés et $|c|\leq a/2$. Comme $0\leq c^2=aAm+b$ et $0\leq b<a$, on a $A\geq 0$ et comme b est sans facteurs carrés on a $A\neq 0$ et donc $A>0$. En outre on a $aAm^2<c^2\leq a^2/4$ on a $A\leq Am^2<a/4<a$.

(i) : posons $b=b_1d$ et $a=a_1d$ avec $d=a\wedge b$. Comme a et b sont sans facteurs carrés, on a $a_1\wedge d=b_1\wedge d=1$. De $c^2-b_1d=a_1dAm^2$, on tire $d|c$ car d est sans facteurs carrés ; $c=c_1d$ avec $dc_1^2-b_1=a_1Am^2$ i.e. $A(a_1m)^2\equiv -a_1b_1 \mod d$. Or d'après (iii), $-a_1b_1$ est un carré modulo d et comme $m\wedge d=1$, i.e. m est inversible modulo d, car sinon $b_1\wedge d\neq 1$, on en déduit que A est un carré modulo d. En reprenant le même raisonnement modulo b_1 à partir de $c^2\equiv aAm^2 \mod b_1$ et en utilisant que a est un carré modulo b et donc modulo b_1, on obtient que A est un carré modulo b_1 et donc d'après le lemme chinois car $b_1\wedge d=1$, A est un carré modulo b.

(ii) : $b\equiv c^2 \mod A$.

(iii) : posons $A=rA_1$ et $b=rb_2$ avec $r=A\wedge b$. De $c^2-rb_2=arA_1m^2$, on en déduit comme r est sans facteur carré que $r|c$: $c=rc_2$ et donc $aA_1m^2\equiv -b_2 \mod r$. Comme a est un carré modulo b et donc modulo r, on a bien $-A_1b_2$ qui est un carré modulo r, en utilisant que comme $m\wedge r=1$, m est inversible modulo r.

Supposons alors que $AX^2+bY^2=Z^2$ possède une solution non triviale alors en multipliant $AX^2=Z^2-bY^2$ par $c^2-b=aAm^2$, on obtient

$$a(AXm)^2=(Z^2-bY^2)(c^2-b)=(Zc+bY)^2-b(cY+Z)^2$$

d'après la multiplicativité de l'application $N(x+y\sqrt{b})=x^2-by^2$ de $\mathbb{Q}(\sqrt{b})$, on en déduit que $(x=AXm, y=cT+Z, z=Zc+bY)$ est une solution de $ax^2+by^2=z^2$. □

On peut alors montrer que $ax^2+by^2+cz^2=0$ vérifie le principe de Hasse : rappelons que d'après le lemme de Hensel, une équation a une solution dans $\mathbb{Q}_p$ si et seulement si elle a une solution modulo p^n pour tout $n\geq 0$.

Corollaire 4.24. — *Soient* a,b,c *des entiers non tous de même signe, sans facteurs carrés et premiers entre eux deux à deux. Si pour tout premier* p *et tout entier* m*, la congruence*

$$ax^2+by^2+cz^2\equiv 0 \mod p^m$$

possède une solution (x,y,z) *non tous divisibles par* p *alors* $ax^2+by^2+cz^2=0$ *a une solution entière non triviale.*

Preuve : On se ramène comme précédemment à l'équation $ax^2+by^2=z^2$ avec a et b positifs sans facteurs carrés. Pour $m=2$ et $p|a$, soit (x,y,z) une solution modulo p^2 non triviale modulo p. Si $p|y$ alors $p|z$ et comme p^2 ne divise pas a alors $p|x$ ce qui n'est pas. On en déduit donc que b est un carré modulo p et comme cela est vrai pour tout $p|a$ et que a est sans facteurs carrés, d'après le lemme chinois, b est un carré modulo a. De la même façon a est un carré modulo b.

Soit alors $p|d=a\wedge b$; on a $p|z$ et si p divisait x ou y alors comme p^2 ne divise pas a ou b, on en déduit que p divise x,y,z, ce qui n'est pas. On a donc $-\frac{a}{d}x^2\equiv\frac{b}{d} \mod p$ et donc $-ab/d^2$ est un carré modulo p. Comme précédemment, on conclut, comme d est sans facteurs carrés, que $-ab/d^2$ est un carré modulo d. Le résultat découle alors de la proposition précédente. □

