Pourquoi y a-t-il beaucoup de nombres premiers de la forme n^2+n+41 ?

Daniel Perrin

1 Introduction

1.1 Pourquoi les nombres premiers ?

Il fut un temps où s'intéresser aux nombres premiers pouvait passer pour un passe-temps futile. Depuis 1977 et l'invention du code RSA, ils ont pris une place de choix en cryptographie et la quête de grands nombres premiers ne relève plus seulement de *l'honneur de l'esprit humain*, comme aurait dit Jacobi (voir 8.1), mais peut plus prosaïquement poursuivre un but lucratif. Bref, on peut répondre à la question : pourquoi les nombres premiers ? *parce que c'est utile.*

En ce qui me concerne, n'étant que moyennement intéressé par les sous, je répondrai plutôt : *parce que j'aime ça !* En effet, les nombres premiers ont toujours été pour moi un sujet fascinant. Ceux qui déjeunent avec moi savent que je factorise chaque jour de tête le total (en centimes) de mon ticket de cantine ainsi que mon numéro de transaction, ce qui peut ne pas être immédiat, voir les exemples ci-dessous.

Pour que les choses soient claires, je rappelle toutefois que je ne suis

nullement un spécialiste de ce domaine et qu'il ne faut pas s'attendre ici à des nouveautés. D'ailleurs, en ce domaine, les conjectures sont nombreuses, mais les théorèmes sont rares [1], comme on le verra.

1.2 Le Graal des primophiles

C'est une question très ancienne (et ramenée au premier plan avec l'utilisation des nombres premiers en cryptographie) que de détenir un procédé de fabrication de nombres premiers, ou mieux, une formule donnant à coup sûr des nombres premiers. On peut faire remonter ce souci à Euclide qui montre l'existence d'une infinité de nombres premiers (en utilisant [2] un facteur premier de $p_1 \cdots p_r + 1$).

On sait que Fermat pensait avoir trouvé une telle formule avec les $2^{2^n}+1$. Voilà ce qu'il dit :

Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme 3, 5, 17, 257, 65537, 4 294 967 297 et le suivant de 20 lettres 18 446 744 073 709 551 617; etc. Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurois peine à me dédire.

Hélas, Euler a montré que 641 divise $2^{32}+1$, ruinant cet espoir, voir par exemple [18].

Le même Euler, en 1772, dans un commentaire sur un mémoire [3] de Jean Bernoulli, remarque que les nombres n^2-n+41 sont premiers pour $0 \leq n < 40$. Voir *Nouveaux mémoires de l'Académie royale des sciences de Berlin*, p. 36, 1772 (ou p. 381, 1774). Voilà ce que dit Euler :

Cette progression $41, 43, 47, 53, 61, 71, 83, 97, 113, 131$ *etc. dont le terme général est* $41 - x + xx$ *est d'autant plus remarquable que les* 40 *premiers termes sont tous des nombres premiers.*

1.1 *Remarque.* Dans ce qui suit on utilisera plutôt les n^2+n+41, qui sont les mêmes avec un décalage de un : $n^2-n+41 = (n-1)^2+(n-1)+41$. Si on pose $f(n) = n^2+n+41$ et $g(n) = n^2-n+41$, la série des nombres premiers peut s'écrire sous la forme $f(n)$ pour $n = 0, 1, \ldots, 39$ ou $g(n)$ pour $n = 1, \ldots, 40$ (on note que $g(0) = g(1) = f(-1) = f(0) = 41$).

1. Car il y a beaucoup d'appelés, mais peu d'élus *(Matthieu, 22.14)*.

2. Une autre preuve, voisine, consiste à regarder les facteurs premiers de $n!+1$. On peut d'ailleurs se demander si ce nombre est lui-même premier. C'est rarement le cas (pour $n \leq 100$, seuls $n = 1, 2, 3, 11, 27, 37, 41, 73$ et 77 donnent $n!+1$ premier).

3. Voir Annexe 8.2.1.

C'est un résultat remarquable, surtout si on le présente ainsi [4] : on part de 41, il est premier, on ajoute 2, on trouve 43, il est premier, on ajoute 4, on trouve 47, il est premier, on ajoute 6, on trouve 53, il est premier, on ajoute 8, on trouve 61, il est premier, on ajoute 10, on trouve 71, il est premier, on ajoute 12, on trouve 83, il est premier, on ajoute 14, on trouve 97, il est premier, on ajoute 16, on trouve 113, il est premier. On peut continuer ainsi, en ajoutant chaque fois le nombre pair suivant, jusque 1601, avec des nombres premiers à chaque pas. En hommage à Euler, on appellera ici **eulériens** les nombres premiers de la forme $n^2 + n + 41$.

1.2 *Remarque.* Il est clair que, pour $n = 41$, $n^2 + n + 41$ n'est pas premier (c'est 41×43), de même pour n multiple de 41. Pour $n = 40$ il ne l'est pas non plus : $40^2 + 40 + 41 = 40 \times 41 + 41 = 41^2$.

1.3 *Remarque.* Une question non évidente est de repérer, parmi les nombres premiers, ceux de la forme $n^2 + n + 41$. Si l'on retranche 41, il faut diagnostiquer un $n(n + 1)$. Deux remarques :

1) Si N est de la forme $n^2 + n$ on a $n = [\sqrt{N}]$ et il n'y a plus qu'à vérifier.

2) Un entier de la forme $n^2 + n + 41$ se termine par $1, 3, 7$ en base 10 mais pas par 9 (car $n^2 + n$ se termine par $0, 2, 6$). Plus précisément, on constate qu'il y a à peu près le même nombre de premiers se terminant par $1, 3$ et deux fois moins par 7. Par exemple, pour $n \leq 10^6$: on obtient 104240 nombres premiers $n^2 + n + 41$ se terminant par 1, 104681 par 3 et 52160 par 7. C'est normal car parmi les produits $n(n+1)$ modulo 10 pour $n = 0, \ldots, 9$ on trouve 4 fois 0 ou 2 et 2 fois 6.

1.3 La spirale d'Ulam

Stanisław Ulam (1909-1984) est un mathématicien américain d'origine juive polonaise. Il est connu pour avoir contribué à développer la théorie qui permit la construction de la bombe à hydrogène (la structure dite de Teller-Ulam), mais aussi pour la fameuse spirale [5] d'Ulam qui concerne les nombres premiers. L'histoire de cette spirale est la suivante. Un jour, Ulam se trouva coincé, contraint d'écouter "un exposé très long et très ennuyeux" selon ses propres mots. Il passa son temps à gribouiller des entiers consécutifs, commençant par 1 au centre, dans une espèce de spirale. Il obtint une grille régulière de nombres dont il entoura tous les nombres premiers. À sa grande surprise, les nombres entourés tendaient à s'aligner le long de lignes diagonales, voir Figure 1.

4. C'est la même chose car on a $(n + 1)^2 + (n + 1) + 41 = n^2 + n + 41 + (2n + 2)$.
5. Elle apparut sur la couverture de Scientific American en mars 1964.

En fait, voir Figure 2 et Annexe 8.2.5, ce phénomène correspond à l'existence de constantes entières b et c telles que la fonction $f(n) = n^2 + bn + c$ engendre un grand nombre de nombres premiers.

Si on dessine la spirale de Ulam à partir de $a = 41$, les termes de la diagonale principale sont les n^2+n+41, alternativement à droite et à gauche. On constate, avec émerveillement, que tous ces nombres sont premiers pour n variant de 0 à 39. Il y a donc 40 termes premiers de suite sur cette diagonale. La Figure 3 en montre quelques-uns.

362	363	364	365	366	**367**	368	369	370	371	372	**373**	374	375	376	377	378	**379**	380	381
361	290	291	292	**293**	294	295	296	297	298	299	300	301	302	303	304	305	306	**307**	382
360	289	226	**227**	228	**229**	230	231	232	**233**	234	235	236	237	238	**239**	240	**241**	308	**383**
359	288	225	170	171	172	**173**	174	175	176	177	178	**179**	180	**181**	182	183	242	309	384
358	287	224	169	122	123	124	125	126	**127**	128	129	130	**131**	132	133	184	243	310	385
357	286	**223**	168	121	82	**83**	84	85	86	87	88	**89**	90	91	134	185	244	**311**	386
356	285	222	**167**	120	81	50	51	52	**53**	54	55	56	57	92	135	186	245	312	387
355	284	221	166	119	80	49	26	27	28	**29**	30	**31**	58	93	136	187	246	**313**	388
354	**283**	220	165	118	**79**	48	25	10	**11**	12	**13**	32	**59**	94	**137**	188	247	314	**389**
353	282	219	164	117	78	**47**	24	9	**2**	**3**	14	33	60	95	138	189	248	315	390
352	**281**	218	**163**	116	77	46	**23**	8	1	4	15	34	**61**	96	**139**	190	249	316	391
351	280	217	162	115	76	45	22	**7**	6	**5**	16	35	62	**97**	140	**191**	250	**317**	392
350	279	216	161	114	75	44	21	20	**19**	18	**17**	36	63	98	141	192	**251**	318	393
349	278	215	160	**113**	74	**43**	42	**41**	40	39	38	**37**	64	99	142	**193**	252	319	394
348	**277**	214	159	112	**73**	72	**71**	70	69	68	**67**	66	65	100	143	194	253	320	395
347	276	213	158	111	110	**109**	108	**107**	106	105	104	**103**	102	**101**	144	195	254	321	396
346	275	212	**157**	156	155	154	153	152	**151**	150	**149**	148	147	146	145	196	255	322	**397**
345	274	**211**	210	209	208	207	206	205	204	203	202	201	200	**199**	198	**197**	256	323	398
344	273	272	**271**	270	**269**	268	267	266	265	264	**263**	262	261	260	259	258	**257**	324	399
343	342	341	340	339	338	**337**	336	335	334	333	332	**331**	330	329	328	327	326	325	400

FIGURE 1 – La spirale d'Ulam

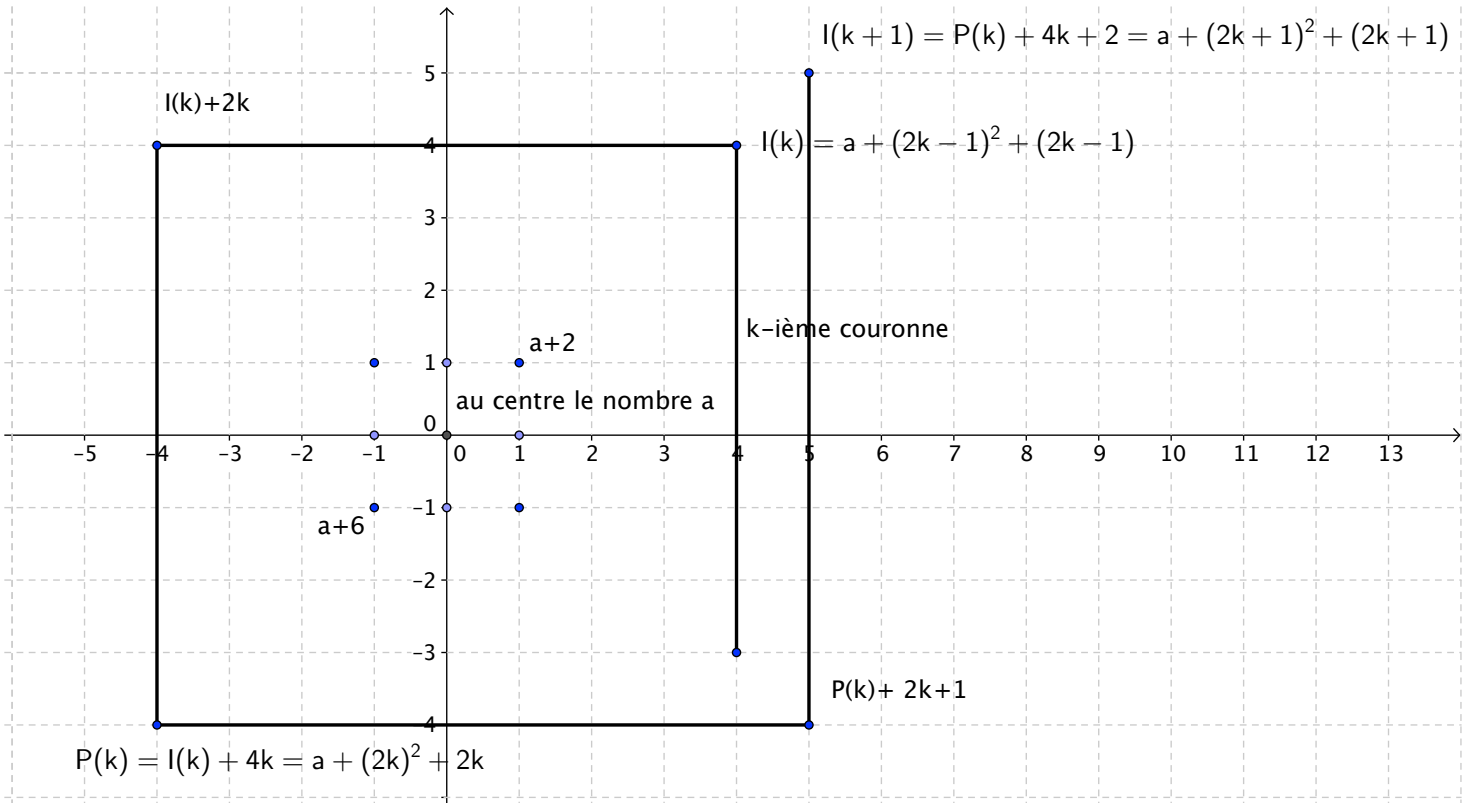

FIGURE 2 – La spirale d'Ulam centrée en a

6													224	223
7	185	184	183	182	181	180	179	178	177	176	175	174	173	222
8	186	141	140	139	138	137	136	135	134	133	132	131	172	221
9	187	142	105	104	103	102	101	100	99	98	97	130	171	220
10	188	143	106	77	76	75	74	73	72	71	96	129	170	219
11	189	144	107	78	57	56	55	54	53	70	95	128	169	218
12	190	145	108	79	58	45	44	43	52	69	94	127	168	217
13	191	146	109	80	59	46	41	42	51	68	93	126	167	216
14	192	147	110	81	60	47	48	49	50	67	92	125	166	215
15	193	148	111	82	61	62	63	64	65	66	91	123	165	214
16	194	149	112	83	84	85	86	87	88	89	90	123	164	213
17	195	150	113	114	115	116	117	118	119	120	121	122	163	212
18	196	151	152	153	154	155	156	157	158	159	160	161	162	211
19	197	198	199	200	201	202	203	204	205	206	207	208	209	210
20														

FIGURE 3 – Quelques-uns des nombres $n^2 + n + 41$

1.4 Les polynômes $F(n)$ et les nombres premiers

Notons déjà qu'il est vain de chercher une formule du genre $F(n)$, où F est un polynôme, donnant à coup sûr un nombre premier pour n entier :

1.4 Proposition. *Soit $F(X) = a_r X^r + \cdots + a_1 X + a_0$ un polynôme à coefficients dans $\mathbf{Z}$ avec $r > 0$. Alors, il existe une infinité de $n \in \mathbf{N}$ tel que $F(n)$ soit composé.*

Démonstration. Il existe $a \in \mathbf{N}$ tel que $F(a) \neq 0, 1, -1$ (sinon, l'un des polynômes $F(X)$, $F(X) - 1$, $F(X) + 1$ aurait une infinité de racines). Soit alors p un facteur premier de $F(a)$. Pour $k \in \mathbf{N}$ on a $F(a + kp) \equiv F(a) \equiv 0 \pmod{p}$ et, comme $F(a + kp)$ tend vers l'infini (en valeur absolue) quand k tend vers l'infini, il est $> p$ pour k assez grand, et multiple de p, donc composé.

1.5 La conjecture de Bunyakovsky

Une question plus raisonnable est de savoir si un tel polynôme $F(n)$ en une variable peut donner une infinité de nombres premiers. C'est le cœur de ce texte. Il y a sur ce thème une conjecture très générale (Bunyakovsky 1857) qui dit que si $F(X)$ est un polynôme à coefficients entiers, il y a une infinité de n tels que $F(n)$ est premier, pourvu que le contraire ne soit pas évident. Précisément, si l'on a :

$$F(X) = a_r X^r + a_{r-1} X^{r-1} + \cdots + a_1 X + a_0, \quad \text{avec } a_i \in \mathbf{Z} \text{ et } a_r > 0,$$

il y a une infinité de $n \in \mathbf{N}$ pour lesquels $F(n)$ est premier, pourvu que les conditions suivantes soient réalisées :

• *Le polynôme est irréductible sur $\mathbf{Z}$.*

Cette condition est nécessaire. En effet, considérons par exemple le polynôme $X^2 - 8X + 15$. Il admet deux racines entières $x = 3$ et $x = 5$ et on a donc $F(n) = (n - 3)(n - 5)$. Cela montre que ce nombre ne peut jamais être premier, même au signe près, sauf si l'un des facteurs vaut ± 1. Cela ne se produit que pour $n = 2, 4$ ou 6 et seuls $n = 2$ ou 6 donnent le nombre premier 3.

• *Les $F(n)$, pour n variant dans $\mathbf{N}$, sont premiers entre eux (cela implique que les coefficients de F sont premiers entre eux).*

Cette condition est nécessaire comme le montre l'exemple de $F(n) = n^2 + n + 2$, ou $n^2 + n + 40$, qui est toujours pair ! Pour avoir la condition il suffit de détenir m, n tels que $F(m)$ et $F(n)$ soient premiers entre eux, par exemple deux nombres premiers distincts [6].

6. Ce qui est bien le moins si l'on souhaite en avoir une infinité.

1.5 *Remarque.* En fait, à l'heure actuelle, la conjecture de Bunyakovsky est prouvée pour les polynômes de degré 1 (c'est le théorème de Dirichlet, voir paragraphe suivant), mais pour aucun autre degré ! Pire, on ne sait même pas s'il y a au moins un (seul) nombre premier. Par exemple, avec $F(n) = n^{12} + 488669$, il n'y a pas de valeur première avant $n = 616980$.

1.6 Le théorème de Dirichlet

Il s'agit du résultat suivant, dû à Johann Peter Gustav Lejeune-Dirichlet [7] (1805-1859), appelé encore théorème de la progression arithmétique :

1.6 Théorème. *Soient a, b deux entiers positifs premiers entre eux. Il existe une infinité de nombres premiers de la forme $an+b$, pour $n \in \mathbf{N}$, c'est-à-dire de nombres premiers congrus à b modulo a.*

La démonstration utilise les séries L et n'est pas élémentaire, voir par exemple Serre *Cours d'arithmétique* Ch. VI. On trouvera en Annexe 7.1 quelques cas particuliers faciles. En voici un :

1.7 Proposition. *Il y a une infinité de nombres premiers de la forme $10n+1$, autrement dit dont l'écriture décimale se termine par 1.*

Démonstration. Dire que p se termine par 1 c'est dire que 10 divise $p-1$. Si l'on se souvient du petit théorème de Fermat, on sait que l'on a, modulo p, $x^{p-1} \equiv 1$ pourvu que x soit premier à p. Ce théorème est évident si l'on pense en termes de groupes : si p est premier, l'anneau $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est un corps et son groupe multiplicatif $\mathbf{F}_p^*$ est d'ordre $p-1$, de sorte que l'ordre de x est un diviseur de $p-1$, ce qui donne Fermat. Pour être sûr que 10 divise $p-1$, il suffit donc de trouver un élément qui vérifie $x^{10} \equiv 1 \pmod{p}$ (et qui soit vraiment d'ordre 10). C'est une question de polynômes. En effet, on a :

$$X^{10}-1 = (X^5-1)(X^5+1) = (X-1)(X^4+X^3+X^2+X+1)(X+1)(X^4-X^3+X^2-X+1)$$

de sorte que les éléments qui sont vraiment d'ordre 10 vérifient :

$$\Phi_{10}(x) := x^4 - x^3 + x^2 - x + 1 \equiv 0 \pmod{p}.$$

Précisément, on a le lemme suivant :

1.8 Lemme. *Soit $n \in \mathbf{N}$, $n \geq 2$ et p un diviseur premier de $\Phi_{10}(n)$. Alors, p est congru à 1 modulo 10, sauf peut-être si $p = 5$ et si $n \equiv -1 \pmod{5}$.*

7. Mathématicien allemand d'origine belge (du village de Richellette près de Liège, d'où son nom De Richellette, devenu Dirichlet).

Démonstration. On note déjà que p est impair. Dans $\mathbf{F}_p$ on a $n^5 = -1$, donc $n^{10} = 1$, de sorte que n est d'ordre un diviseur de 10, donc $1, 2, 5$ ou 10. Comme p n'est pas égal à 2, l'ordre ne peut être ni 1, ni 5 (on aurait $n^5 = 1 = -1$). Si c'est 2, on a $n = -1$ et p divise 5 donc est égal à 5, c'est le cas d'exception. Sinon, l'ordre est 10 et donc 10 divise $p - 1$.

Pour trouver des nombres premiers se terminant par 1, il suffit de prendre des diviseurs de $\Phi_{10}(n)$ (avec n non congru à -1 modulo 5). Par exemple, avec $n = 2, 3, 6$ on obtient 11, 61, 521, etc.

Pour avoir de tels nombres premiers arbitrairement grands, on regarde $N = \Phi_{10}(n!) = (n!)^4 - (n!)^3 + (n!)^2 - n! + 1$ avec $n \geq 5$. Si p est un diviseur premier de N, il est $> n$ et, comme $n!$ est multiple de 5, p ne l'est pas, donc il se termine par 1.

1.9 *Remarque.* En fait, si n est congru à -1 modulo 5, il y a le facteur 5, mais seulement à l'ordre 1, car $\Phi_{10}(n)$ est congru à 5 modulo 25. Il y a donc toujours des facteurs premiers de la forme $10n + 1$ (car $\Phi_{10}(n)$ n'est jamais égal à 5). Par exemple, on a $\Phi_{10}(4) = 5 \times 41$.

2 Le nombres de la forme $n^2 + n + 41$ pour n petit

Le résultat suivant est celui annoncé par Euler. On peut évidemment le vérifier entier par entier, mais c'est fastidieux et pas très instructif. On va en donner une autre preuve, qui permet de mieux comprendre le phénomène et fournit des idées pour étudier les grands nombres de cette forme.

2.1 Théorème. *Les entiers de la forme $n^2 + n + 41$ sont premiers pour $0 \leq n \leq 39$.*

2.1 Introduire l'anneau

En arithmétique, il est souvent intéressant d'écrire les nombres sous forme de produits [8], témoin l'exemple de $n^2-8n+15$ qui se factorise en $(n-3)(n-5)$, ce qui montre qu'il ne peut donc jamais (ou presque) être premier.

Pour voir si $n^2 + n + 41$ est premier ou non, on peut essayer de faire la même chose, donc de factoriser cette expression. Bien sûr, le polynôme $x^2 + x + 41$ n'a pas de racines réelles, mais il en a dans les complexes :

8. Par exemple, pour chercher les triplets d'entiers dits pythagoriciens, qui vérifient $x^2 + y^2 = z^2$, on a intérêt à écrire $x^2 = z^2 - y^2 = (z - y)(z + y)$.

$\frac{-1 \pm i\sqrt{163}}{2}$ ce qui donne la factorisation :

$$n^2 + n + 41 = \big(n + \frac{1}{2} + \frac{i\sqrt{163}}{2}\big)\big(n + \frac{1}{2} - \frac{i\sqrt{163}}{2}\big) = (n + \alpha)(n + \overline{\alpha})$$

où l'on a posé $\alpha = \dfrac{1 + i\sqrt{163}}{2}$. On voit qu'on est naturellement amené à travailler dans l'anneau $A := \mathbf{Z}[\alpha]$ (les combinaisons linéaires à coefficients entiers de 1 et α ; on note en effet qu'on a $\overline{\alpha} = 1 - \alpha$).

2.2 *Remarque.* L'anneau $\mathbf{Z}[\alpha]$ est ce qu'on appelle l'anneau des entiers du corps $\mathbf{Q}(i\sqrt{163})$. Lorsqu'on connaît un peu la théorie des anneaux d'entiers des corps quadratiques imaginaires $\mathbf{Q}(i\sqrt{d})$, on sait que pour $d \equiv -1 \pmod 4$, l'anneau naturel $\mathbf{Z}[i\sqrt{d}]$ n'est pas le bon (il n'est pas intégralement clos) et qu'il faut le remplacer par l'anneau $A_d = \mathbf{Z}[\alpha_d]$ avec $\alpha_d = \dfrac{1 + i\sqrt{d}}{2}$ comme ci-dessus, voir [28] ou [19].

2.2 L'argument de divisibilité

Nous allons maintenant donner une "démonstration" du théorème 2.1. Dans un premier temps, elle sera très discutable, mais elle s'affinera au fur et à mesure.

Supposons que $f(n) = n^2 + n + 41$ n'est pas premier. En vertu du crible d'Ératosthène, il admet donc un diviseur premier $p < \sqrt{f(n)}$). Pour $n < 40$, on a $p^2 < n^2 + n + 41 < 40^2 + 40 + 41 = 41^2$, donc $p < 41$.

L'idée est de travailler dans $\mathbf{Z}[\alpha]$, sans crainte, comme auraient fait les mathématiciens du début du XIX-ième siècle. La factorisation ci-dessus montre que p divise $(n + \alpha)(n + \overline{\alpha})$ dans cet anneau. Ah, mais **si p est encore premier** dans cet anneau, et **si on a toujours le lemme d'Euclide**, cela montre que p divise $n + \alpha$ ou $n + \overline{\alpha}$ dans $\mathbf{Z}[\alpha]$. Mais cela signifie par exemple qu'on a $n + \alpha = p(a + b\alpha)$, avec a, b entiers. En identifiant les coefficients de α (car 1 et α sont linéairement indépendants sur $\mathbf{R}$), on a $1 = pb$ et c'est impossible puisque p est premier.

2.3 Irréductible ?

La preuve précédente est très séduisante, mais repose sur deux points discutables : p est-il encore premier dans A et le lemme d'Euclide y est-il encore valable ? Rappelons d'abord la définition suivante, qui généralise celle de nombre premier ordinaire :

2.3 Définition. *Soit A un anneau intègre et z un élément non inversible de A. On dit que z est* **irréductible** *dans A si la relation $z = wt$ avec $w, t \in A$ implique w ou t inversible dans A.*

Dans le cas contraire, z est dit **réductible**.

Pour comprendre ces notions, il faut dire un mot de la norme, l'arme absolue dans l'anneau $\mathbf{Z}[\alpha]$.

