SOME MATHEMATICAL REMARKS
ON THE POLYNOMIAL SELECTION IN NFS

RAVAN BARBULESCU AND ARMAND LACHAND

Abstract. In this work, we consider the proportion of friable (free of large prime factors) values of a binary form \( F(X_1, X_2) \in \mathbb{Z}[X_1, X_2] \). 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 \( \alpha \) 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 cryptography 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 \( P(n) \leq y \) – has been 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

\[
(H_\varepsilon) \quad x \geq 3, \quad \exp \left( (\log \log x)^{5/3+\varepsilon} \right) \leq y \leq x.
\]

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

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

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

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

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


2010 Mathematics Subject Classification. Primary 11E76, 11N25, 11N36; Secondary 11Y05, 11Y16.

©2016 American Mathematical Society

397
Theorem B (Main Corollary, [Sai89]). There exists $C > 0$ such that, for any fixed $J \geq 0$, $\varepsilon > 0$ and uniformly for $(x, y)$ in the region $(H_{\varepsilon})$ satisfying

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

we have

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

where $\gamma_j$ are the coefficients of the Taylor series in $s = 0$ of $\gamma(x, y)$, In particular, we have $\gamma_0 = 1$ and $\gamma_1 = \gamma - 1$.

Let $x$ and $y$ be two positive reals, $F(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ a binary form and $\mathcal{K}$ a compact subset of $\mathbb{R}^2$ 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

$$\Psi_F^{(1)}(x\mathcal{K}, y) := \# \{ (n_1, n_2) \in x\mathcal{K} \cap \mathbb{Z}^2 : \gcd(n_1, n_2) = 1 \text{ and } P(F(n_1, n_2)) < y \}.$$

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

$$\Psi_{F_1, \ldots, F_k}^{(1)}(x\mathcal{K}, x^{1/u}) \geq c_{F_1, \ldots, F_k, \mathcal{K}}(u)x^2.$$

In particular, one can take

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

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 light of Theorem A we can conjecture that in a domain to be made precise we have

$$\Psi_{F_1, \ldots, F_k}^{(1)}(x\mathcal{K}, x^{1/u}) \sim \frac{6}{\pi^2} A(\mathcal{K})x^2 \rho(d_1 u) \cdots \rho(d_k u),$$

where $A(\mathcal{K})$ 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 [Po93], 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 [KAF10]. Discrete logarithm variants of NFS are the state-of-the-art for finite fields of large and medium characteristic [Sch93, JL03, JLSV06]. The largest discrete logarithm computation undertaken with NFS corresponds to the field $\mathbb{F}_p$ of a 180-digit prime $p$ [BGI14].

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 $y \geq 2$ and we search for $y$ pairs of coprime integers $(n_1, n_2)$ such that $F(n_1, n_2) := n_2^d g(f(n_1/n_2))$ and $G(n_1, n_2) := n_2^d g(n_1/n_2)$ are $y$-friable. The collected pairs allow us to obtain a $y \times y$ linear system over $\mathbb{Z}/2\mathbb{Z}$. 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 $a^2 \equiv b^2 \pmod{N}$, 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 $\mathbb{E} : \mathbb{Z}[X] \times \mathbb{Z}[X] \to \mathbb{R}$ 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 one to compare asymptotically $\psi_{F_1G_1}^{(1)}(xK,y)$ and $\psi_{F_2G_2}^{(1)}(xK,y)$. 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 $\mathbb{E} : \mathbb{Z}[X] \times \mathbb{Z}[X] \to \mathbb{R}$ which allows one 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 $\sigma$, defined as follows:

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

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:

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

where $I = \prod_{i=0}^{d} I_i$ 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:

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

Murphy defined a function \( \alpha : \mathbb{Z}[X] \to \mathbb{R} \) for which he gave strong evidence that, for polynomials with the same size property, it allows one to rank the polynomials \( f \) with respect to \( r \), for all parameters \( x \) and \( y \). In addition to its efficiency, \( \alpha \) has a simple formula, based on the number of roots of \( f \) modulo powers of primes, which allows one 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 of choosing polynomials \( f \) in the set \( E(d, I) \) 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 for a function \( \alpha : \mathbb{Z}[X] \to \mathbb{R} \) which, given two irreducible polynomials \( f_1 \) and \( f_2 \) (with associated binary forms \( F_1 \) and \( F_2 \)), allows one to compare \( \psi_{F_1}^{(1)}(xK, y) \) and \( \psi_{F_2}^{(1)}(xK, y) \). 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 of finding good approximations of \( \alpha(f) \) and determines the cost of the polynomial selection in NFS.