Remarque : dans la situation ci-dessus, la connaissance d'une solution permet de les obtenir toutes ; on renvoie le lecteur au chapitre IV de [**8**]. En illustration on traite un exemple tiré de loc. cit., soit l'équation $x^2+11y^2-3z^2$ avec la solution $(1,1,2)$. On paramètre alors comme suit :

$$(x,y,z)=(1.r,1.r+p,2.r+q)\qquad (p,q)\in\mathbb{Q}^2$$

de sorte que l'équation s'écrit

$$(22p-12q)r=11p^2-3q^2.$$

On élimine alors r pour faire apparaître x,y,z ce qui donne :

$$\begin{array}{l} gx=11p^2-3q^2\\ gy=33p^2-12pq-3q^2\quad (*)\\ gz=22p^2+22pq-18q^2\end{array}$$

où on a posé $g=22p-12q$. Si on cherche des solutions rationnelles, vu l'homogénéité du système ci-dessus, les solutions sont données par (*) en prenant $g=1$. En ce qui concerne les solutions entières, quitte à multiplier p et q par le ppcm de leur dénominateur, on peut les supposer entiers et premiers entre eux. Il s'agit alors de trouver les valeurs g telles que l'équation

$$A\begin{pmatrix}p^2\\ pq\\ q^2\end{pmatrix}\equiv 0 \mod g\qquad A=\begin{pmatrix}11&0&-3\\ 33&-12&-3\\ 22&22&-18\end{pmatrix}$$

a des solutions. On calcule alors la forme de Smith de A qui est $\mathrm{diag}(66,2,1)$; p et q étant premiers entre eux, on en déduit $g|66$. Ainsi l'ensemble des solutions entières est la réunion pour $g|66$ des ensembles

$$\{\frac{1}{g}(11p^2-3q^2, y=33p^2-12pq-3q^2, 22p^2+22pq-18q^2):\ p\wedge q=1,\ A\begin{pmatrix}p^2\\ pq\\ q^2\end{pmatrix}\equiv 0 \mod g\}$$

dont le calcul explicite ne pose pas de problème.

5. Développements

- décomposition en produit direct de groupes cycliques des $(\mathbb{Z}/n\mathbb{Z})^\times$ [**5**]
- loi de réciprocité quadratique [**?**] [**1**]
- nombres de Mersenne [**1**] [**2**] [**4**]
- nombres de Carmichael
- infinité de premiers congrus...

– le théorème de Fermat, le cas $n = 2$ et $n = 4$ en mettant en évidence le point qui utilise une congruence [**6**]
– calculs modulaires

6. Questions

Exercice 6.1. — *Montrez que* 7 *divise* $3^{105} + 4^{105}$.

Exercice 6.2. — *Montrez l'équivalence* $3|a$ *et* $3|b \iff 3|a^2 + b^2$.

Exercice 6.3. — *Proposez à vos amis doués en calcul mental le jeu suivant : multiplier par* 13 *leur jour de naissance, multiplier par* 14 *leur mois de naissance, additionner ces deux résultats pour former un nombre* n *qu'il vous communique. Comment retrouver les données cachées ?*

Exercice 6.4. — *Un nouveau jeu pour des amis coopératifs : choisir un nombre* k *entre* 1 *et* 8*, puis communiquer le résultat* $n = 10A - 9k$ *où* A *est l'âge du candidat. Expliquez comment vous retrouvez* A.

Exercice 6.5. — *(i) Donnez le cardinal de l'ensemble des éléments d'ordre divisant* d *dans* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(ii) Pour $d = pq$ *avec* p *et* q *premiers divisant* n*, donnez le nombre d'éléments d'ordre* d *dans* $(\mathbb{Z}/n\mathbb{Z})^2$.

Exercice 6.6. — *En rappelant le cadre général, donnez les sous-groupes de* $\mathbb{Z}/24\mathbb{Z}$ *ainsi que leurs relations d'inclusion. On précisera aussi le sous-groupe engendré par* 18 *(resp.* 16*) ainsi que les sous-groupes contenant* (16) *et* (10) *puis ceux contenant* (16) *et inclus dans* (18).

Exercice 6.7. — *Donnez les morphismes de groupe* $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ *puis ceux de* $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$. *Trouvez une condition nécessaire et suffisante sur* m *et* n *pour que tout morphisme* $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ *soit nul.*

Exercice 6.8. — *Montrez l'équivalence* $6|a + b + c \iff 6|a^3 + b^3 + c^3$.

Exercice 6.9. — *Montrez que* 429 *est inversible dans* $\mathbb{Z}/700\mathbb{Z}$ *et donnez son inverse.*

Exercice 6.10. — *Soit* $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *l'application qui à* $k \in \mathbb{Z}$ *associe sa classe modulo* n *et* m. *Précisez le noyau et l'image de* π. *Donnez alors l'ensemble des* $k \in \mathbb{Z}$ *tels que*

(i) $k \equiv 2 \mod 5$ *et* $k \equiv 4 \mod 7$ *;*
(ii) $k \equiv 3 \mod 10$ *et* $k \equiv 2 \mod 6$ *;*
(iii) $k \equiv 4 \mod 10$ *et* $k \equiv 2 \mod 6$ *;*

Que peut-on dire de la congruence de k *modulo* 10 *sachant* $k \equiv 3 \mod 6$ *?*

Exercice 6.11. — *Résoudre dans* $\mathbb{Z}$ *les congruences suivantes :*

(i) $3x \equiv 4 \mod 7$ *;*
(ii) $9x \equiv 12 \mod 21$ *;*
(iii) $103x \equiv 612 \mod 676$.

