Some mathematical remarks on the polynomial selection in NFS

Razvan Barbulescu, Armand Lachand

Some mathematical remarks on the polynomial selection in NFS

Razvan Barbulescu [*1,2] and Armand Lachand[†1,3]

[1]Université de Lorraine
[2]CNRS, INRIA
[3]Institut Elie Cartan de Lorraine (CNRS/Univ. Lorraine)

Abstract

In this work, we consider the proportion of friable (free of large prime factors) values of a binary form $F(X_1, X_2) \in \mathbf{Z}[X_1, X_2]$. In the particular case of quadratic forms, we give an asymptotic equivalent for this proportion which depends on F. This is related to Murphy's α function, which is known in the cryptologic community, but which has not been studied before from a mathematical point of view. This has consequences on the first step, called polynomial selection, of the Number Field Sieve, the fastest algorithm of integer factorization.

1 Introduction

1.1 Context

Friable – or smooth – numbers, defined as integers without large prime factors, are a celebrated topic in analytic number theory and have a key importance in cryptology today. The distribution of y-friable integers – an integer n is y-friable if its greatest prime factor, denoted by $P(n)$ with the convention $P(\pm 1) = 1$, satisfies $P(n) \leqslant y$ – has made the object of many works (for an overview, we refer to [HT93] and [Gra08]). For example, Hildebrand proved in [Hil86] an asymptotic formula in the region

$$x \geqslant 3, \qquad \exp\left((\log\log x)^{5/3+\varepsilon}\right) \leqslant y \leqslant x. \tag{H_ε}$$

Theorem A (Theorem 1, [Hil86]). *For any fixed $\varepsilon > 0$ and uniformly for (x, y) in the region (H_ε), we have*

$$\Psi(x, y) := \left|\{n \in [1, x] : P(n) \leqslant y\}\right| = x\rho(u)\left(1 + O\left(\frac{\log(u+1)}{\log y}\right)\right),$$

where $u := \frac{\log x}{\log y}$ and ρ denotes the Dickman function, namely the one defined by the delay differential equation

$$\begin{cases} u\rho'(u) + \rho(u-1) = 0 & \text{if } u > 1, \\ \rho(u) = 1 & \text{if } 0 \leqslant u \leqslant 1. \end{cases}$$

A few years later, Saias refined this result by giving an asymptotic expansion of $\Psi(x, y)$.

Theorem B (Main corollary, [Sai89]). *There exists $C > 0$ such that, for any fixed $J \geqslant 0$, $\varepsilon > 0$ and uniformly for (x, y) in the region (H_ε) satisfying*

$$0 < u < J + 1 \Rightarrow (u - \lfloor u \rfloor) > C(J+1)\frac{\log\log y}{\log y},$$

*razvan.barbulescu@imj-prg.fr
†armand.lachand@univ-lorraine.fr

we have

$$\Psi(x,y) = x\left(\sum_{j=0}^{J}\gamma_j\frac{\rho^{(j)}(u)}{(\log y)^j} + O\left(\rho(u)\left(\frac{\log(u+1)}{\log y}\right)^{J+1}\right)\right),$$

where γ_j are the coefficients of the Taylor series in $s=0$ of $\frac{s\zeta(s+1)}{s+1}$. In particular, we have $\gamma_0 = 1$ and $\gamma_1 = \gamma - 1$.

Let x and y be two positive reals, $F(X_1, X_2) \in \mathbf{Z}[X_1, X_2]$ a binary form and $\mathcal{K}$ a compact subset of $\mathbf{R}^2$ whose boundary is a continuous closed curve with piecewise continuous derivatives. By $x\mathcal{K}$ we denote the set $\mathcal{K}$ rescaled by a factor x. In order to study the distribution of the y-friable integers of the form $F(n_1, n_2)$ for coprime integers n_1 and n_2, we consider the cardinal $\Psi_F^{(1)}(\mathcal{K}x, y)$ defined by

$$\Psi_F^{(1)}(x\mathcal{K}, y) := \left|\left\{(n_1,n_2) \in x\mathcal{K}\cap\mathbf{Z}^2 : \gcd(n_1,n_2) = 1 \text{ and } P(F(n_1,n_2)) \leqslant y\right\}\right|.$$

In [BBDT12], Balog, Blomer, Dartyge and Tenenbaum developed an argument which can be easily adapted to show the following result.

Theorem C (Theorems 1 and 2, [BBDT12])**.** *Let $\mathcal{K}$ be a compact subset of $\mathbf{R}^2$ whose boundary is a continuous closed curve with piecewise continuous derivatives, $k \geqslant 1$ and $F_1(X_1, X_2), \dots, F_k(X_1, X_2) \in \mathbf{Z}[X_1, X_2]$ some irreducible binary forms of degree $d_1 \geqslant \cdots \geqslant d_k$. There exists $u(d_1, \dots, d_k) > 1/d_1$ with the following property. For any $\varepsilon > 0$, there exists a constant $c_{F_1,\dots,F_k,\mathcal{K},\varepsilon}(u)$ such that, for any $u < u(d_1, \dots, d_k) - \varepsilon$ and $x \geqslant 2$, we have*

$$\Psi_{F_1\dots F_k}^{(1)}\left(x\mathcal{K}, x^{1/u}\right) \geqslant c_{F_1,\dots,F_k,\mathcal{K}}(u)x^2.$$

In particular, one can take

$$u(d_1,\dots,d_k) := \begin{cases} +\infty & \text{if } k \geqslant 2 \text{ and } d_1 + \cdots + d_k \leqslant 3,\\ e^{\frac{1}{2}} & \text{if } k = 1 \text{ and } d_1 = 3.\end{cases}$$

In cryptology it is common to make the assumption that integers represented by a given binary form have the same probability to be y-friable as arbitrary integers of the same size. Consequently, in the light of Theorem A, we can conjecture that, in a domain to be made precise, we have

$$\Psi_{F_1\dots F_k}^{(1)}(x\mathcal{K}, x^{1/u}) \sim \frac{6}{\pi^2}\mathcal{A}(\mathcal{K})x^2\rho(d_1u)\dots\rho(d_ku), \tag{1}$$

where $\mathcal{A}(\mathcal{K})$ denotes the area of $\mathcal{K}$. The second author proved in [Lac14a] and [Lac14b] that this is actually true when $k = 1$ and $d_1 = 3$ and, respectively, when $k = 2$, $d_1 = 1$ and $d_2 = 2$.

1.2 Motivation

We are motivated by the Number Field Sieve (NFS), the fastest algorithm of integer factorization and of discrete logarithm computations. First used in 1989 by Pollard [Pol93], the algorithm was developed in a series of articles grouped in a dedicated book [LL93]. In 2009, a record computation was undertaken using NFS for the factorization of a 768-bit (232-digit) integer [KAF+10]. Discrete logarithm variants of NFS are the state-of-art for finite fields of large and medium characteristic [Sch93],[JL03],[JLSV06]. The largest discrete logarithm computation undertaken with NFS corresponds to the field $\mathbf{F}_p$ of a 180-digit prime p [BGI+14].

Briefly, if N is an integer to be factored, NFS can be summarized as follows. In the first step, called polynomial selection, we select two irreducible polynomials with integer coefficients f and g, which have a common root m modulo N, i.e. $f(m) \equiv g(m) \equiv 0 \pmod N$. In the next step, we fix a real parameter $y \geqslant 2$ and we search for y pairs of coprime integers (n_1, n_2) such that $F(n_1, n_2) := n_2^{\deg f} f(n_1/n_2)$ and $G(n_1, n_2) := n_2^{\deg g} g(n_1/n_2)$ are y-friable. The collected pairs allow us to obtain a $y \times y$ linear system over $\mathbf{Z}/2\mathbf{Z}$. Next, we compute a linear combination of the rows of the system. By a square root computation in a number field, we find a non-trivial solution (a, b) of the equation $a^2 \equiv b^2 \bmod N$, which gives a non-trivial factor of N. Computing the complexity of the algorithm requires then to find the distribution of coprime pairs (n_1, n_2) which are y-friable with respect to the irreducible binary forms F and G.

One can select the polynomials f and g from a large set of pairs, obtained using one of the two methods of Kleinjung: ([Kle06], [Bai11, Section 4.1] and [Kle08], [Bai11, Section 4.2]). The question is how to define a function $\mathbb{E} : \mathbf{Z}[X] \times \mathbf{Z}[X] \to \mathbf{R}$ with a simple formula such that, given the values of $\mathbb{E}$ for two pairs of binary forms (F_1, G_1) and (F_2, G_2), it allows to compare asymptotically $\psi^{(1)}_{F_1G_1}(x\mathcal{K}, y)$ and $\psi^{(1)}_{F_2G_2}(x\mathcal{K}, y)$. A complete answer to the question seems to be out of reach, but there have been many experiments with NFS which generated a series of experimental laws. To our knowledge none of these experimental results has been proven before this article, and they can be studied as independent conjectures.

In his thesis, Murphy [Mur99] introduced a function $\mathbb{E} : \mathbf{Z}[X] \times \mathbf{Z}[X] \to \mathbf{R}$ which allows to compare most pairs, but all results on $\mathbb{E}$ are experimental. Moreover, $\mathbb{E}$ has a difficult formula, which is hard to evaluate in practice. Hence, computer scientists do not usually use $\mathbb{E}$ and instead look for two properties that Murphy called *size property* and *root property*. The size property can be formalized by the function σ, defined as follows

$$\sigma(f, g, \mathcal{K}, x, X_f, X_g) := \frac{|\{(n_1, n_2) \in x\mathcal{K} \cap \mathbf{Z}^2 : |F(n_1, n_2)| \leqslant X_f \text{ and } |G(n_1, n_2)| \leqslant X_g\}|}{|x\mathcal{K} \cap \mathbf{Z}^2|}.$$

The size property is related to the size of coefficients of f and g and to their real roots. Murphy explained that most of the polynomials of the following set have the same size property:

$$E(d, \mathbf{I}) = \left\{ f = \sum_{i=0}^{d} f_i X^i \in \mathbf{Z}[X] : f \text{ is irreducible}, (\forall i), f_i \in I_i \right\}, \tag{2}$$

where $\mathbf{I} = \prod_{i=0}^{d} I_i$ is the product of $(d+1)$ intervals.