In order to prove the efficiency of \( \alpha \), 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 \( \Psi_{F_1}^{(1)}(xK, y) \). Due to technical reasons, we restrict ourselves to the case of irreducible quadratic polynomials \( f \) whose discriminant is fundamental, i.e. such that \( \text{Disc}(f) \) satisfies one of the following conditions:

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

**Theorem 1.1.** Let \( F(X_1, X_2) \in \mathbb{Z}[X_1, X_2] \) be an irreducible quadratic form such that \( \text{Disc}(F) \) is negative and fundamental. Let \( K_F \) be the compact defined by

\[
K_F := \left\{ (x_1, x_2) \in \mathbb{R}^2 : |F(x_1, x_2)| \leq 1 \right\}.
\]

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

\[
x \geq 3, \quad \exp\left((\log \log x)^{5/3+\varepsilon}\right) \leq y \leq x^2(\log x)^{-\kappa},
\]

we have

\[
\frac{\Psi_{F}^{(1)}(xK_F, y)}{\Psi_{F}^{(1)}(xK_F, +\infty)} = \frac{\Psi(x^2e^{\alpha(f)}, y)}{\Psi(x^2e^{\alpha(f)}, +\infty)} \left( 1 + O\left( \frac{(\log(u+1))^2}{(\log y)^2} \right) \right)
\]

where \( \alpha(f) \) denotes Murphy’s \( \alpha \) 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 \( \alpha \) over the set \( E(d, I) \). It gives a lower bound for the best value of \( \alpha \) 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, \( K \) stands for a number field and \( d_K, \mathcal{O}_K, U_K, G_K \), \( \zeta_K \) and \( \lambda_K \) denote respectively its degree, ring of integers, unit group, class group, Dedekind zeta function and residue of \( \zeta_K \). The letters \( p, \mathfrak{p} \) and \( \mathfrak{I} \) denote respectively a rational prime, a prime ideal and an arbitrary ideal of \( \mathcal{O}_K \). 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 \( \Psi_F^{(1)}(xK, y) \) 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 \( (n_1, n_2) \in xK \cap \mathbb{Z}^2 \) is given by
   \[
   \text{cont}_p(f, K) := \lim_{x \to \infty} \frac{\sum_{(n_1, n_2) \in xK \cap \mathbb{Z}^2, \gcd(n_1, n_2, p) = 1} \text{val}_p F(n_1, n_2)}{\left\lvert \{(n_1, n_2) \in xK \cap \mathbb{Z}^2 : \gcd(n_1, n_2, p) = 1\} \right\rvert}
   \]
   with the convention \( \text{val}_p(0) = 0 \).

2. Let \( z \leq y \) 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
   \[
   \left\lvert F^{(+, z)}(n_1, n_2) \right\rvert \approx \frac{|F(n_1, n_2)|}{\prod_{p \leq z} p^{\text{cont}_p(f, K)}}
   \]
   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 \( \approx \log |F(n_1, n_2)| + \alpha(f, K, z) \) to be \( y \)-friable, where
   \[
   \alpha(f, K, z) = \sum_{p \leq z} \alpha_p(f, K)
   \]
   with
   \[
   \alpha_p(f, K) = (\log p) \left( \frac{1}{p - 1} - \text{cont}_p(f, K) \right).
   \]

This suggests the following definition.

**Definition 2.1.** Let \( f \in \mathbb{Z}[X] \) be a polynomial and \( \mathcal{K} \) a compact subset of \( \mathbb{R}^2 \) whose boundary is a continuous closed curve with piecewise continuous derivatives. Under the reserve of proving the convergence of the series below, we define
   \[
   \alpha(f, K) = \sum_{p \text{ prime}} \alpha_p(f, K).
   \]
To get another expression for \( \text{cont}_p(f, \mathcal{K}) \), we split the region
\[
\left\{ (n_1, n_2) \in x\mathcal{K} \cap \mathbb{Z}^2 : \gcd(n_1, n_2, p) = 1 \right\}
\]
into congruence classes modulo \( p^k \) and write
\[
\left| \left\{ (n_1, n_2) \in x\mathcal{K} \cap \mathbb{Z}^2 : \gcd(n_1, n_2, p) = 1, p^k | F(n_1, n_2) \right\} \right|
= \left| \left\{ (n_1, n_2) \in [1, p^k]^2 : \gcd(n_1, n_2, p) = 1, p^k | F(n_1, n_2) \right\} \right| \left( \text{Vol}(\mathcal{K}) \frac{x^2}{p^{2k}} + O_{\mathcal{K}}(x) \right).
\]
We can remark that
\[
\left| \left\{ (n_1, n_2) \in [1, p^k]^2 : \gcd(n_1, n_2, p) = 1, p^k | F(n_1, n_2) \right\} \right| = \varphi(p^k)n_{p^k}(f),
\]
where
\[
n_{p^k}(f) = \left| \left\{ n_1 \in [0, p^k - 1] : f(n_1) \equiv 0 \mod p^k \right\} \right|
+ \left| \left\{ n_2 \in [0, p^k - 1] : n_2 \equiv 0 \mod p, \ F(1, n_2) \equiv 0 \mod p^k \right\} \right|.
\]
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 \( \text{Disc}(f) \), then \( n_{p^k}(f) = n_p(f) \). In the general case, for any prime \( p \) and \( k \geq 1 \), we have
\[
n_{p^k}(f) \leq 2 \deg(f)p^{\min(2\text{val}_p(\text{Disc}(f)), k)}.
\]

**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
\[
\left| \left\{ n \in [0, p^k - 1] : f(n) \equiv 0 \mod p^k \right\} \right| \leq \deg(f)p^{\min(2\text{val}_p(\text{Disc}(f)), k)}.
\]
When applied to \( F(X, 1) \) and \( F(1, X) \), this implies the second assertion. \( \square \)