2.3.1 La norme

Pour $z = a + b\alpha$ avec $a, b \in \mathbf{Z}$ on définit la **norme** de z par la formule :

$$N(z) = z\overline{z} = (a + \frac{b}{2})^2 + \frac{163\, b^2}{4} = a^2 + ab + 41b^2$$

(tiens, tiens[9] !). On voit que $N(z)$ est un entier ≥ 0 et que la norme est multiplicative : $N(zw) = (z\overline{z})(w\overline{w}) = (zw)\overline{(zw)} = N(z)N(w)$. La norme d'un $z \in \mathbf{Z}$ est simplement son carré et sinon, si b est non nul, on a $N(z) \geq \frac{163}{4} = 40{,}75$ donc $N(z) \geq 41$.

2.4 *Remarques.* 1) En particulier, $n^2 + n + 41$ est la norme de $n + \alpha$.

2) Un entier de la forme $n = a^2 + 163b^2$ avec $a, b \in \mathbf{N}$ est une norme : $n = (a-b)^2 + 2b(a-b) + 41 \times 4b^2$, mais la réciproque est inexacte, voir 7.22.

2.3.2 Applications

L'usage de la norme montre immédiatement deux choses :

1) Un nombre z est inversible si et seulement si il est de norme 1, et cela impose $z = \pm 1$. En effet, si $N(z) = z\overline{z} = 1$, il est clair que z est inversible. Inversement, si $zw = 1$ on a $N(z)N(w) = 1$ ce qui dans les entiers positifs, n'est possible que si $N(z) = N(w) = 1$. Cela impose que z est dans $\mathbf{Z}$, puis qu'il vaut ± 1.

2) Un nombre premier p de $\mathbf{N}$ est réductible dans A si et seulement si c'est une norme. En effet, si on a $p = zw$, avec $z, w \in \mathbf{Z}[\alpha]$, non inversibles, donc de normes > 1, cela donne $N(p) = p^2 = N(z)N(w)$, donc $p = N(z) = N(w)$ est une norme.

En conséquence, si p est < 41, comme ce n'est pas une norme, il reste irréductible[10] dans A : notre première hypothèse est vérifiée.

9. Attention, les normes (qui sont de la forme $x^2 + xy + 41y^2$ avec $x, y \in \mathbf{Z}$) ne sont pas toutes de la forme $n^2 + n + 41$, voir 7.24.

10. On peut montrer plus généralement que les irréductibles de A sont les p premiers de $\mathbf{Z}$ qui ne sont pas des normes et les $z \in A$ dont la norme est un entier premier.

2.4 Le lemme d'Euclide ?

2.4.1 Euclide et factoriel

Ce lemme affirme que si p est irréductible et s'il divise un produit, il divise l'un des facteurs. Dans un anneau quelconque, seuls les irréductibles qui vérifient cette propriété méritent le nom de **premiers**.

Depuis Euclide, on sait que c'est ce lemme qui assure **l'unicité** de la décomposition en facteurs premiers dans $\mathbf{Z}$ et en fait donc un anneau factoriel. Parlons un instant de factorialité, c'est-à-dire de l'existence d'une décomposition unique en produit d'irréductibles. Contrairement à ce que l'on pourrait penser, l'existence de la décomposition est le plus souvent triviale. C'est le cas ici grâce à la norme (si $z = wt$ on $N(z) = N(w)N(t)$ et si w, t ne sont pas inversibles, la norme décroît, de sorte que le processus s'arrête au bout d'un nombre fini d'opérations).

En revanche, le point crucial est le lemme d'Euclide[11]. En fait, vu le lemme suivant il est très proche de notre condition :

2.5 Lemme. *Soit p un nombre premier de $\mathbf{Z}$ qui reste irréductible dans A (c'est-à-dire qui n'est pas une norme). Les propriétés suivantes sont équivalentes :*

1) Si p divise un produit zw avec $z, w \in A$, p divise z ou w.

2) Si p divise une norme $N(z)$, avec $z \in A$, il divise z.

Si l'anneau A vérifie cette propriété, il est factoriel.

Démonstration. Le sens 1) $\Longrightarrow$ 2) est immédiat. Pour l'autre, si p divise zw, on a $zw = pt$, donc $p^2N(t) = N(z)N(w)$ dans $\mathbf{Z}$, donc p, qui divise $N(z)N(w)$, divise l'un d'eux, disons $N(z)$, donc il divise z.

La factorialité de l'anneau s'ensuit facilement, voir par exemple [19], mais pour prouver notre théorème nous n'aurons pas besoin de ce fait, il suffira de montrer que la propriété 2) est vraie.

2.4.2 Diviser une norme ?

Cette condition a une traduction très simple :

11. Dans les anneaux de nombres, il n'est que très rarement vérifié. Par exemple dans $\mathbf{Z}[i\sqrt{5}]$, on a la décomposition en irréductibles $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ mais 2 et 3 ne divisent pas les facteurs du second membre. Pour les $d \equiv 3 \pmod 4$, l'anneau des entiers n'est factoriel que pour $d = 3, 7, 11, 19, 43, 67$ et 163, ce qui donne des séries de nombres premiers de la forme $n^2 + n + \frac{d+1}{4}$, avec $\frac{d+1}{4} = 1$, 2, 3, 5, 11, 17 ou 41, voir 7.27. Cette difficulté est l'une des premières à laquelle ont été confrontés les arithméticiens du XVIII-ième et du XIX-ième siècle, Euler, Lagrange, Gauss, Dirichlet et surtout Kümmer qui inventa les "nombres idéaux" pour la surmonter.

2.6 Lemme. *Un nombre premier p de $\mathbf{Z}$ divise une norme $N(z)$ pour $z \in A$ sans diviser z si et seulement si p est impair et si -163 est un carré modulo p. Cette condition est encore équivalente au fait que p est un carré modulo* 163.

Démonstration. Supposons que p divise $N(x + \alpha y) = x^2 + xy + 41y^2$. S'il divise y, il divise aussi x donc z. Sinon, on peut diviser par y modulo p et le polynôme $x^2 + x + 41$ a une racine modulo p. On voit déjà que p est $\neq 2$ (le polynôme $x^2 + x + 1$ n'a pas de racine modulo 2). On peut alors calculer modulo p comme on le fait dans $\mathbf{R}$ et le polynôme a des racines si et seulement si son discriminant -163 est un carré modulo p.

Passer de -163 est un carré modulo p à p est un carré modulo 163 est une conséquence de la loi de réciprocité quadratique, voir 7.14. Pour une tentative de justification de cette loi, voir 7.2.

2.7 Corollaire. *Si l'un des nombres premiers $2, 3, 5, 7$ divise une norme $N(z)$, il divise z. Ces nombres sont donc non seulement irréductibles, mais premiers dans A.*

Démonstration. Pour 2 on l'a déjà vu. Pour les autres, il s'agit de vérifier que -163 n'est pas un carré modulo p. Mais c'est clair car on a $-163 \equiv -1 \pmod 3$, $-163 \equiv 2 \pmod 5$ et $-163 \equiv -2 \pmod 7$.

2.8 *Remarque.* On peut continuer jusqu'à $p = 37$, par exemple $-163 \equiv 2 \pmod{11}$, $-163 \equiv 6 \pmod{13}$ (mais à partir de là on a vraiment intérêt à utiliser la réciprocité quadratique). En fait, on n'en a pas besoin car les nombres $2, 3, 5, 7$ nous suffisent.

2.4.3 Factoriel ?

Le théorème suivant permet d'achever de montrer que tous les n^2+n+41 pour $0 \leq n \leq 39$ sont premiers :

2.9 Théorème. *L'anneau A vérifie la propriété 2) de 2.5 (donc est factoriel).*

Démonstration. Il reste à traiter le cas des $p > 7$. On suppose que p divise une norme, donc qu'il existe $K \in \mathbf{N}^*$ tel que Kp est une norme. On montre alors, en utilisant le théorème de Minkowski ou le principe des tiroirs (voir [19]) ou l'algorithme de Cornacchia, (voir 7.3 ci-dessous), qu'il existe k avec $k \leq \sqrt{\frac{163}{3}}$ ou $k \leq \frac{2}{\pi}\sqrt{163}$ ou $k \leq \frac{2\sqrt{41}+1}{\sqrt{2}}$ (donc $k \leq 7$ ou $k \leq 8$ ou $k \leq 10$) tel que kp soit une norme $N(z)$.

On en déduit que p est une norme. En effet, on choisit k le plus petit possible, on en prend un facteur premier q, qui est ≤ 7, il est premier dans A,

donc il divise z ou $\overline{z}$ donc z. Posons $k = qk'$. Si $z = qw$, on a $qk'p = q^2N(w)$, donc $k'p = qN(w)$. Comme q est premier avec p, il divise k' et on a $k' = qk''$, donc $k''p = N(w)$, contredisant la minimalité de k.

Cela achève de prouver le théorème 2.1. En voici une variante :

2.10 Proposition. *Soit n un entier pair compris entre 0 et 38. Alors, $n^2 + 163$ est premier.*

Démonstration. Sinon, il a un diviseur premier p (impair puisque n est pair) qui est < 41 (car $41^2 = 1681 > 38^2 + 163 = 1607$). Ce n'est donc pas une norme de A_d, donc il est premier. Mais alors, p divise $(n + i\sqrt{163})(n - i\sqrt{163}) = (n - 1 + 2\alpha)(n + 1 - 2\alpha)$ avec $\alpha = \dfrac{1 + i\sqrt{163}}{2}$, donc il divise l'un des facteurs et c'est impossible car p devrait diviser 2, or p est impair.

2.4.4 Une conséquence

La factorialité de l'anneau permet de raffiner le lemme 2.6 :

2.11 Corollaire. *Un nombre premier p de* **N est** *une norme de A_d si et seulement si c'est un carré modulo* 163.

Cela montre, par Dirichlet, qu'il y a une infinité de nombres premiers qui sont des normes, un sur deux, en fait. À défaut de prouver l'infinitude des premiers de la forme $n^2 + n + 41$, cela montre le résultat analogue avec un polynôme à deux variables :

2.12 Corollaire. *Il y a une infinité de nombres premiers de la forme $x^2 + xy + 41y^2$ avec $x, y \in \mathbf{N}$.*

En fait, ce résultat vaut pour tout polynôme homogène de degré 2 dont les coefficients sont premiers entre eux, voir 8.5.

3 Les nombres de la forme n^2+n+41, n grand

3.1 La constatation expérimentale

Non seulement les nombres de la forme $n^2 + n + 41$ sont tous premiers pour $n \leq 39$, mais, au-delà, la proportion de nombres premiers parmi ces nombres est très grande. On peut s'en convaincre en faisant l'expérience avec un logiciel de calcul, par exemple *xcas*. Il suffit d'écrire quelques lignes de programme [12], voir Annexe 9.3.

12. Avec Pari, comme me l'a indiqué Bill Allombert, il n'y a pas même besoin de programme, la commande $sum(n = 0, 10^6, isprime(n^2 + n + d))$ donne la réponse.

Voici quelques chiffres pour $n \leq 10^6$:

• Il y a 54110 nombres premiers de la forme n^2+1 pour $n \leq 10^6$ (soit 5% environ).

Bien entendu, les polynômes de la forme $n^2 + a$ ont un gros défaut : ils prennent des valeurs paires une fois sur deux. Essayons donc avec n^2+n+a avec a impair qui ne donne que des nombres impairs. On constate que le résultat est très variable.

• Il y a 88118 nombres premiers de la forme n^2+n+1 pour $0 \leq n \leq 10^6$ (soit 9% environ)

• Il y a 105797 nombres premiers de la forme n^2+n+37 pour $0 \leq n \leq 10^6$ (soit 10% environ)

• Il y a 164220 nombres premiers de la forme n^2+n+17 pour $0 \leq n \leq 10^6$ (soit 16% environ)

• Il y a 261081 nombres premiers de la forme n^2+n+41 pour $0 \leq n \leq 10^6$ (soit 26% environ) !!!

• Mais il y a seulement 25897 nombres premiers de la forme n^2+n+33 pour $0 \leq n \leq 10^6$ (soit 2,6% environ).

Il est utile de compléter la définition vue ci-dessus :

3.1 Proposition-Définition. *On appelle* **eulériens** *les nombres premiers de la forme $f(n) = n^2+n+41$ et $\mathcal{E}$ leur ensemble.*

On appelle $\mathcal{A}$ l'ensemble des $n \in \mathbf{N}$ tels que $f(n)$ soit premier. L'application f est une bijection de $\mathcal{A}$ sur l'ensemble $\mathcal{E}$ des nombres premiers eulériens.

Bien entendu, la conjecture principale c'est que $\mathcal{E}$ ou $\mathcal{A}$ est infini.

3.2 Ératosthène

Le crible d'Ératosthène assure que $f(n)$ est premier si aucun nombre premier $p \leq \sqrt{f(n)}$ ne divise $f(n)$. Or on a le lemme suivant :

3.2 Lemme. *Si $n > 40$ on a $n < \sqrt{f(n)} < n+1$.*

Démonstration. Si $n > 40$, on a $n^2 < f(n) = n^2+n+41 < n^2+n+n+1 = (n+1)^2$.

Comme les $f(n)$ sont tous premiers pour $n < 40$ et que $f(40)$ et $f(41)$ ne le sont pas, le corollaire suivant complète l'examen de tous les cas :

3.3 Corollaire. *Pour $n \geq 41$, le nombre $f(n)$ est premier si et seulement si il n'est multiple d'aucun nombre premier $p \leq n$.*

3.3 Caractérisation des nombres premiers réductibles

Prenons donc un $p \leq n$. À quelle condition p divise-t-il n^2+n+41 ? Cela signifie que n est une racine du polynôme $f(X) = X^2 + X + 41$ modulo p. Or, le discriminant Δ de f vaut -163. Pour que ce polynôme admette des racines modulo p, il faut donc (et il suffit) que -163 soit un carré modulo p. La proposition suivante a déjà été prouvée plus haut :

3.4 Proposition. *Soit $p \in \mathbf{N}$ un nombre premier impair. Les conditions suivantes sont équivalentes :*

1) L'équation $x^2 + x + 41 = 0$ admet une solution modulo p (ou encore, p **divise** *un nombre de la forme $n^2 + n + 41$),*

2) -163 est un carré modulo p,

3) p est un carré modulo 163,

4) p est une norme de A_{163} c'est-à-dire de la forme $a^2 + ab + 41b^2$ avec $a, b \in \mathbf{N}$,

5) p est réductible dans A_{163}.

On désignera simplement un tel nombre premier sous le nom de **réductible**, *sous-entendu dans l'anneau des entiers de $\mathbf{Q}(i\sqrt{163})$.*

3.5 Corollaire. *Soit n un entier naturel et p un nombre premier.*

1) Si p est égal à 2 ou si p est impair et irréductible, p ne divise pas $f(n) = n^2 + n + 41$.

2) Si p est réductible $\neq 163$, on note u et v les racines du polynôme $f(X) = X^2 + X + 41$ modulo p. Alors p divise $f(n)$ si et seulement si n est congru modulo p à u ou v.

3) Le nombre $p = 163$ divise $f(n)$ si et seulement si n est congru à 81, unique racine de f modulo 163.

3.4 Description ensembliste

Le corollaire précédent incite à introduire les ensembles suivants [13] :

3.6 Définition. *Soit p un nombre premier. On pose $\mathcal{A}(p) = \{n \in \mathbf{N} \mid p$ ne divise pas $f(n)\}$ et $\mathcal{A}^*(p) = \{n \in \mathbf{N} \mid p$ ne divise pas $f(n)$* ou *$p = f(n)\}$. Pour $R \in \mathbf{N}$ on pose $\mathcal{A}(p, R) = \mathcal{A}(p) \cap [0, R]$ et de même pour $\mathcal{A}^*(p, R)$.*

3.7 *Remarque.* Si p est irréductible on a $\mathcal{A}(p) = \mathbf{N}$. Si p est réductible distinct de 163 et si u, v sont les racines de $x^2 + x + 41$ modulo p, $\mathcal{A}(p)$ est formé des n qui ne sont congrus ni à u ni à v modulo p. Dans ce cas, p n'est pas

13. Pour comprendre l'intérêt des ensembles $\mathcal{A}^*$, voir 3.12.

nécessairement eulérien, mais s'il l'est, il existe un unique $n_0 \in \mathbf{N}$ tel que $f(n_0) = p$ (l'autre racine est négative) et l'ensemble $\mathcal{A}^*(p)$ contient $\mathcal{A}(p)$ et n_0. Par exemple, pour $n = 151$ on a $n_0 = 10$ et les éléments de $\mathcal{A}(p)$ sont les n qui ne sont congrus ni à 10 ni à -11 modulo 151, $\mathcal{A}^*(p)$ contenant 10 en plus. Si $p = 163$, $\mathcal{A}(p)$ est formé des n non congrus à 81 modulo 163 et on a $\mathcal{A}(p) = \mathcal{A}^*(p)$.

3.5 Calcul des probabilités

On renvoie à l'Annexe 1 (section 6) pour les rappels sur les probabilités. Rappelons que, si R est un entier, on note $\mathbf{P}_R$ la probabilité naturelle sur l'ensemble $[0, R] \cap \mathbf{N}$. Si A est une partie de cet ensemble on a donc $\mathbf{P}_R(A) = \dfrac{|A|}{R+1}$. Si A est une partie de $\mathbf{N}$ et A_R sa trace sur $[0, R]$, on définit alors $\mathbf{P}(A)$ comme la limite (si elle existe) de $\mathbf{P}_R(A_R)$ quand R tend vers l'infini. L'application $\mathbf{P}$ se prolonge en une application définie sur toutes les parties de $\mathbf{N}$ et appelée **probabilité naturelle** sur $\mathbf{N}$ (elle est additive mais non σ-additive, voir 6.6).

3.8 Proposition. *Soit p un nombre premier. On a $\mathbf{P}(\mathcal{A}(p)) = 1$ si p n'est pas réductible, $\mathbf{P}(\mathcal{A}(p)) = 1 - \dfrac{2}{p}$ si p est réductible distinct de 163 et $\mathbf{P}(\mathcal{A}(p)) = 1 - \dfrac{1}{p}$ si $p = 163$. Les probabilités des $\mathcal{A}^*(p)$ sont les mêmes. En posant $\mathcal{A}(p, R) = \mathcal{A}(p) \cap [0, R]$, on obtient :*

$$\mathbf{P}(A(p)) = \lim_{R \to +\infty} \frac{|\mathcal{A}(p, R)|}{R+1}.$$

Démonstration. Si p est réductible distinct de 163, on a $\mathcal{A}(p) = \mathbf{N} - (C_{p,u} \cup C_{p,v})$ où $C_{p,u}$ désigne l'ensemble des $n \equiv u \pmod p$. On en déduit $\mathbf{P}(\mathcal{A}(p)) = 1 - \frac{2}{p}$ en vertu de 6.9. La formule avec la limite résulte de la définition de la probabilité naturelle.

Comme $\mathcal{A}^*(p)$ s'obtient en ajoutant au plus un élément à $\mathcal{A}(p)$, sa densité naturelle est la même.

On sait aussi calculer la probabilité de l'intersection des $\mathcal{A}(p)$:

3.9 Corollaire. *Soit N un entier ≥ 163. On a la formule : $\mathbf{P}\big(\bigcap_{p \leq N} \mathcal{A}(p)\big) = \prod_{p \leq N} \mathbf{P}(\mathcal{A}(p)) = \dfrac{162}{163} \prod_p (1 - \dfrac{2}{p})$ où le dernier produit est étendu aux nombres*

premiers $p \leq N$ réductibles distincts de 163 *et on a :*

$$\lim_{R\to+\infty} \frac{\left|\bigcap_{p\leq N} \mathcal{A}(p,R)\right|}{R+1} = \frac{162}{163} \prod_p (1-\frac{2}{p}).$$

Démonstration. C'est exactement 6.14.

3.6 Minorer la probabilité des eulériens

3.10 Définition. *Soit $N \in \mathbf{N}$. On pose $\mathcal{A}_N = \mathcal{A} \cap [0,N]$, ensemble des $n \leq N$ tels que $f(n)$ soit premier*[14] *et $P(N) = |\mathcal{A}_N|$.*

3.11 Lemme. *Soit $N \in \mathbf{N}$, $N \geq 41$. On a la formule :*

$$\mathcal{A}_N = \bigcap_{p\leq N} \mathcal{A}^*(p,N) \supset \bigcap_{p\leq N} \mathcal{A}(p,N).$$

On a $\mathbf{P}_N(\mathcal{A}_N) = \mathbf{P}_N(\bigcap_{p\leq N} \mathcal{A}^*(p,N)) \geq \mathbf{P}_N(\bigcap_{p\leq N} \mathcal{A}(p,N))$ et :

$$(*) \qquad P(N) \geq (N+1)\ \mathbf{P}_N(\bigcap_{p\leq N} \mathcal{A}(p,N)).$$

Démonstration. Soit $n \in \mathcal{A}_N$, de sorte que $q = f(n)$ est premier. Soit p premier, $p \leq N$. Si n n'est pas dans $\mathcal{A}(p,N)$ c'est que p divise $f(n)$, donc qu'on a $p = q$. Mais alors, n est bien dans $\mathcal{A}^*(p,N)$.

Inversement, soit n dans l'intersection. Notons d'abord qu'on a $n \neq 40$. En effet, on a $f(40) = 41^2$, de sorte que 40 n'est pas dans $\mathcal{A}^*(41,N)$. Si $n > 40$, cela signifie ou bien que $f(n) = p$ est premier, ou bien que pour tout $p \leq N$, donc *a fortiori* pour tout $p \leq n$, donc pour tout $p \leq \sqrt{f(n)}$, p ne divise pas $f(n)$, donc encore que $f(n)$ est premier et n est dans $\mathcal{A}_N$. Si n est ≤ 39, on sait que $f(n)$ est premier, donc n est dans $\mathcal{A}_N$.

La dernière formule de probabilité est claire avec la note ci-dessous.

3.12 *Remarques.* 1) En fait, la formule ci-dessus est vraie pour tout $N \neq 40$.

2) Attention, $\mathcal{A}_N$ n'est pas l'intersection des $\mathcal{A}(p,N)$ pour $n \leq N$. En effet, on a $0 \in \mathcal{A}_N$ pour tout $N \geq 0$ mais, comme $N \geq 41$, 0 n'est pas dans $\mathcal{A}(41,N)$ mais dans $\mathcal{A}^*(41,N)$.

14. On a donc $\mathbf{P}_N(\mathcal{A}_N) = \dfrac{P(N)}{N+1}$.

3.6.1 Ça se gâte ...

À partir de là, il y a une série de difficultés.

• Pour minorer $\mathbf{P}_N(\mathcal{A}_N)$ à l'aide de la formule $(*)$ on a envie de dire que la probabilité de l'intersection des $\mathcal{A}(p,N)$ est le produit des probabilités de chaque terme : $\mathbf{P}_N(\bigcap_{p\leq N}\mathcal{A}(p,N)) = \prod_{p\leq N}\mathbf{P}(\mathcal{A}(p,N))$. C'est bien entendu une question d'indépendance des événements considérés.

• Comme on l'a vu en 3.9, si l'on regarde les probabilités sur $\mathbf{N}$ tout entier, les événements "p ne divise pas n" pour $p \leq N$ sont indépendants et on a bien $\mathbf{P}\big(\bigcap_{p\leq N}\mathcal{A}(p)\big) = \prod_{p\leq N}\mathbf{P}(\mathcal{A}(p))$. La situation semble donc favorable.

• Mais la difficulté est la suivante. Il est bien vrai que $\mathbf{P}(\mathcal{A}(p))$ est la limite de $\mathbf{P}_N(\mathcal{A}(p,N))$ quand N tend vers l'infini, mais dans l'expression $\prod_{p\leq N}\mathbf{P}(\mathcal{A}(p,N))$ on veut garder fixe le N qui est en indice du produit, mais faire tendre vers l'infini celui de $\mathbf{P}(\mathcal{A}(p,N))$, cruel dilemme !

3.6.2 La conjecture pour n^2+n+41

Si l'on saute résolument par-dessus les obstacles vus ci-dessus, on peut proposer, en vertu de 3.9 :

3.13 Conjecture. *On a :* $P(N) \sim N \times \dfrac{162}{163} \times \prod_p (1-\dfrac{2}{p}) := N\theta(N)$, *le produit étant étendu aux nombres premiers réductibles* $p \leq N$, $p \neq 163$.

3.14 *Remarque.* Voir en 9.4 ci-dessous le programme $den(N,d)$ sous *xcas*. Pour $N = 10^6$ et $d = 163$ on trouve $P(N) = 269872$ au lieu de 261081 en réalité ce qui n'est pas si mal ! Pour une discussion sur cette conjecture, voir les paragraphes suivants.

3.7 Pour comprendre la difficulté : l'exemple $N = 100$

Pour comprendre les difficultés vues ci-dessus, examinons un exemple. On reviendra sur cette question, dans un cas plus simple, au §6.6.

On cherche à déterminer le nombre d'entiers vérifiant $0 \leq n \leq 100$ tels que $f(n)$ soit premier, à le comparer avec celui annoncé par la conjecture et à comprendre l'écart entre les deux. Un calcul direct montre que, pour $0 \leq n \leq 100$, les n tels que $f(n)$ n'est pas premier sont $40, 41, 44, 49, 56, 65, 76, 81, 82, 84, 87, 89, 91, 96$ (il y a 14 nombres en tout). On a donc $P(100) = 87$.

Ensuite, on détermine les nombres premiers $p \leq 100$ qui sont réductibles. On sait qu'il n'y en a aucun en dessous de 37 et ensuite, ce sont les nombres

eulériens $p_1, \ldots, p_8$: 41, 43, 47, 53, 61, 71, 83 et 97. La valeur conjecturée pour $P(100)$ est alors $101 \times \prod_{i=1}^{8}(1 - \frac{2}{p_i}) \simeq 75.82$. On voit donc un écart [15] important avec la valeur réelle qui est 87.

Les congruences à éviter par rapport aux nombres premiers réductibles sont très simples. Il s'agit de 0 et -1 pour $p = 41$, 1 et -2 pour $p = 43$, 2 et -3 pour $p = 47$, 3 et -4 pour $p = 53$, 4 et -5 pour $p = 61$, 5 et -6 pour $p = 71$, 6 et -7 pour $p = 83$ et enfin [16], 7 et -8 pour $p = 97$. Les nombres $n \leq 100$ qui correspondent à ces congruences sont les quatorze nombres repérés ci-dessus. On notera en effet que certains d'entre eux (41, 44, 49, 56, 65, 76 et 89) apparaissent pour deux congruences, par exemple 49 est congru à la fois à 2 modulo 47 et à -4 modulo 53.

