

Polynômes prenant des valeurs premières

François Dress et Michel Olivier

TABLE DES MATIÈRES

- 1. Introduction
 - 2. Records ponctuels
 - 3. Modèles heuristiques probabilistes
 - 4. Premier modèle probabiliste, pour $k = n$
 - 5. Deuxième modèle probabiliste, pour $k < n$
 - 6. Complétion des résultats de Boston et Greenwood ($n = 100$)
 - 7. Résultats numériques : records "en continu"
 - 8. Deux remarques pour la recherche d'une explication
 - 9. Polynômes de degré supérieur
- Remerciements
Bibliographie

On décrit, essentiellement pour les polynômes du second degré, deux modèles heuristiques probabilistes donnant le nombre k de valeurs premières prises par ces polynômes sur un intervalle de n valeurs consécutives de la variable. Le premier modèle est consacré au cas $k = n$ et fait apparaître un "mur de Schinzel", d'ordre de grandeur n^n , en-dessous duquel l'évènement " n valeurs premières pour n valeurs consécutives de la variable" est statistiquement exceptionnel, et au-dessus duquel il est statistiquement fréquent s'il n'y a pas d'obstruction arithmétique. Le deuxième modèle est consacré au cas $k < n$ et est fondé sur une loi binomiale avec une probabilité qui dérive de la constante de Hardy-Littlewood. Pour ce modèle comme pour le précédent, les expérimentations numériques présentent une concordance satisfaisante. Ce travail est complété par une table des meilleurs polynômes trouvés jusqu'à $n = 40338$. Enfin, on donne des résultats numériques pour les polynômes de degré 3, 4 et 5.

We describe two heuristic probabilistic models that give the number k of prime values of quadratic polynomials on an interval of n consecutive values of the variable. The first model is devoted to the case $k = n$ and reveals a "Schinzel barrier", of size n^n : below this barrier, the event " n prime values for n consecutive values of the variable" is statistically exceptional, and above, it is statistically frequent provided that there is no arithmetic obstruction. The second model is devoted to the case $k < n$ and is based on a binomial law with a probability deriving from the Hardy-Littlewood constant. For both models, numerical experiments show a satisfactory similarity. This work is illustrated with a list of the best polynomials found for $n \leq 40338$. We also give some numerical results for polynomials of degree 3, 4 and 5.

1. INTRODUCTION

Le problème des polynômes à coefficients entiers prenant beaucoup de valeurs premières présente quatre aspects principaux.

a. Le premier est la recherche de polynômes prenant *exactement* n valeurs premières pour n valeurs consécutives de la variable. Le polynôme $x^2 + x + 41$ d'Euler (1772) prend 40 valeurs premières à partir de $x = 0$; on connaît exactement 3 polynômes qui

sont meilleurs: $103x^2 + 31x - 3391$ ($n = 43$, Fung, 1988), $47x^2 + 9x - 5209$ ($n = 43$, Fung, 1988), et $36x^2 + 18x - 1801$ ($n = 45$, Ruby, 1989). Tous ces résultats sont cités par Mollin et Williams [1990] et Ribenboim [1996].

Pour le second degré, on dispose du critère de Rabinowitch [1913] pour les polynômes de la forme $F_D(x) = x^2 + x + \frac{1-D}{4}$ avec $D < 0$ et $D \equiv 1 \pmod{4}$: le polynôme d'Euler ($D = -163$) est le "dernier" polynôme de la forme $x^2 + x + c$ à donner exactement n valeurs premières pour n valeurs consécutives de la variable (voir également [Mollin 1996]).

Numériquement, on verra dans cet article qu'un modèle probabiliste du problème laisse peu d'espoir de dépasser le résultat de Ruby.

Les conventions et notations utilisées sont celles de Boston et Greenwood [1995]. On présentera les polynômes particuliers sous leur forme normalisée. Deux polynômes F et G sont dits *équivalents* s'il existe m tel que $G(x) = \pm F(m \pm x)$. Il existe, dans chaque classe d'équivalence, un unique polynôme $F(x) = a_0x^d + a_1x^{d-1} + \dots + a_d$ qui vérifie $a_0 \geq 1$ et $0 \leq a_1 \leq \frac{d}{2}a_0$, à deux exceptions près qui sont des "effets de bord":

- si $a_1 = 0$, il peut exister deux tels polynômes F_1 et F_2 avec $F_1(x) = (-1)^d F_2(-x)$ (ces deux polynômes ont même coefficient a_2 , et on normalise alors par la condition $a_{2k+1} > 0$, où a_{2k+1} est le premier coefficient d'indice impair non nul);
- si $a_1 = \frac{d}{2}a_0$, il peut exister deux tels polynômes F_1 et F_2 avec $F_1(x) = (-1)^d F_2(-x - 1)$ (ces deux polynômes ont même coefficient a_2 , et on prend par exemple comme polynôme normalisé celui des deux qui a le plus grand coefficient a_k , où a_k est le premier coefficient où ils diffèrent (si $a_2 \neq 12d \times (d - 1)$, ce coefficient est a_3)).

Certains résultats dans la littérature ne sont pas présentés selon ces conventions.

b. La recherche des polynômes donnant *le plus grand nombre de valeurs premières* s'est concentrée sur 50, 100, 500 et 1000 valeurs consécutives de la variable.

Boston et Greenwood [1995] ont pris comme règle que les valeurs premières prises soient toutes distinctes (pour éviter notamment de considérer comme un record que $x^2 + x + 41$ donne 95 valeurs premières sur 100 valeurs consécutives de la variable,

de $x = -35$ à $x = 64$). Dans le cas des polynômes du deuxième degré, cela amène à se restreindre aux valeurs positives de x pour les polynômes avec symétrie $ax^2 + ax + c$ et $2ax^2 + c$. Pour les degrés supérieurs, la situation est plus compliquée. Ainsi le polynôme sans symétrie $3x^3 + 3x^2 - 402x + 1597$, prend 47 valeurs premières sur 47 valeurs consécutives de la variable, de $x = -26$ à $x = 20$, mais prend 3 fois la valeur 2389 (pour $x = -11, -2$ et 12), et 3 fois la valeur 3469 (pour $x = -8, -6$ et 13). La règle la plus simple est de compter seulement les valeurs premières *distinctes* (en module).

Les records classiques sont les suivants:

- sur 50 valeurs consécutives de la variable, $16x^2 + 10x - 547$ donne 48 valeurs premières, de x à $x + 49$, pour 8 valeurs de x de -34 à -26 (Greenwood 1993, cité dans [Boston et Greenwood 1995]); ce record a été ensuite égalé par plusieurs polynômes, dont $8x^2 + 2x - 1097$ (3 valeurs de x , de -31 à -25);
- sur 100 valeurs consécutives de la variable, $41x^2 + 33x - 43321$ donne 90 valeurs premières, de x à $x + 99$, pour $x = -57$ (loc. cit.);
- sur 1000 valeurs consécutives de la variable, $9x^2 + 3x - 16229$ donne 628 valeurs premières, de x à $x + 999$, pour 4 valeurs de x de -520 à -485 (loc. cit.); il faut néanmoins signaler le polynôme $2x^2 - 215011$, trouvé par Williams en 1993 et cité par Ribenboim [1996] sous la forme $2x^2 - 1584x + 98621$ qui n'est pas normalisée et sans restriction à des valeurs différentes: avec les conventions et règles de Boston et Greenwood que nous avons adoptées, il fournit 631 valeurs premières, de $x = 6$ à 1005 .

Nous améliorons le record du 50 (avec le polynôme de Ruby $36x^2 + 18x - 1801$, qui donne 49 valeurs premières). Nous n'améliorons pas le record du 100 mais nous donnons un polynôme qui fournit 89 valeurs premières, et nous complétons la liste de Boston et Greenwood des polynômes donnant 88, 87 et 86 valeurs premières. Nous améliorons — considérablement — le record du 1000 (avec le polynôme $x^2 + x - 1354363$, qui donne 698 valeurs premières).

Nous terminons en donnant "en continu" les meilleurs polynômes jusqu'à 40338 valeurs consécutives de la variable.

c. Un troisième aspect du problème est la *densité des nombres premiers* fournis par un polynôme F , i.e. l'étude de la fonction :

$$\pi_F(x) = \text{card}\{n \mid |F(n)| \leq x \text{ et } |F(n)| \text{ premier}\}.$$

Une conjecture, due à Hardy et Littlewood [1923] pour les polynômes du second degré, relie cette densité au logarithme intégral par une constante qui dépend du polynôme F . Dans le cas le plus simple où $F(x) = x^2 + x + c$, et si le discriminant Δ n'est pas un carré parfait, cette conjecture s'énonce :

$$\pi_F(x) \sim 2 C_\Delta L_F(x),$$

où

$$\begin{aligned} C_\Delta &= \prod_{p \geq 3} \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{1 + \left(\frac{\Delta}{p}\right)}{p}\right) \\ &= \prod_{p \geq 3} \left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p-1}\right), \end{aligned}$$

$\left(\frac{\Delta}{p}\right)$ étant le symbole de Legendre, et

$$L_F(x) = \int^{\sqrt{x}} \frac{dt}{2 \log t} \sim \frac{\sqrt{x}}{\log x}.$$

Le calcul de la constante de Hardy–Littlewood et des expérimentations numériques ont été faites dans le cas $F(x) = x^2 + x + c$, avec la restriction $c > 0$. Les travaux les plus récents sont ceux de Fung et Williams [1990].

On utilisera, dans le modèle probabiliste qui sera développé au paragraphe 3, la constante qui généralise cette constante dans le cadre de l'*hypothèse H* [Hardy et Littlewood 1923; Schinzel et Sierpiński 1958; Schinzel 1961/1962; Bateman et Horn 1962].

d. Le quatrième aspect est la *conjecture de Schinzel*, forme qualitative de l'hypothèse H, que l'on peut énoncer pour n valeurs successives d'un même polynôme : s'il n'existe aucun nombre premier qui, pour tout m , divise au moins l'un des entiers

$$F(m), F(m + 1), \dots, F(m + n - 1),$$

alors il existe une infinité de m tels que les entiers $F(m), F(m + 1), \dots, F(m + n - 1)$ soient tous premiers.

Cette conjecture est hors d'atteinte aujourd'hui (son cas particulier le plus simple donnerait l'existence d'une infinité de nombres premiers jumeaux), mais elle possède une base heuristique très forte. On

peut néanmoins remarquer que, quel que soit n , il existe un polynôme qui prend exactement n valeurs premières pour n valeurs consécutives de la variable. En effet, dans le cas où les n valeurs imposées sont toutes égales modulo $(n - 1)!$, il est immédiat de vérifier que le polynôme d'interpolation est à coefficients entiers.

Nous développons un modèle probabiliste simplifié cohérent avec l'hypothèse H, et qui permet de conserver un intérêt aux records que nous avons évoqués plus haut. En effet, ce modèle probabiliste suggère que, si l'on n'a pas battu le record pour n avec des "petits" polynômes et des "petites" valeurs, alors il faut dépasser ce que nous appellerons un *mur de Schinzel* (pour les coefficients et/ou les valeurs de la variable) pour trouver un polynôme convenable. L'ordre de grandeur du mur de Schinzel est n^n .