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

**Proposition 2.3.** Let \( \mathcal{K} \) be a compact subset of \( \mathbb{R}^2 \) whose boundary is a continuous closed curve with piecewise continuous derivatives and \( f \in \mathbb{Z}[X] \) an irreducible polynomial. We have, for every prime \( p \),
\[
\alpha_p(f, \mathcal{K}) = \log p \left( \frac{1}{p-1} - \frac{p}{p+1} \sum_{k \geq 1} \frac{n_{p^k}(f)}{p^k} \right).
\]
Moreover, if \( p \) does not divide \( \text{Disc}(f) \), then we have

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

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

\[
\sum_{(n_1, n_2) \in x\mathcal{K} \cap \mathbb{Z}^2} \text{val}_p(F(n_1, n_2)) = \Sigma_1(p, \mathcal{K}, x) + \Sigma_2(p, \mathcal{K}, x)
\]

with

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

and

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

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

\[
\Sigma_1(p, \mathcal{K}, x) = \sum_{k \leq k_p(x)} \varphi(p^k) n_{p^k}(f) \left( \frac{\text{Vol}(\mathcal{K}) x^2}{p^{2k}} + O(x) \right)
= \text{Vol}(\mathcal{K}) x^2 \left( 1 - \frac{1}{p} \right) \sum_{k \leq k_p(x)} \frac{n_{p^k}(f)}{p^k} + O\left( xp^{k_p(x)} \right).
\]

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

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

Finally, we note that

\[
\left| \left\{ (n_1, n_2) \in x\mathcal{K} \cap \mathbb{Z}^2 : \gcd(n_1, n_2, p) = 1 \right\} \right|
= \left| \left\{ (n_1, n_2) \in x\mathcal{K} \cap \mathbb{Z}^2 : p \nmid n_1 \right\} \right| + \left| \left\{ (n_1, n_2) \in x\mathcal{K} \cap \mathbb{Z}^2 : p | n_1 \text{ and } p \nmid n_2 \right\} \right|
= \left( 1 - \frac{1}{p^2} \right) \text{Vol}(\mathcal{K}) x^2 + O(x).
\]

The result follows when \( x \) tends to infinity since then \( k_p \) tends to infinity. \( \square \)
2.2. **Convergence of $\alpha(f)$**. Let $\omega$ be a root of $f$, $K = \mathbb{Q} (\omega)$ a rupture field of $f$ and $\tilde{\omega} := F(1, 0) \omega$ an integer of $K$. It follows from a result of Dedekind [Ded78] that if a prime $p$ does not divide $F(1, 0)$ nor the index $[\mathcal{O}_K : \mathbb{Z}[\tilde{\omega}]]$, 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 $\text{Disc}(f)$, the problem of convergence of $\alpha(f)$ is reduced to showing the convergence of the series

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

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

$$p_0 := \max \{ p \text{ prime } : p|F(1,0)F(0,1) \text{ or } p|\text{Disc}(F) \text{ or } p|[\mathcal{O}_K : \mathbb{Z}[\tilde{\omega}]] \} .$$

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

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

On the one hand, from the Chebyshev estimation

$$\sum_{p \leq t} \log p \leq \epsilon t$$

with $\epsilon := 1.01624$ (see Theorem 9 of [RS62]), we can use Abel’s summation formula to get, for any $t_2 \geq t_1 \geq d_K$,

$$\left| \sum_{t_1 < p \leq t_2} \frac{\log p}{p(p-1)} \left( 1 - \frac{n_p(K)}{p+1} \right) \right| \leq \sum_{t_1 < p \leq t_2} \frac{\log p}{p(p-1)} \leq \frac{\epsilon}{t_1 - 1}.$$

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

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

where $R$ is the rest term defined by

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

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 $\zeta_K$ and $\zeta_Q$. But on the other hand, we have a good estimation relying on no assumptions.
Theorem D (Theorem 9.2, [LO77]).

(1) Call $d_K$ the degree of $K$. There exists an absolute effectively computable constant $c_1 > 0$ such that if $t \geq \exp\left(4d_K(\log \text{Disc}(K))^2\right)$, then

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

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

(2) Moreover, if the Riemann Hypothesis holds for $\zeta_K$, there exist explicit constants $a_K$, $b_K$ and $c_K$ such that, for $t \geq 2$, we have

$$\left| \sum_{N(p^k) \leq t} \log N(p) - t \right| \leq t^{1/2} \left(a_K + b_K \log t + c_K(\log t)^2\right).$$

Remarks 2.4.

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

$$\beta(K) \leq \max\left(1 - \frac{16d_K! \log \text{Disc}(K)}{t}, 1 - \frac{(c_2 \text{Disc}(K)^{1/d_K})^{-1}}{t}\right).$$

- Numerical values for $a_K$, $b_K$ and $c_K$ are given without proof in [Oes79]. The explicit values $a_K = \frac{4781}{96} \log(\text{Disc}(K)) + \frac{5861}{113} d_K$, $b_K = \frac{23}{3} \log(\text{Disc}(K)) + \frac{68}{3} d_K$ and $c_K = \frac{863}{31} d_K$ 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 $t \geq 2$,

$$\sum_{N(p^k) \leq t} \log N(p) \leq d_K \sum_{k \geq 2} \sum_{p \leq t^k} \log p$$

$$\leq c d_K \left(t^{1/2} + \frac{\log t}{2 \log 2} t^{1/3}\right).$$

Consequently, we have, for $t \geq \exp\left(4d_K(\log \text{Disc}(K))^2\right)$,