In this paper, we discuss the question of how to select the best pair among a set of pairs with the same size property. Experiments show that the influence of the linear polynomial g is small. Hence, we have to decide if f has a good root property, defined as follows

$$r(f, x, y) = \frac{|\{(n_1, n_2) \in \mathbf{Z}^2 : (n_1, n_2) = 1,\ |F(n_1, n_2)| \leqslant x \text{ and is } y\text{-friable}\}|}{|\{(n_1, n_2) \in \mathbf{Z}^2 : (n_1, n_2) = 1 \text{ and } |F(n_1, n_2)| \leqslant x\}|}.$$

Murphy defined a function $\alpha : \mathbf{Z}[X] \to \mathbf{R}$ for which he gave strong evidence that, for polynomials with the same size property, it allows to rank the polynomials f with respect to r, for all parameters x and y. In addition to its efficiency, α has a simple formula, based on the number of roots of f modulo powers of primes, which allows to compute rapidly an approximation of $\alpha(f)$. Hence, in order to select a good pair (f, g), one generates a large number of pairs, computes $\alpha(f)$ for each of them, and finds the pair with the best value. Our model of the polynomial selection consists in choosing polynomials f in the set $E(d, \mathbf{I})$ with uniform probability, and in computing $\alpha(f)$ for each such polynomial.

1.3 Main results

To sum up the previous discussion, the NFS algorithm motivates the search of a function $\alpha : \mathbf{Z}[X] \to \mathbf{R}$ which, given two irreducible polynomials f_1 and f_2 (with associated binary forms F_1 and F_2), allows to compare $\psi^{(1)}_{F_1}(x\mathcal{K}, y)$ and $\psi^{(1)}_{F_2}(x\mathcal{K}, y)$. In Section 2, we give a rigorous definition of Murphy's $\alpha(f)$, which is defined as the sum of a series and was little studied in the literature. We also study the speed of convergence of this series because it measures the difficulty to find good approximations of $\alpha(f)$, and determines the cost of the polynomial selection in NFS.

In order to prove the efficiency of α, we search an asymptotic formula for the root property $r(f, x, y)$ which contains $\alpha(f)$. In the case of quadratic polynomials f we prove such a formula, obtaining hence a refinement of Theorem C, by making explicit the second term in the asymptotic expansion of $\Psi^{(1)}_{F_1}(x\mathcal{K}, y)$. Due to technical reasons, we restrict ourselves to the case of irreducible quadratic polynomials f whose discriminant is fundamental, i.e. such that $\mathrm{Disc}(f)$ satisfies one of the following conditions:

- $\mathrm{Disc}(f) \equiv 1 \pmod 4$ and is square-free,
- $\mathrm{Disc}(f) = 4m$ where $m \equiv 2$ or $3 \pmod 4$ is square-free.

Theorem 1.1. *Let $F(X_1, X_2) \in \mathbf{Z}[X_1, X_2]$ be an irreducible quadratic form such that* $\mathrm{Disc}(F)$ *is negative and fundamental. Let $\mathcal{K}_F$ be the compact defined by*

$$\mathcal{K}_F := \left\{(x_1, x_2) \in \mathbf{R}^2 : |F(x_1, x_2)| \leqslant 1\right\}$$

Then, there exists $\kappa > 0$ such that, for any $\varepsilon > 0$ and uniformly in the domain

$$x \geqslant 3, \qquad \exp\left((\log\log x)^{5/3+\varepsilon}\right) \leqslant y \leqslant x^2(\log x)^{-\kappa},$$

we have

$$\frac{\Psi_F^{(1)}(x\mathcal{K}_F, y)}{\Psi_F^{(1)}(x\mathcal{K}_F, +\infty)} = \frac{\Psi(x^2 e^{\alpha(f)}, y)}{\Psi(x^2 e^{\alpha(f)}, +\infty)} \left(1 + O\left(\frac{(\log(u+1))^2}{(\log y)^2}\right)\right) \tag{3}$$

where $\alpha(f)$ denotes the Murphy's α function defined by (4) and (5) infra.

Note that the left hand side is equal to the root property $r(f, x, y)$.

In Section 3 we essentially compute the average value of α over the set $E(d, \mathbf{I})$. It gives a lower bound for the best value of α over the same set.

Finally, in Section 4 we prove and generalize Theorem 1.1, and we introduce a modification of NFS where the generalized theorem is relevant.

Notation In what follows, $\mathbf{K}$ stands for a number field and $d_{\mathbf{K}}$, $\mathcal{O}_{\mathbf{K}}$, $U_{\mathbf{K}}$, $G_{\mathbf{K}}$, $\zeta_{\mathbf{K}}$ and $\lambda_{\mathbf{K}}$ denote respectively its degree, ring of integers, unit group, class group, Dedekind zeta function and residue of $\zeta_{\mathbf{K}}$. The letters p, $\mathfrak{p}$ and $\mathfrak{I}$ denote respectively a rational prime, a prime ideal and an arbitrary ideal of $\mathcal{O}_{\mathbf{K}}$. Small caps letters f and g denote polynomials and capital letters F and G denote the associated binary forms.

2 Definition and convergence of Murphy's $\alpha(f)$

2.1 Definition of $\alpha(f)$

Murphy introduced $\alpha(f)$ explicitly for arbitrary polynomials f, but he gives credit to Montgomery for using the formula in the case of quadratic polynomials [Boe96]. Experiments show that one can obtain a good guess of $\Psi_F^{(1)}(x\mathcal{K}, y)$ by the following heuristic method (see [Boe96, Section 4]):

1. Let p be a prime. The average p-adic valuation of the values $F(n_1, n_2)$ with coprime $(n_1, n_2) \in x\mathcal{K} \cap \mathbf{Z}^2$ is given by

$$\mathrm{cont}_p(f, \mathcal{K}) := \lim_{x\to\infty} \frac{\sum_{(n_1,n_2)\in x\mathcal{K}\cap\mathbf{Z}^2, \gcd(n_1,n_2,p)=1} \mathrm{val}_p\, F(n_1, n_2)}{\left|\left\{(n_1, n_2) \in x\mathcal{K} \cap \mathbf{Z}^2 : \gcd(n_1, n_2, p) = 1\right\}\right|}$$

   with the convention $\mathrm{val}_p(0) = 0$.

2. Let $z \leqslant y$ be a large sifting parameter and $F^{(+,z)}(n_1, n_2)$ the z-sifted part of $F(n_1, n_2)$, namely the largest divisor of $F(n_1, n_2)$ without prime factors less than z. We can assume that

$$\left|F^{(+,z)}(n_1, n_2)\right| \approx \frac{|F(n_1, n_2)|}{\prod_{p\leqslant z} p^{\mathrm{cont}_p(f,\mathcal{K})}}$$

   and that the probability for $F^{(+,z)}(n_1, n_2)$ to be y-friable is roughly the same as the probability for a generic z-sifted integer $n \approx |F^{(+,z)}(n_1, n_2)|$. By doing the same for the specific form $F(X_1, X_2) = X_1$, we can expect that the probability for $F(n_1, n_2)$ to be y-friable is given by the probability for a generic integer of logarithm size $\approx \log|F(n_1, n_2)| + \alpha(f, \mathcal{K}, z)$ to be y-friable, where

$$\alpha(f, \mathcal{K}, z) = \sum_{p\leqslant z} \alpha_p(f, \mathcal{K})$$

   with

$$\alpha_p(f, \mathcal{K}) = (\log p)\left(\frac{1}{p-1} - \mathrm{cont}_p(f, \mathcal{K})\right). \tag{4}$$

This suggests the following definition.

Definition 2.1. Let $f \in \mathbf{Z}[X]$ be a polynomial and $\mathcal{K}$ a compact subset of $\mathbf{R}^2$ whose boundary is a continuous closed curve with piecewise continuous derivatives. Under the reserve of proving the convergence of the series below, we define

$$\alpha(f,\mathcal{K}) = \sum_{p \text{ prime}} \alpha_p(f,\mathcal{K}). \tag{5}$$

To get an other expression for $\mathrm{cont}_p(f,\mathcal{K})$, we split the region

$$\left\{(n_1,n_2) \in x\mathcal{K} \cap \mathbf{Z}^2 : \gcd(n_1,n_2,p) = 1\right\}$$

in congruence classes modulo p^k and write

$$\begin{aligned}&\left|\left\{(n_1,n_2) \in x\mathcal{K} \cap \mathbf{Z}^2 : \gcd(n_1,n_2,p) = 1, p^k | F(n_1,n_2)\right\}\right| \\ =&\left|\left\{(n_1,n_2) \in [1,p^k]^2 : \gcd(n_1,n_2,p) = 1, p^k | F(n_1,n_2)\right\}\right| \left(\mathrm{Vol}(\mathcal{K})\frac{x^2}{p^{2k}} + O_{\mathcal{K}}(x)\right).\end{aligned}$$

We can remark that

$$\left|\left\{(n_1,n_2) \in [1,p^k]^2 : \gcd(n_1,n_2,p) = 1, p^k | F(n_1,n_2)\right\}\right| = \varphi(p^k) n_{p^k}(f), \tag{6}$$

where

$$\begin{aligned}n_{p^k}(f) = &\left|\left\{n_1 \in [0,p^k-1] : f(n_1) \equiv 0 \mod p^k\right\}\right| \\ &+ \left|\left\{n_2 \in [0,p^k-1] : n_2 \equiv 0 \mod p,\ F(1,n_2) \equiv 0 \mod p^k\right\}\right|.\end{aligned} \tag{7}$$

Nagell [Nag21] proved what survives of Hensel's lemma when the hypothesis on the derivative fails. We adapt his result to obtain an upper bound on $n_{p^k}(f)$.