2. RECORDS PONCTUELS

L'essentiel de cette étude se limite aux polynômes du second degré et les records pour les polynômes de degré supérieur sont rassemblés dans le dernier paragraphe. On notera que le premier degré est un problème à part, pour lequel des recherches numériques gigantesques ont été réalisées, avec des résultats intéressants en soi, mais inférieurs à ceux des polynômes de degré supérieur. On trouvera l'historique et les derniers résultats dans [Ribenoim 1996].

Nos résultats les plus marquants sont récapitulés ci-dessous. La notation " $[m_1 \dots m_2]_n$ " signifie que le record est obtenu pour n valeurs de départ de la variable, la plus petite étant m_1 et la plus grande m_2 .

- sur 50 valeurs consécutives de la variable :
 - nouveau record 49 avec $36x^2 + 18x - 1801$ $[-41 \dots -33]_5$;
 - pour 48, nous avons trouvé 10 polynômes en plus des 2 précédemment connus ; en termes de valeurs du coefficient directeur a , les extrêmes sont $x^2 + x - 1354363$ $[1139 \dots 1139]_1$ et $123x^2 + 9x - 5783$ $[-28 \dots -28]_1$;
- sur 100 valeurs consécutives de la variable :
 - le record 90 de Boston et Greenwood avec le polynôme $41x^2 + 33x - 43321$ $[-57 \dots -57]_1$ n'est pas battu ;

- pour 89, aucun polynôme n'était connu, et nous avons trouvé

$$3x^2 + 3x - 765949 \quad [439 \dots 439]_1 ;$$

- pour 88, nous avons recensé 13 polynômes, soit 4 de plus que Boston et Greenwood ;
- sur 1000 valeurs consécutives de la variable :
 - nous avons porté le record à 698 avec le polynôme $x^2 + x - 1354363 \quad [574 \dots 642]_5$;
 - meilleures valeurs suivantes 685 (avec $x^2 + x - 752293 \quad [352 \dots 373]_5$ et $4x^2 + 2x - 349513 \quad [-570 \dots -570]_1$), 684 (avec $4x^2 + 2x - 501229 \quad [-566 \dots -564]_3$), 681, etc.

Notre méthode d'exploration repose sur une recherche exhaustive portant — dans certaines limites des coefficients — sur les polynômes qui satisfont à un certain test relatif aux diviseurs premiers périodiques. Nous appelons diviseur premier périodique, en abrégé "dpp", d'un polynôme F , tout nombre premier p qui, pour tout m , divise au moins l'un des entiers $F(m), F(m + 1), \dots, F(m + p - 1)$ (si c'est le cas, alors p divise en principe deux valeurs, et une seule pour un nombre fini de p). Notre méthode a en commun avec celle de Boston et Greenwood [1995] que le test repose sur la condition :

$$\sum_{\substack{p \text{ dpp} \\ p \leq p_0}} \frac{1}{p} \leq t,$$

avec p_0 et t convenablement choisis. Elle en diffère par contre sur le point suivant : nous effectuons la recherche par des boucles emboîtées portant dans l'ordre sur les coefficients a, b, c de $F(x) = ax^2 + bx + c$ (normalisé par $a \geq 1$ et $0 \leq b \leq a$), avec le test dans la boucle interne sur c , tandis que Boston et Greenwood exploraient les polynômes en fonction de leur discriminant Δ (en effet, le caractère p dpp est équivalent à $(\frac{\Delta}{p}) = 0$ ou 1). Cette exploration en fonction du discriminant, qui paraissait au début intéressante, se révèle ensuite à la fois plus lente et moins efficace que l'exploration exhaustive.

3. MODÈLES HEURISTIQUES PROBABILISTES

3.1. Introduction

On va tout d'abord préciser les éventuelles obstructions à l'hypothèse de Schinzel. Introduisons :

$$\omega^{(n)}(p) = \text{card}\{x = 0, 1, \dots, p - 1 \mid F(x)F(x + 1) \cdots F(x + n - 1) \equiv 0 \pmod{p}\}.$$

Cette fonction, qui interviendra ultérieurement dans le calcul de la constante de Hardy–Littlewood de notre modèle probabiliste, est comprise entre 0 et p , et provoque une obstruction à l'hypothèse de Schinzel lorsqu'elle est égale à p . Sa valeur peut être calculée très simplement. Soit r le nombre de racines de F modulo p . On a $r = 0, 1$ ou 2 ; lorsque $r = 2$, considérons les deux représentants entiers standards de ces racines : $0 \leq \alpha_1 < \alpha_2 \leq p - 1$, et définissons $\delta = \min(\alpha_2 - \alpha_1, p - \alpha_2 + \alpha_1)$. On a alors :

$$\begin{aligned} \text{si } r = 0, & \quad \omega^{(n)}(p) = 0, \\ \text{si } r = 1, & \quad \omega^{(n)}(p) = \min(n, p), \\ \text{si } r = 2, & \quad \omega^{(n)}(p) = \min(2n, n + \delta, p). \end{aligned}$$

On notera que, si par exemple un polynôme ne possède pas de dpp inférieur à $2n$, alors il ne présente aucune obstruction à l'hypothèse de Schinzel. On peut alors demander quel intérêt il y a à dire que le polynôme $36x^2 + 18x - 1801$ (polynôme de Ruby) prend 45 valeurs premières pour 50 valeurs consécutives de la variable (le plus petit intervalle étant $[-31, 18]$) ? En effet, on peut trouver des polynômes sans dpp inférieur à 100 (par exemple $37x^2 + 37x - 20323$ ou $x^2 + x - 65288413$ ou encore $x^2 + x - 213577963$) et, en vertu de la remarque qui précède, l'hypothèse de Schinzel dit qu'un tel polynôme prendra (une infinité de fois) 50 valeurs premières sur 50.

La réponse sera donnée par le modèle probabiliste qui suggère que, si les 50 valeurs premières sur 50 n'ont pas été obtenues avant des valeurs (du polynôme) de l'ordre de quelques milliers, alors il faudra attendre un ordre de grandeur de 50^{50} pour les trouver.

3.2. Notations générales

Etant donné un polynôme du second degré à coefficients entiers $F(x) = ax^2 + bx + c$, on fixe un entier positif n et on s'intéresse, pour tout m compris entre 0 et n , à la fonction

$$A_{F,m} = \text{nombre de valeurs premières sur les } n \text{ valeurs } F(m), F(m + 1), \dots, F(m + n - 1),$$

qui sera naturellement modélisée par une variable aléatoire B_m .

Le premier modèle probabiliste concerne la recherche d'exactly n valeurs premières de F pour n valeurs consécutives de la variable, avec pour finalité de donner une estimation (le mur de Schinzel) du temps d'attente de l'évènement « $B_m = n$ » à partir de m_0 . On verra que ce mur de Schinzel est dans une zone allant de $n^{n/9}$ (considération de tous les polynômes d'un certain ensemble) à n^n (considération d'un seul polynôme).

Le second modèle étudie l'espérance et l'écart-type de la loi de B_m , et "explique" notamment les résultats de Fung et Williams [1990].

Dans les deux cas, le point de départ de la modélisation est une suite de variables aléatoires de Bernoulli $(X_m)_{m \geq 0}$, avec comme première contrainte que la probabilité que $X_m = 1$, qui symbolise la condition $F(m)$ premier, soit décroissante et asymptotiquement égale à la fréquence des valeurs premières de F "autour" de la valeur m de la variable.

4. PREMIER MODÈLE PROBABILISTE, POUR $k = n$

4.1. Modèle probabiliste fondamental : cas d'un seul polynôme

On pose $E_m = \llbracket B_m = n \rrbracket$ et on associe à cet évènement une variable de Bernoulli Y_m .

Si on considère un polynôme F et un modèle probabiliste associé à F , une valeur de n ainsi qu'une fonction $\varepsilon(T) = o(1)$, on définit le *mur de Schinzel* de F comme la valeur de T telle que l'espérance mathématique du temps d'attente de E_m sur l'intervalle $[T^{1-\varepsilon}, T]$ soit égale à T . Cette définition dépend de la fonction ε mais cela n'affecte pas son ordre de grandeur (on ne peut pas prendre l'intervalle $[0, T]$ car il y a une probabilité — faible mais non négligeable — d'obtenir E_m pour des "petites" valeurs de m).

Comme $X_m = 1$ doit symboliser $F(m)$ premier, et en supposant que F n'a aucun dpp jusqu'à n — on négligera dans ce modèle très simplifié l'influence des dpp compris entre n et $2n$ — on pose :

$$P(X_m = 1) = \prod_{n < p \leq m\sqrt{a}} \left(1 - \frac{1}{p}\right),$$

que l'on remplace, en vertu du théorème de Mertens, par son équivalent :

$$P(X_m = 1) = \frac{\log n}{\log m}.$$

Il faudra bien sûr supposer $m \geq n$, mais la validité même du modèle pourra être plus restreinte, car on ne peut pas s'affranchir pour les petites valeurs de m de l'effet des coefficients a et c .

On peut faire alors une double approximation : d'une part considérer que, sur un intervalle de type $[T^{1-\varepsilon}, T]$, où $\varepsilon = \varepsilon(T) = o(1)$, on peut remplacer $\log m$ par $\log T$, d'autre part estimer le temps d'attente de E_m par l'inverse de la densité des évènements E_m . Cette estimation est justifiée car elle est valide dans le cas d'une probabilité constante (répétition d'une épreuve de Bernoulli de paramètre p).

Le compte des évènements E_m sur $[T^{1-\varepsilon}, T]$ est l'espérance mathématique de la somme des Y_m , que l'on peut exprimer, sans être gêné par le fait que les évènements E_m ne sont pas indépendants, comme la somme des $E(Y_m)$. Compte tenu de la première approximation on considère $P(X_m = 1)$ comme constante sur l'intervalle $[T^{1-\varepsilon}, T]$, en lui attribuant la valeur $u = u(T) = \frac{\log n}{\log T}$. On a alors

$$E(Y_m) = P(E_m) = u^n,$$

de sorte que l'estimation du temps d'attente est

$$\frac{1}{u^n} = \left(\frac{\log T}{\log n}\right)^n.$$

Le mur de Schinzel est caractérisé par la condition :

$$\left(\frac{\log T_{\text{sch}}}{\log n}\right)^n \sim T_{\text{sch}},$$

et on obtient $T_{\text{sch}} \sim n^n$.

Proposition 1. *Si on associe au polynôme F (du deuxième degré) et à l'entier naturel n le modèle probabiliste décrit ci-dessus, caractérisé notamment par la probabilité uniforme :*

$$P(X_m = 1) = \frac{\log n}{\log m}$$

et l'hypothèse d'indépendance des évènements E_m , et si on prend comme évaluation du temps d'attente l'inverse de la densité des évènements E_m , alors l'estimation de la valeur du mur de Schinzel est :

$$T_{\text{sch}} \sim n^n.$$

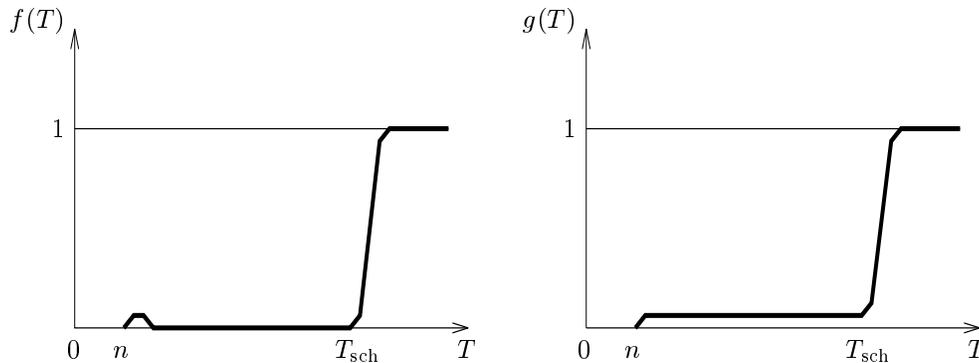


FIGURE 1. Comportement des probabilités $f(T)$ et $g(T)$.