Si l'on regarde, pour l'un des nombres premiers p réductibles, la probabilité qu'il ne divise pas $f(n)$ pour $n \leq 100$, cette probabilité est voisine de la valeur espérée $1 - 2/p$. Par exemple, pour $p = 47$, il y a quatre nombres n à écarter : 44, 49, 91 et 96, ce qui donne $4/101 \simeq 0.039$ tandis que $1 - 2/47 \simeq 0.042$. La raison est que la tranche de nombres entre 0 et 100 contient deux tranches de longueur 47 et donc que le calcul de probabilités n'est erroné qu'à cause d'effets de bords minimes.

En revanche, lorsqu'on s'intéresse à la congruence modulo **tous** les nombres premiers réductibles $p_1 = 41, \ldots, p_8 = 97$, le calcul de probabilité, qui provient d'un dénombrement de classes de congruences par le lemme chinois (si $P := p_1 \cdots p_8$, on a $\mathbf{Z}/P\mathbf{Z} = \mathbf{Z}/p_1\mathbf{Z} \times \cdots \times \mathbf{Z}/p_8\mathbf{Z}$) ne serait valable que sur une plage de longueur minimale égale à $P = 153131328472673 \sim 1,5 \times 10^{14}$. Or, on voudrait appliquer ce calcul sur un échantillon de 100 individus. Sachant que $1,5 \times 10^{14}$ c'est plus de 10000 fois la population de la terre, se contenter d'un sondage sur 100 personnes c'est prendre le risque de se Tromper ! Pour comprendre le problème en termes de crible, voir 6.28.

3.15 *Remarque.* En réalité, la situation n'est pas aussi catastrophique. En effet, si l'on reprend l'exemple des nombres premiers $p_i \leq 100$ réductibles, la proportion de $n \leq N$ tels que n ne soit pas congru aux mauvais chiffres modulo tous ces nombres premiers est très proche de la probabilité théorique, même pour des N beaucoup plus petits que le produit $P = p_1 \cdots p_8$ qui est de l'ordre de 10^{14}. En effet, la probabilité théorique (c'est-à-dire le produit des $(p-2)/2$) vaut $0,750718$ et la proportion réelle vaut $0,782$ pour $N = 100$, $0,75$ pour $N = 1000$, $0,750742$ pour $N = 100000$. En réalité, il n'y

15. Ici, la valeur conjecturée est plus petite, mais pour $N \geq 24000$ c'est le contraire.

16. Cette remarquable régularité des valeurs à éviter n'a rien de mystérieux. Si $p = f(n)$ est premier, on a $f(n) = f(-n-1) = n^2 + n + 41 = p$, de sorte que n et $-n-1$ sont les racines de f modulo p.

a pas vraiment d'aléatoire dans cette situation, seulement une incapacité à dénombrer précisément des ensembles de congruences, qui semblent plus réguliers qu'on ne l'attendrait.

3.8 La conjecture générale pour $x^2 + bx + c$

Dans la même veine que 3.13, on peut proposer la conjecture suivante :

3.16 Conjecture. *Soit $f(x) = x^2 + bx + c$ un polynôme irréductible à coefficients entiers et posons $b^2 - 4c := -d$. Soit $P(N)$ le nombre d'entiers $n \leq N$ tels que $f(n)$ soit premier. On a $P(N) \sim \epsilon N \prod_p (1 - \frac{1}{p}) \prod_p (1 - \frac{2}{p}) := N\theta(N)$ où ϵ vaut 0 si b est impair et c pair, $\frac{1}{2}$ si b est pair et 1 si b et c sont impairs, où le premier produit est indexé par les facteurs premiers de d et où le second est étendu aux nombres premiers impairs $\leq N$ tels que $-d$ soit un carré non nul modulo p.*

3.9 L'infinitude à partir de la conjecture

3.17 Théorème. *Si l'on admet la conjecture 3.13 (resp. 3.16), il y a une infinité de nombres premiers de la forme $n^2 + n + 41$ (resp. de la forme $n^2 + bn + c$ sauf dans le cas b impair et c pair).*

Démonstration. Il suffit de montrer que $P(N)$ tend vers l'infini avec N, ou encore que $\ln P(N)$ tend vers l'infini. Or, on a :

$$\ln P(N) \sim \ln N + \sum_p \ln(1 - \frac{2}{p}) + C,$$

où C est une constante et où la somme est étendue aux nombres premiers réductibles $\leq N$. Notons une inégalité sur les logarithmes :

3.18 Lemme. *Soit x compris entre 0 et 1/2. On a $-\frac{3}{2}x \leq \ln(1-x) \leq -x$.*

Démonstration. L'inégalité de droite est bien connue. Pour l'autre, on pose $f(x) = \ln(1-x) + \frac{3}{2}x$. On a $f'(x) = -\frac{1}{1-x} + \frac{3}{2} = \frac{1-3x}{2(1-x)}$. On voit que f admet un maximum pour $x = 1/3$ et qu'elle est positive sur $[0, \frac{1}{2}]$.

On déduit de ce lemme la minoration $\sum_p \ln(1 - \frac{2}{p}) \geq -3 \sum_p \frac{1}{p}$, la deuxième somme étant étendue aux nombres premiers réductibles compris entre 5 et N. Cette somme est plus petite que la somme de tous les inverses des nombres premiers $\leq N$ et on conclut avec le résultat suivant (car alors l'équivalent de $\ln P(N)$ est $\geq (1 - 3k) \ln N + C$) :

3.19 Lemme. *Posons* $S_N = \sum_{p \leq N} \frac{1}{p}$, *la somme étant étendue à tous les nombres premiers* $\leq N$. *Alors, il existe* $k < \frac{1}{3}$ *tel que l'on ait, pour* N *assez grand,* $S_N \leq k \ln N$.

Démonstration. Voir 7.31 pour une preuve élémentaire. On peut prendre $k = \frac{2}{7}$ en vertu de 7.33.

3.20 *Remarque.* Bien entendu, la majoration donnée par le lemme est très grossière. En effet, le théorème des nombres premiers donne l'équivalent $S_N \sim \ln(\ln N)$, et le théorème de Mertens donne une majoration du même type, voir 7.30.

3.10 La conjecture de Hardy-Littlewood

3.10.1 La conjecture et ses variantes

Il s'agit d'une conjecture célèbre proposée en 1923 par Hardy et Littlewood [17] :

3.21 Conjecture. (Hardy-Littlewood, 1) *Soit* $f(x) = x^2 + bx + c$ *un polynôme irréductible à coefficients entiers. Soit* N *un entier et* $P(N)$ *le nombre de nombres premiers parmi les* $f(n)$, $1 \leq n \leq N$.

Alors, on a $P(N) \sim \frac{C}{2} \int_2^N \frac{dt}{\ln t} \sim \frac{C}{2} \frac{N}{\ln N}$ *où* C *est le produit, indexé par les nombres premiers :* $C = \prod_p \frac{1 - \frac{N(p)}{p}}{1 - \frac{1}{p}}$ *dans lequel* $N(p)$ *est le nombre de solutions de la congruence* $f(n) \equiv 0 \pmod{p}$.

3.22 *Remarque.* Attention, la convergence du produit vers C n'est pas évidente (elle n'est pas absolue). On n'oubliera pas qu'en vertu de Mertens, le produit $\prod_p \frac{p}{p-1}$ diverge. Cela rend difficile le calcul de la constante C. Pour $d = 163$, on a [18] :

$$C/2 = 3.319773177471421665323556857649887966468554585653...$$

3.23 *Remarques.* On pose $-d = b^2 - 4c$ (discriminant de f).

1) Le terme relatif à $p = 2$ dans C vaut 0 si b est impair et c pair, 1 si b est pair et 2 si b et c sont impairs.

17. Reprise par Bateman et Horn dans le cas d'un polynôme de degré quelconque ou de plusieurs polynômes.

18. Voir le papier d'Henri Cohen [5]. Attention, Cohen commet une erreur d'un facteur 2 dans son calcul.

2) Le terme $\dfrac{1-\frac{N(p)}{p}}{1-\frac{1}{p}}$ relatif à p impair dans C vaut $1-\dfrac{\left(\frac{-d}{p}\right)}{p-1}$. En particulier, si p divise d, il est égal à 1.

3) Si d est premier et congru à 3 modulo 4, la loi de réciprocité quadratique permet de remplacer $\left(\frac{-d}{p}\right)$ par $\left(\frac{p}{d}\right)$ dans l'expression précédente, voir aussi 7.15 pour le cas d non premier.

Avec ces remarques, on peut reformuler la conjecture, dans le cas qui nous intéresse :

3.24 Conjecture. (Hardy-Littlewood, 2) *Soit $f(x)=x^2+bx+c$ un polynôme irréductible à coefficients entiers et posons $b^2-4c:=-d$. Soit N un entier et $P(N)$ le nombre de nombres premiers parmi les $f(n)$, $1\leq n\leq N$.*

Alors, on a $P(N)\sim \epsilon\, C\displaystyle\int_2^N \frac{dt}{\ln t}\sim \epsilon C\frac{N}{\ln N}$ où ϵ vaut 0 si b est impair et c pair, $\frac{1}{2}$ si b est pair et 1 si b et c sont impairs et où C est le produit de deux quantités

$$C_1=\prod_{non}\frac{p}{p-1}\quad\text{et}\quad C_2=\prod_{oui}\frac{p-2}{p-1}$$

les produits étant indexés par les nombres premiers p impairs, l'indice oui (resp. non) signifiant que $-d$ est un carré non nul modulo p (resp. n'est pas un carré modulo p).

Si d est premier et congru à 3 modulo 4, le fait que $-d$ est un carré modulo p est équivalent au fait que p est un carré modulo d. Si d est premier et congru à 1 modulo 4, la condition signifie que p est un carré (resp. un non carré) s'il est congru à 1 (resp. 3) modulo 4.

3.10.2 Résultats numériques

Dans le cas $d=163$, on a vu que le coefficient $C/2$ vaut environ 3.319773. Si l'on note $P(N)$ le nombre de $n\leq N$ tels que $f(n)$ soit premier et $HL(N)$ la valeur de ce nombre selon la conjecture de Hardy-Littlewood avec le logarithme intégral [19], on a les résultats suivants : $N=10^6$, $P(N)=261081$, $HL(N)=261022$, $N=10^8$, $P(N)=19132653$, $HL(N)=19129223$, $N=10^9$, $P(N)=168806741$, $HL(N)=168807913$. La précision de la conjecture est tout bonnement extraordinaire !

19. Les valeurs du logarithme intégral, ainsi que les deux dernières valeurs de $P(N)$, sont calculées avec le logiciel *Pari*. On a $\mathrm{Li}\,(10^6)=78626.5$, $\mathrm{Li}\,(10^8)=5762208.3$, $\mathrm{Li}\,(10^9)=50849233.9$.

3.10.3 Le lien avec la conjecture 3.16

Pour faire le lien avec la conjecture proposée ci-dessus, on peut donner une variante en écrivant C comme une limite :

3.25 Conjecture. (Hardy-Littlewood, 3) *Soit $f(x) = x^2 + bx + c$ un polynôme irréductible à coefficients entiers et posons $b^2 - 4c := -d$. Soit N un entier et $P(N)$ le nombre de nombres premiers parmi les $f(n)$, $1 \leq n \leq N$.*

Alors, on a $P(N) \sim \epsilon\, C_N \displaystyle\int_2^N \frac{dt}{\ln t} \sim \epsilon\, C_N \frac{N}{\ln N}$ où ϵ vaut 0 si b est impair et c pair, $\frac{1}{2}$ si b est pair et 1 si b et c sont impairs et où C_N est le produit de deux quantités $C_{1,N} = \displaystyle\prod_p \frac{p}{p-1}$ indexée par les nombres premiers p tels que $3 \leq p \leq N$ et que $-d$ n'est pas un carré modulo p et $C_{2,N} = \displaystyle\prod_p \frac{p-2}{p-1}$ indexée par les nombres premiers p tels que $3 \leq p \leq N$ et que $-d$ est un carré non nul modulo p. On note $P(N) \sim N\psi(N)$.

Le lien avec la conjecture 3.13 est le suivant :

3.26 Proposition. *Soit $N \in \mathbf{N}$. On a la formule $\psi(N) \sim \dfrac{e^\gamma}{2} \displaystyle\prod_{p|d} \frac{p}{p-1}\, \theta(N)$.*

Démonstration. Le terme $C_{2,N}$ de Hardy-Littlewood peut s'écrire $\displaystyle\prod_{oui} \frac{p}{p-1} \times \prod_{oui} \frac{p-2}{p}$ (l'indice *oui* signifie que $-d$ est un carré non nul modulo p) et le second terme est celui qui apparaît dans $\theta(N)$. On voit que HL devient :

$$\psi(N) = \frac{1}{\ln N} \times \prod_p \frac{p}{p-1} \times \theta(N)$$

où le produit porte sur tous les nombres premiers ≥ 3 qui ne divisent pas d. Par Mertens, on en déduit la formule annoncée.

On voit que la conjecture de Hardy-Littlewood n'est autre que la correction par **??** de 3.13 c'est-à-dire la multiplication par $e^\gamma/2 \simeq 0,89$.

3.10.4 La justification heuristique de la conjecture

J'expose ici cette heuristique selon Bateman et Horn, voir [1]. Le théorème des nombres premiers permet d'affirmer que la probabilité qu'un nombre $n \leq N$ soit premier est $\dfrac{1}{\ln N}$. On en déduit que la probabilité $\mathbf{P}$ que $f(n)$

soit premier pour $n \leq N$ doit être $\frac{1}{\ln f(N)} \sim \frac{1}{2\ln N}$. Mais ce calcul est incorrect car les $f(n)$ ne sont pas des n comme les autres (penser au cas de n^2+n+40 qui n'est jamais premier). On corrige donc cette quantité en tenant compte, pour chaque nombre premier p, de la probabilité r_p qu'a un nombre de la forme $f(n)$ de n'être pas multiple de p par rapport à la probabilité s_p pour un n quelconque de n'être pas multiple de p. On multiplie alors la quantité $\frac{1}{2\ln N}$ par le produit des r_p/s_p. Or, on connaît r_p : c'est 1 si $-d$ n'est pas un carré modulo p et $1-2/p$ sinon et on connaît aussi s_p : c'est $1-1/p$. On note déjà (dans le cas usuel de n^2+n+c avec c impair) qu'on a $r_2=1$ et $s_2=1/2$ ce qui enlève le facteur 2. On en déduit $\mathbf{P} = \frac{1}{\ln N}\prod_{oui}\frac{p-2}{p}\prod_{tous}\frac{p}{p-1} = \frac{1}{\ln N}\prod_{oui}\frac{p-2}{p-1}\times\prod_{non}\frac{p}{p-1}$ comme annoncé.

4 Le lien avec le nombre de classes

4.1 Introduction

On a vu ci-dessus le lien entre deux résultats en apparence très éloignés :
• tous les nombres n^2+n+41 sont premiers pour $0 \leq n < 40$,
• l'anneau des entiers de $\mathbf{Q}(i\sqrt{163})$ est factoriel.

On peut montrer, plus généralement, que les n^2+n+c pour $n < c-1$ sont tous premiers si et seulement si l'anneau des entiers de $\mathbf{Q}(i\sqrt{d})$ (avec $-d = 1-4c$) est factoriel, voir 7.27. Mais le phénomène ne s'arrête pas là et il concerne aussi les n grands.

On sait (voir [23], [28], [2], [4], etc.) que l'anneau des entiers de $\mathbf{Q}(i\sqrt{d})$ ($d>0$) admet deux formes selon la congruence de d modulo 4. Pour simplifier, **on se limitera désormais** au cas le plus intéressant [20] (au sens où il fournit beaucoup de nombres premiers), qui est le cas $d \equiv 3 \pmod 4$. Dans ce cas, l'anneau des entiers est $A_d = \mathbf{Z}[\frac{1+i\sqrt{d}}{2}]$. Cet anneau est principal [21] pour les fameux nombres $d = 3, 7, 11, 19, 43, 67$ et 163 et seulement pour eux. Dans le cas général, on introduit le groupe des classes d'idéaux de A_d. C'est un groupe abélien fini, de cardinal $h(d)$. Ce nombre vaut 1 si l'anneau est principal et, sinon, il peut prendre des valeurs arbitrairement grandes. Nous allons montrer ici le lien entre le nombre (conjectural) $P(N)$ des nombres premiers de la forme n^2+n+c avec $n \leq N$ et la taille de $h(d)$ (ou plus précisément de $h(d)/\sqrt{d}$) avec $d = 4c-1$.

20. Et même, essentiellement, au cas où d est un nombre premier $\equiv 3 \pmod 8$.
21. Pour les anneaux de nombres principal équivaut à factoriel, voir [19].

4.2 Formule analytique pour h

Sur ce sujet on renvoie aux références et notamment [2] et [4].

Soit $\mathbf{Q}(i\sqrt{d})$ un corps quadratique imaginaire. Pour simplifier, on suppose d premier, $d \equiv 3 \pmod 4$ et [22] $d > 3$. Soit A_d son anneau d'entiers.

On considère le caractère de Dirichlet χ, qui, dans le cas présent, n'est autre que le symbole de Legendre :

4.1 Définition. *Soit d comme ci-dessus. Si x est un entier, on définit le caractère χ par la formule $\chi(x) = \left(\frac{x}{d}\right)$.*

4.2 *Remarque.* Pour $d \equiv 3 \pmod 8$ on a $\chi(2) = -1$.

On peut alors définir la série L associée :

4.3 Proposition-Définition. *La série L associée à χ est définie par l'une des formules suivantes :*

$$L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}},$$

où le produit est étendu à **tous** *les nombres premiers (y compris 2).*

4.4 *Remarque.* On montre que la série et le produit convergent pour $\mathrm{Re}\, s > 1/2$, en particulier pour $s = 1$.

Le théorème [23] qui donne la valeur du nombre de classes est alors le suivant :

4.5 Théorème. *Avec les hypothèses précédentes, on a la formule :*

$$h(d) = \frac{\sqrt{d}}{\pi} L(1,\chi).$$

Le corollaire suivant est alors immédiat (on notera que, dans le cas considéré, le terme du produit correspondant à $p = 2$ vaut $2/3$) :

4.6 Corollaire. *On suppose d premier, $d \equiv 3 \pmod 8$ et $d > 3$. Alors, on a la formule :*

$$h(d) = \frac{2\sqrt{d}}{3\pi} \prod_p \left(1 - \frac{\left(\frac{p}{d}\right)}{p}\right)^{-1} = \frac{2\sqrt{d}}{3\pi} \prod_{oui} \frac{p}{p-1} \prod_{non} \frac{p}{p+1}.$$

où les produits sont étendus aux nombres premiers impairs, l'indice oui (resp. non) signifiant que p est un carré modulo d (resp. n'est pas un carré).

22. Pour $d = 3$ la formule donnant $h(d)$ doit être corrigée à cause des éléments inversibles.
23. Il est dû à Dirichlet.

4.7 *Remarques.* 1) Il est facile de programmer cette fonction sur *xcas* (voir 9.5 ci-dessous) et, comme $h(d)$ est un entier, il n'y a pas besoin d'une très grande précision. Par exemple, pour $d = 163$ on a :

$$h(163) = 1 = \frac{\sqrt{163}}{\pi} \prod_p \frac{1}{1 - \frac{\chi(p)}{p}}$$

On en déduit la belle formule :

$$\prod_p 1 - \frac{\left(\frac{p}{163}\right)}{p} = \frac{\sqrt{163}}{\pi}$$

que l'on vérifie avec *xcas* : le second membre vaut $4,06390857$ et le premier, avec un produit jusque 1000000, donne $4,0647024$.

2) Pour une autre formule, voir 5.4 ci-dessous.

3) On montre que $h(d)$ tend vers l'infini avec d, voir 5.6 pour des précisions.

4.3 Le lien avec les nombres de la forme $n^2 + n + c$

4.3.1 Rappels

On considère un nombre impair c et le polynôme $f(x) = x^2 + x + c$. Son discriminant est $-d = 1 - 4c$ et d est congru à 3 modulo 8. On suppose de plus que d est premier. On note $P(N)$ le nombre de n avec $0 \leq n \leq N$ tels que $f(n)$ soit premier.

Rappelons la conjecture de Hardy-Littlewood dans ce cas, voir 3.24 :

4.8 Conjecture. *On a* $P(N) \sim C \int_2^N \frac{dt}{\ln t} \sim C \frac{N}{\ln N}$ *où* $C = C_1 C_2$ *avec :*

$$C_1 = \prod_{non} \frac{p}{p-1} \quad \text{et} \quad C_2 = \prod_{oui} \frac{p-2}{p-1}$$

les produits étant indexés par les nombres premiers p impairs, l'indice oui (rep. non) signifiant que p est, ou non, un carré modulo d.

Rappelons aussi la formule dérivée de celle qui donne $h(d)$, avec les mêmes conventions, voir 4.6 :

$$\frac{h(d)}{\sqrt{d}} = \frac{2}{3\pi} \prod_{non} \frac{p}{p+1} \prod_{oui} \frac{p}{p-1}.$$

4.3.2 La conjecture reformulée

Avec ces remarques, on obtient :

4.9 Conjecture. *On pose :*

$$K(d) = \frac{2}{3\pi} \prod_{non} \frac{p^2}{p^2-1} \prod_{oui} \frac{p(p-2)}{(p-1)^2}$$

où les produits sont étendus aux nombres premiers impairs, l'indice oui (resp. non) signifiant que p est, ou non, un carré modulo d. On a $0,1401 \leq K(d) \leq 0,2618$ *et la conjecture 3.24 devient :*

$$P(N) \sim \frac{\sqrt{d}}{h(d)} K(d) \frac{N}{\ln N} \sim \frac{\sqrt{d}}{h(d)} K(d) \operatorname{Li}(N).$$

Démonstration. La formule est immédiate en calculant $K(d) := C\dfrac{h(d)}{\sqrt{d}}$ avec les formules précédentes. Il reste à prouver l'encadrement. Pour cela, on écrit :

$$K(d) = \frac{2}{3\pi} \prod_{tous} \frac{p^2}{p^2-1} \prod_{oui} \frac{(p+1)(p-2)}{p(p-1)}.$$

Le premier produit converge vers une valeur indépendante de d dont on peut donner une valeur approchée : $1,2337005429$. Les termes du second sont tous plus petits que 1, de sorte que le produit est ≤ 1 et on peut le minorer par [24] $\displaystyle\prod_{tous} \frac{(p+1)(p-2)}{p(p-1)}$, qui ne dépend plus de d et vaut environ $0,5351070188$. On en déduit le résultat.

4.10 *Remarques.* 1) L'encadrement de $K(d)$ n'est pas loin d'être optimal. En effet, côté majoration, on a $K(d) = 0,2600344895$ pour $d = 163$ et $K(d) = 0,260789$ pour $d = 111763$. Côté minoration, on a $K(d) = 0,144097$ pour $d = 131$, $K(d) = 0,141439$ pour $d = 12011$ ($h(d) = 65$).

2) Pour $d = 163$, la variante de 4.9 avec Li donne $P(10^6) \simeq 261067$ au lieu de 261081 ! Pour $d = 179$ on a $h(d) = 5$, $K(d) = 0,151465$, la conjecture donne 31871 au lieu de 32060.

4.11 *Remarque.* Évidemment, on peut trouver gênante la présence du terme $K(d)$ et il serait plus agréable d'avoir une formule ne dépendant que de $h(d)$ et de d et qui expliquerait la constatation expérimentale que $K(d)$ est plus près de son maximum quand $h(d)$ est petit et d grand. Certes ...

24. On rencontre ce genre de constantes dans le problème des nombres premiers jumeaux, voir [5].

5 En guise de conclusion, finalement, pourquoi sont-ils si nombreux ?

On peut maintenant – au moins conjecturalement – tenter de répondre à la question initiale : *Pourquoi y a-t-il beaucoup de nombres premiers de la forme* n^2+n+41 *?* Pour cela, on va comparer aux autres formules du même type, en se limitant aux polynômes de la forme[25] $f(x) = x^2 + bx + c$. Le discriminant de ce polynôme vaut $b^2 - 4c := -d$ et on suppose $d > 0$. On note $P(N)$ le nombre de nombres premiers parmi les $f(n)$, $0 \leq n \leq N$.

Rappelons l'une des conjectures proposées pour $P(N)$ (voir 3.16) :

5.1 Conjecture. *On a* $P(N) \sim \epsilon N \prod_p (1 - \frac{1}{p}) \prod_p (1 - \frac{2}{p})$ *où* ϵ *vaut* 0 *si* b *est impair et* c *pair,* $\frac{1}{2}$ *si* b *est pair et* 1 *si* b *et* c *sont impairs, où le premier produit est indexé par les facteurs premiers de* d *et où le second est étendu aux nombres premiers impairs* $\leq N$ *tels que* $-d$ *soit un carré non nul modulo* p*.*

Bien entendu, le cas b impair et c pair, qui donne $\epsilon = 0$, est à rejeter (les $f(n)$ sont tous pairs). De plus, dans la conjecture ci-dessus, la présence du coefficient ϵ montre que, toutes choses étant égales par ailleurs, il y a deux fois plus de $f(n)$ premiers dans le cas où b, c sont impairs que dans le cas où b est pair.

Nous nous limiterons donc au cas b, c impairs. On a alors $d = 4c - b^2 \equiv 3 \pmod 8$. En effet, on pose $b = 2b' + 1$ et $c = 2c' + 1$ et on a $d = 8c' - 4b'(b' + 1) + 3$ et $b'(b' + 1)$ est pair.

5.1 Un principe et trois arguments en sa faveur

La recette, dite de manière un peu vague, est la suivante :

5.2 Principe. *Le polynôme* $f(n)$ *fournit beaucoup de nombres premiers si et seulement si son discriminant* $-d$ *n'est pas un carré modulo les petits nombres premiers* p*.*

5.1.1 Argument 1 : Ératosthène et factorialité

Dire que $f(n) = n^2+n+c$ est premier c'est dire qu'aucun nombre premier $p < \sqrt{n^2 + n + c}$ ne divise $n^2 + n + c$ donc que f n'a pas de racine modulo p

25. Voir Annexe 8.4 pour le cas général.

ou encore que son discriminant $-d$ n'est pas un carré modulo p, autrement dit, c'est exactement 5.2 : $-d$ n'est pas un carré modulo les petits p !