Exercice 6.12. — *Soient* p *et* q *des nombres premiers distincts.*

(a) Quel est le cardinal de $(\mathbb{Z}/pq\mathbb{Z})^*$ *? Combien y a-t-il d'éléments de* $(\mathbb{Z}/pq\mathbb{Z})^*$ *égaux à leur inverse ?*

(b) Montrer la congruence :

$$\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}} \equiv 1 \bmod pq$$

(même méthode que pour le théorème de Wilson : $(p-1)! \equiv -1 \mod p$).

Exercice 6.13. — *Donnez la congruence modulo 17 de $(1035125)^{5642}$.*

Exercice 6.14. — *Donnez la congruence modulo 18 de 1823^{242} puis celle de 2222^{321} modulo 20.*

Exercice 6.15. — *Montrez que $n^7 \equiv n \mod 42$.*

Exercice 6.16. — *Montrez que si $p \neq 2$ premier divise a^2+b^2, $a, b \in \mathbb{N}$ non divisible par p, alors $p \equiv 1 \mod 4$.*

Exercice 6.17. — *Montrez que $n^7 \equiv n \mod 42$.*

Exercice 6.18. — *(***** théorème de Erdös-Ginzburg-Ziv**) Soit p premier et $\{x_1, \cdots, x_{2p-1}\} \subset \mathbb{N}$; pour $I \subset [1, 2p-1]$, on note $S_I = \sum_{i \in I} x_i$ et*

$$\Sigma = \sum_{I \subset [1,2p-1],\ |I|=p} S_I^{p-1}.$$

Montrez que $\Sigma \equiv 0 \mod p$ et en déduire qu'il existe I tel que $S_I \equiv 0 \mod p$. En déduire que pour tout ensemble de $2n-1$ entiers, on peut en extraire n dont la somme est divisible par n.

Exercice 6.19. — ** Soit p un nombre premier impair.*

(i) Montrez que $1+p+\cdots+p^{p-1}$ admet un facteur premier q impair non congru à 1 modulo p^2.

(ii) Montrez que pour tout entier n, q ne divise pas $n^p - p$.

Exercice 6.20. — ** Déterminez tous les entiers $n > 0$ qui sont premiers avec tous les nombres de la forme $2^k + 3^k + 6^k - 1$.*

Exercice 6.21. — *Étudiez les solutions entières de l'équation $(x^2-9)(x^2-16) = y^2$.*

Exercice 6.22. — *On considère l'équation $y^2 = x^3 + 7$:*

(i) Montrez qu'il n'y a pas de solutions avec x pair ;

(ii) En écrivant l'équation sous la forme $y^2 + 1 = x^3 + 8 = (x+2)(x^2-2x+4)$ et en utilisant l'exercice 1 b, en déduire qu'il n'existe pas de solutions entières.

Exercice 6.23. — *Trouvez les entiers $n, m \in \mathbb{Z}$ tels que les trois derniers chiffres de l'écriture décimale de 2008^n soient les mêmes et dans le même ordre que ceux de 2008^m.*

Exercice 6.24. — ** En raisonnant modulo 3 puis modulo 9, montrez que l'équation*

$$x^3 - 3xy^2 + y^3 = 2891$$

n'a pas de solutions entières.

Exercice 6.25. — ** Existe-t-il des couples $(a, b) \in \mathbb{N}^2$ tels que :*

- *$ab(a+b)$ n'est pas divisible par 7 ;*
- *$(a+b)^7 - a^7 - b^7$ est divisible par 7^7 ?*

7. Solutions

6.1 Comme $4 \equiv -3 \mod 7$ et que 105 est impair, on a $4^{105} \equiv -3^{105}$ d'où le résultat.

6.2 Le sens $\Rightarrow$ est évident ; en ce qui concerne l'autre sens, il suffit de faire un petit tableau des sommes $a^2 + b^2$ avec $a, b \in \mathbb{Z}/3\mathbb{Z}$ pour s'apercevoir que $a^2 + b^2 \equiv 0 \mod 3 \Rightarrow a, b \equiv 0 \mod 3$.

6.3 L'entier n est congru au mois M de naissance modulo 13 ce qui le détermine parfaitement ; il suffit alors de calculer le jour directement à partir de $n - 14M$.