On peut compléter ce résultat en donnant le comportement des fonctions :

$$f(T) = P(\text{au moins un évènement } E_m \text{ sur l'intervalle } [\frac{1}{2}T, T]),$$

$$g(T) = P(\text{au moins un évènement } E_m \text{ sur l'intervalle } [n, T]),$$

que l'on obtient en raccordant une simulation numérique pour les "petites" valeurs de T avec notre estimation asymptotique (voir la figure 1).

Ce modèle est très simplifié (par exemple, il néglige l'influence, déjà évoquée plus haut, des coefficients a et c pour les "petites" valeurs de T) mais, lorsque nous l'affinerons, la description du comportement de $f(T)$ et de $g(T)$ restera qualitativement inchangée, et seuls les paramètres numériques devront être ajustés (à noter que les résultats ne sont pas modifiés de façon significative par le remplacement de $[\frac{1}{2}T, T]$ par $[\lambda T, T]$ ou par $[T^{1-\epsilon}, T]$).

On notera la cohérence entre la valeur proposée pour le mur de Schinzel et le fait que le polynôme d'interpolation évoqué à la fin du paragraphe 1 prend des valeurs (et possède des coefficients) d'ordre de grandeur $(n - 1)!$, qui est logarithmiquement équivalent à n^n .

4.2. Première variation : polynômes de degré égal ou supérieur à 3

En restant dans le cas simplifié, la modélisation de $P(X_m = 1)$ pour un polynôme $F(x) = ax^d + \dots$ devient naturellement :

$$P(X_m = 1) = \prod_{n < p \leq \sqrt{am^d}} \left(1 - \frac{1}{p}\right),$$

que l'on remplace par son équivalent :

$$P(X_m = 1) = \frac{2 \log n}{d \log m}.$$

L'estimation du temps d'attente est alors :

$$\left(\frac{d \log T}{2 \log n}\right)^n,$$

et le mur de Schinzel est caractérisé par :

$$\left(\frac{d \log T_{sch}}{2 \log n}\right)^n \sim T_{sch};$$

on ne peut plus donner d'équivalent simple de T_{sch} mais on peut néanmoins calculer un développement limité généralisé de $\log T_{sch}$:

Proposition 2. *Si on étend au polynôme F , de degré d , le modèle probabiliste précédemment décrit, on obtient comme estimation de la valeur du mur de Schinzel :*

$$\log T_{sch} = n \log \left(\frac{d}{2}n\right) + O\left(\frac{n}{\log n}\right).$$

Ce résultat est cohérent avec la remarque expérimentale que les meilleures valeurs sont obtenues avec des polynômes du second degré (le cas des polynômes du premier degré étant toujours exclu), et que la performance décroît avec le degré.

4.3. Deuxième variation : introduction d'une constante propre au polynôme

Nous revenons maintenant au cas des polynômes du second degré. La modélisation :

$$P(X_m = 1) = \prod_{n < p \leq m\sqrt{a}} \left(1 - \frac{1}{p}\right)$$

est une sorte de valeur médiane, et doit être corrigée par une constante multiplicative propre au polynôme particulier considéré.

En commençant par effectuer cette correction de façon individuelle (i.e. en conservant l’hypothèse des X_m indépendantes), on écrirait :

$$P(X_m = 1) = \prod_{n < p \leq m\sqrt{a}} \left(1 - \frac{\omega(p)}{p}\right),$$

où $\omega(p)$ est le nombre de solutions modulo p de la congruence $F(x) \equiv 0 \pmod{p}$. On a $\omega(p) = 0, 1$ ou 2 et cela peut être précisé comme suit (on suppose que les coefficients a, b, c de F sont premiers entre eux) :

- si p divise a , $\omega(p) = 0$ ou 1 selon que $b \equiv 0$ ou non,
- si p ne divise pas a , on écrit

$$4aF(x) = (2ax + b)^2 - \Delta,$$

et on en déduit :

$\omega(p) = 1$ si p est un diviseur du discriminant Δ du polynôme F ,

$\omega(p) = 2i$ ou 0 selon que Δ est ou n’est pas résidu quadratique modulo p .

On pourrait alors, toujours en conservant les hypothèses de base de la modélisation (indépendance des X_m , $m \in [T^{1-\varepsilon}, T]$ et T tend vers l’infini), multiplier l’estimation initiale

$$\begin{aligned} P(X_m = 1) &= \prod_{n < p \leq m\sqrt{a}} \left(1 - \frac{1}{p}\right) \\ &\sim \prod_{n < p \leq m} \left(1 - \frac{1}{p}\right) \sim \frac{\log n}{\log m}, \end{aligned}$$

par le facteur correctif

$$\prod_{p > n} \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{\omega(p)}{p}\right).$$

Il est préférable d’introduire le produit infini “complet”, pour $p \geq 3$, de manière à obtenir une présentation uniforme. Pour éviter toute ambiguïté, on peut rappeler la difficulté majeure des premiers modèles probabilistes, mise en lumière dans l’article fondateur de Hardy et Littlewood [1923], et qui trouve son origine dans le fait que la densité des nombres premiers au voisinage de x n’est pas équivalente au

produit $\prod_{p \leq \sqrt{x}} (1 - 1/p)$ et qu’il faut un facteur correctif $e^\gamma/2$. La constante C_Δ introduite au premier paragraphe s’interprète alors comme une correction arithmétique de la “probabilité” standard $1/\log x$ d’être premier lorsque les valeurs du polynôme sont voisines de x .

Mais, s’il est raisonnable de modéliser par une probabilité $1 - 1/p$ (ou $1 - \omega(p)/p$) la non-divisibilité par p d’une valeur $F(m)$, il n’est pas souhaitable de modéliser par $(1 - 1/p)^n$ (ou $(1 - \omega(p)/p)^n$) la non-divisibilité par p de n valeurs $F(m), F(m + 1), \dots, F(m + n - 1)$ pour des valeurs de p peu supérieures à n , et on doit remplacer le modèle où les variables X_m sont indépendantes par un modèle plus réaliste. Cela peut se faire en reprenant la fonction introduite au début du paragraphe 3 :

$$\omega^{(n)}(p) = \text{card}\{x = 0, 1, \dots, p - 1 \mid F(x)F(x + 1) \dots F(x + n - 1) \equiv 0 \pmod{p}\},$$

pour exprimer le facteur local $1 - \omega^{(n)}(p)/p$.

En rassemblant toutes ces considérations, on remplace l’estimation :

$$E(Y_m) = P(E_m) = \left(\frac{\log n}{\log T}\right)^n$$

du modèle simplifié initial par :

$$E(Y_m) = P(E_m) = \frac{C_F^{(n)}}{(\log T)^n},$$

avec :

$$C_F^{(n)} = \prod_{p \geq 3} \left(1 - \frac{1}{p}\right)^{-n} \left(1 - \frac{\omega^{(n)}(p)}{p}\right)$$

(le facteur $(1 - \frac{1}{2})^{-n}$ qui fait défaut dans l’expression de $C_F^{(n)}$ est annulé par un facteur $(\frac{1}{2})^n = 1/(\text{deg } F)^n$).

Le mur de Schinzel est maintenant caractérisé par la condition :

$$\frac{(\log T_{\text{sch}})^n}{C_F^{(n)}} \sim T_{\text{sch}}.$$

Il n’y a pas d’équivalent simple mais on peut obtenir un développement limité du logarithme :

Proposition 3. *Si on associe au polynôme F du second degré et à l’entier n le modèle probabiliste lié à l’arithmétique de F , caractérisé notamment par la probabilité globale :*

$$P(E_m) = \frac{C_F^{(n)}}{(\log T)^n},$$

et si on pose pour simplifier les notations $C_F^{(n)} = (K \log n)^n$, alors on obtient le développement limité généralisé suivant du logarithme du mur de Schinzel:

$$\log T_{\text{sch}} = n \left(\log n + \log \log n - \frac{\log K}{\log n} + O\left(\frac{1}{\log^2 n}\right) \right).$$

On notera que le premier terme du développement de $\log T_{\text{sch}}$ est $n \log n$, terme unique du modèle simplifié.

On peut présenter trois estimations numériques (pour les polynômes cités au début du paragraphe 3), qui permettront de se faire une idée des ordres de grandeur des constantes de Hardy–Littlewood, de comparer $C_F = C_F^{(1)}$ et $(C_F^{(n)})^{1/n}$, et de constater que le K introduit ci-dessus pour exprimer le développement limité est très voisin de 1 :

n	$F(x)$	C_F	$(C_F^{(n)})^{1/n}$	K
50	$37x^2 + 37x - 20323$	4.218	3.872	0.990
50	$x^2 + x - 65288413$	4.316	4.190	1.071
50	$x^2 + x - 213577963$	4.121	3.817	0.976

Pour l’expérimentation numérique que nous avons menée pour valider ce modèle, le gigantisme du mur de Schinzel nous a contraint à nous limiter à des valeurs $n \leq 7$ (le plus grand mur dans notre expérimentation vaut 330.10^6). Les résultats, qui sont rapportés en détail à la fin de ce paragraphe, confirment ce que nous avons écrit précédemment : d’une part des évènements E_m surviennent dans la zone du mur de Schinzel, d’autre part les évènements E_m sont rares entre les “petites” valeurs de m et le voisinage du mur de Schinzel (néanmoins ce phénomène n’est pas aussi marqué que nous l’avons prédit).

4.4. Troisième variation : recherche exhaustive

On souhaite modéliser maintenant, non pas le comportement d’un polynôme donné, mais la recherche sur un ensemble de polynômes et un intervalle de valeurs de la variable. Nous continuerons à nous limiter aux polynômes du deuxième degré.