De plus, on a vu en 2.4.1 que le fait que les $n^2 + bn + c$ soient premiers pour n petit est directement lié à la factorialité de l'anneau A_d des entiers de $\mathbf{Q}(i\sqrt{d})$. On a vu aussi, cf. 2.5 que ce qui empêche cet anneau d'être factoriel est la présence de petits nombres premiers p tels que p divise $N(z)$ sans diviser z et que cela signifie que $-d$ est un carré modulo p, voir 2.6.

On voit donc, à rebours, que lorsque 5.2 est satisfait, l'anneau a tendance à être factoriel, donc les nombres $n^2 + bn + c$ à être premiers.

5.1.2 Argument 2 : les formules donnant $P(N)$

Reprenons la conjecture[26] 5.1 ci-dessus. Dans cette formule, les termes $1 - \frac{2}{p}$ sont < 1, donc ont tendance à faire diminuer $P(N)$ et ce d'autant plus que p est petit (donc $2/p$ grand). Autrement dit, comme annoncé, $P(N)$ est d'autant plus grand qu'il y a peu de p petits tels que $-d$ soit un carré modulo p.

5.3 *Exemple.* Les premières valeurs des $1-2/p$, celles qui font le plus diminuer le produit (donc le nombre de premiers de la bonne forme), sont $1/3 \sim 0.66$, $3/5 \sim 0.6$, $5/7 \sim 0.71$, etc. Ce qui se passe dans le cas de $n^2 + n + 41$, donc de $d = 163$, c'est que -163 **n'est pas un carré modulo les nombres premiers** $p \leq 40$. Le premier $1 - 2/p$ à prendre en compte correspond à $p = 41$, et c'est $39/41 \sim 0.95$. Au contraire, pour $d = 131$ par exemple, qui correspond au polynôme $x^2 + x + 33$, les nombres premiers qui apparaissent dans le produit sont $3, 5, 7, 11, 13$, etc. ce qui fait que le produit jusqu'à 40, qui vaut 1 dans le cas 163, vaut ici seulement 0.099 !

5.1.3 Argument 3 : les formules donnant $h(d)$

On a vu en 4.9 le lien entre $P(N)$ et $h(d)$: $P(N) \sim \dfrac{\sqrt{d}}{h(d)} K(d) \dfrac{N}{\ln N}$. On voit que $P(N)$ est d'autant plus grand que $h(d)$ est petit. On a vu aussi la formule de Dirichlet qui donne $h(d)$:

$$h(d) = \frac{2\sqrt{d}}{3\pi} \prod_{oui} \frac{p}{p-1} \prod_{non} \frac{p}{p+1}.$$

Dans cette formule, les p tels que $-d$ n'est pas un carré (qui correspondent à l'indice *non*) donnent des termes $\frac{p}{p+1} < 1$, donc ont tendance à faire décroître

26. La même analyse vaut avec la conjecture de Hardy-Littlewood 3.24.

h, tandis que ceux pour lesquels $-d$ est un carré (l'indice *oui*) ont tendance à le faire croître. On retrouve encore le principe 5.2. D'ailleurs, dans le cas où d est premier [27], il y a une autre formule, très spectaculaire, qui confirme encore ce principe, en liant directement $h(d)$ aux carrés et non carrés :

5.4 Théorème. *Soit d un nombre premier $\equiv 3 \pmod 8$ et soit $h(d) = h(\mathbf{Q}(i\sqrt{d}))$. On a $h(d) = \frac{1}{3}(C - N)$ où C (resp. N) est le nombre d'entiers n avec $0 < n < d/2$ tel que n soit un carré modulo d (resp. un non carré).*

Voir [2] ou [4] th. 9.1 et th. 9.17. Cette formule corrobore le rôle des petits nombres premiers. En effet, si $n = p_1 \cdots p_r$, si tous les p_i sont des carrés, n est aussi un carré, mais si certains des p_i sont non carrés, n n'est un carré que si les non carrés sont en nombre pair.

5.2 Application du principe

Même maintenant qu'on a compris le principe, il demeure un point assez mystérieux : qu'est-ce qui fait qu'un entier d a un $h(d)$ petit, c'est-à-dire que $-d$ n'est pas un carré modulo les petits nombres premiers ? La question n'est pas évidente car il y a une part d'aléatoire dans la distribution des nombres premiers et des carrés, mais à défaut de comprendre ce mystère, on peut se faire démiurge en posant la question : *comment fabriquer de tels d ?*

La méthode est la suivante. D'abord, on ne garde que les nombres d qui sont premiers et parmi eux que ceux qui sont congrus à 3 modulo 8. Ensuite, on parcourt les petits nombres premiers $p = 3, 5, 7...$, on considère les classes de congruences modulo p et on ne garde que les d tels que $-d$ ne soit pas un carré modulo p. Ainsi, pour 3 on garde $d \equiv 1$, pour 5 on garde $d \equiv \pm 2$, pour 7 on garde $d \equiv 1, 2, -3$, pour 11, $d \equiv 1, 4, -2, 5, 3$, etc. En regardant les congruences modulo $3, 5, 7, 11$ on voit que, pour $d < 200$ il ne reste que $d = 67$ et $d = 163$.

Si l'on borne le nombre de p considérés, disons $p_1, \ldots, p_r$, les d convenables sont ceux qui vérifient certaines congruences modulo le produit $p_1 \cdots p_r$ en vertu du lemme chinois et il existe une infinité de d premiers convenables en vertu du théorème de Dirichlet. Ces d sont les candidats à avoir un petit $h(d)$. Si l'on dispose de tels d assez grands, le rapport $\sqrt{d}/h(d)$ sera d'autant plus favorable à un $P(N)$ grand.

5.5 *Exemples.* 0) Il n'y a plus qu'à écrire un programme qui détermine les

27. On rappelle qu'alors $-d$ est un carré modulo p si et seulement si p est un carré modulo d.

candidats d, voir [28] $recherd(N, M)$ en 9.6 ci-dessous. On détermine ainsi les entiers premiers $d \leq 120000$ qui sont tels que $-d$ ne soit un carré modulo p pour aucun nombre premier $p < 40$. Il fournit trois résultats : $d = 163$, $d = 77683$ et $d = 111763$.

1) Le cas $d = 163$ est celui d'Euler. Rappelons qu'il y a 261081 nombres premiers de la forme $n^2 + n + 41$, avec $n \leq 10^6$. Ici, on a $h(d) = 1$, donc $\sqrt{d}/h(d) \simeq 12.7$ et la constante $C/2$ de la conjecture de Hardy-Littlewood (voir 3.21) vaut 3.3197.

2) La valeur $d = 111763 = 4 \times 27941 - 1$ a été découverte par Beeger en 1938. Il y a 286129 nombres premiers de la forme $n^2 + n + 27941$ avec $n \leq 10^6$ (c'est donc un peu mieux que le cas d'Euler). On a $h(d) = 24$ et $\sqrt{d}/h(d) \simeq 13.929$ est un peu meilleur que dans le cas $d = 163$, de même, pour le $C/2 \simeq 3.631$.

3) Le cas $d = 77683$ correspond aux nombres de la forme $n^2 + n + 19421$. Il y en a 259459 qui sont premiers pour $n \leq 10^6$. Ici on a $h(d) = 22$ et $\sqrt{d}/h(d) \simeq 12.67$.

3bis) Les entiers précédents ne sont pas premiers : on a $77683 = 131 \times 593$ et $111763 = 73 \times 1531$. On a un meilleur exemple avec $d = 1333963$ (et il est premier !), $c = 333491$, $P(10^6) = 300002$. Ici $h(d) = 79$ (avec la formule 5.4 le calcul de h est super-rapide). On a $\sqrt{d}/h(d) \simeq 14.6199$ et $C/2 \simeq 3.812$.

4) Fung et Williams, voir [8] donnent comme exemple le polynôme $f(x) = x^2 + x + 132874279528931$, de discriminant $-d$ avec $d = 531497118115723$. On a $h(d) = 1185668$ et un quotient $\sqrt{d}/h(d) = 19.444$ et $C/2 \sim 5.089$. Dans ce cas, on a $P(10^6) = 312975$. C'est, à ce jour, le record absolu de nombres premiers pour un polynôme de cette forme avec $n \leq 10^6$.

On notera que d n'est pas premier (c'est 223×2383395148501).

5) L'article [10] de Jacobson et Williams fournit (avec une méthode analogue à celle décrite ci-dessus) des valeurs de c tel que le nombre $P(N)$ pour x^2+x+c soit asymptotiquement plus grand encore. Il donne par exemple $c = 3399714628553118047$ avec comme constante de Hardy-Littlewood $C/2 \simeq 5.367$ ou encore :

$$c = 33251810980696878103150085257129508857312847751498190349983874538507313,$$

qui atteint $C/2 \simeq 5.657$.

6) On notera que les valeurs de $K(d)$ (voir 4.9) correspondant aux records sont toutes étonnamment proches de 0.26 et on peut se demander s'il y a une bonne raison pour cela.

28. Le programme n'impose pas d premier. Dans ce cas il vaut mieux mettre $-d$ non carré modulo p, même si *xcas* calcule le symbole de Legendre avec un d non premier. (Il calcule le symbole de Jacobi, voir 7.15 et on a encore la formule $\left(\frac{-d}{p}\right) = \left(\frac{p}{d}\right)$).

5.6 *Remarque.* À propos de records, une question naturelle est de savoir si l'on peut espérer les battre indéfiniment. Cette question est liée à celle du comportement asymptotique de $h(d)$. On sait que $h(d)$ est de l'ordre de $\sqrt{d}$, mais on a des résultats plus précis, dûs à Littlewood (en utilisant l'hypothèse de Riemann généralisée), voir [12], [7], [30] :

1) On a, pour tout $d > 0$, $d \equiv 3 \pmod 4$, $h(d) \leq 2(c + o(1))\sqrt{d}\,\ln(\ln d)$ avec $c = e^\gamma/\pi$. Pour notre problème, cela donne pour $P(N)$ (ou son équivalent conjectural), $P(N) \geq \dfrac{K(d)}{2c\ln(\ln d)}\,\mathrm{Li}\,(N)$.

2) Il y a une infinité de d tels que $h \geq (c+o(1))\sqrt{d}\ln(\ln d)$, ce qui donne, **pour ces** d, $P(N) \leq \dfrac{K(d)}{c\ln(\ln d)}\,\mathrm{Li}\,(N)$, mais aussi une infinité de d tels que $h(d) < \dfrac{\pi}{6e^\gamma}\,\dfrac{\sqrt{d}}{\ln(\ln d)}$, ce qui donne $P(N) \geq \dfrac{6e^\gamma}{\pi}\ln(\ln d)K(d)\,\dfrac{N}{\ln N}$.

On voit que, avec ces dernières valeurs correspondant à d grand, comme h est petit, $P(N)$ peut être très grand. Attention toutefois, si d est grand, il faudra aussi prendre N très grand [29].

6 Annexe 1 : les probabilités de la théorie des nombres

6.1 Introduction : densité naturelle

6.1.1 Définition

Sur une partie finie X de $\mathbf{N}$, il y a une mesure de probabilité "fréquentiste" canonique, qui associe à une partie $A \subset X$ le nombre $|A|/|X|$. En revanche, il n'est pas simple de définir une mesure de probabilité sur $\mathbf{N}$. Bien sûr, on a la notion de densité [30] naïve :

6.1 Proposition. *Soit A une partie de $\mathbf{N}$ et N un entier ≥ 0. On pose $I_N = \{0, 1, \ldots, N\}$, $A_N = I_N \cap A$ et $a_N = |A_N|$. On dit que A a une* **densité naturelle** *si la quantité $a_N/(N+1)$ a une limite quand N tend vers l'infini et on note $\delta(A)$ cette limite (qui est la densité en question).*

6.2 *Remarques.* 1) La densité naturelle d'une partie finie est nulle.

29. Par exemple, Shanks donne dans [27] la valeur $d = 30059924764123$ qui vérifie $h(d) = 296475$. La conjecture 4.9, appliquée à $N = 10^6$ donnerait alors $P(N) = 1100550$, ce qui est beaucoup pour un nombre réputé $\leq 10^6$ ...

30. J'ai une petite hésitation pour savoir s'il faut se placer sur $\mathbf{N}$ ou sur $\mathbf{N}^*$. Finalement je choisis $\mathbf{N}$.

2) Il y a des parties qui n'ont pas de densité naturelle. Par exemple la réunion A des intervalles entiers $]2^{2p-1}, 2^{2p}]$ pour p entier ≥ 1. En effet, le nombre d'éléments de A qui sont $\leq 2^{2p}$ vaut $\dfrac{2^{2p+1}-2}{3}$, et c'est aussi le nombre d'éléments de A qui sont $\leq 2^{2p+1}$, de sorte que la limite de a_N/N est égale à $2/3$ si $N = 2^{2p}$ et à $1/3$ si $N = 2^{2p+1}$.

3) Il n'est pas évident (pour moi) que la réunion de deux parties admettant une densité naturelle en ait une, mais c'est clair pour des parties disjointes et la densité de la réunion est alors la somme des densités.

6.1.2 L'exemple fondamental : les congruences

L'exemple le plus convaincant de la notion de densité naturelle est celui des congruences. Nous y reviendrons plus bas, mais nous allons montrer dès maintenant l'existence de cette densité. Commençons par un dénombrement élémentaire :

6.3 Proposition. *Soient p un entier ≥ 2, a un entier compris entre 0 et $p-1$ et N un entier. Alors, le cardinal de l'ensemble :*

$$C_{N,p,a} = \{x \in \mathbf{N} \mid 0 \leq x \leq N \text{ et } x \equiv a \pmod{p}\}$$

est égal[31] *à $c_{N,p,a} := \left[\frac{N-a}{p}\right] + 1 = \left[\frac{N+p-a}{p}\right]$. Lorsque N tend vers l'infini, $c_{N,p,a}/(N+1)$ tend vers $1/p$, autrement dit la classe de congruence à a modulo p, notée $C_{p,a}$, admet une densité naturelle égale à $1/p$. C'est le cas en particulier de $C_{p,0} = p\mathbf{N}$.*

Démonstration. Les éléments de $C_{N,p,a}$ sont $a, a+p, a+2p, \ldots, a+kp$ avec $a+kp \leq N$ et $a+(k+1)p > N$. On en déduit facilement le résultat.

6.4 *Remarques.* 1) La formule est exacte même si N est plus petit que a. En effet, si l'on a $0 < a$, on a $-p < -a \leq N-a < 0$ et donc $-1 < \frac{N-a}{p} < 0$. La partie entière est donc -1 et on trouve bien 0 comme cardinal.

2) L'inégalité précise qui donne la limite est la suivante :

$$\frac{N+1}{p} - 1 < c_{N,p,a} \leq \frac{N}{p} + 1.$$

31. L'exemple de $N = 30$, $p = 7$, $a = 5$ montre que ce n'est ni $\left[\frac{N+a}{p}\right]$, ni $\left[\frac{N-a}{p}\right]$.

6.2 Il n'y a pas de mesure de probabilité sur N !

La difficulté de l'application des méthodes probabilistes en théorie des nombres vient notamment du résultat suivant [32] :

6.5 Théorème. *Il n'existe pas de mesure de probabilité σ-additive sur* $\mathbf{N}$ *telle que la probabilité de* $p\mathbf{N}$*,* $p \in \mathbf{N}^*$*, soit égale à* $1/p$*.*

Démonstration. On montre que sinon, la probabilité d'un singleton est nulle, donc, par σ-additivité, celle de $\mathbf{N}$ aussi et on a $0 = 1$.

Pour cela, on note que les événements $p\mathbf{N}$ et $q\mathbf{N}$ sont indépendants [33] dès que p et q sont premiers entre eux. En effet, on a alors $p\mathbf{N} \cap q\mathbf{N} = pq\mathbf{N}$, donc $\mathbf{P}(p\mathbf{N} \cap q\mathbf{N}) = 1/pq = \mathbf{P}(p\mathbf{N}) \times \mathbf{P}(q\mathbf{N})$. Il en résulte que leurs complémentaires X_p et X_q le sont aussi (c'est une propriété générale). On en déduit $\mathbf{P}(X_p \cap X_q) = (1 - \frac{1}{p})(1 - \frac{1}{q})$. On note ensuite que, si m, n sont des entiers avec $m < n$, le singleton $\{m\}$ est contenu dans l'intersection $X_{p_1} \cap \cdots \cap X_{p_r}$ où les p_i sont les nombres premiers vérifiant $m < p_1 < \ldots < p_r \leq n$. En effet, il est clair que m n'est pas multiple de p_i. On a donc $\mathbf{P}(\{m\}) \leq (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$ autrement dit $\mathbf{P}(\{m\}) \leq \prod_{m<p\leq n} (1 - \frac{1}{p})$ pour tout $n > m$. Si on pose $A = \prod_{p\leq m}(1 - \frac{1}{p})$, la formule de Mertens (voir 6.32) donne $\prod_{m<p\leq n} (1 - \frac{1}{p}) \sim \frac{e^{-\gamma}}{A} \frac{1}{\ln n}$ et cette quantité tend vers 0 quand n tend vers l'infini. On a donc bien $\mathbf{P}(\{m\}) = 0$.

6.3 Il y a une mesure de probabilité sur N !

Cependant, le résultat précédent ne prouve pas – à mon avis – que l'approche probabiliste soit vouée à l'échec. En effet, la σ-additivité ne semble pas raisonnable du tout en ce domaine. Il faudrait en effet attribuer une probabilité p_n à chaque entier, avec des probabilités différentes (puisque la série des p_n doit être convergente) et ce n'est guère conforme à l'intuition qu'on peut avoir. En fait, si on oublie la σ-additivité, on a le résultat inverse [34] :

32. Voir par exemple le livre de G. Tenenbaum *Introduction à la théorie analytique et probabiliste des nombres* p. 301.

33. Voir plus loin une généralisation.

34. Je m'inspire d'une construction proposée par Christophe Chalons sur le forum *les-mathematiques.net*.

6.6 Proposition. *Il existe une mesure de probabilités* $\mathbf{P}$ *sur* $\mathcal{P}(\mathbf{N})$ *(additive mais non* σ*-additive) telle que si* A *a une densité naturelle* $\delta(A)$ *on a* $\mathbf{P}(A) = \delta(A)$*. On la désigne sous le nom de* **probabilité naturelle** *sur* $\mathbf{N}$*.*

6.3.1 Rappels

On renvoie à [3], Chapitre I pour des détails.

Rappelons qu'un filtre $\mathcal{F}$ sur un ensemble E est un ensemble non vide de parties de E ne contenant pas l'ensemble vide, stable par intersection finie et par augmentation. Si E est un espace topologique, on dit qu'un filtre $\mathcal{F}$ converge vers $a \in E$ s'il est plus fin que le filtre des voisinages de a (i.e. tout voisinage de a est dans $\mathcal{F}$).

Un ultrafiltre $\mathcal{U}$ est un filtre maximal. En vertu du théorème de Zorn il existe un ultrafiltre qui majore n'importe quel filtre. Les ultrafiltres sont caractérisés par le fait que, pour toute partie $X \subset E$, X ou ${}^cX$ est dans $\mathcal{U}$. Si K est un espace topologique compact, tout ultrafiltre sur K est convergent.

6.3.2 La définition

L'idée est de définir $\mathbf{P}(A)$ comme la limite de $a_N/(N+1)$ si cette limite existe et de la forcer à exister en utilisant un ultrafiltre.

On considère le filtre de Fréchet $\mathcal{F}$ sur $\mathbf{N}$, c'est-à-dire le filtre des complémentaires des parties finies et un ultrafiltre $\mathcal{U}$ majorant $\mathcal{F}$.

Soit A une partie de $\mathbf{N}$ et a_N le nombre d'éléments de A qui sont $\leq N$. On considère l'application $f_A : \mathbf{N} \to I := [0,1]$ définie par $f_A(N) = a_N/(N+1)$. On pose :

$$\mathcal{V}_A = \{X \subset I \ \mid \ f_A^{-1}(X) \in \mathcal{U}\}.$$

6.7 Lemme. *L'ensemble* $\mathcal{V}_A$ *est un ultrafiltre de* I*.*

Démonstration. Cela résulte des propriétés de l'image réciproque.

Comme I est compact on peut définir :

6.8 Définition. *On définit la probabilité* $\mathbf{P}(A)$ *comme la limite de l'ultrafiltre* $\mathcal{V}_A$*.*

On peut maintenant prouver 6.6. On vérifie qu'on a $\mathbf{P}(\emptyset) = 0$ (resp. $\mathbf{P}(\mathbf{N}) = 1$) car $\mathcal{V}_A$ est alors l'ensemble des parties contenant 0 (resp. 1).

Montrons d'abord l'additivité (simple) de $\mathbf{P}$. Soient $A, B \subset \mathbf{N}$, disjoints. Il est clair que l'on a $f_{A\cup B} = f_A + f_B$. Posons $a = \mathbf{P}(A)$, $b = \mathbf{P}(B)$ et montrons qu'on a $a + b = \mathbf{P}(A \cup B)$. Soit W un voisinage de $a+b$. Il existe des voisinages U de a et V de b tels que $U + V \subset W$. Comme U est dans

$\mathcal{V}_A$ et V dans $\mathcal{V}_B$, $f_A^{-1}(U)$ est dans $\mathcal{U}$ ainsi que $f_B^{-1}(V)$. Il s'agit de montrer que $f_{A\cup B}^{-1}(W)$ est aussi dans $\mathcal{U}$ (ce qui montrera que W est dans $\mathcal{V}_{A\cup B}$ donc que $\mathcal{V}_{A\cup B}$ converge vers $a+b$). Mais, cet ensemble contient $f_A^{-1}(U)\cap f_B^{-1}(V)$ qui est dans $\mathcal{U}$ et on a le résultat. En effet, si n est dans l'intersection on a $f_A(n)\in U$, $f_B(n)\in V$ donc $f_{A\cup B}(n)=f_A(n)+f_B(n)\in U+V\subset W$.

Il reste à vérifier que, si A a une densité naturelle $\delta=\delta(A)$, on a bien $\mathbf{P}(A)=\delta(A)$. En effet, soit V un voisinage de $\delta(A)$. Il s'agit de montrer que V est dans $\mathcal{V}_A$, autrement dit que $f_A^{-1}(V)$ est dans $\mathcal{U}$. Mais, on a $f_A^{-1}(V)=\{N\in\mathbf{N}\ \mid\ a_N/(N+1)\in V\}$ et comme la suite $a_N/(N+1)$ converge vers δ, cet ensemble contient une section finissante de $\mathbf{N}$, donc est dans $\mathcal{F}$, donc dans $\mathcal{U}$.

6.4 Les probabilités naturelles des classes de congruence

6.4.1 La probabilité des classes

6.9 Proposition. *1) Soient p et a deux entiers. On note $C_{p,a}$ l'ensemble des n congrus à a modulo p, c'est-à-dire l'événement $[x\equiv a \pmod p]$. On a $\mathbf{P}(C_{p,a})=1/p$, autrement dit, la probabilité naturelle que n soit congru à a modulo p est égale à $1/p$ et (et donc la probabilité pour que n ne soit pas congru à a modulo p est $1-\dfrac{1}{p}=\dfrac{p-1}{p}$).*

2) Plus généralement, si p est un entier >1 et $a_1,\dots,a_r$ des entiers distincts modulo p, on note $C_{p,a_1,\dots,a_r}$ l'ensemble des n congrus à a_1 ou a_2 ... ou a_r modulo p. On a $\mathbf{P}(C_{p,a_1,\dots,a_r})=\dfrac{r}{p}$.

3) Si p est un entier >1 et $a_1,\dots,a_r$ des entiers distincts modulo p, on note $X_{p,a_1,\dots,a_r}$ l'ensemble des n qui ne sont congrus à aucun des a_i modulo p. On a $\mathbf{P}(X_{p,a_1,\dots,a_r})=1-\dfrac{r}{p}$.

Démonstration. La proposition 6.3 montre que la densité naturelle de l'ensemble des $n\equiv a \pmod p$ vaut $1/p$, d'où 1). Pour 2), on utilise la formule $C_{p,a_1,\dots,a_r}=C_{p,a_1}\cup\dots\cup C_{p,a_r}$ (union disjointe), pour 3), le fait que $X_{p,a_1,\dots,a_r}$ est le complémentaire de $C_{p,a_1,\dots,a_r}$.

6.10 *Remarques.* 1) En vertu de 6.4.2, on a l'inégalité :

$$\frac{1}{p}-\frac{1}{N+1}<\mathbf{P}(C_{N,p,a})\leq\frac{1}{p}+\frac{1}{N+1}.$$

On voit que pour que le minorant soit >0 il faut que N soit $\geq p$.

2) On peut calculer exactement le cardinal de $C_{N,p,a_1,\dots,a_r}$, ensemble des n congrus à a_1 ou a_2 ... ou a_r modulo p et vérifiant $0\leq n\leq N$. On a la

formule :

$$c_{N,p,a_1,\ldots,a_r} := |C_{N,p,a_1,\ldots,a_r}| = \big[\frac{N-a_1}{p}\big] + \cdots + \big[\frac{N-a_r}{p}\big] + r.$$

3) Ce n'est pas parce que la probabilité naturelle pour un entier n de ne pas être multiple de p est de $1 - \dfrac{1}{p}$, qu'il faut en déduire que le nombre d'entiers n avec $0 \leq n \leq N$ qui ne sont pas multiples de p vaut $N(1 - \frac{1}{p})$. Le calcul précis a été fait en 6.3 ci-dessus. Par exemple, pour $p = 2$, le nombre $i(N)$ d'entiers impairs $\leq N$ est $N/2$ si N est pair, mais $(N+1)/2$ si N est impair. Pour $p = 3$, le nombre d'entiers $\leq N$ non multiples de 3 est $2N/3$, $(2N+1)/3$ ou $(2N+2)/3$ selon que N est congru à $0, 1$ ou 2 modulo 3. À cause de ces effets de bord, la formule n'est donc vraie qu'asymptotiquement.

6.4.2 Indépendance

Le lemme crucial est le suivant :

6.11 Lemme. *Soient p, q des entiers premiers entre eux et considérons les événements $C_{p,a} := [x \equiv a \pmod p]$ et $C_{q,b} := [x \equiv b \pmod q]$. Alors, la probabilité de leur intersection est $\dfrac{1}{pq}$ (de sorte que ces événements sont indépendants). Le même résultat vaut pour des entiers $p_1, \ldots, p_k$ deux à deux premiers entre eux.*

Démonstration. Le lemme chinois dit qu'on a un isomorphisme $\theta : \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z} \to \mathbf{Z}/pq\mathbf{Z}$ et on en déduit $C_{p,a} \cap C_{q,b} = C_{pq,\theta(a,b)}$. Comme les probabilités sont $1/p$, $1/q$ et $1/pq$, les événements sont indépendants.