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

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

$$\left| \sum_{t_1 < p \leq t_2} \frac{\log p}{p} \left(1 - n_p(K)\right) \right| \leq \frac{|R(t_1)|}{t_1} + \frac{|R(t_2)|}{t_2} + \int_{t_1}^{t_2} \frac{|R(s)|}{s^2} ds$$

$$\ll d_K t_1^{1/2} + \frac{t_1^{\beta(K)-1}}{\beta(K)} + (\log t_1)^{1/2} \exp\left(-c_1 (d_K)^{-1/2}(\log t_1)^{1/2}\right),$$

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

THE POLYNOMIAL SELECTION IN NFS

405
In order to get a good estimation of the convergence speed, we now assume that the Riemann Hypothesis holds for \( \zeta_Q \) and \( \zeta_K \). It follows from Theorem D that we have, for \( t \geq 2 \),

\[
|R(t)| \leq \epsilon d_K t^{1/2} + \epsilon d_K t^{1/3} \log t \log 2 + a_K t^{1/2} + b_K t^{1/2}(\log t) + c_K t^{1/2}(\log t)^2.
\]

As a consequence of the previous discussion, we can get that, for \( t \geq 2 \),

\[
\sum_{p \leq t} \frac{\log p}{p} (1 - n_p(K)) \leq \frac{|R(t)|}{t} + \int_{t}^{+\infty} \frac{|R(s)|}{s^2} ds \\
\leq t^{-1/2} \left( (3a_K + 3d_K + 4b_K + 16c_K + (3b_K + 8c_K) \log t + 3c_K(\log t)^2) \\
+ t^{-1/6} \frac{\epsilon d_K}{\log 4} \left( \frac{9}{2} + 5 \log t \right) \right).
\]

It follows that the speed of convergence is given, for \( t \geq \max(p_0, d_K) \), by

\[
|\alpha(f) - \sum_{p \leq t} \alpha_p(f)| \leq t^{-1/2} \left( \frac{\epsilon t^{1/2}}{t - 1} + t^{-1/6} \frac{\epsilon d_K}{\log 4} \left( \frac{9}{2} + 5 \log t \right) \\
+ (3a_K + 3d_K + 4b_K + 16c_K + (3b_K + 8c_K) \log t + 3c_K(\log t)^2) \right).
\]

By using the best numerical values in Remark 2.4, one gets some explicit constants for the convergence speed of \( \alpha(f) \), available under the Riemann Hypothesis for \( \zeta_K \) and \( \zeta_Q \).

**Proposition 2.5.** Let \( f \in \mathbb{Z}[X] \) be an irreducible polynomial of degree \( d \) and \( K \) a rupture field of \( f \). Suppose that the Riemann Hypothesis holds for \( \zeta_K \) and \( \zeta_Q \). Then, we have, for any \( t \geq p_0 \),

\[
|\alpha(f) - \sum_{p \leq t} \alpha_p(f)| \leq t^{-1/2} \left( 2105d_K + 181 \log \text{Disc}(K) \\
+ (23 \log \text{Disc}(K) + 295d_K) \log t + 84d_K(\log t)^2 \right).
\]

**Example 2.6.** Consider \( F(X_1, X_2) = X_1^2 + qX_2^2 \) with \( q = 10^{39} + 57 \). By computing the partial sum of \( \alpha \) for primes \( p \) less than \( t = 4 \cdot 10^{10} \) we obtain \( |\sum_{p \leq t} \alpha_p(f) - 2.39| < 0.01 \). Here we have \( d_K = 2 \) and \( \log(D_K) \approx 70.46 \). Proposition 2.5 allows one to conclude that, under the assumption that Riemann’s hypothesis holds for \( \zeta_Q \) and \( \zeta_K \), we have

\[
|\alpha(f) - 2.39| < 1.
\]

In the next section we essentially show that the average of \( \alpha \) is \( \approx 0.56 \), so our polynomial has a bad value of \( \alpha \). The term \( 84d_K \log(t)^2 \) 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 analogy to Murphy’s \( \alpha \) when \( f \in \mathbb{F}_2[t][X] \). The first author proved [Bar15, Theorem 2.14] that \( \alpha \) has a better speed of convergence in that case, as no factor in \( (\log t)^2 \) is needed.
3. TOWARDS THE AVERAGE OF $\alpha$ ON A SET OF POLYNOMIALS

The polynomial selection stage of NFS consists of 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 $\alpha$ can be further tested with longer tests or by direct sieving. In any case, by computing the average of $\alpha$ we guarantee a value of $\alpha$ for the best polynomials.

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

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

Note the introduction of the parameter $m$ in the definition of $E^{(1)}(m, d, I)$, which plays an important role. In practice, it can be computed from $I$ 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 $E^{(1)}(m, d, I)$ rather than on the set $E(d, I)$ introduced by (2) in the introduction of this article.

**Theorem 3.1.** We have the mean value

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

**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 $d \geq 2$. In view of Proposition 2.3 we have, for any prime $p$,

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

For any integer $k$, we put

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

Then we have

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

where, for a $k_p$ specified below,

$$\Sigma_p^{(1)}(m, d, I) := \frac{p \log p}{p + 1} \sum_{k=1}^{k_p} \frac{S_p(k, m, d, I)}{p^k},$$

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

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

$$|\text{Disc}(f)| \leq (2d-1)! m^{2d-1}.$$
Consider \( k_p = 2 \left\lfloor \log_p \left( (2d - 1)!m^{2d - 1} \right) \right\rfloor + \left\lceil \log_p (md) \right\rceil \).