On considère le “produit” ensemble de polynômes \times intervalle de valeurs de la variable, dont on représentera les éléments par des suites de valeurs prises. Si $(v_0, v_1, \dots, v_{n-1})$ est une suite de valeurs prises par un polynôme du deuxième degré à coefficients

entiers, elle vérifie la condition de différences secondes constantes et peut être représentée de façon bijective par le triplet de termes $\{v_0, v_{[n/2]}, v_{n-1}\}$. Si on fixe V (positif), on définit un ensemble $\mathcal{S}(V)$ de suites par

$$v = \max(|v_0|, |v_{[n/2]}|, |v_{n-1}|) \in [V/2, V].$$

Il y a *a priori* $\frac{7}{3}V^3 + O(V^2)$ ensembles de 3 entiers vérifiant cette localisation, mais interviennent deux conditions de divisibilité, par $2n$ et par n^2 , qui donnent

$$\text{card } \mathcal{S}(V) \sim \frac{7V^3}{6n^3}.$$

Si on prend $m_0 = 2^s$ et si on donne à V les valeurs successives $2^{s+1}, 2^{s+2}, \dots$, les $\mathcal{S}(V)$ forment une suite exhaustive par rapport aux polynômes et aux valeurs de la variable. On peut en déduire des majorations des coefficients d’un polynôme de $\mathcal{S}(V)$ et des valeurs “typiques” (maximums de vraisemblance heuristique et non pas moyennes) sont d’ordre de grandeur

$$\frac{V^{1/3}}{n^{4/9}} \text{ pour } |a|, V \text{ pour } |c|, \text{ et } n^{2/9}V^{1/3} \text{ pour } |x|.$$

Le modèle qui serait obtenu en introduisant la constante propre à chaque polynôme est beaucoup trop compliqué pour pouvoir être étudié, et on négligera donc les constantes de Hardy–Littlewood des polynômes. On pose donc :

$$P(X_m = 1) = \prod_{n < p \leq \sqrt{V}} \left(1 - \frac{1}{p}\right).$$

L’estimation de Mertens donne maintenant

$$P(X_m = 1) = u(V) \sim \frac{2 \log n}{\log V},$$

et le mur de Schinzel de la recherche exhaustive est caractérisé par la condition :

$$\left(\frac{\log V}{2 \log n}\right)^n \sim \frac{7V^3}{6n^3},$$

d’où l’on déduit :

Proposition 4. *Si l’on associe aux polynômes du deuxième degré et à l’entier n le modèle probabiliste simplifié exhaustif exposé ci-dessus, alors on obtient pour le logarithme de la variable V , le développement limité généralisé suivant :*

$$\log V = \frac{n}{3} \left(\log n - \log 6 + O\left(\frac{1}{\log n}\right) \right).$$

Corollaire 1. *Les maximums de vraisemblance heuristiques des murs de Schinzel sont alors (en se limitant à l'exponentielle du premier terme) :*

$$\begin{aligned} n^{n/9} & \text{ pour le coefficient } |a|, \\ n^{n/3} & \text{ pour le coefficient } |c|, \\ n^{n/9} & \text{ pour la variable } |x|. \end{aligned}$$

Si on prend $n = 45$, et si on applique non pas $n^{n/9}$ et $n^{n/3}$, mais les estimations déduites exactement des valeurs “typiques”, on obtient $|a|$ vers 4000, $|c|$ vers 10^{13} , et $|x|$ vers 50000. Tout cela est extrêmement grossier, mais il n'est pas interdit d'espérer que l'on pourra peut-être améliorer — un peu — le record de Ruby...

4.5. Validation numérique du modèle probabiliste

Nous avons effectué une statistique, pour des valeurs de $n \leq 7$ (cela donne des murs de Schinzel allant jusqu'à $330 \cdot 10^6$, et on ne peut pas faire de statistique significative avec $n \geq 8$), du temps d'attente des premières suites de n valeurs premières (pour n valeurs consécutives de la variable).

L'“échantillon” a été constitué par 8 polynômes $x^2 + x + c$, avec $c = 11, 17, -19, -103, 167, -199, 227, -283$ (et 20 valeurs de n entre 4 et 7), ensemble qui a été choisi pour donner un très large éventail des constantes de Hardy–Littlewood et des murs de Schinzel.

Les constantes de Hardy–Littlewood interviennent, non pas par leur valeur exacte (délicate à calculer), mais par la valeur obtenue en tronquant le produit infini à la racine carrée du mur de Schinzel $T^{(n)}$. Pour annuler un “effet de chance” pour les petites valeurs de la variable, nous avons choisi de chercher les débuts t de n -blocs supérieurs à $\sqrt{T^{(n)}}$, en considérant comme caractéristique la deuxième valeur t_2 , pour laquelle nous avons calculé le quotient $r_2 = t_2/T^{(n)}$; nous avons enfin considéré le nombre total k de t trouvés dans l'intervalle $I = [\sqrt{T^{(n)}}, 10T^{(n)}]$. Un résumé significatif des résultats numériques est le suivant :

- les 20 valeurs de r_2 varient entre 0.005 et 5.80, la médiane est à 0.5 ;
- les 20 valeurs de k varient entre 3 et 12, la médiane est à 6.

On peut faire deux commentaires. D'une part il n'y a aucun cas sans n -bloc dans l'intervalle

$$[\sqrt{T^{(n)}}, 10T^{(n)}],$$

ce qui nous paraît valider expérimentalement la notion de mur de Schinzel. D'autre part il y a une très grande irrégularité de distribution, surtout vers les petites valeurs de r_2 ; cela “explique” que les valeurs effectivement trouvées pour $\nu(n)$ (voir paragraphe 7 pour cette notation) soient meilleures que ce que le modèle probabiliste pourrait laisser espérer (à noter que pour un polynôme donné, il y a parfois de très fortes différences de performance d'une valeur de n à une autre).

5. DEUXIÈME MODÈLE PROBABILISTE, POUR $k < n$

L'idée de base est d'utiliser $2C_F/\log y$ comme fournissant une estimation du paramètre p d'une loi binomiale lorsque $|F(x)|$ est d'ordre de grandeur de y . C'est l'esprit des tables numériques [Fung et Williams 1990; Lukes et al. 1995; Stephens et Williams 1990] qui considèrent les polynômes $F(x) = x^2 + x + c$ ($c > 0$) et donnent notamment une suite de valeurs croissantes de la constante de Hardy–Littlewood C_F (alias C_Δ) correspondant à une suite de valeurs croissantes de c . Nous donnons ici un modèle probabiliste simplifié pour la croissance de C_F lorsque $|c|$ tend vers l'infini.

Nous compléterons ensuite ce modèle en en déduisant une valeur heuristique de l'optimum “ k sur n ” en fonction de n .

5.1. Croissance de la constante de Hardy–Littlewood

Fixons une valeur z et considérons l'ensemble \mathcal{C}_z des valeurs de c telles que les polynômes $x^2 + x + c$ n'aient aucun dpp inférieur ou égal à z . Cet ensemble est déterminé par une suite de congruences modulo les nombres premiers inférieurs ou égaux à z :

$$\begin{aligned} c & \equiv 1 \pmod{2}, \\ c & \equiv 2 \pmod{3}, \\ c & \equiv 1 \text{ ou } 2 \pmod{5}, \\ c & \equiv 3, 4 \text{ ou } 6 \pmod{7}, \\ & \text{etc.} \end{aligned}$$

Soit p_k le plus grand nombre premier inférieur ou égal à z . Si on pose :

$$P_k = \prod_{p \leq p_k} p,$$

ce système de congruences possède exactement :

$$N_k = \prod_{3 \leq p \leq p_k} \frac{p-1}{2} = \frac{1}{2^k} P_k \prod_{3 \leq p \leq p_k} \left(1 - \frac{1}{p}\right)$$

solutions, de sorte que l'écart moyen entre deux solutions consécutives est :

$$\delta_k = 2^k \prod_{3 \leq p \leq p_k} \left(1 - \frac{1}{p}\right)^{-1},$$

et qu'une médiane de la plus petite valeur absolue d'un élément $c \in \mathcal{C}_z$ est (théorème de Mertens) :

$$\frac{1}{4} \delta_k \sim e^\gamma 2^{k-3} \log z.$$

Pour un polynôme "au hasard" F sans dpp inférieur ou égal à z , on peut écrire :

$$\begin{aligned} C_F &= \prod_{p \geq 3} \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{\omega(p)}{p}\right) \\ &= \prod_{3 \leq p \leq p_k} \left(1 - \frac{1}{p}\right)^{-1} \prod_{p > p_k} \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{\omega(p)}{p}\right) \\ &= C'(z) C_F''(z), \end{aligned}$$

avec :

$$C'(z) \sim h(z) = \frac{1}{2} e^\gamma \log z,$$

tandis que $C_F''(z)$ fluctue autour de 1 en fonction de la balance entre $\omega(p) = 0$ ou 2 pour les $p > p_k$. On peut supposer que le polynôme correspondant au coefficient c de plus petite valeur absolue est "au hasard" par rapport à cette balance et que la valeur "typique" de sa constante $C_F''(z)$ est donc 1.

Le tableau 1 donne, pour les nombres premiers entre 59 et 139, $z = p_k$ et k , une valeur arrondie de $\delta_k/4$, celle du coefficient c de plus petite valeur absolue, la valeur du discriminant $\Delta = 1 - 4c$ du polynôme

$$F(x) = x^2 + x + c$$

(de façon à permettre la comparaison avec les tables de Fung et Williams — dont on rappelle qu'ils se sont restreints aux valeurs positives de c), la valeur médiane $h(z)$ de la constante de Hardy–Littlewood, et enfin une approximation sommaire de la constante C_F (alias C_Δ) du polynôme F .

Les valeurs expérimentales sont en excellent accord avec la modélisation probabiliste de cette situation très simple (bien entendu, lorsque c est positif, on retrouve la valeur de la table 2.1 de Fung et Williams), avec néanmoins des fluctuations qui ne sont pas négligeables.

$z = p_k$	k	$\delta_k/4$	c	Δ	$h(z)$	C_F
59	17	122500	-53509	214037	3.361	3.270
61	18	249000	-501229	2004917	3.661	4.008
67	19	505600	9063641	-36254563	3.744	3.637
71	20	1025600	12899891	-51599563	3.796	3.851
73	21	2079700	24073871	-96295483	3.821	3.853
79	22	4212800	24073871	-96295483	3.891	3.853
83	23	8528000	28537121	-114148483	3.935	4.033
89	24	17250500	-40880029	165520117	3.997	3.831
97	25	34860000	-40880029	165520117	4.074	3.831
101	26	70418000	-65288413	261153653	4.110	4.316
103	27	142220000	-65288413	261153653	4.127	4.316
107	28	287120000	146452961	-585811843	4.161	4.119
109	29	579550000	-432015433	1728061733	4.178	4.245
113	30	1169450000	-432015433	1728061733	4.210	4.245
127	31	2357460000	-2361810469	9447241877	4.314	4.554
131	32	4751200000	-4888301653	19553200613	4.342	4.625
137	33	9572300000	-12276955783	49107823133	4.381	4.842
139	34	19283000000	-12276955783	49107823133	4.394	4.842

TABLEAU 1. Comparaison entre les valeurs du modèle probabiliste et les valeurs expérimentales.

On peut rassembler les valeurs heuristiques trouvées.

Proposition 5. *Dans le modèle probabiliste de la croissance des constantes de Hardy–Littlewood décrit ci-dessus, étant donné un paramètre réel z , et en posant $k = \pi(z) \sim z/\log z$, on a les résultats suivants:*

- *il existe un polynôme $F(x) = x^2 + x + c$, sans dpp inférieur ou égal à z , avec:*

$$|c| \approx \frac{1}{4} \delta_k = 2^{k-2} \prod_{3 \leq p \leq p_k} \left(1 - \frac{1}{p}\right)^{-1} \\ \sim e^\gamma 2^{k-3} \log z;$$

- *pour ce polynôme on a $C_F \approx \frac{1}{2} e^\gamma \log z$, ce qui donne une densité de nombres premiers au voisinage de l'origine:*

$$p \approx \frac{2C_F}{\log |c|} \sim \frac{e^\gamma \log z}{k \log 2} \sim \frac{e^\gamma}{\log 2} \cdot \frac{\log^2 z}{z}.$$

Ces équivalents donnent pour les petites valeurs de z des valeurs très médiocres. Pour des calculs ultérieurs dans la zone 50 à 200 qui nous intéresse le plus, on utilisera des approximations asymptotiquement équivalentes mais numériquement meilleures: $k \approx z/(\log z - 1)$, et $\log |c| \approx (k - 3) \log 2 - \log \log z + \gamma$.