6.12 *Remarque.* Le lemme chinois montre que les intersections $C_{p_1,a_1} \cap \cdots \cap C_{p_k,a_k}$ ont une densité naturelle. En vertu de 6.2.3, il en est de même des unions disjointes de ces intersections.

6.13 *Remarque.* Là encore, on sait calculer le cardinal $|C_{N,p,a} \cap C_{N,q,b}|$ des entiers $n \leq N$ qui sont congrus à a modulo p et à b modulo q. Vu le lemme chinois, c'est $\big[\dfrac{N - \theta(a,b)}{pq}\big] + 1$.

6.14 Corollaire. *On considère des entiers $p_1, \ldots, p_k$ deux à deux premiers entre eux et, pour chaque $i = 1, \ldots, k$, r_i classes a_{ij} distinctes modulo p_i. On appelle $C_{\underline{p},\underline{a}}$ l'ensemble des $n \in \mathbf{N}$ vérifiant :*

$$\forall i = 1, \ldots, k,\ \exists j = 1, \ldots, r_i,\ \textit{tel que } n \equiv a_{ij} \pmod{p_i}.$$

Alors, on a $\mathbf{P}(C_{\underline{p},\underline{a}}) = \prod_{i=1}^{k} \frac{r_i}{p_i}$.

Si l'on note $X_{\underline{p},\underline{a}}$ *l'ensemble des* $n \in \mathbf{N}$ *qui ne sont congrus à aucun des* a_{ij} *modulo aucun des* p_i *on a* $\mathbf{P}(X_{\underline{p},\underline{a}}) = \prod_{i=1}^{k}(1 - \frac{r_i}{p_i})$.

Démonstration. On a la formule $C_{\underline{p},\underline{a}} = \bigcap_{i=1}^{k} \bigcup_{j=1}^{r_i} C_{p_i,a_{ij}}$ où l'union est disjointe. On peut encore écrire cet ensemble de la manière suivante. On considère l'ensemble Φ de toutes les applications φ de $\{1, 2, \ldots, k\}$ dans $\mathbf{N}$ vérifiant $1 \leq \varphi(i) \leq r_i$. Alors, $C_{\underline{p},\underline{a}}$ est l'union disjointe indexée par Φ des intersections $\bigcap_{i=1}^{k} C_{p_i,a_{i\varphi(i)}}$. En vertu de 6.11, la probabilité de l'intersection est le produit $\frac{1}{p_1 \cdots p_k}$ et comme on a $|\Phi| = r_1 \cdots r_k$, on en déduit $\mathbf{P}(C_{\underline{p},\underline{a}}) = \frac{r_1 \cdots r_k}{p_1 \cdots p_k}$, d'où le résultat.

L'autre formule n'est qu'une variante de celle-ci avec comme liste des a_{ij} le complémentaire de celle donnée.

6.15 *Remarque.* Appelons θ l'isomorphisme du lemme chinois $\mathbf{Z}/p_1\mathbf{Z} \times \cdots \times \mathbf{Z}/p_k\mathbf{Z} \to \mathbf{Z}/(p_1 \cdots p_k)\mathbf{Z}$. On peut calculer le cardinal de l'intersection $\bigcap_{i=1}^{k} C_{N,p_i,a_{i\varphi(i)}}$ qui est égal à $\big[\frac{N - \theta(a_{1\varphi(1)}, \ldots, a_{k\varphi(k)})}{p_1 \cdots p_k}\big] + 1$. On en déduit le cardinal de $C_{\underline{p},\underline{a}}$ qui est la somme de toutes les expressions précédentes correspondant aux applications $\varphi \in \Phi$.

6.16 *Remarque.* **Attention**, $X_{\underline{p},\underline{a}}$ n'est pas le complémentaire de $C_{\underline{p},\underline{a}}$, $C_{\underline{p},\underline{a}}$ est l'intersection des C_i, $X_{\underline{p},\underline{a}}$ l'intersection des complémentaires des C_i. Si les uns sont indépendants, les autres aussi.

6.5 Les calculs avec les formules de crible

Le but de ce paragraphe est de calculer le nombre $P(N)$ d'entiers $n \leq N$ tels que $f(n) = n^2 + n + 41$ soit premier, en utilisant des formules de crible. Cela permet un calcul exact, certes peu pratique, mais qui donne cependant une autre justification (non probabiliste) de la conjecture 3.13. Ce type de technique est notamment utilisé par Shanks, voir [25], [26].

6.5.1 Quelques formules

6.17 Lemme. *Soient $x_1, \dots, x_r$ des indéterminées. On a la formule :*

$$\prod_{i=1}^{r}(1-x_i) = 1-\sum_{i=1}^{r} x_i + \sum_{1\le i<j\le r} x_i x_j + \cdots + (-1)^k \sum_{1\le i_1<\cdots<i_k\le r} x_{i_1}\cdots x_{i_k} + \cdots + (-1)^r x_1\cdots x_r.$$

6.18 Corollaire. *Pour des entiers non nuls $p_1, \dots, p_r$, on a la formule :*

$$\prod_{i=1}^{r}(1-\frac{1}{p_i}) = 1-\sum_{i=1}^{r} \frac{1}{p_i} + \sum_{1\le i<j\le r} \frac{1}{p_i p_j} + \cdots + (-1)^k \sum_{1\le i_1<\cdots<i_k\le r} \frac{1}{p_{i_1}\cdots p_{i_k}} + \cdots + (-1)^r \frac{1}{p_1\cdots p_r}.$$

Désormais, j'omettrai les termes intermédiaires dans les formules, le lecteur les rétablira sans peine.

6.19 Lemme. (Formule du crible) *Si $A_1, \dots, A_r$ sont des parties d'un ensemble on a :*

$$\Big|\bigcup_{i=1}^{r} A_i\Big| = \sum_{i=1}^{r} |A_i| - \sum_{1\le i<j\le r} |A_i \cap A_j| + \cdots + (-1)^{r+1} |A_1 \cap \cdots \cap A_r|.$$

6.5.2 Le crible d'Ératosthène

6.20 Lemme. *Soient N et p des entiers, avec $p \ge 1$. Le cardinal de l'ensemble des n vérifiant $1 \le n \le N$ qui sont multiples de p est égal à $\big[\frac{N}{p}\big]$.*

6.21 Corollaire. *Soit N un entier et $p_1, \dots, p_r$ des nombres premiers distincts. On note $P(N)$ le cardinal de l'ensemble des n avec $1 \le n \le N$ qui ne sont divisibles par aucun des p_i. Alors on a la formule :*

$$P(N) = N-\sum_{i=1}^{r} \big[\frac{N}{p_i}\big] + \sum_{1\le i<j\le r} \big[\frac{N}{p_i p_j}\big] + \cdots + \sum_{1\le i_1<\cdots<i_k\le r} (-1)^k \big[\frac{N}{p_{i_1}\cdots p_{i_k}}\big] + \cdots + (-1)^r \big[\frac{N}{p_1\cdots p_r}\big].$$

Démonstration. On applique la formule du crible avec les ensembles A_i des $1 \le n \le N$ qui sont multiples de p_i et on prend le complémentaire de l'union des A_i. Comme les p_i sont premiers, l'intersection de $A_{i_1}, \dots, A_{i_k}$ est l'ensemble des multiples de $p_{i_1}\cdots p_{i_k}$.

6.22 *Remarques.* 1) Toute la question est de comparer cette expression avec :

$$N\prod_{i=1}^{r}(1-\frac{1}{p_i}) = N-\sum_{i=1}^{r} \frac{N}{p_i} + \sum_{1\le i<j\le r} \frac{N}{p_i p_j} + \cdots + \sum_{1\le i_1<\cdots<i_k\le r} \frac{(-1)^k N}{p_{i_1}\cdots p_{i_k}} + \cdots + \frac{(-1)^r N}{p_1\cdots p_r}.$$

La différence vient du passage à la partie entière qui change chaque terme et les fait même disparaître lorsque N est plus petit que le produit des p_i.

L'expérience avec *xcas*, en prenant $N = 1000$ et les p_i de 2 jusqu'à 29 inclus, est intéressante. Les chiffres sont les suivants. On a $P(1000) = 160$ (les 158 nombres premiers ≥ 30 et ≤ 1000 plus le nombre 1 et le nombre $961 = 31^2$). C'est bien ce que donne le calcul avec le crible : $160 = 1000 - 1528 + 930 - 264 + 22 - 0$. Mais, si on remplace chaque terme en enlevant les parties entières, on voit apparaître une erreur importante à chaque pas, les valeurs approchées étant respectivement 1533, 953, 317, 63, 8 (je ne compte pas les produits de 6 et plus). Ces erreurs se compensent car la somme totale sans partie entière donne 157.947, ce qui est excellent !

2) On peut évidemment encadrer (mais de manière trop grossière) la somme avec les parties entières au cran k :

$$\sum_{1\leq i_1<\cdots<i_k\leq r} \Big[\frac{N}{p_{i_1}\cdots p_{i_k}}\Big] \leq \sum_{1\leq i_1<\cdots<i_k\leq r} \frac{N}{p_{i_1}\cdots p_{i_k}} \leq \sum_{1\leq i_1<\cdots<i_k\leq r} \Big[\frac{N}{p_{i_1}\cdots p_{i_k}}\Big] + \binom{r}{k}.$$

6.5.3 Le crible des congruences

Rappelons les résultats vus ci-dessus en 6.3 et 6.10 :

6.23 Lemme. *1) Soient p, N des entiers positifs et a un entier avec $0 \leq a \leq p-1$. Le nombre d'entiers n avec $0 \leq n \leq N$ qui sont congrus à a modulo p vaut $c_{N,p,a} = \big[\frac{N-a}{p}\big] + 1 = \big[\frac{N+p-a}{p}\big]$ et il vérifie $\big[\frac{N+1}{p}\big] \leq c_{N,p,a} \leq \big[\frac{N}{p}\big] + 1$.*

2) Soit p un entier et soient $a_1, \ldots, a_k$ des entiers distincts compris entre 0 et $p-1$. Soit N un entier. Le nombre $c_{N,p,a_1,\ldots,a_r}$ d'entiers n avec $0 \leq n \leq N$ qui sont congrus à l'un des a_i modulo p vaut $\big[\frac{N-a_1}{p}\big] + \cdots + \big[\frac{N-a_r}{p}\big] + r$ et il vérifie :

$$r\big[\frac{N+1}{p}\big] \leq c_{N,p,a_1,\ldots,a_r} \leq r\big(\big[\frac{N}{p}\big] + 1\big) = r\big[\frac{N+p}{p}\big].$$

6.24 *Remarque.* On déduit de 2) deux façons d'encadrer le nombre de n qui ne sont congrus à aucun des a_i (soit directement, soit par différence). Les résultats sont légèrement différents, mais à moins de p près.

6.25 Corollaire. *Soient $p_1, \ldots, p_r$ des nombres premiers distincts. On suppose données, pour chaque $i = 1, \ldots, r$, des classes de congruence $a_{i,j}$, $j = 1, \ldots, m_i$, distinctes, avec $0 \leq a_{i,j} \leq p_i - 1$. Soit k un entier compris entre*

1 *et* r. *On note* $a_{i_1,j_1,\dots,i_k,j_k}$ *la classe de congruence modulo* $p_{i_1}\cdots p_{i_k}$ *dont les images modulo les* p_{i_u} *sont les* a_{i_u,j_u}.

Soit N *un entier. Alors, les* n *vérifiant* $0 \leq n \leq N$ *qui sont congrus modulo* p_i *à l'un des* $a_{i,j}$ *sont en nombre* $Q(N)$ *où* $Q(N)$ *est la somme de termes* $(-1)^{k+1}Q_k(N)$ *avec* $1 \leq k \leq r$, $Q_k(N)$ *étant lui-même la somme des* $\big[\dfrac{N - a_{i_1,j_1,\dots,i_k,j_k}}{p_{i_1}\cdots p_{i_k}}\big] + 1$.

Le nombre $Q(N)$ *est majoré par la somme suivante :*

- *Pour* k *impair, la somme des* $m_{i_1}\cdots m_{i_k}\big(\big[\dfrac{N}{p_{i_1}\cdots p_{i_k}}\big] + 1\big)$,
- *Pour* k *pair, l'opposée de la somme des* $m_{i_1}\cdots m_{i_k}\big[\dfrac{N+1}{p_{i_1}\cdots p_{i_k}}\big]$.

On obtient une minoration de manière analogue en échangeant les termes.

Le nombre d'entiers n *qui évitent les congruences aux* $a_{i,j}$ *modulo tous les* p_i *est égal à* $N + 1 - Q(N)$.

Démonstration. Cela résulte de 6.23 et de 6.19.

6.5.4 Le cas de $n^2 + n + 41$

Rappelons qu'on note $P(N)$ le nombre d'entiers n avec $0 \leq n \leq N$ tels que $f(n) = n^2 + n + 41$ soit premier. Dire que $f(n)$ est premier, pour $n \geq 41$, signifie qu'aucun nombre premier $p \leq n$ ne divise $n^2 + n + 41$. On sait que cette condition est automatique si $p = 2$ ou si p n'est pas un carré modulo 163 et que, sinon, elle signifie que n est distinct des racines de f modulo p. On a la proposition suivante :

6.26 Proposition-Définition. *Soit* N *un entier et soient* $p_1, \dots, p_r$ *les nombres premiers réductibles (au sens de 3.4) qui sont* $\leq N$. *On appelle* $P_0(N)$ *le nombre d'entiers* $n \leq N$ *qui sont tels que* $f(n)$ *n'ait pas de racine modulo* $p_1, \dots, p_r$. *Alors on a* $P(N) \geq P_0(N)$.

Démonstration. En effet, si $f(n)$ n'a pas de racine modulo les $p_i \leq N$ c'est vrai *a fortiori* pour les $p_i \leq n$.

On peut calculer exactement $P_0(N)$ par une méthode de crible, à la manière de [25], comme en 6.25 ci-dessus :

6.27 Proposition. *Soit* N *un entier et* $p_1, \dots, p_r$ *les nombres premiers réductibles* $\leq N$. *Pour chaque* p_i *on note* $a_{i,1}$ *et* $a_{i,2}$ *les congruences interdites et* $a_{i_1,j_1,\dots,i_k,j_k}$ *la classe de congruence modulo* $p_{i_1}\cdots p_{i_k}$ *dont les images modulo les* p_{i_u} *sont les* a_{i_u,j_u} *(il y a* 2^k *telles classes).*

Alors, le nombre $P_0(N)$ est égal à $N+1-Q(N)$ où $Q(N)$ est la somme de termes $(-1)^{k+1}Q_k(N)$ avec $1 \leq k \leq r$, $Q_k(N)$ étant lui-même la somme des $\big[\dfrac{N-a_{i_1,j_1,\ldots,i_k,j_k}}{p_{i_1}\cdots p_{i_k}}\big]+1$ avec $1 \leq i_1 < \cdots < i_k \leq r$ et $j_u = 1$ ou 2.

6.28 *Exemple.* Voici, pour $p \leq 100 = N$, la liste des nombres premiers réductibles et des congruences interdites :

$$41 : 0, 40\,;\ 43 : 1, 41\,;\ 47 : 2, 44\,;\ 53 : 3, 49\,;\ 61 : 4, 56\,;\ 71 : 5, 65\,;\ 83 : 6, 76 \text{ et } 97 : 7, 89.$$

Pour calculer $P_0(N)$ on écrit d'abord que n n'est pas congru à 0 modulo 41, ce qui élimine $\big[\dfrac{N}{41}\big]+1 = \big[\dfrac{N+41}{41}\big]$ valeurs. Pour la congruence à 40, il faut éliminer $\big[\dfrac{N-40}{41}\big]+1 = \big[\dfrac{N+1}{41}\big]$ valeurs. On continue de même, par exemple pour 47 on élimine $\big[\dfrac{N+3}{47}\big]$ et $\big[\dfrac{N+45}{47}\big]$ valeurs.

6.29 Corollaire. *Avec les notations précédentes, on a $P_0(N) \geq N+1-Q^*(N)$ où $Q^*(N)$ est un majorant de $Q(N)$, donné par la formule :*

$$\sum_{k=1,k\,\text{impair}}^{r} 2^k \sum_{1\leq i_1<\cdots<i_k\leq r} \big(\big[\frac{N}{p_{i_1}\cdots p_{i_k}}\big]+1\big) - \sum_{k=1,k\,\text{pair}}^{r} 2^k \sum_{1\leq i_1<\cdots<i_k\leq r} \big[\frac{N+1}{p_{i_1}\cdots p_{i_k}}\big].$$

Ce corollaire, en oubliant les parties entières, mène à la conjecture usuelle :

6.30 Conjecture. *On a :*

$$\frac{P(N)}{N+1} \geq 1-\sum_i \frac{2}{p_i}+\sum_{i,j}\frac{4}{p_ip_j}+\cdots+(-1)^k\sum_{i_1,\ldots,i_k}\frac{2^k}{p_{i_1}\cdots p_{i_k}}+\cdots+(-1)^r\frac{2^r}{p_1\cdots p_r},$$

autrement dit, $\dfrac{P(N)}{N+1} \geq \displaystyle\prod_{i=1}^{r} 1-\frac{2}{p_i}\cdot$

6.31 *Remarque.* Attention, la conjecture découlerait évidemment du corollaire si l'on avait les deux inégalités :

- pour k impair, $\big[\dfrac{N}{p_{i_1}\cdots p_{i_k}}\big]+1 \leq \dfrac{N+1}{p_{i_1}\cdots p_{i_k}}$,
- pour k pair, $\big[\dfrac{N+1}{p_{i_1}\cdots p_{i_k}}\big] \geq \dfrac{N+1}{p_{i_1}\cdots p_{i_k}}\cdot$

Malheureusement, aucune de ces formules n'est correcte ! Cependant l'expérience montre que la conjecture n'est pas si mauvaise, voir en 6.36 ci-dessous une conjecture qui pourrait expliquer ce phénomène.

6.6 Le paradoxe des probabilités sur l'exemple de la densité des nombres premiers

Nous revenons ici sur les difficultés rencontrées à propos de la conjecture 3.13 en étudiant un exemple plus simple (et pour lequel on connaît les valeurs exactes des probabilités), celui de la répartition des nombres premiers.

6.6.1 Deux rappels

Rappelons deux grands résultats de la fin du XIX-ième siècle, tout d'abord le théorème de Mertens (1874) :

6.32 Théorème. *Le produit, indexé par les nombres premiers,* $\prod_{p=2}^{N}(1-\frac{1}{p})$, *est équivalent à* $e^{-\gamma}/\ln N$, *où* $\gamma \sim 0{,}577$ *désigne la constante d'Euler. On en déduit :* $\prod_{p=3}^{N}(1-\frac{1}{p}) \sim 2e^{-\gamma}/\ln N$.

Ensuite, le théorème des nombres premiers (Hadamard ou De La Vallée-Poussin, 1896) :

6.33 Théorème. *Le nombre* $\pi(N)$ *de nombres premiers* $\leq N$ *est équivalent à* $\mathrm{Li}\,(N) := \int_2^N \frac{dt}{\ln t} \sim N/\ln N$ *quand* N *tend vers l'infini.*

Par exemple, pour $N = 10^6$ on a $\pi(N) = 78498$, $N/\ln N \sim 72382$ et $\mathrm{Li}\,(N) \sim 78627$.

6.6.2 La probabilité d'être premier ?

1) Pour un entier $n \leq N$, la probabilité d'être premier, c'est-à-dire la fréquence des nombres premiers dans $[0, N]$, est environ $\frac{1}{\ln N}$ parce qu'il y a (pour N grand) environ $N/\ln N$ premiers $\leq N$: c'est le théorème des nombres premiers, argument inattaquable.

2) Un autre calcul, qui ressemble à celui mené au paragraphe 3.6 ci-dessus, est le suivant.

Un entier n est premier s'il n'est divisible par aucun nombre premier $p \leq \sqrt{n}$. Si N est un entier fixé, un entier $n \leq N$ est donc premier, *a fortiori*, s'il n'est divisible par aucun nombre premier $p \leq \sqrt{N}$.

Si p est un nombre premier fixé, la probabilité, pour un entier $n \in \mathbf{N}$, qu'il ne soit pas multiple de p vaut $1 - \frac{1}{p}$ en vertu de 6.9. Plus généralement, la

probabilité qu'il ne soit divisible par aucun des nombres premiers $\leq \sqrt{N}$ est égale au produit $\prod_{p\leq\sqrt{N}}(1-\frac{1}{p})$, voir 6.14. On aurait donc envie de proposer :

6.34 Conjecture. *La probabilité qu'un nombre $n \leq N$ soit premier est égale à* $\prod_{p\leq\sqrt{N}}(1-\frac{1}{p}) \sim \frac{2e^{-\gamma}}{\ln N}$ *en vertu de Mertens.*

Ce qui est vraiment troublant c'est qu'on obtient ainsi $1{,}122/\ln N$, qui est trop gros par rapport à la probabilité réelle qui est $1/\ln N$, alors qu'on a écrit des conditions superflues (il suffit de regarder les p jusqu'à $\sqrt{n}$ et pas jusque $\sqrt{N}$).

6.6.3 Explication du paradoxe

Soit N un entier. On pose $\mathcal{P}(N) = \{n \leq N \mid n \text{ est premier}\}$ et $\pi(N) = |\mathcal{P}(N)|$. On sait que, pour N tendant vers l'infini, on a $\pi(N) \sim N/\ln N$.

Soit p un nombre premier. On pose $\mathcal{Q}(p) = \{n \in \mathbf{N} \mid p \text{ ne divise pas } n\}$ et $\mathcal{Q}(p,R) = \{n \leq R \mid p \text{ ne divise pas } n\}$. On a, avec la probabilité naturelle, $\mathbf{P}(\mathcal{Q}(p)) = 1 - \frac{1}{p}$ et, comme la notion de probabilité naturelle prolonge celle de densité, cela signifie que $\mathbf{P}_R(\mathcal{Q}(p,R)) = \dfrac{|\mathcal{Q}(p,R)|}{R+1}$ tend vers $1-\frac{1}{p}$ quand R tend vers l'infini, voir 6.9.

On considère alors, pour N fixé :

$$\mathcal{Q}(\sqrt{N},R) = \bigcap_{p\leq\sqrt{N}} \mathcal{Q}(p,R) = \{n \leq R \mid \forall p \leq \sqrt{N},\ p \not| n\}.$$

En vertu de 6.14, on a $\lim_{R\to+\infty} \dfrac{|\mathcal{Q}(\sqrt{N},R)|}{R+1} = \prod_{p\leq\sqrt{N}} 1-\frac{1}{p}$, donc

$$(*) \qquad |\mathcal{Q}(\sqrt{N},R)| \sim R \prod_{p\leq\sqrt{N}} 1-\frac{1}{p} \text{ quand } R \text{ tend vers } +\infty.$$

Par ailleurs, on a l'inclusion : $\mathcal{Q}(\sqrt{N},N) = \bigcap_{p\leq\sqrt{N}} \mathcal{Q}(p,N) \subset \mathcal{P}(N)$. En effet, si un entier n est dans l'intersection, d'abord il est $\leq N$ et ensuite, il n'est divisible par aucun premier $\leq \sqrt{N}$, donc *a fortiori* par aucun premier $\leq \sqrt{n}$, donc il est premier par Ératosthène. On a donc $P(N) \geq |\mathcal{Q}(\sqrt{N},N)|$.

Si l'on applique $(*)$ avec $R = N$, on obtient :

$$\pi(N) \geq |\mathcal{Q}(\sqrt{N}, N)| \sim N \prod_{p \leq \sqrt{N}} 1 - \frac{1}{p} := N\mu(\sqrt{N}).$$

C'est ici qu'apparaît le paradoxe : on a $\pi(N) \sim N/\ln N$ et, par Mertens, le produit $\mu(\sqrt{N})$ est équivalent à $2e^{-\gamma}/\ln N$, mais comme $2e^{-\gamma}$ est > 1, l'inégalité est dans le mauvais sens[35]. Par exemple, pour $N = 10^8$, on a $\pi(N) = 5761455$ mais $\mu(10^4) = 0,060885$, donc $\mu(10^4) \times 10^8 = 6088500$.

Essayons de comprendre ce phénomène. Bien sûr c'est l'application de $(*)$ qui est incorrecte car N, dans cette formule, est un entier fixé et en faisant $R = N$ on le fait tendre vers l'infini. Regardons d'un peu plus près la situation en prenant $N = 10000$, donc $\sqrt{N} = 100$. Pour dire qu'un nombre $n \leq 10000$ est premier il suffit de voir qu'il n'est multiple d'aucun nombre premier ≤ 100. La probabilité de ne pas être multiple de ces nombres premiers est alors $\mu = \mu(100) = \prod_{p \leq 100} 1 - \frac{1}{p}$, **mais** ce résultat (qui exprime l'indépendance des conditions "p ne divise pas n") repose sur le lemme chinois, qui requiert de regarder modulo le produit des nombres premiers ≤ 100, lequel est gigantesque, de l'ordre de $K = 2 \times 10^{37}$. Si l'on regarde sur les K premiers entiers le nombre de ceux qui ne sont pas multiples des $p \leq 100$, on obtient **exactement** μK comme ce qu'annonce la formule du produit. Mais ce qu'on voudrait en déduire c'est que parmi les $N = 10000$ premiers entiers, le nombre de ceux qui ne sont pas multiples d'un $p \leq 100$ est μN. On est en train de faire une statistique sur 10000 pour déterminer une proportion qui porte sur 2×10^{37}. Même la SOFRES n'oserait pas faire ça !

6.7 Des conjectures optimistes ?

Dans ce paragraphe, je cède à ma propension à l'optimisme en proposant des conjectures[36] *osées sur les questions étudiées ci-dessus. Mais, par les temps qui courent, un peu d'optimisme ne peut pas faire de mal ...*

On commence par rappeler quelques certitudes :

6.35 Rappel. *On considère des nombres premiers $p_1 < p_2 < \cdots < p_k$ et, pour chaque $i = 1, \ldots, k$, r_i classes a_{ij} distinctes modulo p_i. On appelle $X_{\underline{p},\underline{a}}$ l'ensemble des $n \in \mathbf{N}$ qui ne sont congrus à aucun des a_{ij} modulo aucun*

35. Au moins pour N grand car, pour N petit, elle peut être dans le sens attendu. Ainsi, pour $N = 100$ on a $P(100) = 25$ tandis que $\mu(10) = 0.2285714$ (très exactement $48/210 = 8/35$). De même $P(10000) = 1229$ alors que $\mu(100) = 0.12032$.