6.4 On a $n \equiv A \mod 9$; il reste alors à déterminer A exactement ce qui est aisé puisque $k < 9$ de sorte que l'ordre de grandeur de n fixe A.

6.5 Notons pour tout entier e, A_e (resp. B_e) l'ensemble des éléments de $(\mathbb{Z}/n\mathbb{Z})^2$ d'ordre e (resp. d'ordre divisant e) et soit a_e (resp. b_e) son cardinal. Un élément (x, y) appartient à A_e si et seulement si x et y sont d'ordre divisant e dans $\mathbb{Z}/n\mathbb{Z}$, de sorte que pour tout e, $b_e = (e \wedge n)^2$. Par ailleurs B_d est la réunion disjointe de $A_d \coprod A_p \coprod A_q \coprod A_1$, où A_1 est réduit à l'élément nul. De même B_p (resp. B_q) est la réunion disjointe de $A_p \coprod A_1$ (resp. $A_q \coprod A_1$). En prenant les cardinaux, on obtient alors :

- $b_d = (n \wedge d)^2 = a_d + a_p + a_q + 1$,
- $b_p = (n \wedge p)^2 = a_p + 1$ et $b_q = (n \wedge q)^2 = a_q + 1$;

soit $a_d = (n \wedge (pq))^2 - (n \wedge p)^2 - (n \wedge q)^2 + 1$.

6.6 On rappelle que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont indexés par les diviseurs d de n ; concrètement l'application $d|n \mapsto (n/d)$ qui à un diviseur d de n associe le sous groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par n/d, est une bijection. Rappelons rapidement l'argument ; soit $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique et soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$; $\pi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ de la forme $d\mathbb{Z}$ qui contient $\operatorname{Ker}\pi = n\mathbb{Z}$ soit d divise n de sorte que π étant surjective H est engendré par l'image de d. En outre le sous-groupe engendré par un élément m est celui étiqueté par (n, m) ; en effet (m) est clairement inclu dans (m, n). L'inclusion réciproque se déduit de la relation de Bezout $un + vm = (n, m)$.

Pour $n = 24$, les sous-groupes sont ceux engendrés par $1, 2, 3, 4, 6, 8, 12, 0$ avec les relations d'inclusion

$$\begin{array}{ccccccc} (8) & \subset & (4) & \subset & (2) & \subset & (1) \\ \cup & & \cup & & \cup & & \cup \\ (0) & \subset & (12) & \subset & (6) & \subset & (3) \end{array}$$

On a en outre $(16) = (8)$ et $(18) = (6)$ de sorte que les sous-groupes contenant (8) et (6) sont (2) et (1) et qu'il n'y en a aucun contenant (8) inclus dans (6).

De manière générale les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ contenant (m_1) et inclus dans (m_2) sont les (d) avec (m_2, n) divisant d et d divisant (m_1, n).

6.7 On rappelle qu'un morphisme d'un groupe cyclique de cardinal n dans un groupe G est complètement déterminé par l'image g d'un générateur quelconque telle $g^n = 1_G$, soit g d'ordre divisant n. Dans le premier cas comme 3 et 4 sont premiers entre eux, les seuls éléments d'ordre divisant 3 dans $\mathbb{Z}/4\mathbb{Z}$ sont le seul d'ordre 1 à savoir 0 de sorte que tout morphisme $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ est nul.

Dans $\mathbb{Z}/15\mathbb{Z}$ les éléments d'ordre divisant 12 sont donc d'ordre divisant $12 \wedge 15 = 3$ et sont donc $0, 5, 10$, ce qui donne 3 morphismes distincts.

D'après les raisonnements ci-dessus, on en déduit donc qu'une CNS pour qu'il n'y ait pas de morphisme non nul $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ est donc $n \wedge m = 1$.

6.8 Il suffit de remarquer que $a^3 - a$ est divisible par 2 et 3 et donc 6 divise $(a^3 - a) + (b^3 - b) + (c^3 - c)$ et donc $a^3 + b^3 + c^3 \equiv a + b + b \mod 6$.

6.9 On rappelle que 700 n'étant pas premier, 429 est inversible dans $\mathbb{Z}/700\mathbb{Z}$ si et seulement si il est premier avec 700 et son inverse est donné par la relation de Bezout, i.e. si $1 = 700a + 429b$ alors l'inverse cherché est b. Il suffit alors d'appliquer l'algorithme d'Euclide :

$$\begin{aligned} 700 &= 429 + 271 \\ 429 &= 271 + 158 \\ 271 &= 158 + 113 \\ 158 &= 113 + 45 \\ 113 &= 2.45 + 23 \\ 45 &= 23 + 22 \\ 23 &= 22 + 1 \end{aligned}$$

On remonte alors les calculs et on obtient la relation de Bezout : $1 = 19.700 - 31.429$ de sorte que l'inverse de 429 dans $\mathbb{Z}/700\mathbb{Z}$ est -31.