Lemma 2.2. *If p does not divide $\mathrm{Disc}(f)$, then $n_{p^k}(f) = n_p(f)$. In the general case, for any prime p and $k \geqslant 1$, we have*

$$n_{p^k}(f) \leqslant 2\deg(f) p^{\min(2\,\mathrm{val}_p(\mathrm{Disc}(f)),k)}.$$

Proof. The first assertion is a direct consequence of [Nag21, Theorem 1] which asserts that

$$\left|\left\{n \in [0,p^k-1] : f(n) \equiv 0 \mod p^k\right\}\right| = \left|\left\{n \in [0,p-1] : f(n) \equiv 0 \mod p\right\}\right|.$$

In the proof of [Nag21, Theorem 2], it is shown that

$$\left|\left\{n \in [0,p^k-1] : f(n) \equiv 0 \mod p^k\right\}\right| \leqslant \deg(f) p^{\min(2\,\mathrm{val}_p(\mathrm{Disc}(f)),k)}.$$

When applied to $F(X,1)$ and $F(1,X)$, this implies the second assertion. □

Based on this observation, Murphy suggests to replace $\mathrm{cont}_p(f,\mathcal{K})$ by $\frac{n_p(f)}{p-1}\frac{p}{p+1}$ for any primes which do not divide $\mathrm{Disc}(f)$. In the following proposition, we show that $\mathrm{cont}_p(f,\mathcal{K})$ can be expressed using $n_{p^k}(f)$ and does not depend on $\mathcal{K}$, which justify the writing $\alpha(f) = \alpha(f,\mathcal{K})$.

Proposition 2.3. *Let $\mathcal{K}$ be a compact subset of $\mathbf{R}^2$ whose boundary is a continuous closed curve with piecewise continuous derivatives and $f \in \mathbf{Z}[X]$ an irreducible polynomial. We have, for every prime p,*

$$\alpha_p(f,\mathcal{K}) = \log p \left(\frac{1}{p-1} - \frac{p}{p+1}\sum_{k\geqslant 1}\frac{n_{p^k}(f)}{p^k}\right). \tag{8}$$

Moreover, if p does not divide $\mathrm{Disc}(f)$, then we have

$$\alpha_p(f,\mathcal{K}) = \frac{\log p}{p-1}\left(1 - n_p(f)\frac{p}{p+1}\right). \tag{9}$$

Proof. We first focus on the numerator of $\mathrm{cont}_p(f,\mathcal{K})$ and we fix a prime p. For any prime p and any real $x \geqslant 2$, one can choose $k_p(x) \geqslant 1$ the least integer such that $x^{1/2} \leqslant p^{k_p(x)} < px^{1/2}$. We write

$$\sum_{\substack{(n_1,n_2)\in x\mathcal{K}\cap\mathbf{Z}^2\\ \gcd(n_1,n_2,p)=1}} \mathrm{val}_p(F(n_1,n_2)) = \Sigma_1(p,\mathcal{K},x) + \Sigma_2(p,\mathcal{K},x)$$

with

$$\Sigma_1(p,\mathcal{K},x) = \sum_{k\leqslant k_p(x)} \left|\left\{(n_1,n_2)\in x\mathcal{K}\cap\mathbf{Z}^2 : \gcd(n_1,n_2,p)=1 \text{ and } p^k|F(n_1,n_2)\right\}\right|$$

and

$$\Sigma_2(p,\mathcal{K},x) = \sum_{k> k_p(x)} \left|\left\{(n_1,n_2)\in x\mathcal{K}\cap\mathbf{Z}^2 : \gcd(n_1,n_2,p)=1 \text{ and } p^k|F(n_1,n_2)\right\}\right|.$$

In view of the formula (6) and Lemma 2.2, we have the following estimation for the first summation, uniformly for $x \geqslant 2$,

$$\begin{aligned}\Sigma_1(p,\mathcal{K},x) &= \sum_{k\leqslant k_p(x)} \varphi(p^k) n_{p^k}(f)\left(\frac{\mathrm{Vol}(\mathcal{K})x^2}{p^{2k}} + O(x)\right)\\ &= \mathrm{Vol}(\mathcal{K})x^2\left(1-\frac{1}{p}\right)\sum_{k\leqslant k_p(x)}\frac{n_{p^k}(f)}{p^k} + O\left(xp^{k_p(x)}\right).\end{aligned}$$

On the other hand, since $\mathrm{val}_p\left(F(n_1,n_2)\right) \ll \log x$, we use again Lemma 2.2 to deduce that, uniformly for $x \geqslant 2$, we have

$$\begin{aligned}\Sigma_2(p,\mathcal{K},x) &\ll \log x\left|\left\{(n_1,n_2)\in x\mathcal{K}\cap\mathbf{Z}^2 : \gcd(n_1,n_2,p)=1 \text{ and } p^{k_p(x)}|F(n_1,n_2)\right\}\right|\\ &\ll (\log x)\varphi(p^{k_p(x)})n_{p^{k_p(x)}}(f)x\\ &\ll x^{3/2}\log x.\end{aligned}$$

Finally, we note that

$$\begin{aligned}\left|\left\{(n_1,n_2)\in x\mathcal{K}\cap\mathbf{Z}^2 : \gcd(n_1,n_2,p)=1\right\}\right| &= \left|\left\{(n_1,n_2)\in x\mathcal{K}\cap\mathbf{Z}^2 : p\nmid n_1\right\}\right| +\\ &+ \left|\left\{(n_1,n_2)\in x\mathcal{K}\cap\mathbf{Z}^2 : p|n_1 \text{ and } p\nmid n_2\right\}\right|\\ &= \left(1-\frac{1}{p^2}\right)\mathrm{Vol}(\mathcal{K})x^2 + O(x).\end{aligned}$$

The result follows when x tends to infinity since then k_p tends to infinity. □

2.2 Convergence of $\alpha(f)$

Let ω be a root of f, $\mathbf{K} = \mathbf{Q}(\omega)$ a rupture field of f and $\tilde{\omega} := F(1,0)\omega$ an integer of $\mathbf{K}$. It follows from a result of Dedekind [Ded78] that, if a prime p does not divide $F(1,0)$ nor the index $[\mathcal{O}_{\mathbf{K}} : \mathbf{Z}[\tilde{\omega}]]$, then $n_p(f)$ is the number of ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) = p$. Since the formula (9) of $\alpha_p(f)$ gets a simple form when p does not divide $\mathrm{Disc}(f)$, the problem of convergence of $\alpha(f)$ is reduced to showing the convergence of the series

$$\sum_{p>p_0}\log p\left(\frac{1}{p-1} - \frac{n_p(\mathbf{K})}{p-1}\left(\frac{p}{p+1}\right)\right)$$

where $n_p(\mathbf{K})$ denotes the number of ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) = p$ and

$$p_0 := \max\left\{p \text{ prime} : p|F(1,0)F(0,1) \text{ or } p|\,\mathrm{Disc}(F) \text{ or } p|[\mathcal{O}_{\mathbf{K}} : \mathbf{Z}[\tilde{\omega}]]\right\}.$$

We first remark that, for any $t \geqslant 2$, we can write

$$\sum_{p\leqslant t}\log p\left(\frac{1}{p-1}-\frac{n_p(\mathbf{K})}{p-1}\left(\frac{p}{p+1}\right)\right)=\sum_{p\leqslant t}\frac{\log p}{p}\left(1-n_p(\mathbf{K})\right)+\sum_{p\leqslant t}\frac{\log p}{p(p-1)}\left(1-\frac{n_p(\mathbf{K})}{p+1}\right).$$

On the one hand, from the Chebyshev estimation

$$\sum_{p\leqslant t}\log p\leqslant \epsilon t \tag{10}$$

with $\epsilon := 1.01624$ (see Theorem 9 of [RS62]), we can use Abel's summation formula to get, for any $t_2 \geqslant t_1 \geqslant d_{\mathbf{K}}$,

$$\begin{aligned}\left|\sum_{t_1<p\leqslant t_2}\frac{\log p}{p(p-1)}\left(1-\frac{n_p(\mathbf{K})}{p+1}\right)\right| &\leqslant \sum_{t_1<p\leqslant t_2}\frac{\log p}{p(p-1)}\\ &\leqslant \frac{\epsilon}{t_1-1}.\end{aligned}$$

On the other hand, using Abel's summation formula a second time, we have

$$\sum_{t_1<p\leqslant t_2}\frac{\log p}{p}\left(1-n_p(\mathbf{K})\right)=\frac{R(t_2)}{t_2}-\frac{R(t_1)}{t_1}+\int_{t_1}^{t_2}\frac{R(s)}{s^2}\mathrm{d}s,$$

where R is the rest term defined by

$$R(t):=\sum_{p\leqslant t}(1-n_p(\mathbf{K}))\log p.$$

Therefore, it suffices to use a sufficiently sharp estimation of $R(t)$, which is the object of the next theorem. On the one hand, we can obtain a very sharp estimation using the Riemann hypothesis for $\zeta_{\mathbf{K}}$ and $\zeta_{\mathbf{Q}}$. But on the other hand, we have a good estimation relying on no assumptions.