**Case** \( k \leq k_p \). Since the elements of \( E^{(1)}(m, d, I) \) are monic, we can write, in view of the definition (7) of \( n_p(f) \),

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

We consider first the cardinality of \( E^{(1)}(m, d, I) \). Given \((f_1, \ldots, f_{d-1}) \in I_1 \times \cdots \times I_{d-1} \), the polynomial \( dX^{d-1} + \sum_{i=1}^{d-1} f_i X^{i-1} \) 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 \( \sum_{i=0}^{d-1} f_i z^i = 0 \). Hence there are at most \( d |I|/|I_0| \) polynomials \( f \) of zero discriminant and coefficients in \( I \). It follows that

\[
E^{(1)}(m, d, I) = \left| \left\{ (f_0, \ldots, f_{d-1}) \in I \cap \mathbb{Z}^d \right\} \right| \\
- \left| \left\{ (f_0, \ldots, f_{d-1}) \in I \cap \mathbb{Z}^d : \text{Disc} \left( X^d + \sum_{i=0}^{d-1} f_i X^i \right) = 0 \right\} \right| \\
= |I| \left( 1 + O \left( \frac{d}{\min_j |I_j|} \right) \right).
\]

Let \( k \leq k_p \) be an integer and \( r \in [0, p^k - 1] \). For each \((d-1)\)-tuple \((f_1, \ldots, f_{d-1}) \in I_1 \times \cdots \times I_{d-1} \), 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

\[
\left| \left\{ f \in E^{(1)}(m, d, I), f(r) \equiv 0 \pmod{p^k} \right\} \right| \\
= \left| \left\{ (f_0, \ldots, f_{d-1}) \in I \cap \mathbb{Z}^d : f(r) \equiv 0 \pmod{p^k} \right\} \right| \\
+ O \left( \left| \left\{ (f_0, \ldots, f_{d-1}) \in I \cap \mathbb{Z}^d : \text{Disc} \left( X^d + \sum_{i=0}^{d-1} f_i X^i \right) = 0 \right\} \right| \right) \\
= \left( \frac{|I_0|}{p^k} + O(1) \right) \frac{|I|}{|I_0|} + O \left( \frac{|d|I|}{\min_j |I_j|} \right) \\
= \frac{|I|}{p^k} + O \left( \frac{|I|d}{\min_j |I_j|} \right).
\]
Then we obtain that
\[
\Sigma_p^{(1)}(m, d, I) \ll \log p \sum_{k < k_p} \frac{|I|d}{\min_j |I_j|} \ll k_p \log p \frac{|I|d}{\min_j |I_j|},
\]

Case $k > k_p$. Due to the choice of $k_p$, we have $k_p \geq 2 \text{val}_p \text{Disc}(f)$ for all polynomials $f$ in $E^{(1)}(m, d, I)$. By Lemma 2.2 and the definition of $k_p$, for all $k \geq k_p$, we have
\[
n_{p^k}(f) \ll d \text{Disc}(f)^2 \ll d \left( (2d - 1)!m^{2d-1} \right)^2 \leq p^{k_p}/m.
\]
By summing over $k > k_p$, we deduce that
\[
\Sigma_p^{(2)}(m, d, I) \ll \frac{|I|}{m} \log p.
\]
When combining the bounds on $\Sigma_p^{(1)}(m, d, I)$ and $\Sigma_p^{(2)}(m, d, I)$, we obtain that, uniformly for $p, m \geq 2$ and $\min_j |I_j| \geq d$, we have
\[
(15) \quad \sum_{f \in E^{(1)}(m, d, I)} \left( \alpha_p(f) - \alpha_p(X) \right) \ll |I| \log p \left( \frac{1}{m} + \frac{d^2(\log(dm))}{\min_j |I_j|} \right).
\]

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 $f(X) = aX + b \in \mathbb{Z}[X]$ 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 $\gamma$ denotes the Euler-Mascheroni constant.

**Proof.** Since $f$ has degree 1 and $\gcd(a, b) = 1$, we have, for every prime $p$ and $k \geq 1$,
\[
n_{p^k}(f) = 1.
\]
Consequently, it follows from Proposition 2.3 that
\[
\alpha(f) = \sum_p \log p \frac{\log p}{p - 1} \left( 1 - \frac{p}{p + 1} \right) = \sum_p \log p \frac{\log p}{p^2 - 1}.
\]
From the formula
\[
\frac{\zeta'(Q)(s)}{\zeta(Q)(s)} = -\sum_p \frac{\log p}{p^s - 1},
\]
which holds for any complex $s$ such that $\Re(s) > 1$, we deduce that
\[
\alpha(f) = \sum_p \frac{\log p}{p^2 - 1} = -\frac{\zeta'(Q)(2)}{\zeta(Q)(2)}.
\]
The result is then a direct consequence of the formulae
\[
\zeta_{Q}(2) = \frac{\pi^2}{6} \quad \text{and} \quad \zeta'_{Q}(2) = \frac{\pi^2}{6} \left( \gamma + \log(2\pi) - 12 \log A \right). \quad \Box
\]