6.10 Il s'agit de redémontrer le théorème chinois, i.e. que $\operatorname{Ker}\pi = (n \vee m)$ où $n \vee m$ est le ppcm de n et m, et $\operatorname{Im}\pi = \{(a,b) \ / \ (n \wedge m) | b - a \ \}$. Il est tout d'abord évident que π est un morphisme de groupes ; en outre si $k \in \operatorname{Ker}\pi$, alors il est divisible d'après le lemme de Gauss par $n \vee m$ de sorte que $\operatorname{Ker}\pi \subset (n \vee m)$, l'inclusion réciproque étant évidente. Soit maintenant a, b tels que $b - a$ est divisible par le pgcd (n, m). On écrit une relation de Bezout $un + vm = (n, m)$ et on pose $k = u\frac{n}{(n,m)}b + v\frac{m}{(n,m)}b$. On a alors $k = un\frac{(b-a)}{(n,m)} + a \equiv a \mod n$; de même on a $k = vm\frac{(a-b)}{(n,m)} + b \equiv b \mod m$, de sorte que l'ensemble donné est inclus dans l'image de π. La réciproque est évidente car $k = a + \lambda n = b + \mu m$ soit $(b - a) = \lambda n - \mu m$ qui est donc divisible par (n, m). En particulier lorsque n et m sont premiers entre eux, π induit un isomorphisme $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(i) 5 et 7 sont premiers entre eux, on trouve la solution particulière $k = 32$, l'ensemble des solutions est alors $32 + \lambda 35$ avec $\lambda \in \mathbb{Z}$;

(ii) $(6, 10) = 2$ or 2 ne divise pas $3 - 2 = 1$, il n'y a donc pas de solutions ;

(iii) cette fois-ci $2 = (6, 10)$ divise $4 - 2$; une solution particulière est $k = 14$, l'ensemble des solutions est alors $14 + 30l$ avec $\lambda \in \mathbb{Z}$.

D'après ce qui précède si $k \equiv 3 \mod 6$, on a alors $k \equiv a \mod 10$ avec $a - 3$ divisible par 2, soit $a = 1, 3, 5, 7, 9$.

6.11 (i) 3 étant premier avec 7, il est inversible dans $\mathbb{Z}/7\mathbb{Z}$; on calcule rapidement que $3.5 \equiv 1 \mod 7$, i.e. $5 = 1/3$ dans $\mathbb{Z}/7\mathbb{Z}$ de sorte que l'équation s'écrit $x \equiv 20 \mod 7$ soit $x \equiv -1 \mod 7$;

(ii) d'après le théorème chinois, il suffit de vérifier l'équation modulo 3 et 7. Modulo 3 l'équation s'écrit $0.x \equiv 0 \mod 3$ et est donc toujours vérifiée. Modulo 7, on obtient $2x \equiv -2 \mod 7$; l'inverse de 2 dans $\mathbb{Z}/7\mathbb{Z}$ est -3, soit donc $x \equiv -1 \mod 7$. Le résultat final est donc $x \equiv -1 \mod 7$;

(iii) on calcule rapidement $676 = 2^2.13^2$; par le théorème chinois, on est donc ramené à résoudre $-x \equiv 0 \mod 4$ et $103x \equiv 105 \mod 169$. L'algorithme d'euclide fournit $64.103 - 39.169 = 1$ soit donc $x \equiv 64.105 \mod 69$ soit $x \equiv -40 \mod 169$ et donc $x \equiv -40 \mod 676$.

On peut aussi résoudre la congruence $103x \equiv 105 \mod 13^2$ de proche en proche, de la façon suivante. On la résoud tout d'abord modulo 13 soit $2x \equiv 4 \mod 13$ soit $x \equiv 2 \mod 13$.

On écrit alors $x = 2 + 13k$ et on est donc ramené à résoudre $206 + 13.103k \equiv 105 \mod 13^2$ soit $13.103k \equiv -13.8 \mod 13^2$ soit en simplifiant par 13, $103k \equiv -8 \mod 13$, soit $2k \equiv -8 \mod 4$ et donc $k \equiv -4 \mod 13$ et donc finalement $x \equiv 2 - 4.13 \mod 13^2$.

6.12 (a) D'après le lemme chinois, on a $(\mathbb{Z}/pq\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ de sorte que ce dernier est de cardinal $(p-1)(q-1)$. Les éléments x égaux à leur inverse sont ceux qui vérifient $x^2 = 1$, i.e. ce sont ceux d'ordre divisant 2, ce qui donne 4 éléments à savoir $(\pm 1, \pm 1)$ soit $x = \pm 1, x_1, x_2$ avec $x_i \equiv (-1)^i \mod p$ et $x_i \equiv (-1)^{i-1} \mod q$, pour $i = 1, 2$.