Theorem D (Theorem 9.2, [LO77]). *1. Call $d_{\mathbf{K}}$ the degree of $\mathbf{K}$. There exists an absolute effectively computable constant $c_1>0$ such that, if $t\geqslant \exp\left(4d_{\mathbf{K}}(\log \mathrm{Disc}(\mathbf{K}))^2\right)$, then*

$$\left|\sum_{N(\mathfrak{p}^k)\leqslant t}\log N(\mathfrak{p})-t+\frac{t^{\beta(\mathbf{K})}}{\beta(\mathbf{K})}\right|\leqslant t\exp\left(-c_1 d_{\mathbf{K}}^{-1/2}(\log t)^{1/2}\right),$$

where $\beta(\mathbf{K})$ denotes the largest real zero of $\zeta_{\mathbf{K}}$ in the interval $(0,1)$ if it exists and $1/2$ otherwise.

2. Moreover, if the Riemann Hypothesis holds for $\zeta_{\mathbf{K}}$, there exist explicit constants $a_{\mathbf{K}}$, $b_{\mathbf{K}}$ and $c_{\mathbf{K}}$ such that, for $t\geqslant 2$, we have

$$\left|\sum_{N(\mathfrak{p}^k)\leqslant t}\log N(\mathfrak{p})-t\right|\leqslant t^{1/2}\left(a_{\mathbf{K}}+b_{\mathbf{K}}\log t+c_{\mathbf{K}}(\log t)^2\right).$$

Remarks 2.4.

- Some effective bounds for $\beta(\mathbf{K})$ are contained in Theorem 1.4 of [LO77]. In particular, there exists an effectively computable constant $c_2>0$ such that we have

$$\beta(\mathbf{K})\leqslant \max\left(1-\left(16d_{\mathbf{K}}!\log\mathrm{Disc}(\mathbf{K})\right)^{-1},1-\left(c_2\,\mathrm{Disc}(\mathbf{K})^{1/d_{\mathbf{K}}}\right)^{-1}\right).$$

- Numerical values for $a_{\mathbf{K}}$, $b_{\mathbf{K}}$ and $c_{\mathbf{K}}$ are given without proof in [Oes79]. The explicit values $a_{\mathbf{K}}=\frac{4781}{96}\log(\mathrm{Disc}(\mathbf{K}))+\frac{58681}{113}d_{\mathbf{K}}$, $b_{\mathbf{K}}=\frac{23}{3}\log(\mathrm{Disc}(\mathbf{K}))+\frac{68}{3}d_{\mathbf{K}}$ and $c_{\mathbf{K}}=\frac{863}{31}d_{\mathbf{K}}$ can be rigorously obtained from Theorem 8.1 of [Win].

In order to use Theorem D, we have to study the contribution of powers of prime ideals. Using Chebyshev's estimation (10), we get for any $t \geqslant 2$

$$\sum_{\substack{N(\mathfrak{p}^k)\leqslant t \\ k\geqslant 2 \text{ or } N(\mathfrak{p}) \text{ not prime}}} \log N(\mathfrak{p}) \leqslant d_{\mathbf{K}} \sum_{k\geqslant 2} \sum_{p\leqslant t^{\frac{1}{k}}} \log p$$
$$\leqslant \epsilon d_{\mathbf{K}} \left(t^{\frac{1}{2}} + \frac{\log t}{\log 2} t^{1/3} \right).$$

Consequently, we have, for $t \geqslant \exp\left(4d_{\mathbf{K}}(\log \mathrm{Disc}(\mathbf{K}))^2\right)$,

$$R(t) \ll d_{\mathbf{K}} t^{\frac{1}{2}} + \frac{t^{\beta(\mathbf{K})}}{\beta(\mathbf{K})} + t \exp\left(-c_1 (d_{\mathbf{K}})^{-1/2} (\log t)^{1/2}\right).$$

By computing the antiderivative of the function in the right hand member, we deduce that we have, for $t_2 \geqslant t_1 \geqslant \exp\left(4d_{\mathbf{K}}(\log \mathrm{Disc}(\mathbf{K}))^2\right)$,

$$\left| \sum_{t_1 < p \leqslant t_2} \frac{\log p}{p} \left(1 - n_p(\mathbf{K})\right) \right| \leqslant \frac{|R(t_1)|}{t_1} + \frac{|R(t_2)|}{t_2} + \int_{t_1}^{t_2} \frac{|R(s)|}{s^2} \mathrm{d}s$$
$$\ll d_{\mathbf{K}} t_1^{-\frac{1}{2}} + \frac{t_1^{\beta(\mathbf{K})-1}}{\beta(\mathbf{K})} + (\log t_1)^{1/2} \exp\left(-c_1 (d_{\mathbf{K}})^{-1/2} (\log t_1)^{1/2}\right),$$

which implies the convergence of $\alpha(f)$.

In order to get a good estimation of the convergence speed, we now assume that the Riemann Hypothesis holds for $\zeta_{\mathbf{Q}}$ and $\zeta_{\mathbf{K}}$. It follows from Theorem D that we have, for $t \geqslant 2$,

$$|R(t)| \leqslant \epsilon d_{\mathbf{K}} t^{1/2} + \epsilon d_{\mathbf{K}} t^{1/3} \frac{\log t}{\log 2} + a_{\mathbf{K}} t^{1/2} + b_{\mathbf{K}} t^{1/2} (\log t) + c_{\mathbf{K}} t^{1/2} (\log t)^2.$$

As a consequence of the previous discussion, we can get that, for $t \geqslant 2$,

$$\left| \sum_{t < p} \frac{\log p}{p} \left(1 - n_p(\mathbf{K})\right) \right| \leqslant \frac{|R(t)|}{t} + \int_t^{+\infty} \frac{|R(s)|}{s^2} \mathrm{d}s$$
$$\leqslant t^{-1/2} \Bigg(\left(3a_{\mathbf{K}} + 3\epsilon d_{\mathbf{K}} + 4b_{\mathbf{K}} + 16c_{\mathbf{K}} + (3b_{\mathbf{K}} + 8c_{\mathbf{K}}) \log t + 3c_{\mathbf{K}} (\log t)^2\right)$$
$$+ t^{-1/6} \frac{\epsilon d_{\mathbf{K}}}{\log 4} \left(\frac{9}{2} + 5 \log t\right) \Bigg).$$

It follows that the speed of convergence is given, for $t \geqslant \max(p_0, d_{\mathbf{K}})$, by

$$\left| \alpha(f) - \sum_{p\leqslant t} \alpha_p(f) \right| \leqslant t^{-1/2} \Big(\frac{\epsilon t^{1/2}}{t-1} + t^{-1/6} \frac{\epsilon d_{\mathbf{K}}}{\log 4} \left(\frac{9}{2} + 5 \log t\right)$$
$$+ \left(3a_{\mathbf{K}} + 3\epsilon d_{\mathbf{K}} + 4b_{\mathbf{K}} + 16c_{\mathbf{K}} + (3b_{\mathbf{K}} + 8c_{\mathbf{K}}) \log t + 3c_{\mathbf{K}} (\log t)^2\right) \Big). \quad (11)$$

By using the best numerical values in Remark 2.4, one gets some explicits constants for the convergence speed of $\alpha(f)$, available under the Riemann Hypothesis for $\zeta_{\mathbf{K}}$ and $\zeta_{\mathbf{Q}}$.

Proposition 2.5. *Let $f \in \mathbf{Z}[X]$ be an irreducible polynomial of degree d and $\mathbf{K}$ a rupture field of f. Suppose that the Riemann Hypothesis holds for $\zeta_{\mathbf{K}}$ and $\zeta_{\mathbf{Q}}$. Then, we have, for any $t \geqslant p_0$,*

$$\left| \alpha(f) - \sum_{p\leqslant t} \alpha_p(f) \right| \leqslant t^{-1/2} \Big(2105 d_{\mathbf{K}} + 181 \log \mathrm{Disc}(\mathbf{K}) + (23 \log \mathrm{Disc}(\mathbf{K}) + 295 d_{\mathbf{K}}) \log t$$
$$+ 84 d_{\mathbf{K}} (\log t)^2 \Big). \quad (12)$$

Example 2.6. Consider $F(X_1, X_2) = X_1^2 + qX_2^2$ with $q = 10^{30} + 57$. By computing the partial sum of α for primes p less than $t = 4 \cdot 10^{10}$ we obtain $|\sum_{p \leqslant t} \alpha_p(f) - 2.39| < 0.01$. Here we have $d_K = 2$ and $\log(D_K) \approx 70.46$. Proposition 2.5 allows to conclude that, under the assumption that Riemann's hypothesis holds for $\zeta_{\mathbf{Q}}$ and $\zeta_{\mathbf{K}}$, we have

$$\big|\alpha(f) - 2.39\big| < 1.$$

In the next section we essentially show that the average of α is ≈ 0.56, so our polynomial has a bad value of α. The term $84 d_K \log(t)^2$ is the most important in this case because it is $\approx 0.56\sqrt{t}$, while the total bound is $0.86\sqrt{t}$. This emphasizes the importance of obtaining small effective constants in Theorem D.

Remarks 2.7. One can define an analogous to Murphy's α when $f \in \mathbf{F}_2[t][X]$. The first author proved [Bar15, Theorem 2.14] that α has a better speed of convergence in that case, as no factor in $(\log t)^2$ is needed.

3 Towards the average of α on a set of polynomials

The polynomial selection stage of NFS consists in enumerating polynomials $f(X) = \sum_{i=0}^{d} f_i X^i$ of a given degree and with a bound on each coefficient f_i and in selecting those with the best value of $\alpha(f)$. Some variants restrict the enumeration to a subset and a short list of polynomials with a good α can be further tested with longer tests or by direct sieving. In any case, by computing the average of α we guarantee a value of α for the best polynomials.