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 \( Q(\omega) \), 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 \( d \geq 2 \) and \( g \) linear such that there exists an integer \( m \) such that \( f(m) \equiv g(m) \equiv 0 \mod N \). Let \( \omega \) 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 \( p \) in the number field \( Q(\omega) \) above primes \( p \) less than or equal to \( y \). Let \( X_f \) and \( X_g \) be the maximal value of \( N(n_1 + n_2\omega) \) and \( |n_1 + n_2m| \) respectively when \( n_1 \) and \( n_2 \) are bounded by the constant used in NFS. Next we collect \( d \)-tuples \( (n_1, \ldots, n_d) \) such that

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

Each polynomial \( n_1 + n_2X + \cdots + n_dX^{d-1} \) 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 \( a^2 \equiv b^2 \mod N \) 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 cause 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 \( K \) be a number field of degree \( d_K \) and \( \omega \) an integral primitive element of \( K \). In view of the previous discussion, we consider the following set

\[
\left\{ (n_1, \ldots, n_d) \in \mathbb{Z}^d : \gcd(n_1, \ldots, n_d) = 1, \left| N(n_1 + \cdots + n_d\omega^{d-1}) \right| \leq x, \right. \\
|n_1 + \cdots + n_dm^{d-1}| \leq x, P(n_1 + \cdots + n_dm^{d-1}) \leq y
\]

\[
\left. \text{and } P \left( N(n_1 + \cdots + n_d\omega^{d-1}) \right) \leq y \right\}.
\]
In this article we drop the conditions over \( n_1 + \cdots + n_d \omega^{d-1} \) by studying a set which is easier to analyze, namely

\[
\left\{ (n_1, \ldots, n_d) \in \mathbb{Z}^d : \gcd(n_1, \ldots, n_d) = 1, |N(n_1 + \cdots + n_d \omega^{d-1})| \leq x \right. \\
\left. \quad \text{and } P\left(N(n_1 + \cdots + n_d \omega^{d-1})\right) \leq y \right\}.
\]

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

\[
\Psi^{(1)}_K(x, y) := \left| \{ \mathfrak{I} \text{ primitive : } N(\mathfrak{I}) \leq x \text{ and } P(N(\mathfrak{I})) \leq y \} \right|.
\]

A standard way – the one followed here – to get an asymptotic formula for \( \Psi^{(1)}_K(x, y) \) consists of applying to the Dirichlet series \( \mathcal{F}_K(s) \) defined by

\[
\mathcal{F}_K(s) := \sum_{\mathfrak{I} \text{ primitive}} \frac{1}{N(\mathfrak{I})^s}
\]

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

\[
\mathcal{F}_K(s) = \sum_{m \geq 1} \mu(m) \sum_{m\mathcal{O}_K \nmid \mathfrak{I}} \frac{1}{N(\mathfrak{I})^s} = \zeta_K(s) \zeta_Q(d_Ks)^{-1}.
\]

Moreover, using the properties of the Riemann zeta function, it is immediate that \( \zeta_Q(d_Ks)^{-1} \) is absolutely convergent for \( \Re(s) > \frac{1}{d_K} \).

In view of the previous discussion, we are now in position 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 \( d_K \geq 2 \). Then, there exists \( C > 0 \) such that, for any \( J \geq 0 \) and \( \varepsilon > 0 \), we have, uniformly for \((x, y)\) in \((H_{\varepsilon})\) and

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

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

where

\[
\gamma_j(K) = \sum_{j_1 + j_2 = j} \frac{1}{j_1! j_2!} \left. \frac{\partial^{j_1} (1 - s^{-1}) \zeta_K(s)}{\partial s^{j_1}} \right|_{s=1} \left. \frac{\partial^{j_2} \zeta_Q(d_Ks)^{-1}}{\partial s^{j_2}} \right|_{s=1}.
\]
In particular, we have

\[ \gamma_0(K) = \frac{\lambda_K}{\zeta_Q(d_K)} \]

where \( \lambda_K \) denotes the residue of \( \zeta_K \) and

\[ \gamma_1(K) = \gamma_0(K) \left( \gamma - 1 + \sum_p \log p \left( \frac{1}{p - 1} - \text{cont}_p(K) \right) \right) \]

with

\[ \text{cont}_p(K) = \left( \sum_{k \geq 1} \frac{k \left\{ \mathcal{I} \text{ primitive}, N(\mathcal{I}) = p^k \right\}}{p^k} \right)^{-1} \times \left( \sum_{k \geq 0} \left\{ \mathcal{I} \text{ primitive}, N(\mathcal{I}) = p^k \right\} \right)^{-1} \]

Proof. In view of equation (16), it is immediate that \( F_K(s) \) 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

\[ \sum P(n) \mu(n) \frac{\log p}{p} \left( \frac{1}{p - 1} - \text{cont}_p(K) \right) \]

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

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

\[ \left. \frac{\partial F_K(s)}{\partial s} - \frac{\partial \zeta_Q(s)}{\partial s} \right|_{s=1} = \sum_p \log p \left( \frac{1}{p - 1} - \text{cont}_p(K) \right) \]

and

\[ \left. \frac{(s-1)\partial \zeta_Q(s)}{\partial s} \right|_{s=1} = \gamma - 1. \]