(b) On considère alors le produit de tous les éléments de $(\mathbb{Z}/pq\mathbb{Z})^\times$ soit le produit des $pq-1$ premiers entiers auxquels il faut enlever tous les multiples de p ainsi que tous les multiples de q. Les multiples de p (resp. q) sont $p, 2p, \cdots, (q-1)p$ (resp. $q, 2q, \cdots, (p-1)q$), de sorte que le produit en question est $\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}}$. Par ailleurs en regroupant les nombres distincts de $\pm 1, x_1, x_2$ avec leur inverse ce produit est égal à $a = 1(-1)x_1x_2$. Or par le lemme chinois, on a $a \equiv 1 \mod p$ et $a \equiv 1 \mod q$ de sorte que $a \equiv 1 \mod pq$, d'où le résultat.

6.13 On a $1035125 \equiv 12 \mod 17$. On pourrait maintenant calculer l'ordre de 12 dans $\mathbb{Z}/17\mathbb{Z}$. D'après le petit théorème de Fermat on a $12^16 \equiv 1 \mod 17$. Or $5642 \equiv 10 \mod 16$; la réponse est alors 12^10 modulo 17. Or $12 \equiv -5 \mod 17$ et $12^2 \equiv 8 \mod 17$ soit $12^4 \equiv -4$ soit $12^8 \equiv -1$ de sorte que l'ordre de 12 est 16. Finalement $12^10 = 12^8 12^2 = -12^2 = -8 = 9 \mod 17$.

6.14 On a $1823 \equiv 5 \mod 18$; or $5 \in (\mathbb{Z}/18\mathbb{Z})^\times$ on peut donc utiliser le petit théorème de Fermat avec $\varphi(18) = \varphi(2)\varphi(9) = 1.6 = 4$ soit $5^6 \equiv 1 \mod 18$. Or on a $242 \equiv 2 \mod 6$ soit $1823^{242} \equiv 5^2 = 7 \mod 18$. De même $2222 \equiv 2 \mod 20$ avec $2 \notin (\mathbb{Z}/20\mathbb{Z})^\times$; on ne peut donc pas utiliser le petit théorème de Fermat (2^8 est pair et ne peut donc pas être congru à 1 modulo 20). On étudie alors la suite $u_n = 2^n$ modulo 20 pour $n \in \mathbb{Z}$: $u_0 = 1$, $u_1 = 2$, $u_2 = 4$, $u_3 = 8$, $u_4 = -4$, $u_5 = -8$, $u_6 = 4$. On remarque qu'à partir de $n \geq 2$ la suite est périodique de période 4 : $u_{n+4} = u_n$. Or $321 \equiv 1 \mod 4$ de sorte que $u_{321} = u_5 = -8$ et donc $2222^{321} \equiv -8 \mod 20$.

La bonne façon de comprendre le phénomène est d'utiliser le lemme chinois. On a $2222 \equiv 2 \mod 4$ de sorte que $2222^n \equiv 0 \mod 4$ dès que $n \geq 2$. On a aussi $2222 \equiv 2 \mod 5$ et $321 \equiv 1 \mod 4$ et donc d'après le petit théorème de Fermat $2222^{321} \equiv 2 \mod 5$ et donc $2222^{321} \equiv 12 \mod 20$.

Remarque : On comprend ainsi que de manière générale la suite $u_n = a^n \mod m$ pour a non premier avec m est périodique à partir d'un certain rang (le temps que pour les premiers p divisant $a \wedge m$, $a^k \equiv 0 \mod m$ soit $k\alpha_a(p) \geq \alpha_m(p)$ où $\alpha_a(p)$ (resp. $\alpha_m(p)$) est la multiplicité de p dans a (resp. dans m)). Une autre façon de le remarquer et de dire qu'elle ne prend qu'un nombre fini de valeurs de sorte qu'il existe n_0 et $n_0 + r$ tels que $u_{n_0} = u_{n_0+r}$ ce qui implique que $u_{n_0+r+k} = u_{n_0+k}$ et donc la périodicité de u_n à partir d'un certain rang.

6.15 On a $42 = 2.3.7$, il suffit alors de verifier la congruence modulo 2, 3 et 7. Pour 2 et 3, on a clairement $n^7 \equiv n$ et pour 7 le résultat découle du petit théorème de Fermat.