For each pair (m, d) of integers and each product of intervals $\mathbf{I} = I_0 \times \cdots \times I_{d-1}$ such that, for all i, $I_i \subset [-m, m]$, we consider the set

$$E^{(1)}(m, d, \mathbf{I}) := \left\{ X^d + \sum_{i=0}^{d-1} f_i X^i : (f_0, f_1, \ldots, f_{d-1}) \in \mathbf{I} \cap \mathbf{Z}^d, \mathrm{Disc}(f) \neq 0 \right\}. \tag{13}$$

Note the introduction of the parameter m in the definition of $E^{(1)}(m, d, \mathbf{I})$, which plays an important role. In practice, it can be computed from $\mathbf{I}$ as the minimal integer m such that $I_i \subset [-m, m]$ for all $i \in \{0, \ldots, d-1\}$. Due to technical reasons, we now study the average of $\alpha(f)$ on $E^{(1)}(m, d, \mathbf{I})$ rather than on the set $E(d, \mathbf{I})$ introduced by (2) in the introduction of this article.

Theorem 3.1. *We have the mean value*

$$\lim_{\substack{m/\log p \to \infty \\ \min_j |I_j|/(d^2 \log(dm) \log p) \to \infty}} \frac{1}{|E^{(1)}(m, d, \boldsymbol{I})|} \sum_{f \in E^{(1)}(m, d, \boldsymbol{I})} \alpha_p(f) = \alpha_p(X). \tag{14}$$

Proof. First note that $\alpha_p(f) = \alpha_p(X)$ for any linear polynomial f (its value is computed in Proposition 3.2), so we can assume $d \geqslant 2$. In view of Proposition 2.3, we have, for any prime p,

$$\alpha_p(f) - \alpha_p(X) = \frac{p \log p}{p+1} \sum_{k \geqslant 1} \frac{1 - n_{p^k}(f)}{p^k}.$$

For any integer k, we put

$$S_p(k, m, d, \mathbf{I}) := \sum_{f \in E^{(1)}(m, d, \mathbf{I})} (1 - n_{p^k}(f)).$$

Then we have

$$\sum_{f \in E^{(1)}(m, d, \mathbf{I})} (\alpha_p(f) - \alpha_p(X)) = \Sigma_p^{(1)}(m, d, \mathbf{I}) + \Sigma_p^{(2)}(m, d, \mathbf{I}),$$

where, for a k_p specified below,

$$\begin{aligned} \Sigma_p^{(1)}(m, d, \mathbf{I}) &:= \frac{p \log p}{p+1} \sum_{k=1}^{k_p} \frac{S_p(k, m, d, \mathbf{I})}{p^k}, \\ \Sigma_p^{(2)}(m, d, \mathbf{I}) &:= \frac{p \log p}{p+1} \sum_{k > k_p} \frac{S_p(k, m, d, \mathbf{I})}{p^k}. \end{aligned}$$

Using the definition of the discriminant, for any f in $E^{(1)}(m,d,\mathbf{I})$, we have the upper bound

$$|\operatorname{Disc}(f)| \leqslant (2d-1)!m^{2d-1}.$$

Consider $k_p = 2\left\lceil \log_p\left((2d-1)!m^{2d-1}\right)\right\rceil + \lceil \log_p(md)\rceil$.

Case $k \leqslant k_p$. Since the elements of $E^{(1)}(m,d,\mathbf{I})$ are monic, we can write, in view to the definition (7) of $n_{p^k}(f)$,

$$\Sigma_p^{(1)}(m,d,\mathbf{I}) = \frac{p\log p}{p+1}\sum_{k=1}^{k_p}\frac{1}{p^k}\left(\left|E^{(1)}(m,d,\mathbf{I})\right| - \sum_{r=0}^{p^k-1}\left|\left\{f\in E^{(1)}(m,d,\mathbf{I}), f(r)\equiv 0 \pmod{p^k}\right\}\right|\right).$$

We consider first the cardinality of $E^{(1)}(m,d,\mathbf{I})$. Given $(f_1,\dots,f_{d-1}) \in I_1\times\cdots\times I_{d-1}$, the polynomial $dX^{d-1}+\sum_{i=1}^{d-1} if_iX^{i-1}$ has at most $d-1$ complex roots. For each such root z, there is at most one value of $f_0\in I_0$ such that $\sum_{i=0}^{d} f_iz^i = 0$. Hence there are at most $d|\mathbf{I}|/|I_0|$ polynomials f of zero discriminant and coefficients in $\mathbf{I}$. It follows that

$$\begin{aligned} E^{(1)}(m,d,\mathbf{I}) &= \left|\left\{(f_0,\dots,f_{d-1})\in \mathbf{I}\cap\mathbf{Z}^d\right\}\right| - \left|\left\{(f_0,\dots,f_{d-1})\in \mathbf{I}\cap\mathbf{Z}^d : \operatorname{Disc}\left(X^d+\sum_{i=0}^{d-1}f_iX^i\right)=0\right\}\right| \\ &= |\mathbf{I}|\left(1+O\left(\frac{d}{\min_j|I_j|}\right)\right). \end{aligned}$$

Let $k\leqslant k_p$ be an integer and $r\in[0,p^k-1]$. For each $(d-1)$-tuple $(f_1,\dots,f_{d-1})\in I_1\times\cdots\times I_{d-1}$, the number of values f_0 such that $f(r)\equiv 0 \pmod{p^k}$ is $\left\lfloor\frac{|I_0|}{p^k}\right\rfloor+\epsilon$ with $\epsilon=0$ or 1. Hence, it follows that

$$\begin{aligned} \left|\left\{f\in E^{(1)}(m,d,\mathbf{I}), f(r)\equiv 0 \pmod{p^k}\right\}\right| &= \left|\left\{(f_0,\dots,f_{d-1})\in\mathbf{I}\cap\mathbf{Z}^d : f(r)\equiv 0 \pmod{p^k}\right\}\right| \\ &\quad + O\left(\left|\left\{(f_0,\dots,f_{d-1})\in\mathbf{I}\cap\mathbf{Z}^d : \operatorname{Disc}\left(X^d+\sum_{i=0}^{d-1}f_iX^i\right)=0\right\}\right|\right) \\ &= \left(\frac{|I_0|}{p^k}+O(1)\right)\frac{|\mathbf{I}|}{|I_0|} + O\left(\frac{d|\mathbf{I}|}{\min_j|I_j|}\right) \\ &= \frac{|\mathbf{I}|}{p^k} + O\left(\frac{|\mathbf{I}|d}{\min_j|I_j|}\right). \end{aligned}$$

Then we obtain that

$$\begin{aligned} \Sigma_p^{(1)}(m,d,\mathbf{I}) &\ll \log p\sum_{k\leqslant k_p}\frac{|\mathbf{I}|d}{\min_j|I_j|} \\ &\ll k_p\log p\frac{|\mathbf{I}|d}{\min_j|I_j|}. \end{aligned}$$

Case $k > k_p$. Due to the choice of k_p, we have $k_p \geqslant 2\operatorname{val}_p\operatorname{Disc}(f)$ for all polynomials f in $E^{(1)}(m,d,\mathbf{I})$. By Lemma 2.2 and the definition of k_p, for all $k\geqslant k_p$, we have

$$n_{p^k}(f) \ll d\operatorname{Disc}(f)^2 \leqslant d\left((2d-1)!m^{2d-1}\right)^2 \leqslant p^{k_p}/m.$$

By summing over $k > k_p$, we deduce that

$$\Sigma_p^{(2)}(m,d,\mathbf{I}) \ll \frac{|\mathbf{I}|}{m}\log p.$$

When combining the bounds on $\sum_p^{(1)}(m,d,\mathbf{I})$ and $\sum_p^{(2)}(m,d,\mathbf{I})$, we obtain that, uniformly for $p, m \geqslant 2$ and $\min_j |I_j| \geqslant d$, we have

$$\sum_{f\in E^{(1)}(m,d,\mathbf{I})} (\alpha_p(f) - \alpha_p(X)) \ll |\mathbf{I}| \log p \left(\frac{1}{m} + \frac{d^2(\log(dm))}{\min_j |I_j|}\right). \tag{15}$$

□

In view of the previous theorem, it seems interesting to compute the value of $\alpha(X)$. This is the aim of the following proposition.

Proposition 3.2. *Let $f(X) = aX + b \in \mathbf{Z}[X]$ be a linear polynomial with $\gcd(a,b) = 1$. Then we have*

$$\alpha(f) = 12\log A - \gamma - \log(2\pi) \approx 0.56.$$

where A denotes the Glaisher-Kinkelin constant and γ denotes the Euler-Mascheroni constant.

Proof. Since f has degree 1 and $\gcd(a,b) = 1$, we have, for every prime p and $k \geqslant 1$,

$$n_{p^k}(f) = 1.$$

Consequently, it follows from Proposition 2.3 that

$$\alpha(f) = \sum_p \frac{\log p}{p-1}\left(1 - \frac{p}{p+1}\right) = \sum_p \frac{\log p}{p^2-1}.$$

From the formula

$$\frac{\zeta'_{\mathbf{Q}}(s)}{\zeta_{\mathbf{Q}}(s)} = -\sum_p \frac{\log p}{p^s - 1},$$

which holds for any complex s such that $\Re(s) > 1$, we deduce that

$$\alpha(f) = \sum_p \frac{\log p}{p^2-1} = -\frac{\zeta'_{\mathbf{Q}}(2)}{\zeta_{\mathbf{Q}}(2)}.$$

The result is then a direct consequence of the formulae

$$\zeta_{\mathbf{Q}}(2) = \frac{\pi^2}{6} \qquad \text{and} \qquad \zeta'_{\mathbf{Q}}(2) = \frac{\pi^2}{6}\left(\gamma + \log(2\pi) - 12\log A\right).$$

□

4 A theoretical modification of NFS

4.1 The algorithm

The main goal of this section is to prove a result concerning friability for binary forms of degree 2, namely Theorem 1.1. We can tackle the problem with multiplicative methods since the values of a quadratic binary form are norms of arbitrary integer elements of a quadratic field. The same result applies to binary forms of higher degrees if we modify the algorithm as below. By doing so, we transfer the difficulty from the field of analytic number theory to that of algorithmic number theory.