Pour se rapprocher des meilleures constantes de Hardy–Littlewood, il faudrait tenir compte de l'observation que le meilleur polynôme de \mathcal{C}_z est souvent très d'être celui qui possède le coefficient c de plus petite valeur absolue. En notant F_1, F_2, \dots la suite des polynômes de \mathcal{C}_z classés par ordre croissant de $|c|$, on peut donner deux exemples, le premier impliquant le polynôme exceptionnel $x^2 + x - 1354363$, le second plus banal:

- pour $z = 37$, $F_1(x) = x^2 + x + 41$, avec $C_F = 3.320$, $F_2(x) = x^2 + x - 18523$, avec $C_F = 3.081$, tandis que $F_{211}(x) = x^2 + x - 1354363$, avec $C_F = 4.330$,
- pour $z = 59$, $F_1(x) = x^2 + x - 53509$, avec $C_F = 3.270$, tandis que $F_2(x) = x^2 + x - 249439$, avec $C_F = 3.786$.

La considération des ensembles \mathcal{C}_z n'optimise pas la recherche des plus grandes constantes de Hardy–Littlewood. On peut imaginer par exemple qu'un polynôme possède un unique "très petit" dpp (ou, dans un sens à préciser, "peu" de petits dpp). Il

serait alors ignoré par les ensembles \mathcal{C}_z et fournirait néanmoins une excellente constante de Hardy–Littlewood. L'exemple est bien sûr le polynôme $x^2 + x - 1354363$ qui a peu de petits dpp. La première question est alors celle-ci: quel est le plus petit c (en valeur absolue) tel que C_{x^2+x+c} soit supérieur à $C_{x^2+x-1354363} = 4.3305$? La table de Fung et Williams donne $C_{x^2+x+398878547} = 4.3617$ mais ce n'est peut-être pas le meilleur.

5.2. Optimum "k sur n" en fonction de n

L'hypothèse implicite faite jusqu'ici sur le second modèle probabiliste est que l'on travaille au voisinage de l'origine, très avant le mur de Schinzel. Dans le paragraphe 7, on proposera de traduire cette hypothèse par la restriction que les valeurs de F soient inférieures (en valeur absolue) à $n^{2\sqrt{n}}$ (et on s'expliquera sur l'apparence arbitraire de cette valeur).

On peut alors améliorer l'expression de la densité de nombres premiers au voisinage de l'origine, en remplaçant $p \approx 2C_F/\log |c|$ par l'expression plus fine

$$p \approx p(n, z) = 2C_F/\log(|c| + n^2),$$

ce qui est nécessaire pour faire apparaître, n étant fixé, un maximum sur z . En remplaçant C_F et $|c|$ par leurs expressions heuristiques asymptotiques, on obtient une fonction de z dont on peut localiser le maximum par référence à la valeur de z pour laquelle $|c| = n^2$, que l'on notera z_0 . On a l'estimation asymptotique $\log z_0 \sim \log \log n^2$. On peut alors montrer que le maximum de $p(n, z)$ s'obtient pour une valeur $z = o(z_0)$, avec néanmoins $\log z \sim \log z_0$, ce qui permet de donner un équivalent de $p(n, z)$.

Proposition 6. *Dans le modèle probabiliste de la croissance des constantes de Hardy–Littlewood décrit ci-dessus, on a le résultat suivant:*

Pour n donné, il existe z défini par:

$$z = z(n) \sim \frac{\log n^2 \log \log n^2}{\log 2}$$

tel que, si F est le polynôme sans dpp inférieur ou égal à z , dont l'existence "heuristique" est énoncée

dans la proposition 5, la densité p de nombres premiers au voisinage de l'origine vaut:

$$p \approx p(n, z) = \frac{2C_F}{\log(|c| + n^2)} \sim \frac{e^\gamma \log z_0}{\log n^2} \sim e^\gamma \frac{\log \log n^2}{\log n^2}.$$

Pour obtenir des valeurs numériques proches de la réalité pour n dans la zone 100 à 10^6 qui nous intéresse le plus, il faut ensuite corriger ce résultat asymptotique.

Pour une première correction, on note que la propriété $z = o(z_0)$ entraîne $|c| = o(n^2)$. On peut alors, en se restreignant aux valeurs négatives de c (le prix à payer est négligeable, la taille heuristique de $|c|$ devenant $\delta_k/2$ au lieu de $\delta_k/4$), prendre z tel que $-c \sim n^2/4$ de façon à diminuer un peu la taille des valeurs de $F(x)$ sur l'intervalle optimal, voisin de $[\sqrt{-c} - n/2 \approx 0, \sqrt{-c} + n/2 \approx n]$. La quantité $|F(x)|$ varie de façon quadratique de $n^2/4$ à 0, puis à $n^2/4$. Or, quand un polynôme varie de façon quadratique de 0 à A , le facteur logarithmique standard $1/\log A$ de la densité des nombres premiers peut être remplacé par un facteur moyen :

$$\frac{1}{\sqrt{A}} \int^{\sqrt{A}} \frac{dt}{2 \log t} \approx \frac{1}{\log A - 1}.$$

On remplace donc $1/\log n^2$ par :

$$\frac{1}{\log(n\sqrt{-c}) - 1} \approx \frac{1}{\log \frac{1}{2}n^2 - 1};$$

pour $n = 1000$ par exemple, on gagne un facteur 1.14.

Une deuxième correction prend en compte que la recherche de l'intervalle optimal, dans le cadre d'un modèle probabiliste de loi binomiale, doit faire intervenir l'écart-type. Par exemple, pour $n = 1000$ et $F(x) = x^2 + x - 1354363$, on peut analyser comme suit la performance de 698 valeurs premières sur l'intervalle $[642, 1641]$, presque centré sur $1164 \sim \sqrt{1354363}$, avec une amplitude de variation A de l'ordre de 1300000: $C_F = 4.33$,

$$2C_F/(\log A - 1) = 0.622,$$

$np = 662$, et écart-type $s = \sqrt{np(1-p)} = 15$, soit donc $698 = np + 2.4s$. Dans les données numériques qui suivent, on prendra pour valeur heuristique $np + 2s$.

Ces deux corrections étant posées, on procède numériquement comme suit: pour n donné, et sur la base des approximations $k \approx z/(\log z - 1)$ et $\log |c| \approx (k - 3) \log 2 - \log \log z + \gamma$, on détermine z tel que $|c| \approx n^2/4$, puis on calcule $2C_F \approx e^\gamma \log z$ et enfin $p(n, z) = 2C_F/(\log(n^2/2) - 1)$.

Le tableau qui suit donne, dans ce modèle numérique approché, pour $n = 100, 1000$ et 10000 , les valeurs de z et de k , la valeur de C_F correspondante, ainsi que $np, np + 2s$ (avec $s = \sqrt{np(1-p)}$) et le maximum $\nu(n)$ (voir paragraphe 7 pour la notation) constaté expérimentalement.

n	z	k	C_F	p	np	$np+2s$	$\nu(n)$
100	37	14	3.216	0.8555	86	93	90
1000	68	21	3.758	0.6199	620	651	698
10000	101	28	4.110	0.4914	4914	5014	5374

La concordance est globalement satisfaisante. Il n'y a pas d'explication évidente à la "trop bonne" valeur du modèle pour $n = 100$. Par contre, pour $n = 1000$ et $n = 10000$, l'essentiel de la discordance en sens inverse s'explique par le fait que le meilleur polynôme, $x^2 + x - 1354363$, n'est pas le polynôme heuristique. Mais il n'est pas possible de savoir si l'amplitude de la discordance est liée à ce polynôme exceptionnel ou persiste en général...

6. COMPLÉTION DES RÉSULTATS DE BOSTON ET GREENWOOD (n = 100)

Boston et Greenwood [1995] ont établi une liste de polynômes qui prennent au moins 86 valeurs premières pour 100 valeurs consécutives de la variable. Nous avons complété cette liste (voir le tableau 2) et nous conjecturons qu'elle ne peut plus être augmentée, sauf bien sûr en se rapprochant du mur de Schinzel.

7. RÉSULTATS NUMÉRIQUES: RECORDS "EN CONTINU"

Nous utilisons la notation introduite par Ribenboim mais en modifiant quelque peu sa signification.

Pour un polynôme donné F du deuxième degré (les notations peuvent être étendues aux degrés supérieurs) nous désignons par $\nu^*(F, n)$ le maximum

$41x^2 + 33x - 43321$		90	$[-57 \dots -57]_1$
$3x^2 + 3x - 765949$	N	89	$[439 \dots 439]_1$
$3x^2 + 3x - 324509$	N	88	$[265 \dots 266]_2$
$4x^2 + 2x + 41$		88	$[-40 \dots -39]_2$
$8x^2 + 2x - 1097$		88	$[-66 \dots -53]_7$
$9x^2 + 3x - 16229$		88	$[-53 \dots -47]_7$
$27x^2 + 3x - 601$		88	$[-58 \dots -58]_1$
$29x^2 + 9x - 22111$		88	$[-60 \dots -60]_1$
$31x^2 + 23x - 25771$	N	88	$[-49 \dots -49]_1$
$37x^2 + x - 25447$	N	88	$[-45 \dots -38]_7$
$37x^2 + 23x - 8863$		88	$[-47 \dots -42]_6$
$59x^2 + 3x - 30109$		88	$[-35 \dots -31]_5$
$67x^2 + 45x - 12569$		88	$[-72 \dots -61]_2$
$73x^2 + 59x - 18541$		88	$[-60 \dots -39]_5$
$164x^2 + 82x - 33023$	N	88	$[-29 \dots -28]_2$
$x^2 + x - 349513$	N	87	$[547 \dots 551]_2$
$x^2 + x - 842629$	N	87	$[851 \dots 854]_4$
$x^2 + x - 1354363$	N	87	$[1129 \dots 1142]_6$
$2x^2 - 199$		87	$[0 \dots 1]_2$
$8x^2 + 6x - 661$		87	$[-71 \dots -71]_1$
$17x^2 + 7x - 20351$		87	$[-57 \dots -56]_2$
$23x^2 + 17x - 40169$	N	87	$[-15 \dots -14]_2$
$31x^2 + 21x - 13679$		87	$[-68 \dots -61]_7$
$41x^2 + 19x - 29879$		87	$[-40 \dots -35]_4$
$41x^2 + 39x - 33829$		87	$[-67 \dots -66]_2$
$46x^2 + 30x - 15803$	N	87	$[-48 \dots -48]_1$
$145x^2 + 55x - 37123$	N	87	$[-52 \dots -52]_1$
$188x^2 + 104x - 17021$	N	87	$[-60 \dots -57]_4$

TABLEAU 2. Complétion de la liste de Boston et Greenwood. Les nouveaux polynômes que nous avons trouvés sont marqués par la lettre N. La notation $[m_1 \dots m_2]_n$ a été définie au paragraphe 2. Nous avons omis les polynômes pour $n = 86$ (4 polynômes de Boston et Greenwood, 14 nouveaux polynômes).

du nombre de valeurs premières pour n valeurs consécutives de la variable avec la restriction que les valeurs de F soient inférieures (en valeur absolue) à $n^2\sqrt{n}$; cette convention est destinée à situer avant le mur de Schinzel les valeurs prises par les polynômes; le coefficient 2 de l'exposant assure une valeur raisonnable pour la première valeur pertinente $n = 46$ (on notera que cette convention exclut légitimement le polynôme d'interpolation signalé à la fin du paragraphe 1, dont les valeurs sont supérieures à $(n-1)!$). Nous désignons par $\nu(F, n)$ le plus grand k pour lequel on a explicitement trouvé k valeurs premières pour n valeurs consécutives de la variable, avec la même restriction. En vertu du modèle probabiliste

que nous avons développé, nous conjecturons que les $\nu^*(F, n)$ sont égaux aux $\nu(F, n)$.