6.16 On rappelle que p étant premier, $(\mathbb{Z}/p\mathbb{Z}, +, *)$ est un corps. Ainsi dans $\mathbb{Z}/p\mathbb{Z}$, on a $\bar{a}^2 + \bar{b}^2 = 0$ soit $(\bar{a}/\bar{b})^2 = -1$, car $\bar{b} \neq 0$. Ainsi -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$: $-1 = x^2$, soit $x^4 = 1$. Or d'après le petit théorème de Fermat, on a $x^{p-1} = 1$, soit $4|p-1$ car 4 est l'ordre de x dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

6.17 On a $42 = 2.3.7$, il suffit alors de verifier la congruence modulo 2, 3 et 7. Pour 2 et 3, on a clairement $n^7 \equiv n$ et pour 7 le résultat découle du petit théorème de Fermat.

6.18 Le nombre Σ est une somme de $x_{i_1}^{a_{i_1}} \cdots x_{i_k}^{a_{i_k}}$, les i_r étant distincts deux à deux et $\sum_{r=1}^{k} a_{i_r} = p-1$; pour que ce terme apparaisse il faut que I contienne les k indices $i_1, \cdots, i_k$ ce qui arrive dans $\binom{p-k}{2p-1-k}$ cas de sorte que le nombre de fois où le terme précédent apparait dans Σ est divisible par ce coefficient binomial lequel est divisible par p : en effet il est égal à $\frac{(2p-1-k)\cdots p}{(p-k)!}$ et comme p est premier p ne divise pas $(p-k)!$ pour tout $1 \leq k \leq p$.

Par ailleurs si aucun des S_I n'était divisible par p alors d'après le petit théorème de Fermat, on aurait $S_I^{p-1} \equiv 1 \mod p$ et donc $\Sigma \equiv \binom{p}{p-1} \not\equiv 0 \mod p$.

Le cas n quelconque s'en déduit immédiatement en remarquant que si le résultat est vrai pour n et m, il l'est pour mn.

6.19 (i) Comme $1+p+\cdots+p^{p-1} \equiv 1 \mod 2$, ses facteurs premiers sont tous impairs ; en outre comme il est congru à $1+p \mod p^2$, il possède au moins un diviseur premier non congru à 1 modulo p^2.

(ii) Raisonnons par l'absurde : soit n tel que $n^p \equiv p \mod q$; on a alors $n^{p^2} \equiv p^p \equiv 1 \mod q$ car $p^p - 1 = (p-1)(1+p+\cdots+p^{p-1}$. Comme q est un nombre premier ne divisant pas n, il est premier avec n et donc d'après le petit théorème de Fermat, on a $n^{q-1} \equiv 1 \mod q$. On en déduit donc, d'après le théorème de Bezout, que $n^{(q-1)\wedge p^2} \equiv 1 \mod q$ et comme ce pgcd est égal à 1 ou p, le cas p^2 étant exclu par le fait que $q \not\equiv 1 \mod p^2$, on a $n^p \equiv 1 \mod q$. Ainsi comme $n^p \equiv p \mod q$, on a $p \equiv 1 \mod q$ et donc $1+p+\cdots+p^{p-1} \equiv p \mod q$ et donc q divise aussi p soit $q = p$ ce qui ne se peut pas car $q | p^p - 1$.

6.20 Il suffit de trouver les n premiers, on obtiendra alors les n généraux en prenant des produits finis de tels premiers. Remarquons déjà que comme $2+3+6-1 \equiv 0 \mod 2$, le premier 2 ne convient pas. De même comme $2^2+3^2+6^2-1 \equiv 0 \mod 3$ alors 3 non plus. Soit alors $p \geq 5$; d'après le petit théorème de Fermat on a

$$6(2^{p-2}+3^{p-2}+6^{p-2}-1) = 32^{p-1}+23^{p-1}+6^{p-1}-6 \equiv 0 \mod p$$

et comme $p \wedge 6 = 1$, on a $2^{p-2}+3^{p-2}+6^{p-2}-1 \equiv 0 \mod p$ et donc p ne convient pas non plus. Finalement 1 est le seul entier qui convient.

6.21 Considérons un pgcd δ de (x^2-9) et (x^2-16) ; celui-ci divise $(x^2-9)-(x^2-16) = 7$, soit $\delta = 1, 7$.

Supposons $\delta = 1$: d'après loc. cit., on en déduit que $x^2-9 = \epsilon t^2$ et $x^2-9 = \epsilon s^2$ avec $\epsilon = \pm 1$ et $t, s \geq 0$ premiers entre eux. On obtient alors $7 = \epsilon(t^2-s^2) = \epsilon(t-s)(t+s)$ d'où $t+s = 7$ et $t-s = \epsilon$. Si $\epsilon = 1$, on a $t = 4$ et $s = 3$ ce qui donne $x = \pm 5$ et $y = \pm 12$. Si $\epsilon = -1$ alors $t = 3$ et $s = 4$ ce qui donne $x = 0$ et $y = \pm 12$.
Remarque : Il nous faut bien sûr vérifier à chaque fois que les solutions obtenues conviennent, car on a simplement raisonné par implication.