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 \( \omega \) be a root of \( f(X) = F(X,1) \) and \( K := Q(\omega) \). Since \( \text{Disc}(f) \) is a fundamental discriminant, we have \( \text{Disc}(K) = \text{Disc}(f) \). Moreover, there exists an ideal \( \mathfrak{d} \) of \( \mathcal{O}_K \) with basis \( (\omega_1, \omega_2) \) such that, for any integers \( n_1 \) and \( n_2 \), one has

\[ F(n_1, n_2) = \frac{N(n_1 \omega_1 + n_2 \omega_2)}{N(\mathfrak{d})}. \]
Since the unit group $U_K$ is finite, we have

\[ \Psi_F^{(1)}(xK_F, y) = \left\{ (n_1, n_2) \in \mathbb{Z}^2 : \gcd(n_1, n_2) = 1, \frac{N(n_1\omega_1 + n_2\omega_2)}{N(d)} \leq x^2, \right\} \]

\[ \left\| \frac{N(n_1\omega_1 + n_2\omega_2)}{N(d)} \right\| \leq y \right\} \]

\[ = |U_K| \left\{ \mathcal{L} \text{ principal : } \mathfrak{d}|\mathcal{L}, \mathcal{L}\mathfrak{d}^{-1} \text{ primitive, } N(\mathcal{L}\mathfrak{d}^{-1}) \leq x^2, \right\} \]

\[ P\left( \frac{N(\mathcal{L}\mathfrak{d}^{-1})}{N(d)} \right) \leq y \right\} \right. \]  

(19)

By writing $\mathcal{L} = \mathfrak{d}$, the problem is then reduced to detecting the primitive and integral ideals $\mathfrak{I}$ in the class of $\mathfrak{d}^{-1}$ satisfying $N(\mathfrak{I}) \leq x^2$ and $P(N(\mathfrak{I})) \leq y$. In order to pick up ideals from the class $\text{cl}(\mathfrak{d}^{-1})$, we can consider the group $\hat{G}_K$ of the multiplicative characters of the class group $G_K$. By the orthogonality property of characters, we have

\[ \left\{ \mathcal{L} \text{ principal : } \mathfrak{d}|\mathcal{L}, \mathcal{L}\mathfrak{d}^{-1} \text{ primitive, } N(\mathcal{L}\mathfrak{d}^{-1}) \leq x^2, P\left( \frac{N(\mathcal{L}\mathfrak{d}^{-1})}{N(d)} \right) \leq y \right\} \]

\[ = \frac{1}{|G_K|} \sum_{\chi \in \hat{G}_K} \chi(\mathfrak{d})\Psi^{(1)}(x^2, y; \chi), \]

(20)

where

\[ \Psi^{(1)}(x, y; \chi) = \sum_{\mathfrak{I} \text{ primitive}} \frac{\chi(\mathfrak{I})}{N(\mathfrak{I})^s} \left( \prod_{p} \left( 1 - \frac{1}{p^{2s}} \right) \right) \]

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

\[ x \geq 3, \quad \exp \left( (\log \log x)^{5/3 + \varepsilon} \right) \leq y \leq x, \]

we have

\[ \Psi^{(1)}(x, y; \chi) \ll x\rho(u) \exp \left( -(\log y)^{3/2 - \varepsilon} \right). \]

(21)

This procedure is essentially formulated in [Ten90] and [FT91].
**Contribution of the trivial character.** For the principal character, denoted by \( \chi_0 \), we use Theorem 2.1. There exists \( \kappa > 0 \) such that, for any \( \varepsilon > 0 \) and uniformly for

\[
x \geq 3, \quad \exp \left( (\log \log x)^{5/3+\varepsilon} \right) \leq y \leq x(\log x)^{-\kappa},
\]

we have

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

where \( \gamma_0(K) = \frac{6\lambda K}{\pi^2} \) and

\[
\gamma_1(K) = \gamma_0(K) \left( \gamma - 1 + \sum_p \log p \left( \frac{1}{p-1} - \text{cont}_p(K) \right) \right).
\]

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

\[
\left| \left\{ J \text{ primitive, } N(J) = p^k \right\} \right| = \begin{cases} 0 & \text{if } p \mid \text{Disc}(K) \text{ and } k \geq 2, \\ n_p(K) & \text{if } k = 1 \text{ or } p \nmid \text{Disc}(K), \\ \end{cases}
\]

and therefore

\[
\text{cont}_p(K) = \begin{cases} \frac{1}{p-1} & \text{if } p \mid \text{Disc}(K), \\ \frac{n_p(K)}{p-1} & \text{otherwise.} \end{cases}
\]

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

(22) \[
\text{cont}_p(K) = \text{cont}_p(f).
\]