36. R. Hartshorne les qualifierait sans doute de conjectures à la Daniel, voir [21].

des p_i. En vertu de 6.14, on a $\mathbf{P}(X_{\underline{p},\underline{a}}) = \mu := \prod_{i=1}^{r}(1 - \frac{r_i}{p_i})$. Si on pose $Q = p_1 \cdots p_r$, on a $|X_{\underline{p},\underline{a}} \cap [0, Q]| = \mu Q$.

La question est de passer de la probabilité de l'ensemble $X := X_{\underline{p},\underline{a}}$ sur $\mathbf{N}$, voire de sa trace sur $[0, Q]$, qui sont connues de manière sûre, à celle de sa trace sur $[0, N]$ avec $N \ll Q$. Si la probabilité était la même, on aurait pour le cardinal de $X \cap [0, N]$ la valeur "attendue" μN, mais on a vu sur l'exemple des nombres premiers qu'elle est excessive. La conjecture proposée ci-dessous est en deux temps, le second plus osé encore que le premier. Elle consiste d'abord à dire que, pour N pas trop petit, la statistique sur $[0, N]$ reflète la probabilité, et propose ensuite une correction dont la seule justification est d'être celle constatée sur la probabilité d'être premier.

6.36 Conjecture. *On conserve les notations de 6.35. Soit N un entier et posons $X_N = X_{\underline{p},\underline{a}} \cap [0, N]$.*

1) Il existe une fonction $\chi(p)$ et une constante $\alpha(\chi) > 0$ telles que l'on ait, pour tout $N \geq \chi(p_k)$, $|X_N| \geq \alpha\mu N$.

2) On peut prendre $\chi(p) = p^2$ et $\alpha = e^\gamma/2$.

6.37 *Remarques.* 1) Ce qui suit est une tentative de justification du choix de la fonction χ et de la constante α, appuyée sur le cas des nombres premiers.

L'idée naturelle de prendre $\chi(p) = p$ ne fonctionne pas dans ce cas. En effet, prenons pour p_i tous les nombres premiers jusqu'à p_k, les r_i tous égaux à 1, les a_{ij} à 0 et $N = p_k$. Alors, X_N est l'ensemble des entiers $\leq p_k$ qui ne sont multiples d'aucun nombre premier $\leq p_k$, et il est donc réduit à $\{1\}$. Pour avoir un α universel, il faudrait qu'il vérifie $\alpha \leq \dfrac{1}{\mu p_k}$. Mais on a $\mu = \mu(p_k) = \displaystyle\prod_{p \leq p_k} 1 - \frac{1}{p}$, on sait par Mertens que $\mu(p_k)$ est équivalent à $\dfrac{e^{-\gamma}}{\ln p_k}$ donc μp_k est équivalent à $\dfrac{e^{-\gamma} p_k}{\ln p_k}$. Comme cette quantité tend vers l'infini avec p_k, l'inverse tend vers 0, donc il n'y a pas de borne inférieure pour α.

En revanche, si l'on prend $\chi(p) = p^2$, donc $N \geq p_k^2$, disons $N = p_k^2$, X_N contient au moins tous les nombres premiers compris entre p_k et p_k^2 qui sont en nombre $\pi(p_k^2) - \pi(p_k)$ et cette quantité est de l'ordre de $\dfrac{p_k^2}{2 \ln p_k}$. On a encore $\mu = \displaystyle\prod_{p \leq p_k} 1 - \frac{1}{p} \sim \frac{e^{-\gamma}}{\ln p_k}$ par Mertens. On a donc $|X_N| \geq \dfrac{p_k^2}{2 \ln p_k} = \mu N \dfrac{e^\gamma}{2}$. On voit qu'avec $\alpha \leq e^\gamma/2$ on obtient le résultat.

2) Dans le cas des nombres premiers de la forme $n^2 + n + 41$ ou de leurs généralisations, on retrouve les conjectures de Hardy-Littlewood en vertu de 3.26 (et il suffit de prendre $\chi(p) = p$).

3) Pour un exemple de correction de ce type, avec le facteur $\dfrac{e^\gamma}{2}$, voir le livre [29] de Tenenbaum et Mendès-France, p. 41.

7 Annexes 2 : quelques détails

7.1 Quelques cas faciles de Dirichlet

7.1.1 Dirichlet modulo 4

On commence par le cas $a = 4$ (donc $b = 1$ ou 3). Le cas $b = 3$ est élémentaire :

7.1 Théorème. *Il existe une infinité de nombres premiers congrus à* 3 *(ou à* -1*) modulo* 4*.*

Démonstration. On suppose qu'il n'y en a qu'un nombre fini $p_1, \ldots, p_r$ et on regarde $n = 2p_1 \cdots p_r + 1$. Comme les p_i sont impairs, $2p_1 \cdots p_r$ est congru à 2 modulo 4, donc n est congru à $3 \equiv -1$ modulo 4, de sorte tous ses diviseurs premiers ne peuvent être tous congrus à 1 modulo 4, sinon n lui-même serait congru à 1. Le nombre n admet donc un diviseur premier $p \equiv -1 \pmod 4$. Mais p est distinct de tous les p_i (sinon il diviserait 1), donc plus grand.

Le cas $b = 1$ nécessite de connaître le lemme suivant :

7.2 Lemme. *Soit p un nombre premier impair. Le nombre -1 est un carré modulo p si et seulement si on a $p \equiv 1 \pmod 4$.*

Démonstration. On sait que $\mathbf{Z}/p\mathbf{Z}$ est un corps et qu'il y a autant de carrés que de non carrés ($\neq 0$) modulo p et il y en a donc $(p-1)/2$. On associe les entiers non nuls modulo p par paires : a et $1/a$, qui sont distincts, sauf si $a = 1$ ou -1. Comme a et $1/a$ sont carrés en même temps, on voit que -1 est un carré si et seulement si les carrés sont en nombre pair, donc si $p - 1$ est multiple de 4.

On en déduit aussitôt :

7.3 Théorème. *Il existe une infinité de nombres premiers congrus à* 1 *modulo* 4*.*

Démonstration. On considère $(n!)^2 + 1$ et un de ses facteurs premiers p, qui est plus grand que n. Modulo p, -1 est le carré de $n!$, donc p est congru à 1

modulo 4 et on a gagné. On peut aussi raisonner par l'absurde en supposant qu'il n'y a qu'un nombre fini de tels nombres premiers $p_1, \ldots, p_r$ et considérer un diviseur premier de $(p_1 \cdots p_r)^2 + 1$.

7.4 *Remarque.* Si l'on est dans l'idée d'avoir une formule, le cas congru à 1 est plus satisfaisant : il y a vraiment une formule $(n!)^2 + 1$ dont tous les facteurs donnent des nombres premiers de la bonne forme.

7.1.2 Le "petit Dirichlet"

Dans la veine précédente, on a aussi :

7.5 Théorème. *Soit n un entier positif. Il existe une infinité de nombres premiers congrus à 1 modulo n.*

Démonstration. Cette fois, ce qu'on utilise c'est que p est congru à 1 modulo n si et seulement si le polynôme cyclotomique Φ_n (ou encore $X^n - 1$) est scindé sur $\mathbf{F}_p$:

7.6 Lemme. *Soit n un entier positif et p un nombre premier ne divisant pas n. Alors, on a $p \equiv 1 \pmod{n}$ si et seulement si Φ_n admet une racine dans $\mathbf{F}_p$ (donc est scindé).*

Démonstration. En effet, dire que $\mathbf{F}_p$ contient une racine de Φ_n signifie qu'il contient une racine primitive n-ième de l'unité, donc un élément d'ordre n pour la multiplication. Cela impose que n divise le cardinal de $\mathbf{F}_p^*$ qui vaut $p - 1$ et la réciproque est vraie car ce groupe est cyclique [37].

On peut alors prouver le théorème. On rappelle que Φ_n est unitaire et qu'on a, pour $n \geq 2$, $\Phi_n(0) = 1$. On considère $\Phi_n(k!)$ pour $k \in \mathbf{N}$. Lorsque k tend vers $+\infty$, cette quantité tend vers $+\infty$, donc, pour $k \geq k_0$, on a $\Phi_n(k!) \neq \pm 1$. Soit k un tel nombre. Si p est un facteur premier de $\Phi_n(k!)$, on a $\Phi_n(k!) \equiv 0 \pmod{p}$, ce qui, par le lemme, assure que p est congru à 1 modulo n. Mais on a :

$$\Phi_n(k!) = (k!)^{\varphi(n)} + \sum_{i=1}^{\varphi(n)-1} a_i (k!)^i + 1$$

et on voit qu'aucun nombre premier plus petit que k ne divise ce nombre (sinon il diviserait 1). Cela montre que p est plus grand que k et comme cela vaut pour tout $k \geq k_0$, il y a une infinité de p premiers congrus à 1 modulo n.

37. Si l'on est savant, on peut aussi dire que le groupe de Galois du corps de décomposition de Φ_n sur $\mathbf{F}_p$ est engendré par le Frobenius $F(\zeta) = \zeta^p$ et qu'il est égal à l'identité (de sorte que l'extension est triviale) si p est congru à 1 modulo n.

7.1.3 Modulo 3

La congruence à 1 relevant du petit Dirichlet, il reste celle relative à -1 :

7.7 Théorème. *Il y a une infinité de nombres premiers congrus à* -1 *modulo* 3.

Démonstration. Supposons qu'il n'y en ait qu'un nombre fini $p_1, \ldots, p_r$. On considère le nombre $N := 3p_1 \cdots p_r - 1$, qui est plus grand que 3. Ses facteurs premiers ne peuvent tous être congrus à 1 modulo 3 (sinon N le serait aussi). Il admet donc un facteur premier $p \equiv -1 \pmod 3$, qui est distinct des p_i.

7.1.4 Les congruences autres que 1

La méthode précédente montre plus généralement :

7.8 Proposition. *Soit* n *un entier* > 3. *Il existe une infinité de nombres premiers* p *qui ne sont pas congrus à* 1 *modulo* n.

Démonstration. On suppose qu'il n'y a qu'un nombre fini de p_i qui ne sont ni diviseurs de n ni congrus à 1 modulo n. On considère $p_1 \cdots p_r + 1$. Il ne peut être congru à 1 modulo n. S'il n'est pas multiple de n, l'un de ses facteurs n'est pas congru à 1. S'il est multiple de n on considère $p_1 \cdots p_r + 3$.

Le lecteur résoudra sans peine l'exercice suivant :

7.9 *Exercice.* Montrer qu'il y a une infinité de nombres premiers congrus à 2 ou -2 modulo 5 (considérer $5p_1 \cdots p_r + 2$ par exemple).

En revanche, il se cassera peut-être les dents, même pour $n = 5$, sur :

7.10 Théorème. *Soit* n *un entier* ≥ 2. *Il y a une infinité de nombres premiers congrus à* -1 *modulo* n.

Attention, si on regarde $p_1 \cdots p_r + 3$ avec r pair[38], il est congru à -1 modulo 5, mais il peut avoir des facteurs congrus à 2 ou -2. Par exemple, pour $1 \leq n \leq 10$, $19 \times 29 \times 59 \times 79 + n$ n'a aucun facteur premier congru à -1 modulo 5. Dirichlet n'est pas un théorème trivial !

7.2 La loi de réciprocité quadratique expliquée aux enfants

7.2.1 Le cas $n = 5$

7.11 Proposition. *Soit* p *un nombre premier* $\neq 2, 5$. *Alors,* 5 *est un carré modulo* p *si et seulement si* p *est un carré modulo* 5.

38. Même difficulté avec $5p_1 \cdots p_r - 1$, par exemple $5 \times 19 \times 29 \times 59 \times 79 - 1 = 2 \times 97 \times 66191$.

Démonstration. Rappelons que, quand on travaille modulo p, on a le petit théorème de Fermat : $x^{p-1} \equiv 1 \pmod{p}$ si x est premier à p. Autrement dit, les éléments de $\mathbf{F}_p^*$ sont d'ordre diviseur de $p-1$ (c'est un groupe cyclique d'ordre $p-1$). De l'autre côté, modulo 5, on sait que les carrés sont ± 1. Mais, dire qu'on a $p \equiv 1 \pmod{5}$ c'est dire que 5 divise $p-1$, donc qu'il y a un élément d'ordre 5 (i.e. une racine cinquième primitive de 1) dans $\mathbf{F}_p$. Si 5 divise $p+1$, il divise p^2-1 et il faut aller chercher la racine cinquième dans $\mathbf{F}_{p^2}$. On regarde donc les racines cinquièmes de l'unité modulo p. Elles sont données par $\zeta^5 - 1 = 0$ et, si l'on écarte 1, par $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$. Pour résoudre cette équation, une vieille ruse, qui marche dans le cas des polynômes "réciproques", consiste à poser $\alpha = \zeta + \zeta^{-1}$, donc $\zeta^2 - \alpha\zeta + 1 = 0$. On se ramène à résoudre $\alpha^2 - \alpha - 1 = 0$ qui donne $\alpha = \dfrac{1 \pm \sqrt{5}}{2}$. On voit que 5 est un carré modulo p si et seulement α est dans $\mathbf{F}_p$, donc si ζ est de degré ≤ 2 sur $\mathbf{F}_p$, donc dans $\mathbf{F}_p$ ou $\mathbf{F}_{p^2}$, donc si 5 divise $p-1$ ou $p+1$. Inversement, si $p \equiv \pm 1 \pmod{5}$ on a un élément ζ d'ordre 5 dans $\mathbf{F}_{p^2}$ et $\zeta^p = \zeta$ ou ζ^{-1}. Il en résulte que $\zeta + \zeta^{-1}$ est invariant par Frobenius, donc est dans $\mathbf{F}_p$, de sorte que 5 est un carré modulo p.

7.2.2 Le cas général

7.12 Théorème. *Soient p et n deux nombres premiers impairs.*

• *Si p ou n est congru à 1 modulo 4, p est un carré modulo n si et seulement si n est un carré modulo p.*

• *Si p et n sont tous deux congrus à 3 modulo 4, p est un carré modulo n si et seulement si n n'est pas un carré modulo p.*

Démonstration. Attention, le raisonnement qui suit est sans doute un peu rapide. Le lecteur scrupuleux pourra consulter [20].

On considère $\mathbf{F}_p$ et le corps de décomposition $L = D_{\mathbf{F}_p}(X^n - 1)$, engendré par une racine primitive n-ième de l'unité ζ. Comme le polynôme cyclotomique Φ_n universel est de degré $n-1$ (c'est $X^{n-1} + X^{n-2} + \cdots + X + 1$) il a en tous cas une racine dans une extension de degré $n-1$ de $\mathbf{F}_p$. On va traduire de deux manières le fait que cette racine habite dans l'extension de degré moitié, $\mathbf{F}_q$, avec $q = p^{(n-1)/2}$.

• Modulo les carrés, le discriminant Δ de Φ_n est ϵn avec $\epsilon = \pm 1$, précisément, c'est n si $n \equiv 1 \pmod{4}$ et $-n$ si $n \equiv -1 \pmod{4}$) et on sait qu'on a toujours $\mathbf{F}_p \subset \mathbf{F}_p(\sqrt{\Delta}) \subset \mathbf{F}_p(\zeta)$. Si $\Delta = \epsilon n$ est un carré de $\mathbf{F}_p$, le degré de l'extension est divisé par 2 :

7.13 Lemme. *Soit $\delta = \sqrt{\Delta} = \displaystyle\prod_{1 \leq i < j \leq n} \zeta^i - \zeta^j$ la racine du discriminant.*

Alors, ζ vérifie une équation de degré $(n-1)/2$ à coefficients dans $K(\delta)$.

Mais dire que ϵn est un carré modulo p c'est dire que n est un carré[39] modulo p, sauf si n et p sont tous deux congrus à 3 modulo 4.

• Rappelons que le groupe de Galois de L sur $\mathbf{F}_p$ est le sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$ (c'est une extension cyclotomique), engendré par p (vu comme $\zeta \mapsto \zeta^p$, l'automorphisme de Frobenius). Dire que L est inclus dans $\mathbf{F}_q$, avec $q = p^{(n-1)/2}$, signifie que le degré d de L divise $(n-1)/2$ donc que son groupe de Galois est d'ordre diviseur de $(n-1)/2$ autrement dit, que p vérifie $p^{(n-1)/2} \equiv 1 \pmod{n}$. Mais cela signifie que p est un carré modulo n (c'est le symbole de Legendre). On a donc montré l'équivalence !

7.2.3 $-d$ carré modulo p ou p carré modulo d ?

Le résultat suivant a été utilisé plusieurs fois dans le texte :

7.14 Proposition. *Soient d et p des nombres premiers impairs, avec $d \equiv 3 \pmod 4$. Alors $-d$ est un carré modulo p si et seulement si p est un carré modulo d. En termes de symboles de Legendre, on a $\left(\frac{-d}{p}\right) = \left(\frac{p}{d}\right)$.*

Démonstration. Il suffit d'appliquer la loi de réciprocité quadratique en distinguant selon les congruences de p modulo 4.

7.15 *Remarques.* Dans les remarques qui suivent on suppose d sans facteur carré.

1) Attention l'assertion précédente est fausse si d n'est pas premier. Par exemple, pour $d = 35$ et $p = 17$, $-35 \equiv -1 \pmod{17}$ est un carré, mais 17 n'est pas un carré modulo 35.

2) Précisément, si l'on écrit $d = d_1 \cdots d_r$ avec les d_i premiers distincts, l'anneau $\mathbf{Z}/d\mathbf{Z}$ est le produit des anneaux $\mathbf{Z}/d_i\mathbf{Z}$ et un entier x est un carré modulo d si et seulement si il l'est modulo chacun des facteurs. C'est ce qui explique que 17 qui n'est un carré ni modulo 3, ni modulo 5, n'est pas un carré modulo 35.

3) On peut toutefois conserver le résultat sur les symboles de Legendre en remplaçant $\left(\frac{p}{d}\right)$ par le symbole de Jacobi, noté de la même manière, et défini, si $d = d_1 \cdots d_r$ comme ci-dessus, par la formule $\left(\frac{p}{d}\right) = \left(\frac{p}{d_1}\right) \times \cdots \times \left(\frac{p}{d_r}\right)$. Dans l'exemple, les deux symboles de Legendre de 17 relatifs à 3 et 5 valant -1, leur produit est bien égal à 1.

39. On utilise ici le fait que -1 est un carré modulo p si $p \equiv 1 \pmod 4$.

7.3 Cornacchia pour la factorialité

On reprend la preuve de 2.9. On utilise l'algorithme de Cornacchia (1908, voir [6]) qui permet de trouver les points de petite norme dans un réseau.

On considère un nombre premier impair p tel que -163 est un carré [40] modulo p, et on choisit une racine $u \in \mathbf{N}$ de $x^2 + x + 41 \equiv 0 \pmod{p}$, avec $u < p$.

L'idée est d'effectuer l'algorithme d'Euclide avec p et u. On pose $r_0 = p$ et $r_1 = u$ puis $r_0 = r_1 q_1 + r_2$ avec $0 \leq r_2 < r_1$, $r_1 = r_2 q_2 + r_3$ avec $0 \leq r_3 < r_2$, etc. $r_{n-1} = r_n q_n + r_{n+1}$ avec $0 \leq r_{n+1} < r_n$.

On sait que l'algorithme d'Euclide peut être utilisé pour trouver les coefficients de Bézout relatifs à p et u. Précisément, on va écrire, pour tout $n \geq 0$: $r_n = a_n p + b_n u$ (relation $(*)$). Pour cela, on pose $a_0 = 1$, $b_0 = 0$, $a_1 = 0$, $b_1 = 1$ et on calcule les suivants grâce aux deux relations de récurrence [41] :

$$(**) \qquad a_{n+1} = a_{n-1} - q_n a_n \quad \text{et} \quad b_{n+1} = b_{n-1} - q_n b_n.$$

On sait que les r_n décroissent et que le dernier reste non nul est le *pgcd* de p et u, c'est-à-dire 1. Une première remarque est la suivante :

7.16 Lemme. *Pour tout $n \geq 0$, $r_n^2 + r_n b_n + 41\, b_n^2$ est multiple de p.*

Démonstration. C'est évident avec la relation $r_n = a_n p + b_n u$, c'est-à-dire $r_n \equiv u b_n \pmod{p}$, et le fait que $u^2 + u + 41 \equiv 0 \pmod{p}$.

Le lemme suivant sera utile :

7.17 Lemme. *Avec les notations précédentes, on a les résultats suivants :*
1) Pour tout $k \geq 0$, b_{2k} est ≤ 0 et $b_{2k+1} \geq 0$.
2) On a $|b_{n+1}| = q_n |b_n| + |b_{n-1}|$. La suite $|b_n|$ est croissante.
3) Pour tout $n \geq 0$, on a $a_n b_{n+1} - a_{n+1} b_n = (-1)^n$.
4) Pour tout $n \geq 0$ on a $b_{n+1} r_n - b_n r_{n+1} = (-1)^n p$.
5) Pour tout $n \geq 0$ on a $|b_{n+1}| r_n + |b_n| r_{n+1} = p$.
6) Les nombres r_n et b_n sont premiers entre eux.

Démonstration. (du lemme 7.17) Le point 1) est immédiat par récurrence sur n grâce à la deuxième relation de $(**)$. L'égalité du point 2) est claire en distinguant selon la parité de n et, comme q_n est ≥ 1, on a bien la croissance de $|b_n|$. Le point 3) s'établit par récurrence. En effet, il est clair pour $n = 0$ et pour passer de n à $n+1$ il suffit d'écrire b_{n+2} et a_{n+2} avec les relations $(**)$.

40. Rappelons que c'est équivalent à dire que p est un carré modulo 163. Comme il y a 81 carrés modulo 163, il y a pléthore de tels p par Dirichlet.

41. On comprend facilement que les b_n vérifient la même relation de récurrence que les r_n si l'on écrit $r_n \equiv b_n u \pmod{p}$.

Le point 4) est alors évident en écrivant r_n et r_{n+1} grâce à $(*)$ et le point 5) n'est que la traduction de 4) en distinguant les signes selon la parité de n. Enfin, comme r_n est plus petit que p, 6) résulte de 4).

Voici maintenant le résultat inspiré de Cornacchia :

7.18 Théorème. *Il existe un entier n tel que l'on ait :*

$$s_n := r_n^2 + r_n b_n + 41\, b_n^2 \leq \frac{2\sqrt{41}+1}{\sqrt{2}}\, p \simeq 9.76\, p.$$

Pour cet entier n, on a $r_n^2 + r_n b_n + 41\, b_n^2 = p$.

Démonstration. Commençons par une remarque sur les normes de l'espace euclidien :

7.19 Lemme. *Soit $(x, y) \in \mathbf{R}^2$. On a l'inégalité $0 \leq x^2 + xy + 41y^2 \leq \dfrac{2\sqrt{41}+1}{2\sqrt{41}}\,(x^2 + 41y^2)$.*

Démonstration. (de 7.19) On pose $r^2 = x^2 + 41y^2$, puis $x = r\cos\theta$ et $y = \dfrac{r\sin\theta}{\sqrt{41}}$. On a alors $|\sin\theta\,\cos\theta| = \frac{1}{2}|\sin 2\theta| \leq \frac{1}{2}$ et le résultat s'ensuit.

Pour montrer le théorème, il suffit maintenant de prouver l'inégalité :

$$(***) \qquad r_n^2 + 41 b_n^2 \leq \sqrt{2}\,\sqrt{41}\, p.$$

En vertu de 7.17.2, la suite $41|b_n b_{n+1}|$ est croissante à partir de 0, tandis que $r_n r_{n+1}$ décroît et finit par valoir 0. Il existe donc un plus petit entier n tel que $41|b_n b_{n+1}| \geq r_n r_{n+1}$ et on a $41|b_n b_{n-1}| < r_n r_{n-1}$. On va montrer que l'inégalité $(***)$ est valable pour $n-1$, n ou $n+1$. On commence par opérer un changement de variables en posant, pour tout n, $r_n = x_n\sqrt{p}\sqrt{\sqrt{41}}$ et $|b_n| = \dfrac{y_n\sqrt{p}}{\sqrt{\sqrt{41}}}$. On considère les vecteurs $V_n = (x_n, y_n)$ et $W_n = (y_n, x_n)$. Si $(x|y)$ désigne le produit scalaire usuel de $\mathbf{R}^2$ et $\|(x, y)\|$ la norme associée, la relation 5) de 7.17 se traduit par $(V_n|W_{n-1}) = (V_n|W_{n+1}) = 1$ et on a aussi $r_n^2 + 41b_n^2 = (x_n^2 + y_n^2)\sqrt{41}\,p = \|V_n\|^2\sqrt{41}\,p = \|W_n\|^2\sqrt{41}\,p$. Il s'agit donc de montrer que l'un des vecteurs W_{n-1}, V_n, W_{n+1} est de norme $\leq \sqrt{\sqrt{2}}$. Pour cela on note que tous ces vecteurs sont strictement dans le premier quadrant de $\mathbf{R}^2$ et que, de plus, si φ_n est l'angle de Ox avec V_n et ψ_n celui de Ox avec W_n, on a $0 < \psi_{n+1} < \varphi_n < \psi_{n-1} < \pi/2$. En effet, cela résulte de l'inégalité sur les tangentes $\dfrac{x_{n+1}}{y_{n+1}} \leq \dfrac{y_n}{x_n} \leq \dfrac{x_{n-1}}{y_{n-1}}$ qui découle des inégalités $41|b_n b_{n+1}| \geq r_n r_{n+1}$ et $41|b_n b_{n-1}| < r_n r_{n-1}$.

On désigne par θ_n l'angle des vecteurs V_n et W_{n-1}, de sorte qu'on a $(V_n|W_{n-1}) = \|V_n\|\,\|W_{n-1}\|\cos\theta_n = 1$ et $(V_n|W_{n+1}) = \|V_n\|\,\|W_{n+1}\|\cos\theta_{n+1} = 1$. Mais, vu la position des vecteurs, on a $\theta_n + \theta_{n+1} = \psi_{n-1} - \psi_{n+1} < \pi/2$. Il en résulte que θ_n ou θ_{n+1} est $< \pi/4$, donc que son cosinus est $> 1/\sqrt{2}$, ce qui montre que l'un des produits $\|V_n\|\,\|W_{n-1}\|$ ou $\|V_n\|\,\|W_{n+1}\|$ est $< \sqrt{2}$, donc que l'une des trois normes est $< \sqrt{\sqrt{2}}$.