De façon similaire, nous désignons par $\nu^*(n)$ le maximum sur tous les polynômes du second degré du nombre de valeurs premières pour n valeurs consécutives de la variable, avec la même restriction, et par $\nu(n)$ le plus grand k pour lequel on a explicitement trouvé un polynôme avec $\nu(F, n) = k$.

Enfin, pour n donné, nous emploierons le terme de *dominant* pour qualifier le(s) polynôme(s) F tel(s) que $\nu(F, n) = \nu(n)$, et éventuellement le terme *sous-dominant* pour qualifier le(s) polynôme(s) suivant(s).

Les résultats qui sont présentés ci-dessous ont été obtenus :

- d'une part à partir de recherches extensives pour un certain nombre de valeurs particulières de n (selon la méthode décrite à la fin du paragraphe 2 incluant un test éliminant les polynômes avec des très petits dpp),
- d'autre part en contrôlant la dominance et la sous-dominance sur les intervalles reliant les valeurs particulières de n explorées (recherche beaucoup plus rapide).

Signalons que, pour une valeur de n donnée, l'intervalle optimal trouvé expérimentalement est toujours inclus dans l'intervalle $[x_1 - 2n, x_2 + 2n]$, où x_1 et x_2 sont les racines du polynôme s'il possède des racines réelles, 0 et 0 sinon (ou dans l'intervalle $[0, x_2 + 2n]$ si le polynôme est symétrique).

Nous présumons qu'aucun polynôme dominant ou sous-dominant n'a échappé à notre recherche jusqu'à une valeur n qui pourrait dépasser 20000.

La présentation des résultats numériques obtenus est faite selon un découpage en intervalles adapté aux dominances successives des polynômes.

7.1. Intervalle (1,45)

Valeurs prises. Dans cette zone $\nu^*(n) = \nu(n) = n$.

Polynômes dominants. Posons

$$nn = \max\{n \mid \nu^*(F, n) = n\}.$$

Nous avons recherché, pour $n \geq 33$, tous les polynômes dominants (i.e. ceux pour lesquels $nn = n$), et nous donnons sur le tableau 3 la statistique de leur nombre $N^*(n)$ (la répartition des coefficients et les limites de la zone explorée permettent de penser qu'aucun polynôme n'a échappé à cette recherche).

n	33	34	35	36	37	38	39	40	41	42	43	44	45
$N^*(n)$	21	10	7	7	6	0	4	7	0	0	2	0	1

TABLEAU 3. Nombre $N^*(n)$ de polynômes dominants pour chaque n .

On peut expliciter quelques polynômes qui permettront de se faire une idée d'ensemble :

– plus grands coefficients a

$$\begin{aligned} 2446x^2 + 904x - 3919 & \quad nn = 33 \\ 1888x^2 + 428x + 22643 & \quad nn = 33 \end{aligned}$$

– plus grands coefficients c

$$\begin{aligned} 768x^2 + 48x - 938887 & \quad nn = 34 \\ 3x^2 + 3x - 675299 & \quad nn = 33 \end{aligned}$$

– plus petit maximum (en valeur absolue) des n valeurs premières prises

$$\begin{aligned} x^2 + x + 41 & \quad nn = 40 \quad (\text{Euler, 1772}) \\ 4x^2 + 2x - 109 & \quad nn = 36 \\ 4x^2 + 4x - 1591 & \quad nn = 35 \\ 8x^2 + 6x - 661 & \quad nn = 40 \end{aligned}$$

– meilleurs polynômes

$$\begin{aligned} 36x^2 + 18x - 1801 & \quad nn = 45 \quad (\text{Ruby, 1989}) \\ 47x^2 + 9x - 5209 & \quad nn = 43 \quad (\text{Fung, 1988}) \\ 103x^2 + 31x - 3391 & \quad nn = 43 \quad (\text{Fung, 1988}) \end{aligned}$$

Outre ces derniers polynômes, on trouvera une liste partielle (non normalisée et redondante) dans Mollin et Williams [1990].

7.2. Intervalle (43,95)

Valeurs prises. Plusieurs tables de ν sont présentées. Elles donnent toutes n et $\nu(n)$ pour une suite convenable de valeurs de n . Pour le tableau 4 les valeurs de n seront les abscisses des valeurs stationnaires de la fonction ν , caractérisées donc par $\nu(n) = \nu(n-1)$ (la propriété triviale $\nu(n+1) = \nu(n) + 0$ ou 1 permet alors d'interpoler immédiatement la fonction ν entre deux abscisses stationnaires consécutives). Pour les autres tables, les valeurs de n seront simplement des entiers "ronds" régulièrement espacés.

Nota: $n = 83$ est la première valeur sans polynôme à $\nu(n) - 1$ ($\nu(83) = 77$, avec le polynôme dominant $73x^2 + 59x - 18541$, et les polynômes sous-dominants sont à 75).

n	$\nu(n)$								
1	1	120	106	173	144	227	184	269	212
46	45	126	111	178	148	230	186	272	214
54	52	131	115	182	151	232	187	274	215
59	56	133	116	188	156	236	190	276	216
68	64	138	120	193	160	237	190	280	219
77	72	144	125	197	163	242	194	283	221
80	74	148	128	201	166	243	194	287	224
84	77	152	131	203	167	244	194	289	225
87	79	156	134	207	170	247	196	298	233
91	82	158	135	213	175	250	198	300	234
92	82	163	138	217	178	253	200		
101	90	165	139	219	179	256	202		
108	96	167	140	223	182	260	205		
115	102	169	141	225	183	266	210		

TABLEAU 4. Valeurs de n et $\nu(n)$, pour $n \leq 300$. On a $\nu(1) = \nu(2) = \dots = \nu(45)$ etc.

Polynômes dominants. Un très grand nombre de polynômes interviennent dans cette zone, avec 2.0 polynômes dominants, en moyenne, pour chaque valeur de n . Les polynômes sont donnés avec le nombre de valeurs de n pour lesquels ils sont dominants, et les valeurs extrêmes.

$47x^2 + 9x - 5209$	(Fung) 1 valeur 43,
$103x^2 + 31x - 3391$	(Ruby) 2 valeurs 43 et 46,
$36x^2 + 18x - 1801$	(Ruby) 17 valeurs de 43 à 59,
$53x^2 + 41x - 16361$	2 valeurs 46 et 47,
$123x^2 + 9x - 5783$	2 valeurs 46 et 47,
$139x^2 + 117x - 9719$	3 valeurs de 46 à 48,
$16x^2 + 10x - 547$	5 valeurs entre 46 et 55,
$73x^2 + 59x - 18541$	24 valeurs entre 54 et 95,
$37x^2 + 23x - 8863$	24 valeurs entre 54 et 95,
$67x^2 + 37x - 6793$	3 valeurs de 59 à 61,
$8x^2 + 2x - 1097$	12 valeurs entre 59 et 80,
$4x^2 + 2x + 41$	(polynôme d'Euler pour $2x$) 3 valeurs entre 59 et 92,
$10x^2 + 10x - 354457$	2 valeurs 59 et 60,
$23x^2 + 17x - 40169$	1 valeur dans cette zone 92,
$67x^2 + 45x - 12569$	1 valeur 92,
$41x^2 + 33x - 43321$	4 valeurs dans cette zone de 92 à 95.

7.3. Intervalle (96,291)

Valeurs prises. Voir ci-dessus.

Polynômes dominants. Le nombre de polynômes qui interviennent est maintenant plus restreint, avec en moyenne 1.3 polynômes dominants pour chaque valeur de n . (Pour abrégé les tables on écrit désormais *d.c.z.* au lieu de “dans cette zone”.)

- $41x^2+33x-43321$ 42 valeurs *d.c.z.* entre 96 et 139
(Boston et Greenwood),
- $9x^2+3x-16229$ 154 valeurs entre 115 et 291,
- $23x^2+17x-40169$ 23 valeurs *d.c.z.* entre 163 et 188,
- $x^2+x-349513$ 2 valeurs 244 et 276,
- $x^2+x-328063$ 5 valeurs *d.c.z.* entre 250 et 276,
- $x^2+x-1354363$ 21 valeurs *d.c.z.* entre 256 et 291.

7.4. Intervalle (292,1635)

Valeurs prises. On donne maintenant une table par valeurs espacées, de 10 puis 25 :

n	$\nu(n)$	n	$\nu(n)$	n	$\nu(n)$	n	$\nu(n)$
290	226	510	377	730	522	1250	855
300	234	520	384	740	528	1275	872
310	241	530	392	750	533	1300	888
320	248	540	399	775	551	1325	903
330	255	550	404	800	566	1350	919
340	262	560	411	825	585	1375	937
350	268	570	416	850	600	1400	953
360	274	580	422	875	614	1425	967
370	282	590	430	900	633	1450	984
380	289	600	438	925	650	1475	1000
390	296	610	444	950	666	1500	1015
400	302	620	452	975	680	1525	1031
410	308	630	458	1000	698	1550	1047
420	316	640	463	1025	713	1575	1062
430	323	650	469	1050	728	1600	1078
440	330	660	475	1075	746	1625	1094
450	337	670	481	1100	762	1650	1109
460	343	680	487	1125	776	1675	1125
470	350	690	495	1150	790	1700	1141
480	357	700	503	1175	808	1725	1158
490	363	710	509	1200	823	1750	1172
500	369	720	517	1225	841		

Polynômes dominants. Il y a encore moins de polynômes qui interviennent, et ils sont isolés sauf exception (la moyenne est de 1.04 polynômes dominants pour chaque valeur de n).

- $x^2+x-1354363$ 1321 valeurs *d.c.z.* entre 283 et 1635 (avec notamment un intervalle continu à partir de 477),
- $x^2+x-328063$ 55 valeurs *d.c.z.* entre 341 et 583,
- $3x^2+3x-268817$ 22 valeurs entre 399 et 432.

7.5. Intervalle (1636,12389)

Valeurs prises. Un phénomène intéressant, qui était apparu au milieu de la zone précédente, concerne maintenant le polynôme dominant $x^2+x-1354363$: pour un polynôme F de la forme ax^2+ax+c , la règle de Boston et Greenwood restreint l’étude aux valeurs positives et, lorsque le meilleur intervalle commence à $x = 0$, le polynôme $4ax^2 + 2ax + c$ donne une valeur de ν égale ou supérieure car le “jeu” entre les valeurs négatives et positives permet d’arbitrer au mieux entre les valeurs impaires et paires de x pour le polynôme initial (néanmoins le gain est assez faible, parfois nul).