Supposons $\delta = 7$: $x^2-9 = 7u$, $x^2-16 = 7v$ et $y^2 = 7^2uv$ avec u et v premiers entre eux. On a alors $uv = (y/7)^2$ de sorte que $u = \epsilon t^2$ et $v = \epsilon s^2$ avec $\epsilon = \pm 1$ et $s, t \geq 0$ premiers entre eux. On trouve alors les solutions $x = \pm 3, 4$ et $y = 0$, qui conviennent.

6.22 (i) Si x est pair, on a $y^2 \equiv -1 \mod 8$. En écrivant y impair sous la forme $2k+1$, on obtient $y^2 = 1+4k(k+1) \equiv 1 \mod 8$ contradiction.

(ii) On a $x^3+8 = (x+2)(x^2-2x+4)$ avec x impair de la forme $2k+1$; $(x^2-2x+4) = 4k^2+3$. On en déduit donc qu'il existe un p premier divisant x^2-2x+4 avec $p \equiv 3 \mod 4$. Or si p premier divise y^2+1 alors $p \equiv 1 \mod 4$, d'où la contradiction.

6.23 Il s'agit donc de déterminer n et m tels que $2008^n \equiv 2008^m \mod 1000$ avec $1000 = 2^3 5^3$ ce qui d'après le théorème chinois est équivalent aux congruences

$$2008^n \equiv 2008^m \mod 8 \qquad 2008^n \equiv 2008^m \mod 5^3.$$

Comme $2008 \equiv 0 \mod 8$, la première congruence est toujours valable, tandis que comme $2008 \equiv 8 \mod 5^3$, la deuxième s'écrit $8^{n-m} \equiv 1 \mod 5^3$. Calculons alors l'ordre de 8 dans $(\mathbb{Z}/5^3\mathbb{Z})^\times$ qui est un diviseur de $\varphi(125) = 100$. Or modulo 5, on a $8^{50} \equiv (-1)^{25} \equiv -1 \mod 5$ de sorte que cet ordre n'est pas un diviseur de 50.

6.24 Modulo3, on a $x^3 \equiv x \mod 3$ de sorte que l'équation donne $x + y \equiv 2 \mod 3$. On est donc dans l'une des situations suivantes :

- $x \equiv y \equiv 1 \mod 3$ de sorte que modulo 9, on a $x^3 - 3xy^2 + y^3 \equiv 1 - 3 + 1 \equiv -1 \mod 9$ alors que $2891 \equiv 2 \mod 9$;
- $x \equiv 0 \mod 3$ et $y \equiv 2 \mod 3$ de sorte que $x^3 - 3xy^2 + y^3 \equiv 0 - 0 - 1 \mod 9$ ce qui est absurde ;
- $x \equiv 2 \mod 3$ et $y \equiv 0 \mod 3$ et donc $x^3 - 3xy^2 + y^3 \equiv -1 - 0 + 0 \mod 9$ ce qui est encore absurde.

6.25 Essayons de factoriser $P(x) = (x+1)^7 - x^7 - 1$ en regardant ses racines : on remarque qu'outre 0 et 1, le nombre complexe $j = e^{2i\pi/3}$ est aussi racine car $j + 1 = -j^2$ de sorte que $P(x)$ est divisible par $x(x+1)(x^2+x+1)$ le quotient étant égal à $x^2 + x + 1$ et donc

$$(a+b)^7 - a^7 - b^7 = 7ab(a+b)(a^2+ab+b^2)^2.$$

On est ainsi amené à résoudre $a^2 + ab + b^2 \equiv 0 \mod 7^3$ qui s'écrit encore

$$(a + \frac{b}{2})^2 \equiv -3(\frac{b}{2})^2 \mod 7^3$$

laquelle possède des solutions si et seulement si le symbole de Legendre $(\frac{-3}{7^3}) = 1$ ce que l'on vérifie aisément en utilisant la loi de réciprocité quadratique.

Références

[1] S. Francinou and Gianella H. *Exercices de mathématiques pour l'agrégation algèbre 1*. Masson, 1994.

[2] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, 1980.

[3] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. Springer-Verlag, 1982.

[4] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. Springer-Verlag, 1982.

[5] D. Perrin. *Cours d'algèbre*. Ellipses, 1998.

[6] P. Samuel. *Théorie algébrique des nombres*. Hermann, 1967.

[7] J.-P. Serre. *Cours d'arithmétique*. Puf, 1970.

[8] N.P. Smart. *The algorithmic resolution of diophantine equations*, volume 41. London Mathematical Society Student Texts, 1998.