Il reste à prouver qu'on a $r_n^2 + r_n b_n + 41\,b_n^2 = p$. Sinon, on a $r_n^2 + r_n b_n + 41\,b_n^2 = z_n\overline{z_n} = kp$ avec $1 < k < 10$ et $z_n = r_n + b_n\alpha$. Soit l un facteur premier de k. Comme on a $l \leq 7$, on a vu en 2.7 que l est premier dans $\mathbf{Z}[\alpha]$ donc divise z_n ou $\overline{z_n}$, donc les deux. Comme l est réel, il divise r_n et b_n, ce qui contredit 7.17.6.

7.20 *Exemple.* On considère le nombre premier $p = 4090937 = r_0$. Modulo p, le polynôme $x^2 + x + 41$ a la racine $u = 1844478 = r_1$. Si on applique l'algorithme, on a successivement $q_1 = 2$, d'où $b_2 = -2$, $r_2 = 401981$, on vérifie qu'on a $r_2^2 + r_2 b_2 + 41 b_2^2 = k_2 p$ avec $k_2 = 39499$, puis $q_2 = 4$, donc $b_3 = 9$, $r_3 = 236554$, $k_3 = 13679$, $b_4 = -11$, $r_4 = 165427$, $k_4 = 6689$, $b_5 = 20$, $r_5 = 71127$, $k_5 = 1237$, $b_6 = -51$, $r_6 = 23173$, $k_6 = 131$ et enfin $b_7 = 173$, $r_7 = 1608$, $k_7 = 1$. Le nombre premier p est donc bien une norme : $4090937 = 1608^2 + 173 \times 1608 + 41 \times 173^2$.

Le même raisonnement que ci-dessus donne le théorème général suivant :

7.21 Théorème. *Soit c un nombre impair positif et posons $d = 4c - 1$. On suppose que $-d$ est un carré modulo un nombre premier p. Alors, il existe des entiers r et b tel que l'on ait $r^2 + rb + cb^2 = kp$ avec $k \leq \dfrac{2\sqrt{c}+1}{\sqrt{2}} = \dfrac{\sqrt{d+1}+1}{\sqrt{2}}$.*

7.4 Compléments sur les normes

7.4.1 Les deux formes de normes

7.22 Proposition. *Soit $n \in \mathbf{N}$.*

1) Si n est de la forme $n = a^2 + 163b^2$, avec $a, b \in \mathbf{N}$, il est de la forme $n = x^2 + xy + 41y^2$ avec $x, y \in \mathbf{Z}$.

2) Inversement, si n est de la forme $n = x^2 + xy + 41y^2$ avec $x, y \in \mathbf{Z}$, et y pair, il est de la forme $a^2 + 163b^2$.

3) Si p est premier et s'il est de la forme $x^2 + xy + 41y^2$ avec y impair (par exemple s'il est de la forme $n^2 + n + 41$!), il n'est pas de la forme $a^2 + 163b^2$.

Démonstration. 1) Supposons $n = a^2+163b^2 = N(a+ib\sqrt{163})$ avec $a, b \in \mathbf{N}$. Comme on a $i\sqrt{163} = 2\alpha - 1$, on en déduit $n = N(a-b+2b\alpha) = (a-b)^2 + 2b(a-b) + 41(2b)^2$, d'où le résultat.

2) Il suffit de poser $b = |y|/2$ et $a = |x + \frac{y}{2}|$.

3) Si p est premier et $p = x^2 + xy + 41y^2$, on a $p = N(z)$ avec $z = x + y\alpha$ et z est premier dans A_d. Si $p = a^2+163b^2$, $p = N(w)$ avec $w = a+bi\sqrt{163} = a - b + 2b\alpha$ et w est premier aussi. On a donc $z\overline{z} = w\overline{w}$. Vu l'unicité de la décomposition en facteurs premiers dans A_d, cela impose que z est associé (donc égal ou opposé) à w ou $\overline{w}$. Il en résulte que y est pair.

7.23 *Remarques.* 1) Attention, dans le premier point, on ne peut pas supposer $x, y \in \mathbf{N}$. Par exemple, $653 = 1 + 4 \times 163$ s'écrit $(-1)^2 + (-1) \times 4 + 41 \times (4^2)$ mais n'est pas de la forme $x^2 + xy + 41y^2$ avec $x, y \in \mathbf{N}$ (y ne peut être que $1, 2, 3$ et on vérifie que c'est impossible).

2) Si n n'est pas premier, et si $n = x^2+xy+41y^2$ avec y impair, il peut très bien être aussi de la forme a^2+163b^2. Par exemple, $4859 = 50^2+50\times7+41\times7^2$ s'écrit aussi $28^2 + 163 \times 5^2$. En fait, 4859 a une autre écriture avec y pair : $4859 = 23^2 + 23 \times 10 + 41 \times 10^2$. L'explication de ce phénomène est la suivante. Si p est premier dans $\mathbf{Z}$ et s'il ne l'est plus dans A_d, sa seule écriture comme norme est $p = z\overline{z}$, au signe près. Ainsi $43 = 1 + 1 + 41 = z\overline{z}$, avec $z = 1 + \alpha$. De même $113 = 8^2 + 8 + 41 = w\overline{w}$ avec $w = 8 + \alpha$. Mais, dans le cas d'un nombre composé, par exemple $4859 = 43 \times 113$, on peut écrire $4859 = N(z\overline{w}) = N(50 + 7\alpha)$ ou $4859 = N(\overline{z}\overline{w}) = N(-23 - 10\alpha)$ d'où les deux écritures ci-dessus.

7.4.2 Nombres eulériens ou normes ?

7.24 *Remarques.* 1) Les normes sont les $m^2 + mn + 41n^2$, pas seulement les $n^2 + n + 41$. D'ailleurs, les $n^2 + n + 41$ ne sont pas multiplicatifs :

$$(n^2+n+41)(m^2+m+41) = (mn-41)^2+(mn-41)(m+n+1)+41(m+n+1)^2.$$

2) En particulier, les nombres premiers qui ne le restent pas dans A (c'est-à-dire ceux qui sont des carrés modulo 163) sont des normes, mais ne sont pas tous de la forme n^2+n+41. Par exemple $167 = N(1+2\alpha) = 1+2+4\times41$ n'est pas de la forme $n^2 + n + 41$.

Cependant, on a cette propriété pour les p petits :

7.25 Lemme. *Soit p un nombre premier impair, $p < 163$. Alors, p est un carré modulo* 163 *si et seulement si p est de la forme n^2+n+41, c'est-à-dire si $p =$* 41, 43, 47, 53, 61, 71, 83, 97, 113, 131 *ou* 151.

Démonstration. Si p est un carré modulo 163, c'est une norme. On a donc $p = n^2 + mn + 41m^2$. Mais, comme p est < 163, on a nécessairement $m = 1$. (Écrire $n^2 + mn + 41m^2 = (n + \frac{m}{2})^2 + \frac{163m^2}{4}$ permet d'écarter les cas $|m| \geq 2$ et $m = -1$ est justiciable de 1.1.)

7.26 *Remarques.* 1) Même si les nombres premiers qui sont des normes ne sont pas tous eulériens, on vérifie que, pour tous les carrés a^2 modulo 163, il y a des n tels que $n^2 + n + 41$ soit premier et congru à a^2 (le carré le plus difficile à obtenir est 133 atteint pour $n = 447$ et $n^2 + n + 41 = 200297$).

2) On peut se demander si tout nombre de la forme $x^2 + x + 41$ admet un diviseur premier de la même forme. Il n'en est rien : le nombre $249^2 + 249 + 41 = 167 \times 373$ a deux facteurs premiers qui sont des normes, mais ne sont pas eulériens.

7.5 Anneaux factoriels et séries de nombres premiers

Le théorème [42] suivant fait le bilan des liens entre les deux notions.

7.27 Théorème. *Soit c un entier ≥ 2 et posons $d = 4c - 1$ ($d \geq 7$). Les entiers de la forme $n^2 + n + c$ sont tous premiers pour $n = 0, 1, \ldots, c-2$ si et seulement si l'anneau* [43] $\mathbf{Z}[\alpha]$ *(avec $\alpha = \dfrac{1 + i\sqrt{d}}{2}$) est factoriel, c'est-à-dire si $d = 7, 11, 19, 43, 67$ ou 163 (autrement dit, $c = 2, 3, 5, 11, 17$ ou 41).*

7.28 *Remarque.* 1) Pour $d = 7$ on trouve seulement 2, pour $d = 11$ on a 3 et 5, pour 19 on a $5, 7, 11$ et 17, toujours avec la règle d'ajouter des nombres pairs croissants, pour $d = 43$, on a les $n^2 + n + 11$ et on trouve 11, 13, 17, 23, 31, 41, 53, 67, 83, 101, pour $d = 67$ ce sont les $n^2 + n + 17$, et on trouve 17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127, 149, 173, 199, 227, 257.

2) On vérifie que tous les nombres premiers ≤ 100 sont de la forme $n^2 + n + \frac{d+1}{4}$ avec $d = 7, 11, 19, 47, 67$ ou 163. En revanche, 103 n'est pas de cette forme.

Démonstration. La preuve, dans le cas où l'anneau est factoriel, est analogue à celle vue pour $c = 41$. Inversement, supposons qu'on a la série de nombres premiers et montrons que $A := \mathbf{Z}[\alpha]$ est factoriel. On note d'abord que l'hypothèse assure que les $n^2 + n + c$ sont premiers pour $0 \leq n \leq c-2$, mais aussi pour $-c+1 \leq n \leq c-2$, ainsi que les $n^2 - n + c$ pour $-c+2 \leq n \leq c-1$ (voir 1.1). Par ailleurs comme les cas $d = 7$ ou 11 donnent des anneaux principaux, on peut supposer $d \geq 15$.

42. Ce résultat est dû à Rabinowitsch, voir [22].

43. Qui est l'anneau des entiers du corps quadratique $\mathbf{Q}(i\sqrt{d})$.

Comme l'anneau A est un anneau de Dedekind, il suffit de montrer qu'il est factoriel et même seulement de prouver le lemme d'Euclide (voir [19]). Il suffit même, voir *loc. cit.* prop. 5.6, de prouver que tout nombre premier de $\mathbf{Z}$, qui reste irréductible dans A (c'est-à-dire qui n'est pas une norme) est encore premier dans A (c'est-à-dire que l'idéal pA est premier).

Soit donc p un nombre premier de $\mathbf{Z}$ qui n'est pas une norme dans A. Dire que l'idéal pA n'est pas premier signifie qu'il existe un entier $\lambda > 1$ tel que λp soit la norme d'un élément $z \in A$, $z \notin \mathbf{Z}$ (voir *loc. cit.* prop. 5.9), et on peut même supposer $\lambda < \sqrt{\dfrac{d}{3}}$ (*loc. cit.* prop. 5.10).

Il suffit alors de montrer que, pour tout $p < \sqrt{\dfrac{d}{3}}$, l'idéal pA est premier (voir *loc. cit.* 5.2.3). On est ramené à montrer le lemme suivant :

7.29 Lemme. *Soit z un élément de A, $z \notin \mathbf{Z}$, tel que $N(z) < \dfrac{d}{3}\cdot$ Alors $N(z)$ est un nombre premier.*

Démonstration. Posons $z = x + y\alpha$. On a :

$$N(z) = x^2 + xy + \frac{d+1}{4}y^2 = \Big(x + \frac{y}{2}\Big)^2 + d\,\frac{y^2}{4}.$$

Comme $N(z)$ est $< d/3$ et que z n'est pas entier, cela impose $|y| = 1$. On a alors $x^2 \pm x + \frac{d+1}{4} - \frac{d}{3} < 0$, ce qui implique que x est entre les racines du trinôme. Le discriminant est $d/3$ et on a donc $\dfrac{-1-\sqrt{d/3}}{2} < x < \dfrac{1+\sqrt{d/3}}{2}\cdot$ Comme d est ≥ 15, on vérifie que cela impose $-c+2 \leq x \leq c-2$. Mais alors $x^2 \pm x + \frac{d+1}{4}$ est premier par hypothèse.

7.6 Majorer la somme des inverses des nombres premiers

7.6.1 Avec le théorème des nombres premiers

Si l'on admet le théorème des nombres premiers (le nombre $\pi(x)$ de nombres premiers $\leq x$ est équivalent à $x/\ln x$) et son corollaire (le n-ième nombre premier p_n est équivalent à $n \ln n$), on montre le théorème suivant :

7.30 Théorème. *La somme $\displaystyle\sum_{p \leq x} \frac{1}{p}$, étendue aux nombres premiers, est équivalente à $\ln(\ln x)$.*

Démonstration. Posons $N = \pi(x)$. On a donc $S(x) := \sum_{p \leq x} \frac{1}{p} = S_N := \frac{1}{p_1} + \cdots + \frac{1}{p_n} + \cdots + \frac{1}{p_N}$. Comme p_n est équivalent à $n \ln n$ et que la série des $1/p_n$ diverge, S_N est équivalent à $\sum_{n=2}^{N} \frac{1}{n \ln n}$ (c'est un lemme du type Césaro). La comparaison avec l'intégrale montre alors que S_N est aussi équivalent à $I_N := \int_2^N \frac{dt}{t \ln t}$ qui se calcule avec le changement de variables $u = \ln t$: $I_N = \ln(\ln N) - \ln(\ln 2)$. On en déduit que S_N est équivalent à $\ln(\ln N)$. Mais, comme $N = \pi(x)$ est équivalent à $x/\ln x$, on a en définitive $S(x) \sim \ln(\ln x)$.

7.6.2 Avec Mertens

On sait, par Mertens, qu'on a $\prod_{p \leq N} 1 - \frac{1}{p} \sim \frac{e^{-\gamma}}{\ln N}$. En prenant les logarithmes on a donc $\sum_{p \leq N} \ln(1 - \frac{1}{p}) \sim -\ln \ln N$ et donc (toujours une variante de Cesaro), $-\sum_{p \leq N} \frac{1}{p} \sim -\ln \ln N$.

7.6.3 Variante élémentaire

Le but de ce paragraphe est de montrer une version très édulcorée du théorème précédent, mais élémentaire, et suffisante pour montrer 3.17.

7.31 Théorème. *Soit a un entier ≥ 2 et N un entier $> a$. On a l'inégalité :*

$$\sum_{p \leq N} \frac{1}{p} \leq \frac{\varphi(a)}{a} \ln N + \sum_{p \leq a} \frac{1}{p} + 2 + \ln a.$$

(Le symbole p désigne un nombre premier et $\varphi(a)$ est l'indicatrice d'Euler.)

En particulier on a, pour $N > 30$:

$$\sum_{p \leq N} \frac{1}{p} \leq \frac{4}{15} \ln N + 7.$$

Démonstration. Rappelons l'encadrement classique, pour x réel > 0 :

$$\ln x \leq \sum_{1 \leq n \leq x} \frac{1}{n} \leq 1 + \ln x.$$

On commence par un lemme sur les congruences.

7.32 Lemme. *Soit a un entier ≥ 2, B une partie de $\mathbf{Z}/a\mathbf{Z}$, de cardinal b et soit N un entier $> a$. On désigne par $\overline{n}$ la classe de n modulo a (prise entre 1 et a). On a l'inégalité :*

$$\sum_{1\leq n\leq N,\, \overline{n}\in B} \frac{1}{n} \leq \frac{b}{a}\,\ln N + 2 + \ln a.$$

Démonstration. On pose $B = \{\alpha_1, \ldots, \alpha_b\}$. Pour $n > a$, $n \equiv \alpha_i \pmod a$, on écrit $n = \alpha_i + ka$ avec $1 \leq k \leq n/a$ et on a $\dfrac{1}{n} = \dfrac{1}{\alpha_i + ka} \leq \dfrac{1}{ka}$. On en déduit que la somme des $1/n$ pour $n > a$, $\overline{n} \in B$ et $n \leq N$ est $\leq \dfrac{b}{a}\displaystyle\sum_k \frac{1}{k}$ avec $1 \leq k \leq N/a$, donc $\leq \dfrac{b}{a}(\ln N - \ln a + 1)$. Comme la somme jusque a est $\leq \ln a + 1$, on a le résultat.

On peut alors prouver le théorème. En effet, dans la somme des $1/p$ il y a d'abord ceux qui correspondent à $p \leq a$, que l'on a fait apparaître, puis les autres. Ceux-là, modulo a, sont inversibles, donc leurs classes sont en nombre $\leq \varphi(a)$, et on peut appliquer le lemme.

Les valeurs numériques, pour $a = 30$, sont les suivantes : $\varphi(30) = 8$, $\ln 30 \leq 3,41$ et $\sum_{p\leq 30} 1/p \leq 1,54$. On en déduit la majoration annoncée.

7.33 Corollaire. *Pour N assez grand, on a l'inégalité :*

$$\sum_{p\leq N} \frac{1}{p} \leq \frac{2}{7}\ln N.$$

Démonstration. Pour $N > 30$ on $\displaystyle\sum_{p\leq N} \frac{1}{p} \leq \frac{4}{15}\ln N + 7$. Mais on a $\dfrac{2}{7} = \dfrac{4}{15} + \dfrac{2}{105}$ et, pour [44] $N \geq \exp(367.5)$, on a $7 \leq \frac{2}{105}\ln N$.

8 Annexes 3 : quelques compléments

8.1 Jacobi

Voici la citation exacte de Jacobi (lettre du 2 juillet 1830 adressée à Adrien-Marie Legendre) : *M. Fourier avait l'opinion que le but principal des mathématiques était l'utilité publique et l'explication des phénomènes naturels ; mais un philosophe comme lui aurait dû savoir que le but unique de la science, c'est l'honneur de l'esprit humain, et que, sous ce titre, une question de nombres vaut autant qu'une question du système du monde.*

44. Bien entendu cette borne est bien trop grande. L'inégalité vaut pour $N \geq 5000$.

8.2 Autour d'Euler

8.2.1 Bernoulli et Euler

Au départ il y a un mémoire de Jean Bernoulli à l'Académie royale des sciences de Berlin (1771) qui s'intitule *Recherches sur les diviseurs de quelques nombres très grands compris dans la forme de la progression géométrique* $1 + 10 + 10^2 + ... + 10^T = S$. Dans cet article, Bernoulli étudie les diviseurs des nombres $10^n \pm 1$ (liés aux développements décimaux périodiques, bien entendu, voir [16].) Je n'y vois pas trace des nombres de la forme $n^2 + n + 41$ (en revanche il apparaît les $n^2 + n - 24$).

Deux anecdotes à propos de ce texte :

• D'abord une erreur page 325 à propos de $10^{11} + 1$. Ce nombre c'est $11 \times 23 \times 395256917$ (et non ...927 comme il est écrit [45]). Bernoulli se demande si le dernier facteur est premier alors qu'il admet le facteur 11 ! Précisément :

$$395256917 = 11 \times 4093 \times 8779$$

Vivent les calculatrices !

• Ensuite, page 330, Bernoulli examine le nombre 5882353 et le reconnaît pour premier (c'est vrai). Il dit : *c'est peut-être le plus grand nombre premier qu'on connaisse ; au moins surpasse-t-il de plus du double le plus grand de ceux que M. Euler a déterminés dans le Mémoire* de numeris primis valde magnis. À quoi Euler rétorque dans l'article de 1771 : *le plus grand nombre premier que nous connaissons est sans doute* $2^{31} - 1 = 2147483647$*, que Fermat a déjà assuré être premier, et moi aussi je l'ai prouvé ...*

8.2.2 Variantes

L'article [14] de Mollin fournit un panorama très intéressant autour des valeurs premières des polynômes du second degré. En voici quelques points.

Il y a d'autres séries de 40 nombres premiers de suite fabriquées à partir de $f(x) = x^2 + x + 41$. Par exemple, le polynôme $g_0(x) = f(3x - 39) = 9x^2 - 231x + 1523$ donne des nombres premiers pour $x = 0, \ldots, 39$ (cet exemple remarquable est dû à Higgins, 1982, attention, ces nombres sont des $n^2 + n + 41$ mais ce ne sont pas les nombres d'Euler, il y en a en commun, mais on les parcourt de trois en trois, dans les deux sens et le plus grand est 6203). À partir de g_0 on peut en fabriquer d'autres, voir [14] :

$$g_n(x) = g_0(x - n) = 9x^2 - (18n + 231)x + 9n^2 + 231n + 1523$$

45. Celui-là est encore moins premier : il est multiple de 3.

et $g_n(x+n)$ premier pour $x = 0, \ldots, 39$ et pour tout n.

Mollin donne aussi un exemple avec des valeurs espacées de 2 avec $f(38-2x)$.

On trouve dans [14] un autre point intéressant. En utilisant une conjecture qui généralise celle des nombres premiers jumeaux, on montre que, si b est un entier positif quelconque, il existe un entier a tel que tous les n^2+n+a soient premiers pour n variant de 0 à b. On obtient ainsi une suite de nombres premiers avec une longueur b arbitraire. Par exemple, avec $b = 9$, les n^2+n sont $0, 2, 12, 20, 30, 42, 56, 72, 90$ et $a = 11$ convient. Notons tout de même qu'on ne connaît aucun exemple qui soit meilleur que le fameux 41 ! (On peut montrer qu'il faudrait $a > 10^{18}$.)

8.2.3 La série de 29

Où se logent parfois les mathématiques : j'ai relevé dans le livre *Code zéro* de Ken Follett (que j'avais emprunté à la médiathèque d'Antony) le passage suivant :

Elle pensa au nombre 29*. Un nombre premier, pas très intéressant. Tout ce qu'on pouvait en dire, c'était que* $29+2\times n$ *était un nombre premier pour tous les nombres après* 28*. Elle calcula mentalement la série :* 29*,* 31*,* 37*,* 47*,* 61*,* 79*,* 101*,* 127 *...*

Bien entendu c'est doublement faux (c'est une erreur de traduction, voir l'original ci-dessous) : il s'agit [46] de $29+2\times n^2$ et c'est un nombre premier pour $n \leq 28$ (un autre lecteur avait rétabli le n^2 et barré le "pour tous"). Voici l'original :

To pass the last minute, she thought about the number 29. It was a prime number—it could not be divided by any other number except 1—but otherwise it was not very interesting. The only unusual thing about it was that 29 plus $2x^2$ *was a prime number for every value of x up to 28. She calculated the series in her head : 29, 31, 37, 47, 61, 79, 101, 127 . . .*

On vérifie que, pour $n \leq 10^6$, il y a 226215 nombres premiers de la forme $2n^2+29$, ce qui n'est pas mal. Ces phénomènes sont liés au fait que $h(58) = 2$ est petit.

8.2.4 L'exemple du calendrier mathématique 2015

Le problème du 3 avril du calendrier mathématique 2015 consiste à trouver le plus petit nombre premier $p > 2$ tel que $p^3 + 7p^2$ soit un carré. Il est clair que cela revient à trouver p premier tel que $p+7$ soit un carré et que $p = 29$ est la plus petite solution. En prenant le problème à l'envers,

46. Il semble que la considération de cette série des $2x^2+29$ soit due à Legendre.

on est amené à chercher les x tels que x^2-7 soit premier et en particulier à se demander s'il y en a une infinité, problème du type de celui étudié ici. L'anneau de nombres associé est $\mathbf{Z}[\sqrt{7}]$ et il est factoriel [47].

Dans ce cas, on calcule facilement avec *xcas* le nombre de premiers de la forme x^2-7 avec $x \leq 10^6$. On trouve 29792. L'approximation par Hardy-Littlewood est excellente : avec $\mathrm{Li}\,(n)$ elle donne 29774 !

8.2.5 Calcul de la spirale d'Ulam centrée en a

Sur la spirale de la Figure 1 on voit se dessiner des couronnes. La première C_1 contient $1, 2, 3, 4$, la seconde contient les nombres 5 à 16, la troisième de 17 à 36.

Plus généralement, si l'on part d'un nombre entier a (par exemple 41), placé au centre d'un quadrillage, voir Figure 2, on effectue d'abord un pas vers la droite et on place $a+1$, puis un pas vers le haut pour placer $a+2$, puis un pas vers la gauche pour placer $a+3$ et $a+4$. On redescend alors en posant $a+5$ et $a+6$, on repart à droite et ainsi de suite, en suivant les bords de la spirale ainsi obtenue. On obtient des couronnes C_k et on montre par récurrence sur k que, sur la k-ième couronne, on a, sur la diagonale principale, en haut à droite $I(k) = a+(2k-1)^2+(2k-1)$ et en bas à gauche $P(k) = a+(2k)^2+2k$, donc des nombres de la forme n^2+n+a avec n alternativement impair et pair. En effet, pour $k=1$ on a bien $I(1) = a+2$ et $P(1) = a+4+2 = a+6$. Dans la couronne k, la ligne supérieure a pour longueur $2k$ ce qui donne $I(k)+2k$ en haut à gauche, de même la colonne de gauche a pour longueur $2k$ et on a donc en bas à gauche $I(k)+4k$ qui est bien égal à $P(k)$. Ensuite, les deux travées suivantes ont pour longueur $2k+1$, ce qui nous amène en bas à droite à $P(k)+2k+1$, puis en haut à droite à $P(k)+4k+2$ et cette quantité est bien égale à $I(k+1)$.

8.2.6 Bunyakovsky

Si on écrit $f(x)$ non pas avec les x^k mais avec les coefficients binomiaux comme base, la deuxième condition de Bunyakovsky (voir paragraphe 1.5) est que les coefficients sont premiers entre eux. En effet, on écrit :

$$f(x) = a_0 + a_1\binom{x}{1} + a_2\binom{x}{2} + \cdots + a_d\binom{x}{d}$$

$$f(x) = a_0 + a_1 x + a_2\frac{x(x-1)}{2} + \cdots + a_d\frac{x(x-1)\cdots(x-d+1)}{d!}.$$

47. Attention, dans le cas quadratique réel il faut se méfier des unités. Par exemple, bien que 3 soit réductible : on a $3 = (-2+\sqrt{7})(2+\sqrt{7})$, ce n'est pas pour autant une norme x^2-7y^2 (regarder modulo 7, c'est -3 qui est une norme : $N(2+\sqrt{7}) = -3$).

Alors, si p divise tous les $f(n)$, on voit qu'il divise a_0 avec $n = 0$, puis a_1 avec $n = 1$, etc.

8.3 Autour du logarithme intégral

Dans ce paragraphe, on fait le point sur l'utilisation de la fonction Li dans l'énoncé des théorèmes et des conjectures de théorie des nombres.

8.3.1 L'équivalent de Li

On rappelle qu'on pose, pour $x \geq 2$, $\mathrm{Li}\,(x) = \displaystyle\int_2^x \frac{dt}{\ln t}$.