In short, in our modification of NFS, instead of considering elements $n_1 + n_2\omega$ of $\mathbf{Q}(\omega)$, we consider arbitrary elements $n_1 + n_2\omega + \cdots + n_d\omega^{d-1}$, where d is the degree of the defining polynomial f. In more detail, the new version of the algorithm is as follows. We select two polynomials f and g, with f irreducible of degree $d \geqslant 2$ and g linear such that there exists an integer m such that $f(m) \equiv g(m) \equiv 0 \mod N$. Let ω be a complex root of f. We use the same factor base as in the classical version of NFS, i.e. if y is the friability bound, the factor base includes primes p up to y and prime ideals $\mathfrak{p}$ in the number field $\mathbf{Q}(\omega)$ above primes p less than or equal to y. Let X_f and X_g be the maximal value of $\mathrm{N}(n_1 + n_2\omega)$ and $|n_1 + n_2 m|$ respectively when n_1 and n_2 are bounded by the constant used in NFS. Next we collect d-tuple $(n_1, \ldots, n_d)$ such that

- $\gcd(n_1, \ldots, n_d) = 1$
- $|\,\mathrm{N}(n_1 + \cdots + n_d\omega^{d-1})| \leqslant X_f$ and $|n_1 + \cdots + n_d m^{d-1}| \leqslant X_g$.
- $|\,\mathrm{N}(n_1 + \cdots + n_d m^{d-1})|$ and $|n_1 + \cdots + n_d m^{d-1}|$ are y-friable.

Each polynomial $n_1 + n_2 X + \cdots + n_d X^{d-1}$ allows us to obtain a relation as explained by Joux, Lercier, Smart and Vercauteren in [JLSV06]. Finally, we use the linear system to obtain a non-trivial solution of equation $a^2 \equiv b^2 \pmod N$ by following step by step the classical variant of NFS.

In the particular case when f is quadratic, enumerating the pairs (n_1, n_2) such that $|F(n_1, n_2)|$ is less than a bound X_f is easy because this set is the union of a small number of convex sets. Hence, the modification of NFS doesn't put any problem. In the general case, the problem of enumerating the set of d-tuples as above is open and goes beyond the scope of this article.

4.2 The friability probability: general case

Let $\mathbf{K}$ be a number field of degree $d_{\mathbf{K}}$ and ω an integral primitive element of $\mathbf{K}$. In view of the previous discussion, we consider the following set

$$\Big\{(n_1, \ldots, n_d) \in \mathbf{Z}^d : \gcd(n_1, \ldots, n_d) = 1, |\,\mathrm{N}(n_1 + \cdots + n_d\omega^{d-1})| \leqslant x, |n_1 + \cdots + n_d m^{d-1}| \leqslant x\ , \\ P(n_1 + \cdots + n_d m^{d-1}) \leqslant y \text{ and } P\left(\mathrm{N}(n_1 + \cdots + n_d\omega^{d-1})\right) \leqslant y\Big\}.$$

In this article we drop the conditions over $n_1 + \cdots + n_d m^{d-1}$ by studying a set which is easier to analyse, namely

$$\Big\{(n_1, \ldots, n_d) \in \mathbf{Z}^d : \gcd(n_1, \ldots, n_d) = 1, |\,\mathrm{N}(n_1 + \cdots + n_d\omega^{d-1})| \leqslant x \\ \text{and } P\left(\mathrm{N}(n_1 + \cdots + n_d\omega^{d-1})\right) \leqslant y\Big\}.$$

If the unit group $U_{\mathbf{K}}$ is infinite (this is the case when $d_{\mathbf{K}} \geqslant 3$ or $\mathbf{K}$ is a real quadratic field), such a set is infinite. However, we can remark that the principal ideals $\mathfrak{I}$ generated by the elements $n_1 + \cdots + n_d\omega^{d-1}$ are primitive, namely that, for any prime p, they satisfy $p\mathcal{O}_{\mathbf{K}} \nmid \mathfrak{I}$. Consequently, it makes sense to focus on the cardinality

$$\Psi_{\mathbf{K}}^{(1)}(x, y) := \Big|\big\{\mathfrak{I} \text{ primitive} : \mathrm{N}(\mathfrak{I}) \leqslant x \text{ and } P(\mathrm{N}(\mathfrak{I})) \leqslant y\big\}\Big|.$$

A standard way – the one followed here – to get an asymptotic formula for $\Psi_{\mathbf{K}}^{(1)}(x, y)$ consists to apply to the Dirichlet series $\mathcal{F}_{\mathbf{K}}(s)$ defined by

$$\mathcal{F}_{\mathbf{K}}(s) := \sum_{\mathfrak{I} \text{ primitive}} \frac{1}{\mathrm{N}(\mathfrak{I})^s}$$

some results of complex analysis, such as Perron's formula. Using the inclusion–exclusion principle, we first remark that we have, for $\Re(s) > 1$,

$$\mathcal{F}_{\mathbf{K}}(s) = \sum_{m \geqslant 1} \mu(m) \sum_{m\mathcal{O}_{\mathbf{K}} | \mathfrak{I}} \frac{1}{\mathrm{N}(\mathfrak{I})^s} = \zeta_{\mathbf{K}}(s)\zeta_{\mathbf{Q}}(d_{\mathbf{K}}s)^{-1}. \tag{16}$$

Moreover, using the properties of the Riemann zeta function, it is immediate that $\zeta_{\mathbf{Q}}(d_{\mathbf{K}}s)^{-1}$ is absolutely convergent for $\Re(s) > \frac{1}{d_{\mathbf{K}}}$.

In view of the previous discussion, we are now in capacity to use asymptotic results of Hanrot, Tenenbaum and Wu [HTW08] based on the saddle-point method. We obtain the following theorem.

Theorem 4.1. *Let K be a number field of degree $d_{\mathbf{K}} \geqslant 2$. Then, there exists $C > 0$ such that, for any $J \geqslant 0$ and $\varepsilon > 0$, we have, uniformly for (x, y) in (H_ε) and*

$$0 < u < J + 1 \Rightarrow (u - \lfloor u \rfloor) > C(J + 1)\frac{\log\log y}{\log y}$$

$$\Psi_{\mathbf{K}}^{(1)}(x,y) = x\left(\sum_{j=0}^{J}\gamma_j(\mathbf{K})\frac{\rho^{(j)}(u)}{(\log y)^j} + O\left(\rho(u)\left(\frac{\log(u+1)}{\log y}\right)^{J+1}\right)\right), \tag{17}$$

where

$$\gamma_j(\mathbf{K}) = \sum_{j_1+j_2=j}\frac{1}{j_1!j_2!}\left.\frac{\partial^{j_1}(1-s^{-1})\zeta_{\mathbf{K}}(s)}{\partial s^{j_1}}\right|_{s=1}\left.\frac{\partial^{j_2}\zeta_{\mathbf{Q}}(d_{\mathbf{K}}s)^{-1}}{\partial s^{j_2}}\right|_{s=1}.$$

In particular, we have

$$\gamma_0(\mathbf{K}) = \frac{\lambda_{\mathbf{K}}}{\zeta_{\mathbf{Q}}(d_{\mathbf{K}})}$$

where $\lambda_{\mathbf{K}}$ *denotes the residue of* $\zeta_{\mathbf{K}}$ *and*

$$\gamma_1(\mathbf{K}) = \gamma_0(\mathbf{K})\left(\gamma - 1 + \sum_p \log p\left(\frac{1}{p-1} - \mathrm{cont}_p(\mathbf{K})\right)\right),$$

with

$$\mathrm{cont}_p(\mathbf{K}) = \left(\sum_{k\geqslant 1}\frac{k\left|\left\{\mathfrak{I}\ primitive, \mathrm{N}(\mathfrak{I}) = p^k\right\}\right|}{p^k}\right)\left(\sum_{k\geqslant 0}\frac{\left|\left\{\mathfrak{I}\ primitive, \mathrm{N}(\mathfrak{I}) = p^k\right\}\right|}{p^k}\right)^{-1}.$$

Proof. In view of Equation (16), it is immediate that $\mathcal{F}_{\mathbf{K}}(s)$ satisfies the condition (1.7) of [HTW08]. Following *mutatis mutandis* the arguments of Section 2.3 of [HTW08], we can see that condition (1.10) in [HTW08] is satisfied, namely that the formula

$$\sum_{P(n)\leqslant y}\frac{\mu(n)}{n^{d_{\mathbf{K}}s}} = \sum_n \frac{\mu(n)}{n^{d_{\mathbf{K}}s}} + O\left(\frac{1}{y^{1-\delta}}\right) \tag{18}$$

holds uniformly for any $\frac{1}{d_{\mathbf{K}}} < \delta < 1$ and uniformly for $\Re(s) \geqslant \delta$. Consequently, we can apply successively Theorem 1.2 and Theorem 1.1 of [HTW08] to deduce (17).