To see this, assume first that \( p \mid \text{Disc}(K) \). In view of the hypothesis on \( \text{Disc}(K) \), a straightforward computation implies that \( n_p(f) = 1 \) and \( n_{p^k}(f) = 0 \) for \( k \geq 2 \), and therefore equation (22) holds. We consider now primes \( p \) which do not divide \( \text{Disc}(K) \), for which we must show that \( n_p(f) = n_p(K) \) (Lemma 2.2 implies then the formula \( n_{p^k}(f) = n_p(K) \) for any \( k \geq 2 \)). If \( p \) does not divide \( 2F(1,0)F(0,1) \), since the index is 1 or 2, Dedekind’s result states that \( n_p(f) = n_p(K) \). If \( p \) is an odd prime which divides \( F(1,0)F(0,1) \), it is not difficult, using the decomposition of \( p \) in \( \mathcal{O}_K \), to see that \( n_p(f) = n_p(K) = 2 \). If \( p = 2 \) and (at least) one of \( F(1,0) \) and \( F(0,1) \) is even, then \( \text{Disc}(K) \equiv 1 \pmod{8} \), which implies that \( n_2(K) = 2 \). But then \( F(0,1) \) and \( F(1,0) \) are even and one obtains \( n_2(f) = 2 = n_2(K) \). Finally, if \( p = 2 \) does not divide \( F(0,1) \) or \( F(1,0) \), all the coefficients of \( F \) are odd and then \( n_2(f) = 0 \). Since, in this case, \( \text{Disc}(K) \equiv 5 \pmod{8} \), we have also \( n_2(K) = 0 = n_2(f) \). For the remaining primes, we have by Lemma 2.2 that \( n_{p^k}(f) = n_p(K) \) for any \( k \geq 1 \), which implies (22).
From this discussion, it finally follows that, uniformly for 
\[ x \geq 3, \quad \exp\left((\log \log x)^{5/3+\varepsilon}\right) \leq y \leq x(\log x)^{-\kappa}, \]
we have
\[
\Psi_F^{(1)}(xK_F, y) = \frac{6\lambda_K|U_K|}{\pi^2|G_K|} x^2 \left( \rho(2u) + (\gamma - 1 + \alpha(f)) \frac{\rho'(2u)}{\log y} + O \left( \rho(2u) \frac{(\log(u + 1))^2}{(\log y)^2} \right) \right).
\]

By using (19) and (20) with \( y = +\infty \), we have, for any \( x \geq 1 \), the estimation
\[
\Psi_F^{(1)}(xK_F, +\infty) = \frac{|U_K|}{|G_K|} \sum_{\chi \in \hat{G}_K} \chi(d) \Psi^{(1)}(x^2; \chi),
\]
where
\[
\Psi^{(1)}(x; \chi) = \sum_{\substack{I \text{ primitive} \ \ \ N(I) \leq x}} \chi(I).
\]

The main term comes from the contribution of the trivial character which can be estimated by using 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 \( x \geq 2 \), we have
\[
\Psi_F^{(1)}(xK_F, +\infty) := \left| \left\{ (n_1, n_2) \in xK_F \cap \mathbb{Z}^2 : \gcd(n_1, n_2) = 1, \right\} \right| = \frac{6\lambda_K|U_K|}{\pi^2|G_K|} x^2 + O \left( x^2 \exp\left(- (\log x)^{3-\varepsilon}\right) \right).
\]

From Theorem [3] (see Section [1]), we also see that for any \( \varepsilon > 0 \) and uniformly for
\[ x \geq 3 \text{ and } \exp\left((\log \log x)^{5/3+\varepsilon}\right) \leq y \leq x^2(\log x)^{-\kappa}, \]
we have
\[
\Psi\left(x^2 e^{\alpha(f)}, y\right) = x^2 e^{\alpha(f)} \left( \rho \left( 2u + \frac{\alpha(f)}{\log y} \right) + (\gamma - 1) \frac{\rho'(2u + \frac{\alpha(f)}{\log y})}{\log y} \right.
\]
\[
\left. + O \left( \rho \left( 2u + \frac{\alpha(f)}{\log y} \right) \frac{(\log(u + 1))^2}{(\log y)^2} \right) \right).
\]
\[
= x^2 e^{\alpha(f)} \left( \rho(2u) + (\gamma - 1 + \alpha(f)) \frac{\rho'(2u)}{\log y} + O \left( \rho(2u) \frac{(\log(u + 1))^2}{(\log y)^2} \right) \right).
\]
while \( \Psi\left(x^2 e^{\alpha(f)}, +\infty\right) = x^2 e^{\alpha(f)} + O(1) \) trivially. This enables us to estimate the right hand term of equation [3] and to deduce the result. \( \square \)
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 \( \alpha \), we know that asymptotically it has less friable values than the random integers of the same size. Nevertheless, many examples of binary forms with good values of \( \alpha \), 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 \( \alpha \) 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 \( \alpha \), in particular by answering the following questions:

- What is the maximum (respectively minimum) value of \( \alpha \) on a given set \( E(d, I) \)? Indeed, if a polynomial with a good value of \( \alpha \) 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 \( \alpha \)? Indeed, experiments indicate that, uniformly on the intervals of products \( I \), the distribution of the values of \( \alpha \) on a set \( E(d, m, I) \) converges to a Gaussian distribution when \( m \) tends to infinity. If one can define and compute the variance of \( \alpha \), 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.

Acknowledgement

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

References


The polynomial selection in NFS


Université de Lorraine, 34 Cours Léopold, 54000 Nancy, France – and – CNRS, INRIA

E-mail address: razvan.barbulescu@imj-prg.fr

Institut Elie Cartan, Université de Lorraine, B.P. 70239, 54506 Vandoeuvre-lès-Nancy Cedex, France

E-mail address: armand.lachand@univ-lorraine.fr