8.1 Proposition. *Quand x tend vers $+\infty$ on a :* $\mathrm{Li}\,(x) \sim \dfrac{x}{\ln x}$.

On intègre par parties en posant $u = \dfrac{1}{\ln t}$ et $dv = dt$. On trouve :

$$\int_2^x \frac{dt}{\ln t} = \frac{x}{\ln x} - \frac{2}{\ln 2} + \int_2^x \frac{dt}{(\ln t)^2}.$$

Posons $I(x) = \displaystyle\int_2^x \frac{dt}{(\ln t)^2}$. Il suffit de montrer que $I(x) = o(\mathrm{Li}\,(x))$. Soit $\epsilon > 0$. Il existe $A \geq 2$ tel que, pour $t \geq A$, $\dfrac{1}{\ln t} \leq \epsilon$. Fixons un tel A et soit $x > A$. On écrit $I(x) = \displaystyle\int_2^A \frac{dt}{(\ln t)^2} + \int_A^x \frac{dt}{(\ln t)^2}$. Si l'on note K la première intégrale (qui est une constante), on a $I(x) \leq K + \epsilon \displaystyle\int_A^x \frac{dt}{\ln t} \leq K + \epsilon \mathrm{Li}\,(x)$. On a donc $\dfrac{I(x)}{\mathrm{Li}\,(x)} \leq \dfrac{K}{\mathrm{Li}\,(x)} + \epsilon$ et comme $\dfrac{K}{\mathrm{Li}\,(x)}$ tend vers 0 quand x tend vers l'infini, on a le résultat.

8.2 *Remarque.* En continuant les intégrations par parties, on montre plus précisément :

$$\mathrm{Li}\,(x) = \frac{x}{\ln x} + \frac{x}{(\ln x)^2} + \frac{2x}{(\ln x)^3} + \cdots + \frac{n!\,x}{(\ln x)^{n+1}} + o\Big(\frac{x}{(\ln x)^{n+1}}\Big).$$

8.3.2 Li ou L_A ?

Dans l'article [8] de Fung et Williams, ils donnent un équivalent pour le nombre de premiers de la forme $f(x) = x^2 + x + A$ pour $x \leq n$ qui

est de la forme $C\,L_A(n)$ avec $L_A(n) = 2\displaystyle\int_0^n \frac{dx}{\ln(f_A(x))}$ alors qu'on donne habituellement une telle formule avec $\mathrm{Li}\,(n) = \int_2^n \frac{dx}{\ln x}$. En fait, c'est la même chose, disons pour $A = 41$. D'abord, comme f_A ne s'annule pas, on peut remplacer l'intégrale de 0 à n par celle de 2 à n. La différence est alors :

$$\int_2^n \Big(\frac{1}{2\ln x} - \frac{1}{\ln(x^2+x+41)}\Big)dx = \int_2^n \frac{\ln(1+\frac{1}{x}+\frac{41}{x^2})}{2\ln x \ln(x^2+x+41)}dx.$$

Or, la fonction à intégrer est équivalente à $\dfrac{1}{4x(\ln x)^2}$ et l'intégrale converge, donc la différence a une limite finie et les deux termes sont bien équivalents.

8.4 Avec d'autres polynômes du second degré

On n'a considéré ici que le polynôme $x^2 + x + 41$, voire $x^2 + bx + c$ et on peut se demander à bon droit si d'autres pourraient aussi faire l'affaire (i.e. donner beaucoup de nombres premiers), avec d'autres coefficients. En particulier, ayant reconnu l'importance du discriminant, on peut se demander si d'autres polynômes avec le même discriminant -163 peuvent convenir. On trouve facilement un tel exemple, comme $x^2 + 3x + 43$, qui donne des nombres premiers pour $x = -1, 0, 1, \ldots, 38$. Mais cet exemple est banal, car on a $x^2+3x+43 = (x+1)^2+(x+1)+41$, autrement dit, il s'agit du même polynôme, à changement de variables près. De même, l'exemple d'Escott (1899) : $x^2 - 79x + 1601$ n'est autre que $f(x - 40)$, voir [14].

En fait, la réponse à cette question est dans le travail de Gauss sur les formes quadratiques entières. On sait que, si on considère les formes $ax^2 + bxy+cy^2$ à changement de variable près dans $SL(2, \mathbf{Z})$, il n'y a qu'un nombre fini de formes de discriminant d fixé et ce nombre est le fameux $h(d)$ (le nombre de classes). Pour $d = -163$ il n'y en a donc qu'une et, pour la trouver, on utilise le résultat de Gauss : toute forme est équivalente à une forme réduite qui vérifie $|b| \leq a \leq c$, avec $b \geq 0$ si $a = |b|$ ou $a = c$. Pour un autre discriminant, en revanche, les formes n'auront pas nécessairement $a = 1$ (mais on a cependant $a \leq \sqrt{d/3}$). Par exemple, pour $d = 347$, on a $x^2 + x + 87$, mais aussi $3x^2 \pm x + 29$ et $9x^2 \pm 7x + 11$. Cet exemple est intéressant. En effet, on voit que $P(N)$, pour $N = 10^6$ n'est pas du même ordre de grandeur. Pour $x^2 + x + 87$ c'est 49218, pour $3x^2 + x + 29$, 93716 et pour $9x^2 + 7x + 11$, 89834. L'explication est dans Hardy-Littlewood. En effet, pour $p = 3$, l'équation $x^2 + x + 87 \equiv x^2 + x \equiv 0$ a deux solutions, mais $3x^2 + x + 29 \equiv 9x^2 + 7x + 11 \equiv x + 2 \equiv 0$ n'en a qu'une, d'où la présence d'un terme 1/3 ou 2/3 dans le produit, qui explique le facteur 2 entre les résultats.

8.5 Plusieurs polynômes, éventuellement de plus grand degré

Il y a aussi des conjectures mettant en jeu plusieurs polynômes. Cette fois, il faut supposer que pour tout p il existe x tel que les $f(x)$ ne soient pas tous multiples de p. Par exemple, avec x et $x+2$ on obtient la conjecture des nombres premiers jumeaux. Avec $x, x+2, x+6, x+8$ on trouve la conjecture des dizaines "riches". Plus généralement, on a vu en 8.2.2 que les n^2+n ($0 \leq n \leq b$) forment une suite "admissible" au sens où l'on espère qu'il existe a tel que les n^2+n+a soient premiers pour tout $n \leq b$. Les conjectures principales sur ce thème sont dues à Bateman et Horn, voir [1]. Il y a d'abord une généralisation de Hardy-Littlewood à un polynôme f de degré quelconque :

8.3 Conjecture. *Soit $f \in \mathbf{Z}[x]$ un polynôme à coefficients entiers sans facteur commun, de degré d. Soit N un entier et $P(N)$ le nombre de nombres premiers parmi les $f(n)$, $1 \leq n \leq N$.*

Alors, on a $P(N) \sim \dfrac{C}{d} \displaystyle\int_2^N \frac{dt}{\ln t} \sim \frac{C}{d} \frac{N}{\ln N}$ où C est le produit, indexé par les nombres premiers : $C = \displaystyle\prod_p \frac{1 - \frac{N(p)}{p}}{1 - \frac{1}{p}}$ dans lequel $N(p)$ est le nombre de solutions de la congruence $f(n) \equiv 0 \pmod{p}$.

Il y a ensuite une variante, avec plusieurs polynômes :

8.4 Conjecture. *Sous des hypothèses minimes, si on a r polynômes à coefficients entiers, le nombre $\pi(x)$ des entiers $n \leq x$ tels que tous les $f_i(n)$ soient premiers est équivalent à :*

$$\frac{C(f_1, \ldots, f_r)}{\deg f_1 \ldots \deg f_r} \frac{x}{(\ln x)^r}$$

avec $C(f_1, \ldots, f_r) = \displaystyle\prod_p \frac{1 - \omega_f(p)/p}{(1-1/p)^r}$ où $\omega_f(p)$ est le nombre de racines[48] *de $f(T) := f_1(T) \cdots f_r(T)$ modulo p.*

Un cas particulier concerne $f_1(T) = T$ et $f_2(T) = T+2$, il donne le nombre de premiers jumeaux $\leq x+2$. Dans ce cas, on a $\omega_f(2) = 1$ et $\omega_f(p) = 2$ pour $p > 2$. On trouve :

$$\pi(x) \sim 2 \prod_{p>2} \frac{p(p-2)}{(p-1)^2} \frac{x}{(\ln x)^2} \simeq 1,3203236 \frac{x}{(\ln x)^2}.$$

48. On ne compte pas les multiplicités, sinon le cas des jumeaux donnerait 0.

Cette formule est très mauvaise. Par exemple, pour $x = 2840420$ on a 20000 premiers jumeaux et la formule en donne seulement 16984. En revanche, la variante en remplaçant $\dfrac{x}{(\ln x)^2}$ par l'intégrale $\displaystyle\int_2^x \frac{dt}{(\ln t)^2}$ donne 19937.

Il y a une formule analogue avec les "jujumeaux" (i.e. p, $p+2$, $p+6$ et $p+8$ premiers) :

$$\pi(x) \sim \frac{27}{2} \prod_{p>3} \frac{p^3(p-4)}{(p-1)^4} \frac{x}{(\ln x)^4}.$$

Pour $x = 10^7$ on obtient 615 alors que la vraie valeur est 898. Avec l'intégrale on trouve 862, c'est mieux.

8.6 Les polynômes à plusieurs variables

En ce qui concerne les polynômes à plusieurs variables on a les résultats suivants :

1) Pour les polynômes (non homogènes) à deux variables, un résultat d'Iwaniec, voir [9], assure qu'un polynôme $P(x, y)$, avec des conditions minimes, représente une infinité de nombres premiers. C'est le cas, par exemple, de $x^2 + y^2 + 1$ (Motohashi, voir [15]). Pour $x, y \leq 100$ il y a 1081 nombres premiers de la forme $x^2 + y^2 + 1$.

2) Contrairement à ce qu'on pourrait penser, il n'est pas évident de donner une démonstration élémentaire de ce dernier résultat. Bien sûr, il suffit de montrer qu'il y a une infinité de premiers p tels que $p - 1$ soit somme de deux carrés (c'est-à-dire que $p-1$ n'a pas de facteur premier $\equiv 3$ élevé à une puissance impaire). Mais ce n'est pas du tout trivial [49]. Voir l'article de Y. Motohashi, Acta Arith. 16 (1970), p. 351 où il conjecture que le nombre de premiers $\leq N$ qui sont de cette forme est $\sim c\dfrac{N}{(\ln N)^{3/2}}$.

3) Le théorème des quatre carrés montre que tout nombre premier est de la forme $x^2 + y^2 + z^2 + t^2 + 1$. Il est même du type $x^2 + y^2 + z^2 + t^2$. En effet, p est soit somme de 3 carrés, soit de la forme $8n - 1$, mais alors $p - 1$ est somme de trois carrés. Voir [24], Appendice du Ch. IV.

4) Dans le cas des polynômes homogènes, on a le résultat suivant :

8.5 Théorème. *Soit $P(x, y)$ un polynôme homogène de degré 2 à coefficients entiers. On suppose que les coefficients de P sont premiers entre eux. Alors*

49. Comme Étienne Fouvry me l'a expliqué, il y a extrêmement peu de sommes de deux carrés (la proportion des sommes de deux carrés parmi les nombres $\leq x$ est de l'ordre de $1/\sqrt{\ln x}$) ! C'est d'autant plus troublant que jusqu'à 10000 il y en a 4012.

il existe une infinité de couples $(x, y) \in \mathbf{Z}^2$ *tels que* $P(x, y)$ *soit un nombre premier.*

Démonstration. Paradoxalement, le cas où P est irréductible est plus difficile que le cas P réductible et on renvoie à [9] pour la preuve. Supposons donc que P soit réductible, $P(x, y) = (ax+by)(cx+dy)$. Le fait que les coefficients de P soient premiers entre eux montre que a, b d'une part et c, d de l'autre le sont aussi. On peut alors trouver des entiers x_0, y_0 tels que $ax_0 + by_0 = 1$ et les autres solutions de cette équation sont de la forme $x = x_0+kb$, $y = y_0-ka$ avec $k \in \mathbf{Z}$. Pour ces x, y on a $cx + dy = cx_0 + dy_0 + k(bc - ad)$. Mais, on a le lemme suivant :

8.6 Lemme. *Avec les notations précédentes, les nombres* cx_0+dy_0 *et* $bc-ad$ *sont premiers entre eux.*

Démonstration. (du lemme) Sinon, ces nombres ont un facteur premier commun p. Comme x_0 et y_0 sont premiers entre eux, on peut supposer que p ne divise pas x_0 et on a alors, modulo p, $c \equiv -\dfrac{dy_0}{x_0}$. En reportant dans $bc - ad$ on obtient $d(ax_0 + by_0) = d \equiv 0 \pmod{p}$. Mais, avec $cx_0 \equiv -dy_0$ et le fait que p ne divise pas x_0, on voit que p divise c, ce qui est absurde.

Le théorème résulte alors du théorème de Dirichlet : il existe une infinité de k tels que $cx + dy$ soit premier et, avec $ax + by = 1$, on a gagné.

8.7 *Remarque.* Dans le cas d'un polynôme quadratique irréductible de discriminant d, la propriété est facile dans le cas $h(d) = 1$, mais sinon ce n'est pas immédiat. Par exemple, il y a effectivement une infinité de nombres premiers p de la forme $x^2 + 5y^2$, mais, pour que p soit de cette forme, il ne suffit pas [50] que -5 soit un carré modulo p : cette condition indique seulement que p ou $2p$ est de la forme $x^2 + 5y^2$ et il faut ensuite utiliser les congruences modulo 4, voir [19].

8.7 Ensembles diophantiens et polynôme de Jones

Sur ce sujet, une référence élémentaire est [11].

Un ensemble $M \subset \mathbf{N}$ est dit diophantien s'il existe un polynôme $D(a, x) = D(a, x_1, \ldots, x_p)$ en $p + 1$ variables, à coefficients entiers, qui vérifie :

$$a \in M \Longleftrightarrow \exists x = (x_1, \ldots, x_p) \in \mathbf{N}^p \; D(a, x) = 0.$$

50. Voir l'exemple de $p = 7$.

8.8 *Exemples.* 1) Les nombres pairs avec $D(a,x) = a - 2x$.

2) Les nombres non premiers avec $D(a,x,y) = a - (x+2)(y+2)$.

3) Les valeurs de la suite de Fibonacci (définie par $u_0 = u_1 = 1$ et $u_{n+2} = u_{n+1} + u_n$ pour $n \geq 0$) avec $D(a,x,y) = a - y(2 - (x^2 + xy - y^2)^2)$. En effet, quand on donne à x, y les valeurs de deux termes consécutifs de la suite de Fibonacci, $x = u_n$ et $y = u_{n+1}$, $(x^2 + xy - y^2)^2$ vaut toujours 1, comme on le vérifie par récurrence, et on a donc $D(a,x,y) = 0 \Longleftrightarrow a = y$.

Le théorème de Matiasevic (1970) est alors le suivant :

8.9 Théorème. *Il y a identité entre les ensembles diophantiens et les ensembles récursivement énumérables.*

Intuitivement, un ensemble récursivement énumérable est un ensemble reconnaissable par une machine de Turing. Il en résulte, en particulier, qu'il existe un polynôme $D(a,x)$ tel que a est premier si et seulement si $D(a,x) = 0$. En fait, Jones a exhibé en 1976 un polynôme P de degré 25 en les 26 variables $a, \ldots, z$ dont l'ensemble des valeurs positives, quand $a, \ldots, z$ varient dans $\mathbf{N}$, est exactement l'ensemble des nombres premiers.

$$(k+2)[1–(wz+h+j–q)^2–[(gk+2g+k+1)(h+j)+h–z]^2$$

$$–(2n+p+q+z–e)^2–[16(k+1)3(k+2)(n+1)2+1–f^2]^2$$

$$–[e^3(e+2)(a+1)^2+1–o^2]^2–[(a^2–1)y^2+1–x^2]^2$$

$$–[16r^2y^4(a^2–1)+1–u^2]^2$$

$$–[((a+u^2(u^2–a))^2–1)(n+4dy)^2+1–(x+cu)^2]^2–[n+l+v–y]^2$$

$$–[(a^2–1)l^2+1–m^2]^2–[ai+k+1–l–i]^2$$

$$–[p+l(a–n–1)+b(2an+2a–n^2–2n–2)–m]^2$$

$$–[q+y(a–p–1)+s(2ap+2a–p^2–2p–2)–x]^2$$

$$–[z+pl(a–p)+t(2ap–p^2–1)–pm]^2]$$

Mais, il n'existe aucune valeur connue de $a, \ldots, z$ qui donne un nombre positif (il y a 14 carrés dans P, munis du signe moins, et il faut que tous donnent 0), de sorte que ce théorème est totalement inutilisable pour trouver des nombres premiers !

8.8 Une autre apparition du nombre 163 : le nombre de Ramanujan

Il s'agit de $e^{\pi\sqrt{163}} \simeq 262537412640768743,99999999999250072$. Ce nombre [51] est remarquable car il est très voisin d'un entier.

Si A_d est l'anneau des entiers d'un corps de nombres quadratique imaginaire avec $h(d) = 1$, l'invariant modulaire de A_d (considéré comme réseau de $\mathbf{C}$) est un entier. Dans le cas de $d = 163$, cela signifie que $j((1+\sqrt{-163})/2)$ est un entier, précisément -640320^3. Mais la fonction $j(z)$ admet un développement en série de la variable $q = \exp(2i\pi z)$: $j(z) = 1/q + 744 + 196884q + ...$ (ici $q = -e^{-\pi\sqrt{163}} \simeq -3 \times 10^{-18}$) et on a donc :

$$-640320^3 = -\exp(\pi\sqrt{163}) + 744 + \sum_{n=1}^{+\infty} c(n)q^n ...$$

avec $c(1) = 196884$, $c(2) = 21493760$, etc. Cela que $\exp(\pi\sqrt{163})$ est "presque" égal à l'entier $640320^3 + 744$. L'erreur est de 7×10^{-13} et le terme suivant est en 3×10^{-28}.

8.9 La constante de Mills

C'est un nombre réel $A \sim 1.306377883863080690468614492602605712 91$, qui est tel que $P_n = [A^{3^n}]$ (partie entière) est un nombre premier, quel que soit n. (Pour $n = 1, 2, 3, 4$, on trouve 2, 11, 1361 et 2521008887). La preuve tient en une page, voir [13]. C'est juste une conséquence d'un théorème de Ingham [52] qui dit que $p_{n+1} - p_n < Kp_n^{5/8}$ où K est un entier positif fixé.

9 Quelques programmes sur *xcas*

9.1 Sélectionner des nombres premiers réductibles

Ce programme détermine p premier entre N et $N + P$, tel que -163 soit un carré modulo p, et la plus petite racine n de $x^2 + x + 41$ modulo p.

```
selection(N,P):={
local p,n;
pour p de N jusque N+P pas 2 faire
si isprime(p)==1 et legendre_symbol(-163,p)==1 alors
pour n de 1 jusque floor(p/2) faire
```

51. Ce paragraphe est inspiré du blog de D. Madore.
52. Qui utilise l'hypothèse de Riemann, semble-t-il.

```
si irem(n^2+n+41,p)== 0 alors
Disp p,n;
fsi fpour fsi fpour }:;
```

9.2 L'algorithme de Cornacchia

Si p est un nombre premier réductible et n une racine de x^2+x+41 modulo p, ce programme retourne une écriture de p comme norme ($p = s^2+sc+41c^2$, $k = 1$).

```
cornac(p,n):={
local r,s,t,b,c,d,q,k;
r:=p; s:=n; b:=0; c:=1;
k:=(s^2+s*c+41*c^2)/p;
tantque k > 8 faire
q:=iquo(r,s);
t:=irem(r,s);
d:=b-q*c;
k:=(s^2+s*c+41*c^2)/p;
Disp s,c,k;
r:=s; s:=t; b:=c; c:=d;
ftantque}:;
```

9.3 Compter les nombres premiers de la série

Le programme ci-dessous compte le nombre de $n \leq N$ tels que n^2+an+b soit premier.

```
comptage(a,b,N):={
local n,s;
s:=0;
pour n de 0 jusque N faire si isprime(n^2+a*n+b)==1 alors
s:=s+1;
fsi fpour retourne s; }:;
```

Pour faire la table des $P_b(10^6)$ (nombre de nombres premiers de la forme n^2+n+b avec $n \leq 10^6$ et b impair $\leq k$).

```
tablecompt(k):={
local b;
pour b de 1 jusque k pas 2 faire
Disp b, comptage(1,b,10^6)
fpour }:;
```

9.4 Calcul avec la conjecture

Le programme suivant calcule le nombre premiers de la forme n^2+n+c avec $c=\frac{d+1}{4}$ et d premier congru à 3 modulo 4 selon la conjecture 3.13.

```
den(N,d):={
local p,P;
P:=1.;
pour p de 3 jusque N pas 2 faire
si isprime(p)==1 et legendre_symbol(p,d)==1 alors
P:=approx(P*(1-2/p));
fsi
fpour
Disp P*((d-1)/d)*N;}:;
```

9.5 La fonction *hache*

Le programme ci-dessous calcule une valeur approchée de l'entier $h(d)$ à l'aide de la formule de Dirichlet (voir 4.5) en tronquant le produit à $p \leq m$:

```
hache(d,m):={
local x,p;
DIGITS:=10;
p:=1;
pour x de 3 jusque m pas 2 faire
si isprime(x)==1 alors
p:=p*(1-legendre_symbol(x,d)/x);
fsi
fpour
retourne (2*sqrt(d))/(3*pi) *approx(p^(-1)); }:;
```

Voici une variante avec la formule 5.4 (valable dans le cas où d est premier congru à 3 modulo 4).

```
hac(d):={
local x,C,N,h;
pour x de 1 jusque (d-1)/2 faire
si legendre_symbol (x,d)==1 alors C:=C+1;
fsi
fpour
N:=(d-1)/2-C;
h:=(C-N)/3;
Disp C; Disp N; Disp h;}:;
```

9.6 Les candidats à la plus grande densité

Le programme ci-dessous détermine les nombres $d \equiv 3 \pmod 8$, $d \leq N$ tels qu'aucun nombre premier $p \leq M$ ne soit un carré modulo d.

```
recherd(N,M):={
local d,p,P,Q;
pour d de 3 jusque N pas 8 faire
P:=0; Q:=0;
pour p de 3 jusque M pas 2 faire
si isprime(p)==1 alors
Q:=Q+1;
si legendre_symbol(-d,p)==-1 alors P:=P+1;
fsi
fsi
fpour
si P==Q alors
Disp d;
fsi fpour}:;
```

Références

[1] Bateman P. T., Horn R. A., *A heuristic asymptotic Formula concerning the Distribution of prime Numbers*, Mathematics of computation, vol. 16, 1962, 363-367.

[2] Borevich Z. I., Shafarevich I. R., *Théorie des nombres*, Gauthier-Villars, 1967.

[3] Bourbaki N., *Topologie générale Ch. 1 et 2*, Hermann, 1965.

[4] Chenevier G., *Théorie algébrique des nombres*, Cours à l'École Polytechnique, 2015-2016.

[5] Cohen H., *High precision computation of Hardy-Littlewood constants*, preprint.

[6] Cornacchia G., *Su di un metodo per la risoluzione in numeri interi dell' equazione* $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$, Giornale di Matematiche di Battaglini, 46, 1908, 33-90.

[7] Duke W., *Number fields with large class groups*,
`http://www.math.ucla.edu/~wdduke/preprints/number.pdf`

[8] Fung G. W., Williams H.C., *Quadratic polynomials which have a high density of prime values*, Mathematics of computation, vol. 55, n° 191, july 1990, 345-353.

[9] Iwaniec H., *Primes represented by quadratic polynomials in two variables*, Acta Arithmetica XXIV, 1974, 435-459.

[10] Jacobson M.C, Williams H.C., *New quadratic polynomials with high densities of prime values*, Mathematics of computation, vol. 72, n° 241, 2002, 499-519.

[11] Jones J.-P., Sato D., Wada H., Wiens D., *Diophantine representation of the set of prime numbers*, Amer. Math.Monthly, 83, 1976, 449-464.

[12] Littlewood J., *On the class number of the corpus* $P(\sqrt{-k})$, Proc. London Math. Soc. 27, (1928), 358-372.

[13] Mills, W. H. *A prime-representing function*, Bull. Amer. Math. Soc. 53, n° 6, (1947), 604.

[14] Mollin R.A. *Prime-Producing Quadratics*, The American Mathematical Monthly, Vol. 104, N° 6, 1997, 529-544.

[15] Motohashi Y., *On the distribution of prime numbers which are of the form* $x^2 + y^2 + 1$, Acta arithmetica, XVI, 1970, 351-363.

[16] Perrin D., *Mathématiques d'école*, Cassini, 2011.

[17] Perrin D., *Cours d'algèbre*, Ellipses, 1996.

[18] Perrin D., *Arithmétique et cryptographie*, sur ma page web :
`http://www.math.u-psud.fr/~perrin/interdisciplines/Cours6cryptographie.pdf`

[19] Perrin D., *Anneaux d'entiers des corps quadratiques imaginaires*, sur ma page web :
`http://www.math.u-psud.fr/~perrin/TER.html`

[20] Perrin D., *La loi de réciprocité quadratique*, sur ma page web :
`http://www.math.u-psud.fr/~perrin/TER.html`

[21] Perrin D., *Problèmes ouverts : pourquoi et comment ?*, sur ma page web :
`http://www.math.u-psud.fr/~perrin/Conferences/IREM2015/IREM2015redaction.pdf`

[22] Rabinowitsch G., *Eindeutigkeit der Zerlegung im Primzahlfaktoren in quadratischen Zahlkörpern*, J. Reine Angew. Math. 142, 1913, 153-164.

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

[24] Serre J.-P., *Cours d'arithmétique*, PUF, 1970.

[25] Shanks D., *On the Conjecture of Hardy and Littlewood concerning the Number of Primes of the Form* $n^2 + a$, Mathematics of Computation, 1960, 321-332.

[26] Shanks D.,*A Sieve Method for Factoring Numbers of the Form* n^2+1, Mathematics of Computation, 1959, 78-86.

[27] Shanks D., *Systematic examination of Littlewood's bounds on* $L(1,\chi)$, Proc. Symp. Pure Math., vol. 24, Amer. Math. Soc., Providence R.-I., 1973, 267-283.

[28] Stewart I., Tall D., *Algebraic number theory and Fermat last theorem*, Chapmann-Hall, 4° ed. 2016.

[29] Tenenbaum G. et Mendès-France M., *Les nombres premiers, entre l'ordre et le chaos*, Dunod, 2011.

[30] Watkins M., *Class numbers of imaginary quadratic fields*, Mathematics of computation, vol. 73, n° 246, p. 907-938, 2003.