The statement on the values $\gamma_0(\mathbf{K})$ and $\gamma_1(\mathbf{K})$ follows from the fact that

$$\left(\frac{\frac{\partial\mathcal{F}_{\mathbf{K}}(s)}{\partial s}}{\mathcal{F}_{\mathbf{K}}(s)} - \frac{\frac{\partial\zeta_{\mathbf{Q}}(s)}{\partial s}}{\zeta_{\mathbf{Q}}(s)}\right)\Bigg|_{s=1} = \sum_p \log p\left(\frac{1}{p-1} - \mathrm{cont}_p(\mathbf{K})\right) \quad \text{and} \quad \left.\frac{\frac{(s-1)\partial\zeta_{\mathbf{Q}}(s)}{\partial s}}{(s-1)\zeta_{\mathbf{Q}}(s)}\right|_{s=1} = \gamma - 1.$$

□

4.3 The friability probability: imaginary quadratic case

In this section, we apply the previous result to get an asymptotic estimation related to the proportion of friable values of quadratic binary forms with fundamental negative discriminant. This gives a proof of Theorem 1.1.

Proof of Theorem 1.1. Let ω be a root of $f(X) = F(X,1)$ and $\mathbf{K} := \mathbf{Q}(\omega)$. Since $\mathrm{Disc}(f)$ is a fundamental discriminant, we have $\mathrm{Disc}(\mathbf{K}) = \mathrm{Disc}(f)$. Moreover, there exists an ideal $\mathfrak{d}$ of $\mathcal{O}_{\mathbf{K}}$ with basis (ω_1, ω_2) such that, for any integers n_1 and n_2, one has

$$F(n_1,n_2) = \frac{\mathrm{N}(n_1\omega_1 + n_2\omega_2)}{\mathrm{N}(\mathfrak{d})}.$$

Since the unit group $U_{\mathbf{K}}$ is finite, we have

$$\begin{aligned}\Psi_F^{(1)}(x\mathcal{K}_F, y) &= \left|\left\{(n_1,n_2)\in\mathbf{Z}^2\ :\ \gcd(n_1,n_2)=1, \frac{\mathrm{N}(n_1\omega_1+n_2\omega_2)|}{\mathrm{N}(\mathfrak{d})}\leqslant x^2, P\left(\frac{\mathrm{N}(n_1\omega_1+n_2\omega_2)}{\mathrm{N}(\mathfrak{d})}\right)\leqslant y\right\}\right| \\ &= |U_{\mathbf{K}}|\left|\left\{\mathfrak{L}\text{ principal }:\ \mathfrak{d}|\mathfrak{L}, \mathfrak{L}\mathfrak{d}^{-1}\text{ primitive}, \mathrm{N}\left(\mathfrak{L}\mathfrak{d}^{-1}\right)\leqslant x^2, P\left(\mathrm{N}\left(\mathfrak{L}\mathfrak{d}^{-1}\right)\right)\leqslant y\right\}\right|.\end{aligned} \tag{19}$$

By writing, $\mathfrak{L} = \mathfrak{I}\mathfrak{d}$, the problem is then reduced to detect the primitive and integral ideals $\mathfrak{I}$ in the class of $\mathfrak{d}^{-1}$ satisfying $\mathrm{N}(\mathfrak{I}) \leqslant x^2$ and $P(\mathrm{N}(\mathfrak{I})) \leqslant y$. In order to pick up ideals from the class $\mathrm{cl}\left(\mathfrak{d}^{-1}\right)$, we can consider the group $\widehat{G_{\mathbf{K}}}$ of the multiplicative characters of the class group $G_{\mathbf{K}}$. By the orthogonality property of characters, we have

$$\begin{aligned}&\left|\left\{\mathfrak{L} \text{ principal } : \ \mathfrak{d}|\mathfrak{L}, \mathfrak{L}\mathfrak{d}^{-1} \text{ primitive}, \mathrm{N}\left(\mathfrak{L}\mathfrak{d}^{-1}\right) \leqslant x^2, P\left(\mathrm{N}\left(\mathfrak{L}\mathfrak{d}^{-1}\right)\right) \leqslant y\right\}\right| \\ =&\frac{1}{|G_{\mathbf{K}}|}\sum_{\chi\in\widehat{G_{\mathbf{K}}}}\chi(\mathfrak{d})\Psi^{(1)}\left(x^2, y; \chi\right), \end{aligned} \tag{20}$$

where

$$\Psi^{(1)}(x, y; \chi) = \sum_{\substack{\mathfrak{I} \text{ primitive} \\ \mathrm{N}(\mathfrak{I})\leqslant x \\ P(\mathrm{N}(\mathfrak{I}))\leqslant y}} \chi(\mathfrak{I}).$$

Contribution of nontrivial characters:

Since $\mathrm{cl}(p\mathcal{O}_{\mathbf{K}})$ is the identity element of the class group $G_{\mathbf{K}}$, the inclusion-exclusion principle implies that

$$\sum_{\mathfrak{I} \text{ primitive}} \frac{\chi(\mathfrak{I})}{\mathrm{N}(\mathfrak{I})^s} = \sum_{\mathfrak{I}} \frac{\chi(\mathfrak{I})}{\mathrm{N}(\mathfrak{I})^s}\left(\prod_p\left(1-\frac{1}{p^{2s}}\right)\right)$$

whenever $\Re(s) > 1$. Consequently, we can adapt, step by step, the proof of Theorem 4.1 to deduce that, for any $\varepsilon > 0$ and uniformly for

$$x \geqslant 3, \qquad \exp\left((\log\log x)^{5/3+\varepsilon}\right) \leqslant y \leqslant x, \tag{H_ε}$$

we have

$$\Psi^{(1)}(x, y; \chi) \ll x\rho(u)\exp\left(-(\log y)^{\frac{3}{5}-\varepsilon}\right). \tag{21}$$

This procedure is essentially made in [Ten90] and [FT91].

Contribution of the trivial character:

For the principal character, denoted by χ_0, we use Theorem 4.1. There exists $\kappa > 0$ such that, for any $\varepsilon > 0$ and uniformly for

$$x \geqslant 3, \qquad \exp\left((\log\log x)^{5/3+\varepsilon}\right) \leqslant y \leqslant x(\log x)^{-\kappa},$$

we have

$$\Psi^{(1)}(x, y; \chi_0) = x\left(\gamma_0(\mathbf{K})\rho(u) + \gamma_1(\mathbf{K})\frac{\rho'(u)}{\log y} + O\left(\rho(u)\left(\frac{\log(u+1)}{\log y}\right)^2\right)\right),$$

where $\gamma_0(\mathbf{K}) = \frac{6\lambda_K}{\pi^2}$ and

$$\gamma_1(\mathbf{K}) = \gamma_0(\mathbf{K})\left(\gamma - 1 + \sum_p \log p\left(\frac{1}{p-1} - \mathrm{cont}_p(\mathbf{K})\right)\right).$$

Recall the definition of $n_p(\mathbf{K})$ introduced in Section 2.2, namely the number of prime ideals $\mathfrak{p}$ satisfying $\mathrm{N}(\mathfrak{p}) = p$. Using the decomposition of rational primes into ideals of $\mathcal{O}_{\mathbf{K}}$ (see for example the discussion in Section 6.4 of [Bue89]), we can note that

$$\left|\left\{\mathfrak{I} \text{ primitive}, \mathrm{N}(\mathfrak{I}) = p^k\right\}\right| = \begin{cases} 0 & \text{if } p \mid \mathrm{Disc}(\mathbf{K}) \text{ and } k \geqslant 2, \\ n_p(\mathbf{K}) & \text{if } k = 1 \text{ or } p \nmid \mathrm{Disc}(\mathbf{K}), \end{cases}$$

and therefore

$$\mathrm{cont}_p(\mathbf{K}) = \begin{cases} \frac{1}{p+1} & \text{if } p|\operatorname{Disc}(\mathbf{K}), \\ \frac{p}{p-1}\frac{n_p(\mathbf{K})}{p+1} & \text{otherwise.} \end{cases}$$

A careful study of $\mathrm{cont}_p(f)$ implies that we have actually

$$\mathrm{cont}_p(\mathbf{K}) = \mathrm{cont}_p(f) \tag{22}$$

To see this, assume first that $p|\operatorname{Disc}(\mathbf{K})$. In view of the hypothesis on $\operatorname{Disc}(\mathbf{K})$, a straightforward computation implies that $n_p(f) = 1$ and $n_{p^k}(f) = 0$ for $k \geqslant 2$, and therefore Equation (22) holds. We consider now primes p which do not divide $\operatorname{Disc}(\mathbf{K})$, for which we must show that $n_p(f) = n_p(\mathbf{K})$ (Lemma 2.2 implies then the formula $n_{p^k}(f) = n_p(\mathbf{K})$ for any $k \geqslant 2$). If p does not divide $2F(1,0)F(0,1)$, since the index is 1 or 2, Dedekind's result states that $n_p(f) = n_p(\mathbf{K})$. If p is an odd prime which divide $F(1,0)F(0,1)$, it is not difficult, using the decomposition of p in $\mathcal{O}_{\mathbf{K}}$, to see that $n_p(f) = n_p(\mathbf{K}) = 2$. If $p = 2$ and (at least) one of $F(1,0)$ and $F(0,1)$ is even, then $\operatorname{Disc}(\mathbf{K}) \equiv 1 \pmod 8$, which implies that $n_2(\mathbf{K}) = 2$. But then $F(0,1)$ and $F(1,1)$ are even and one obtains $n_2(f) = 2 = n_2(\mathbf{K})$. Finally, if $p = 2$ does not divide $F(0,1)$ nor $F(1,0)$, all the coefficients of F are odd and then $n_2(f) = 0$. Since, in this case, $\operatorname{Disc}(\mathbf{K}) \equiv 5 \pmod 8$, we have also $n_2(\mathbf{K}) = 0 = n_2(f)$. For the remaining primes, we have by Lemma 2.2 that $n_{p^k}(f) = n_p(\mathbf{K})$ for any $k \geqslant 1$ which implies (22).