Nous donnons une dernière table (allant au delà de la zone ici détaillée) :

n	$\nu(n)$	n	$\nu(n)$	n	$\nu(n)$	n	$\nu(n)$
1500	1015	4250	2558	9000	4904	19000	9469
1750	1172	4500	2684	9500	5137	20000	9902
2000	1324	4750	2811	10000	5374	22500	10963
2250	1468	5000	2946	11000	5840	25000	12035
2500	1619	5500	3191	12000	6302	27500	13097
2750	1764	6000	3447	13000	6761	30000	14157
3000	1895	6500	3695	14000	7217	35000	16229
3250	2029	7000	3939	15000	7673	40000	18275
3500	2164	7500	4180	16000	8114	45000	20421
3750	2295	8000	4424	17000	8565	50000	22582
4000	2429	8500	4667	18000	9013	60000	26846

Polynômes dominants.

- $x^2+x-1354363$ 139 valeurs entre 1636 et 5133, puis 21 valeurs entre 8811 et 9218, et enfin 17 valeurs entre 12342 et 12389,
- $4x^2+2x-1354363$ 16 valeurs entre 1636 et 1671, puis les intervalles [1675, 4977], [4990, 4991] et [4993, 12389].

Lorsque ces deux polynômes prennent la même valeur, le polynôme sous-dominant est l’un des cinq polynômes suivants :

$4x^2 + 2x - 752293$	en début de zone,
$9x^2 + 3x - 1354363$	en début de zone, pour quelques valeurs,
$x^2 + x - 1776433$	en milieu de zone, pour quelques valeurs,
$4x^2 + 2x - 1776433$	en milieu de zone,
$8x^2 + 2x - 16646459$	en fin de zone.

7.6. Intervalle (12390, 40337)

Polynômes dominants. Dans toute cette zone, le polynôme dominant est $4x^2 + 2x - 1354363$ et le polynôme sous-dominant est $x^2 + x - 1354363$ (mais la différence est faible, de l'ordre de quelques dizaines, et s'annule pour quelques rares valeurs exceptionnelles — elle est même inversée d'une unité pour 13751), seul en début de zone, en alternant avec $x^2 + x - 12276955783$ ensuite.

Le(s) meilleur(s) polynôme(s) suivant(s) est (sont) :

$8x^2 + 2x - 16646459$	en début de zone,
$4x^2 + 2x - 65288413$	pour quelques valeurs vers 30000,
$x^2 + x - 12276955783$	en fin de zone.

7.7. Le cas $n = 40338$

C'est la première valeur où le polynôme $x^2 + x - 12276955783$ ($C = 4.8420$) devient dominant (ex-æquo avec $4x^2 + 2x - 1354363$).

7.8. Liste partielle des polynômes dominants ($n \geq 40$) et sous-dominants ($n \geq 1000$)

Le tableau 5 donne les polynômes dominants pour $n \geq 40$ et sous-dominants pour $n \geq 1000$. Ces polynômes sont donnés avec les valeurs extrêmes de sous-dominance et dominance, ainsi que p leur plus petit dpp et C la valeur de la constante de Hardy-Littlewood.

Note technique : jusqu'à 50000, tous les polynômes figurant sur cette liste ont été contrôlés en continu sur leur zone de meilleure performance.

Des résultats plus complets peuvent être demandés aux auteurs.

8. DEUX REMARQUES POUR LA RECHERCHE D'UNE EXPLICATION

La question fondamentale est : y a-t-il des explications théoriques à la bonne qualité de certains poly-

nômes ? Il ne semble pas exister d'explication aussi simple que le critère de Rabinowitch mais on peut avancer deux remarques.

La première est presque évidente pour des raisons non arithmétiques : les "bons" polynômes doivent présenter des plages de longueur n où ils prennent des valeurs (absolues) faibles. Cela avantage les polynômes de discriminant positif, et aussi, pour les grandes valeurs de n , les polynômes de petit coefficient directeur a .

La seconde remarque provient de l'examen des discriminants (des corps associés). Beaucoup de polynômes définissent le même corps quadratique, le cas le plus marquant étant celui du discriminant 5417453, avec les polynômes :

$x^2 + x - 1354363$	(1ère performance longuement),
$41x^2 + 41x - 33023$	(2ème performance pour $n = 50$),
$73x^2 + 59x - 18541$	(2ème performance pour $n = 50$, et 3ème pour $n = 100$),
$97x^2 + 87x - 13943$,	
$139x^2 + 117x - 9719$	(2ème performance de $n = 40$ à $n = 46$).

Le lien entre les bonnes performances des polynômes et le discriminant des corps quadratiques associés est évident et tient à des constantes de Hardy-Littlewood très voisines (elles diffèrent seulement d'un facteur provenant du coefficient directeur) ; la zone de performance est ensuite fortement fonction de la taille du coefficient directeur.

Notons enfin que l'on trouve des nombres de classes très variés (de 1 à 6 le plus souvent, mais aussi 15, 18, 63, 98).

Pour conclure (provisoirement) la réponse à la question posée, on peut dire que, qualitativement, les performances d'un polynôme apparaissent comme la "somme" d'un terme fonction de sa constante de Hardy-Littlewood et d'un terme aléatoire (si l'on peut parler de hasard dans un contexte déterministe... mais fort complexe). Pour les petites valeurs de n , le terme aléatoire est prépondérant, et les records sont donc fortement dus au hasard. Par contre, pour les grandes valeurs de n , le terme déterministe est prépondérant, et les polynômes sont pratiquement "classés" selon leur constante de Hardy-Littlewood.

Nous faisons encore une remarque. Dans ce problème, le nombre 1 est considéré comme premier,

polynôme	p	C	
$x^2 + x + 41$ (Euler)	41	3.3197732	40 81
$x^2 + x - 328063$	37	3.93644	229 250 583 817
$x^2 + x - 349513$	59	3.97271	92 244 276 1122
$x^2 + x - 752293$	37	4.1037867	663 1226
$x^2 + x - 1354363$	41	4.3304949	46 256 33082 40874
$x^2 + x - 1776433$	41	4.1615621	4973 5083
$x^2 + x - 12276955783$	149	4.8420287	40187 40338 au-delà de 100000
$3x^2 + 3x - 268817$	73	4.0758910	276 399 432 504
$4x^2 + 2x + 41$ (Euler pour $2x$)	41	3.3197732	40 92 101
$4x^2 + 2x - 349513$	59	3.97271	770 1122
$4x^2 + 2x - 501229$	67	4.0077796	1002
$4x^2 + 2x - 752293$	37	4.1037867	1134 2233
$4x^2 + 2x - 1354363$	41	4.3304949	1228 1636 40874 vers 51775
$4x^2 + 2x - 1776433$	41	4.1615621	3467 5133
$4x^2 + 2x - 65288413$	107	4.3158954	29035 33082
$8x^2 + 2x - 1097$	31	3.66133	40 59 80 212
$8x^2 + 2x - 16646459$	53	4.4236782	8811 31859
$8x^2 + 6x - 661$	41	3.42462	40 92
$9x^2 + 3x + 41$ (Euler pour $3x$)	41	3.3197732	40 41
$9x^2 + 3x - 16229$	59	3.90998	46 115 291 318
$9x^2 + 3x - 1354363$	41	4.3304949	1136 1859
$10x^2 + 10x - 354457$	79	4.2233175	40 59 60 73
$16x^2 + 10x - 547$	31	3.66133	40 46 55 59
$23x^2 + 17x - 40169$	23	3.95596	83 92 188 208
$36x^2 + 18x - 1801$ (Ruby)	59	3.90998	40 59 63
$37x^2 + 23x - 8863$	37	4.0489090	40 54 95 104
$41x^2 + 33x - 43321$ (Greenwood)	41	4.2682688	40 92 139 236
$47x^2 + 9x - 5209$ (1 ^{er} de Fung)	47	3.78286	40 43 44
$53x^2 + 41x - 16361$	53	3.94786	40 46 47 59
$59x^2 + 15x - 5923$	59	4.0424031	40 49
$67x^2 + 37x - 6793$	47	3.95160	40 59 61 64
$67x^2 + 45x - 12569$	47	4.1114619	87 92 93
$73x^2 + 59x - 18541$	41	4.3914878	46 54 95 102
$103x^2 + 31x - 3391$ (2 ^e de Fung)	59	4.0120402	40 46 55
$111x^2 + 15x - 11213$	37	4.0769624	40 46
$123x^2 + 9x - 5783$	41	3.96128	40 46 47 50
$137x^2 + 67x - 2543$	59	4.0021339	40 47
$139x^2 + 117x - 9719$	41	4.3621043	40 46 48 56

TABLEAU 5. Polynômes dominants et sous-dominants. Les valeurs extrêmes sont données (à partir de 40) sous la forme “ $a b c d$ ”, avec la signification : a et d valeurs extrêmes de sous-dominance, b et c valeurs extrêmes de dominance.

convention habituelle et cohérente, d’une part avec l’exclusion des diviseurs 2, 3, 5, ..., d’autre part avec les considérations algébriques (l’analogie du critère de Rabinowitch pour les polynômes de la forme $2x^2 + c$ fournit le polynôme $F(x) = 2x^2 - 199$ en considérant $F(10) = -1$ comme si c’était un nombre premier — nous n’avons d’ailleurs trouvé aucun autre “bon” polynôme qui prenne la valeur 1 ou -1).

9. POLYNÔMES DE DEGRÉ SUPÉRIEUR

9.1. Troisième degré

Les seuls résultats connus sont ceux de Goetghe-luck [1989]. Nous adoptons la convention annoncée dans l’introduction de compter seulement les valeurs premières *distinctes* (en module) en utilisant, si besoin, le préfixe “pseudo” pour qualifier les résultats obtenus sans cette restriction. Il sera utile de com-

pléter l'information en définissant $\delta = \delta(F, n)$, différence entre le pseudo-compte et le compte des valeurs premières distinctes (cette différence dépend a priori de n , mais en fait les doublets et triplets sont au centre de la zone optimale et sa valeur est constante pour les valeurs de n considérées). Le cas le pire que nous avons trouvé est celui du polynôme

$$F(x) = 2x^3 - 2366x + 14437,$$

qui présente les 6 triplets $(-39, 13, 26)$, $(-38, 9, 29)$, $(-37, 6, 31)$, $(-31, 6, 37)$, $(-29, -9, 38)$, $(-26, -13, 39)$, et pour lequel

$$\text{pseudo-}\nu(F, 50) = 46$$

(mais $\nu(F, 50) = 46 - 12 = 34$). On notera enfin que, pour les polynômes à valeurs multiples, seule la pseudo-valeur de L peut être donnée car il n'y a pas de compte canonique des valeurs distinctes consécutives, mais cela ne peut pas bien sûr compter pour un record.

Les résultats de Goetgheluck, en normalisant ses polynômes "à la Boston et Greenwood" sont les suivants :

$$F(x) = x^3 + x^2 - 4x + 103, \text{ pseudo-}L = 26, \delta = 3,$$

$$F(x) = 2x^3 + 3x^2 - 5x - 2399, \text{ pseudo-}L = 26,$$

$$\text{pseudo-}\nu(F, 500) = 267, \delta = 2.$$

En fait, la meilleure zone pour le second polynôme, non détectée par Goetgheluck, donne

$$\text{pseudo-}\nu(F, 500) = 272.$$

Nous avons repris la recherche et découvert que, de façon un peu surprenante, les performances ne sont pas très inférieures à celles de polynômes du second degré. Les meilleurs polynômes trouvés sont indiqués dans le tableau 6 (p donne le plus petit dpp).