From this discussion, it finally follows that, uniformly for

$$x \geqslant 3, \qquad \exp\left((\log\log x)^{5/3+\varepsilon}\right) \leqslant y \leqslant x(\log x)^{-\kappa},$$

we have

$$\Psi_F^{(1)}(x\mathcal{K}_F, y) = \frac{6\lambda_K|U_{\mathbf{K}}|}{\pi^2|G_{\mathbf{K}}|}x^2\left(\rho(2u) + (\gamma - 1 + \alpha(f))\frac{\rho'(2u)}{\log y} + O\left(\rho(2u)\frac{(\log(u+1))^2}{(\log y)^2}\right)\right).$$

By using (19) and (20) with $y = +\infty$, we have, for any $x \geqslant 1$, the estimation

$$\Psi_F^{(1)}(x\mathcal{K}_F, +\infty) = \frac{|U_{\mathbf{K}}|}{|G_{\mathbf{K}}|}\sum_{\chi\in\widehat{G_{\mathbf{K}}}}\chi(\mathfrak{d})\Psi^{(1)}(x^2;\chi),$$

where

$$\Psi^{(1)}(x;\chi) = \sum_{\substack{\mathfrak{I}\text{ primitive}\\ \mathrm{N}(\mathfrak{I})\leqslant x}}\chi(\mathfrak{I}).$$

The main term comes from the contribution of the trivial character which can be estimated by using the Perron's formula. This approach is used at the beginning of Section 1.3 of [HTW08] (Equations (1.16) – (1.19)). For the remaining characters, we use (21) and we see eventually that, for any $\varepsilon > 0$ and uniformly for $x \geqslant 2$, we have

$$\Psi_F^{(1)}(x\mathcal{K}_F, +\infty) := \left|\left\{(n_1,n_2) \in x\mathcal{K}_F \cap \mathbf{Z}^2 : \gcd(n_1,n_2) = 1,\right\}\right| = \frac{6\lambda_{\mathbf{K}}|U_{\mathbf{K}}|}{\pi^2|G_{\mathbf{K}}|}x^2 + O\left(x^2\exp\left(-(\log x)^{\frac{3}{5}-\varepsilon}\right)\right).$$

From Theorem B (see Section 1), we see also that for any $\varepsilon > 0$ and uniformly for

$$x \geqslant 3 \text{ and } \exp\left((\log\log x)^{5/3+\varepsilon}\right) \leqslant y \leqslant x^2(\log x)^{-\kappa},$$

we have

$$\begin{aligned}\Psi\left(x^2e^{\alpha(f)}, y\right) &= x^2e^{\alpha(f)}\left(\rho\left(2u + \frac{\alpha(f)}{\log y}\right) + (\gamma-1)\frac{\rho'\left(2u+\frac{\alpha(f)}{\log y}\right)}{\log y} + O\left(\rho\left(2u+\frac{\alpha(f)}{\log y}\right)\frac{(\log(u+1))^2}{(\log y)^2}\right)\right)\\ &= x^2e^{\alpha(f)}\left(\rho(2u) + (\gamma-1+\alpha(f))\frac{\rho'(2u)}{\log y} + O\left(\rho(2u)\frac{(\log(u+1))^2}{(\log y)^2}\right)\right)\end{aligned}$$

while $\Psi\left(x^2e^{\alpha(f)}, +\infty\right) = x^2e^{\alpha(f)} + O(1)$ trivially. This enables us to estimate the right-hand term of Equation (3) and to deduce the result. □

Remark 4.2. The theorem above encompasses a large set of binary forms. For example, since the quadratic binary form $F(X_1, X_2) = X_1^2 + qX_2^2$ defined in Example 2.6 has a fundamental discriminant and a positive value of α, we know that asymptotically it has less friable values than the random integers of same size. Nevertheless, many examples of binary forms with good values of α, i.e. close to zero or negative, have non fundamental discriminants.

5 Conclusion and open questions

The results in this article establish a rigorous connection between Murphy's α and the proportion of friable (smooth) algebraic numbers in a particular set. This might be understood as the efficiency of a polynomial for NFS. One could improve the speed of the algorithm by a deeper understanding of α, in particular by answering the following questions:

- What is the maximum (respectively minimum) value of α on a given set $E(d, \mathbf{I})$? Indeed, if a polynomial with a good value of α is found, one can end the polynomial selection phase, reducing therefore the time spent in this phase of the algorithm.
- Can one define a variance of α? Indeed, experiments indicate that, uniformly on the intervals products $\mathbf{I}$, the distribution of the values of α on a set $E(d, m, \mathbf{I})$ converges to a Gaussian distribution when m tends to infinity. If one can define and compute the variance of α, one will be able to find a good trade-off between the time spent to select a good polynomial and the time used to collect relations using that polynomial.

The presentation of this article was substantially improved due to our reviewers, in considerations of mathematics and cryptology.

References

[Bai11] S. Bai. *Polynomial selection for the number field sieve*. PhD thesis, Australian National University, 2011.

[Bar15] R. Barbulescu. Selecting polynomials for the function field sieve. *Math. Comp.*, 2015.

[BBDT12] A Balog, V. Blomer, C. Dartyge, and G. Tenenbaum. Friable values of binary forms. *Comment. Math. Helv.*, 87(3):639–667, 2012.

[BGI+14] C. Bouvier, P. Gaudry, L. Imbert, H. Jeljeli, and E. Thomé. announcement to the number theory mailing list: Discrete logarithms in GF(p) — 180 digits, 2014. Announcement available at the NMBRTHRY archives, item 004703.

[Boe96] H. Boender. The number of relations in the quadratic sieve algorithm. Technical report, Departement of Numerical Mathematics CWI Amsterdam, 1996.

[Bue89] D. A. Buell. *Binary quadratic forms–Classical theory and modern computations*. Springer-Verlag, New York, 1989.

[Ded78] R. Dedekind. Über den Zusammenhang zwischen der Theorie der Ideale und der höheren Kongruenzen. *Abh. Kgl. Ges. Wiss. Göttingen*, 23:1–23, 1878.

[FT91] É. Fouvry and G. Tenenbaum. Entiers sans grand facteur premier en progressions arithmetiques. *Proc. London Math. Soc. (3)*, 63(3):449–494, 1991.

[Gra08] A. Granville. Smooth numbers: computational number theory and beyond. In *Algorithmic number theory: lattices, number fields, curves cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 267–323. Cambridge Univ. Press, Cambridge, 2008.

[Hil86] A. Hildebrand. On the number of positive integers $\leqslant x$ and free of prime factors $> y$. *J. Number Theory*, 22(3):289–307, 1986.

[HT93] A. Hildebrand and G. Tenenbaum. Integers without large prime factors. *J. Théor. Nombres Bordeaux*, 5(2):411–484, 1993.

[HTW08] G. Hanrot, G. Tenenbaum, and J. Wu. Moyennes de certaines fonctions multiplicatives sur les entiers friables. II. *Proc. Lond. Math. Soc. (3)*, 96(1):107–135, 2008.

[JL03] A. Joux and R. Lercier. Improvements to the general number field for discrete logarithms in prime fields. *Math. Comp.*, 72(242):953–967, 2003.

[JLSV06] A. Joux, R. Lercier, N. P. Smart, and F. Vercauteren. The number field sieve in the medium prime case. In *Advances in cryptology—CRYPTO 2006*, volume 4117 of *Lecture Notes in Comput. Sci.*, pages 326–344, Berlin, 2006. Springer.

[KAF+10] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768–bit RSA modulus. In *Advances in cryptology—CRYPTO 2010*, volume 6223 of *Lecture Notes in Comput. Sci.*, pages 333–350. Springer, 2010.

[Kle06] T. Kleinjung. On polynomial selection for the general number field sieve. *Math. Comp.*, 75(256):2037–2047, 2006.

[Kle08] T. Kleinjung. Polynomial selection, 2008. CADO workshop on integer factorization. Slides available online at `http://cado.gforge.inria.fr/workshop/slides/kleinjung.pdf`.

[Lac14a] A. Lachand. Fonctions arithmétiques et formes binaires irréductibles de degré 3. `https://hal.archives-ouvertes.fr/hal-01053649`, 2014.

[Lac14b] A. Lachand. Valeurs friables d'une forme quadratique et d'une forme linéaire. *Q. J. Math.*, page 10.1093/qmath/hau029, 2014.

[LL93] A. K. Lenstra and H. W. Lenstra. *The development of the number field sieve*. Springer Verlag, 1993.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[Mur99] B. A. Murphy. *Polynomial selection for the number field sieve integer factorisation algorithm*. PhD thesis, Australian National University, 1999.

[Nag21] T. Nagell. Généralisation d'un théorème de Tchebycheff. *J. Math. Pures Appl. (8)*, 4(4):343–356, 1921.

[Oes79] J. Oesterlé. Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée. *Astérisque*, 61:165–167, 1979.

[Pol93] John M Pollard. Factoring with cubic integers. In *The development of the number field sieve*, pages 4–10. Springer, 1993.

[RS62] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[Sai89] É. Saias. Sur le nombre des entiers sans grand facteur premier. *J. Number Theory*, 32(1):78–99, 1989.

[Sch93] Oliver Schirokauer. Discrete logarithms and local units. *Philosophical Transactions of the Royal Society of London. Series A: Physical and Engineering Sciences*, 345(1676):409–423, 1993.

[Ten90] G. Tenenbaum. Sur un problème d'Erdős et Alladi. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 221–239. Birkhäuser Boston, Boston, MA, 1990.

[Win] B. Winckler. Théorème de Chebotarev effectif. Preprint available at `http://hal.archives-ouvertes.fr/docs/00/90/74/10/PDF/chebotarev.pdf`.