Signalons les pseudo-records suivants : pour

$$F(x) = 3x^3 + 3x^2 - 402x + 1597,$$

on a $\text{pseudo-}L = 46$ et $\text{pseudo-}\nu(F, 50) = 49$.

9.2. Quatrième et cinquième degré

Les performances sont médiocres et les temps de recherche deviennent prohibitifs.

Le tableau 7 montre ce que nous avons trouvé en degré 4 et 5.

On peut résumer l'ensemble des records dans le tableau ci-dessous (il est clair que ces records sont

$F(x)$	p	L	$\nu(F, n), n =$			δ
			50	100	500	
meilleurs L						
$6x^3 + 8x^2 + 60x - 331$	79	39	46	83	286	0
$5x^3 + x^2 - 212x + 4003$	47	37	46	71	261	0
$2x^3 + x^2 + 117x + 269$	23	36	44	71	272	0
$4x^3 + x^2 - 59x + 311$	47	35	46	81	294	0
$4x^3 - 202x + 599$	47	35	46	75	261	0
$5x^3 + x^2 - 170x - 443$	47	35	43	76	273	0
meilleurs $\nu(F, 50)$						
$x^3 + x^2 + 66x - 457$	23	33	48	84	293	0
$4x^3 + x^2 - 59x + 311$	47	35	46	81	294	0
$6x^3 + 8x^2 + 60x - 331$	79	39	46	83	286	0
$14x^3 + 10x^2 - 5204x + 12703$	41	23	46	83	275	0
$4x^3 - 202x + 599$	47	34	46	75	261	0
$5x^3 + x^2 - 212x + 4003$	47	37	46	71	261	0
meilleurs $\nu(F, 100)$						
$x^3 + x^2 + 66x - 457$	23	33	48	84	293	0
$6x^3 + 8x^2 - 3396x + 3593$	31	19	45	84	264	0
$x^3 + x^2 - 1544x + 10799$	41	20	45	83	295	0
$6x^3 + 8x^2 + 60x - 331$	79	39	46	83	286	0
$14x^3 + 10x^2 - 5204x + 12703$	41	23	46	83	275	0
$20x^3 + 23x^2 - 17667x + 13381$	73		42	83	293	1
meilleurs $\nu(F, 500)$						
$x^3 + x^2 - 3424x + 8389$	29		41	81	313	2
$4x^3 + 6x^2 - 856x + 2633$	43		44	78	300	2
$x^3 + x^2 - 1544x + 10799$	41	20	45	83	295	0
$4x^3 + x^2 - 59x + 311$	47	35	46	81	294	0

TABLEAU 6. Meilleurs polynômes cubiques trouvés.

destinés à être dépassés en degré ≥ 3 , d'autant plus que nous n'avons fait pratiquement aucune exploration pour les "grandes" valeurs du coefficient a_0 :

degré	L	$\nu(F, 50)$	$\nu(F, 100)$	$\nu(F, 500)$
2	45	49	90	369
3	39	48	84	313
4	27	44	77	259
5	25	43	71	230

REMERCIEMENTS

Nous remercions vivement H. Cohen pour avoir conçu un algorithme de calcul numérique des constantes de Hardy-Littlewood à une précision arbitraire.

Nous remercions vivement B. Landreau dont la contribution à nos programmes d'exploration nous

$F(x)$	p	L	$\nu(F, n), n=$			δ	$F(x)$	p	L	$\nu(F, n), n=$			δ
			50	100	500				50	100	500		
meilleurs L							meilleurs L						
$x^4 + x^3 - 25x^2 + 269x - 27103$	47	27	46	76	235	0	$x^5 - 18x^2 + 1883x - 17317$	59	25	40	65	198	0
$x^4 + x^3 - 3x^2 - 147x + 419$	59	24	44	73	232	0	$x^5 + x^4 + 4x^2 - 30x - 2273$	43	24	40	62	195	0
$2x^4 + 3x^3 - 3x^2 + 78x - 2539$	43	24	43	70	236	0	$x^5 + 2x^2 - 73x - 1601$	43	24	36	58	176	0
$2x^4 + x^3 - 2x^2 - 115x - 1523$	53	23	42	71	235	0	$2x^5 + 2x^4 + 2x^2 - 80x + 307$	41	24	35	59	164	0
meilleurs $\nu(F, 50)$							meilleurs $\nu(F, 50)$						
$x^4 + x^3 - 25x^2 + 269x - 27103$	47	27	46	76	235	0	$2x^5 - x^2 - 367x - 233$	59	18	43	68	198	0
$x^4 - 90x^2 + 247x - 18061$	61		44	76	259	1	$x^5 - 11x^2 - 52x + 1669$	41	20	41	63	214	0
$2x^4 + 4x^3 - 3x^2 + 97x - 4157$	59	17	44	73	245	0	$x^5 + 12x^2 - 1927x - 16759$	43	15	41	67	199	0
$x^4 - 45x^2 + 44x - 1801$	37		44	75	239	1	$x^5 - 28x^2 - 81x + 61$	47		41	64	205	1
$x^4 + x^3 - 3x^2 - 147x + 419$	59	24	44	73	232	0	$2x^5 + 4x^4 - 3x^2 - 287x - 10193$	41	12	41	65	191	0
meilleurs $\nu(F, 100)$							meilleurs $\nu(F, 100)$						
$x^4 + 2x^3 - 26x^2 + 49x - 277$	43		37	77	212	1	$x^5 + x^4 - 37x^2 - 229x + 47147$	41		38	71	204	1
$x^4 - 90x^2 + 247x - 18061$	61		44	76	259	1	$x^5 - 40x^2 + 1289x + 35183$	53	8	38	69	218	0
$x^4 + 2x^3 + 46x^2 + 119x - 13847$	43	11	43	76	252	0	$x^5 + x^4 - 6x^2 - 820x + 26167$	53	9	40	69	200	0
$x^4 + x^3 - 25x^2 + 269x - 27103$	47	27	46	76	235	0	$2x^5 - x^2 - 367x - 233$	59	18	43	68	198	0
$x^4 + 2x^3 - 45x^2 + 112x - 383$	43	22	43	76	231	0	$x^5 - 17x^2 - 566x - 54919$	67	12	40	68	208	0
$x^4 + x^3 - 38x^2 + 228x - 19661$	41	9	41	76	219	0	$x^5 + x^4 + 4x^2 - 290x + 4363$	43	12	40	68	194	0
meilleurs $\nu(F, 500)$							meilleurs $\nu(F, 500)$						
$x^4 - 90x^2 + 247x - 18061$	61		44	76	259	1	$x^5 - 40x^2 - 1881x - 53$	41	23	40	68	189	0
$x^4 + 2x^3 + 46x^2 + 119x - 13847$	43	11	43	76	252	0	$x^5 + x^4 - x^2 + 1007x - 68279$	53	8	36	68	194	0
$x^4 + 2x^3 - 52x^2 + 13x - 673$	43		43	75	245	2	meilleurs $\nu(F, 500)$						
$2x^4 + 4x^3 - 3x^2 + 97x - 4157$	59	17	44	73	245	0	$x^5 - 12x^2 + 1559x + 48121$	43	9	36	66	230	0
							$x^5 + 10x^2 + 1499x + 52729$	41	14	37	66	225	0
							$x^5 + x^4 + 4x^2 + 1148x + 49877$	59	15	39	66	224	0
							$x^5 + x^4 - 37x^2 + 959x + 70853$	41	11	38	66	220	0
							$x^5 - 40x^2 + 1289x + 35183$	53	8	38	69	218	0
							$x^5 - 11x^2 - 52x + 1669$	41	20	41	63	214	0
							$x^5 + 4x^2 + 1763x - 15731$	41	15	39	66	213	0

TABLEAU 7. Meilleurs polynômes de quatrième et cinquième degré.

a permis d'étendre le tableau de polynômes du paragraphe 5.1 et de trouver le polynôme $x^2 + x - 12276955783$ (dominant à partir de 40338).

BIBLIOGRAPHIE

[Bateman et Horn 1962] P. T. Bateman et R. A. Horn, "A heuristic asymptotic formula concerning the distribution of prime numbers", *Math. Comp.* **16** (1962), 363–367.

[Boston et Greenwood 1995] N. Boston et M. L. Greenwood, "Quadratics representing primes", *Amer. Math. Monthly* **102**:7 (1995), 595–599.

[Fung et Williams 1990] G. W. Fung et H. C. Williams, "Quadratic polynomials which have a high density of prime values", *Math. Comp.* **55**:191 (1990), 345–353.

[Goetgheluck 1989] P. Goetgheluck, "On cubic polynomials giving many primes", *Elem. Math.* **44**:3 (1989), 70–73.

[Hardy et Littlewood 1923] G. H. Hardy et J. E. Littlewood, "Some problems of a partitio numerorum, III: On the expression of a number as a sum of primes", *Acta Math.* **44** (1923), 1–70.

[Lukes et al. 1995] R. F. Lukes, C. D. Patterson et H. C. Williams, "Numerical sieving devices: their history and some applications", *Nieuw Arch. Wisk.* (4) **13**:1 (1995), 113–139.

[Mollin 1996] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, FL, 1996.

[Mollin et Williams 1990] R. A. Mollin et H. C. Williams, "Class number problems for real quadratic fields",

pp. 177–195 dans *Number theory and cryptography* (Sydney, 1989), édité par J. H. Loxton, London Math. Soc. Lecture Notes **154**, Cambridge Univ. Press, Cambridge, 1990.

[Rabinowitch 1913] G. Rabinowitch, “Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern”, pp. 418–421 dans *Proc. Fifth Inter. Congress Math.* (Cambridge, 1912), vol. 1, édité par E. W. Hobson et A. E. H. Love, Cambridge Univ. Press, 1913.

[Ribenoim 1996] P. Ribenoim, *The new book of prime number records*, Springer, New York, 1996.

[Schinzel 1961/1962] A. Schinzel, “Remarks on the paper “Sur certaines hypothèses concernant les nombres premiers””, *Acta Arith.* **7** (1961/1962), 1–8.

[Schinzel et Sierpiński 1958] A. Schinzel et W. Sierpiński, “Sur certaines hypothèses concernant les nombres premiers”, *Acta Arith.* **4** (1958), 185–208. Erratum, **5** (1958), 259.

[Stephens et Williams 1990] A. J. Stephens et H. C. Williams, “An open architecture number sieve”, dans *Number theory and cryptography* (Sydney, 1989), édité par J. H. Loxton, London Math. Soc. Lecture Notes **154**, Cambridge Univ. Press, Cambridge, 1990.

François Dress, A2X (UMR 9936), Université Bordeaux I, 351 cours de la Libération, 33 405 Talence, France (dress@math.u-bordeaux.fr)

Michel Olivier, A2X (UMR 9936), Université Bordeaux I, 351 cours de la Libération, 33 405 Talence, France (olivier@math.u-bordeaux.fr)

Received April 15, 1998; accepted in revised form November 11, 1998