THE AUSTRALIAN NATIONAL UNIVERSITY

TR-CS-97-17

On Quadratic Polynomials for the Number Field Sieve

Brian Murphy and Richard P. Brent

August 1997

Joint Computer Science Technical Report Series

Department of Computer Science
Faculty of Engineering and Information Technology

Computer Sciences Laboratory
Research School of Information Sciences and Engineering

This technical report series is published jointly by the Department of Computer Science, Faculty of Engineering and Information Technology, and the Computer Sciences Laboratory, Research School of Information Sciences and Engineering, The Australian National University.

Please direct correspondence regarding this series to:

Technical Reports
Department of Computer Science
Faculty of Engineering and Information Technology
The Australian National University
Canberra ACT 0200
Australia

or send email to:

`Technical.Reports@cs.anu.edu.au`

A list of technical reports, including some abstracts and copies of some full reports may be found at:

`http://cs.anu.edu.au/techreports/`

Recent reports in this series:

TR-CS-97-16 M. Manzur Murshed and Richard P. Brent. *Algorithms for optimal self-simulation of some restricted reconfigurable meshes*. July 1997.

TR-CS-97-15 Peter Strazdins. *Reducing software overheads in parallel linear algebra libraries*. July 1997.

TR-CS-97-14 Michael K. Ng and William F. Trench. *Numerical solution of the eigenvalue problem for Hermitian Toeplitz-like matrices*. July 1997.

TR-CS-97-13 Michael K. Ng. *Blind channel identification and the eigenvalue problem of structured matrices*. July 1997.

TR-CS-97-12 Michael K. Ng. *Preconditioning of elliptic problems by approximation in the transform domain*. July 1997.

TR-CS-97-11 Richard P. Brent, Richard E. Crandall, and Karl Dilcher. *Two new factors of Fermat numbers*. May 1997.

On Quadratic Polynomials for the Number Field Sieve

Brian Murphy †
Richard P. Brent

Abstract

The newest, and asymptotically the fastest known integer factorisation algorithm is the number field sieve. The area in which the number field sieve has the greatest capacity for improvement is polynomial selection. The best known polynomial selection method finds quadratic polynomials. In this paper we examine the smoothness properties of integer values taken by these polynomials. Given a quadratic NFS polynomial, let Δ be its discriminant. We show that p need only appear in the factor base if $(\Delta/p) = 1$. Using this knowledge, we adapt a parameter α, developed for analysis of MPQS, to quadratic NFS polynomials. We estimate the yield of smooth values for these polynomials as a function of α, and conclude that practical changes in α might bring significant changes in the yield of smooth polynomial values, and polynomial values which are smooth but for the appearance of up to two large primes.

Keywords: integer factorisation, number field sieve

1 Introduction

Let N be a large postive integer. We refer to the multiple polynomial quadratic sieve (MPQS) and the number field sieve (NFS) algorithms for factoring N. Details of these algorithms can be found at [10] and [6] respectively . For the MPQS we take N to be the product of some small multiplier and the integer requiring factorisation. Also, we refer to an integer as B-smooth when all its prime factors are less than B.

For our purposes it suffices to understand the following about the number field sieve. Like MPQS, the speed at which the number field sieve can factor N is limited mainly by the supply of smooth integers of a particular form. For NFS, the smooth integers are required to be values taken by an irreducible

†Computer Sciences Laboratory
Research School of Information Sciences and Engineering
Australian National University
CANBERRA ACT 0200
email: murphy@cslab.anu.edu.au, rpb@cslab.anu.edu.au
fax: 02 6279 8645

polynomial $F \in \mathbb{Z}[x]$ of degree d. In fact we usually consider $f \in \mathbb{Z}[x, y]$ given by $f = y^d F(x/y)$, and search for B-smooth values of $|f|$ for some bound B and for coprime $x, y \in \mathbb{Z}$ in a given range (see [6]). The area in which the number field sieve has the greatest capacity for improvement is the selection of f. A "good" polynomial is one whose values are more likely to be B-smooth than random integers of the same size. Amongst polynomials, f_1 is "better" than f_2 if f_1 takes values more likely to be smooth than those taken by f_2.

The probability that a random integer is B-smooth decreases rapidly with the size of the integer. The size of the values taken by f is therefore a key factor in optimising polynomial selection. This factor is usually viewed in terms of the size of the coefficients of f. None of the selection methods used thus far are provably optimal (see [6], [2] and [7]). With the exception of Peter Montgomery's algorithm reported in [9], current methods yield $c_i = O(N^{1/(d+1)})$ where c_i for $i = 0, \ldots, d-1$ are the coefficients of f. The method in [9] however, yields two polynomials of degree $d = 2$ for which, in practice, $c_i = O(N^{1/4})$ (in theory, all that is guaranteed is that the product of the norms of the coefficient vectors is $O(N^{1/2})$). In that sense, Montgomery's method is the best known method for polynomial selection. It is therefore worthwhile examining more closely the quadratic polynomials yielded by this algorithm.

In MPQS, we sieve over values taken by quadratic polynomials $W(x)$ (so called W-values). The factor base (ignoring large primes) initially ought to contain all rational primes p less than some bound B. However by the choice of W, it is known that only primes p for which $(N/p) = 1$ need appear in the factor base. This is significant for two reasons.

1. For sufficiently large B approximately half of the primes less than B satisfy $(N/p) = 1$, so only half the primes up to B need appear in the factor base. Hence, sieving time is reduced by approximately one half.

2. For typical MPQS polynomials, it appears that W-values (given an appropriate choice of a multiplier k) are more likely to be B-smooth than random integers of the same size.

In the next section we note that quadratic number field sieve polynomials f possess a similar reciprocity property. In particular, if $f(x, y) = r$ for coprime $x, y \in \mathbb{Z}$ then all the odd primes dividing r satisfy $(\Delta/p) = 1$, where Δ denotes the discriminant of f. In section 3 we repeat an argument from [3] which estimates smoothness probabilities of f-values given information from the residuosity condition on which primes may appear in their factorisations. In section 4 we use the estimates of section 3 to estimate the yield of smooth f-values, and f-values which are smooth but for the appearance of up to two large primes.

Thus, we give a quantification of relative expected yields from quadratic NFS polynomials. We conclude that, heuristically, varying α within practically attainable values might bring significant increases in the yield of smooth and almost smooth values of quadratic number field sieve polynomials. In practice, this would aid polynomial selection.

2 The Primes in the Factor Base

Montgomery's polynomial selection algorithm produces pairs of binary quadratic forms with integer coefficients. We ask, for coprime integer values of the variables, which integers do these forms represent? After giving some definitions and notation, we give a theorem from [5] which addresses this question.

Definition 1 *A form f primitively represents some $r \in \mathbb{Z}$ if there exist coprime integers x_1 and y_1 for which $f(x_1, y_1) = r$.*

Consider two binary quadratic forms $f_1(x_1, y_1)$ and $f_2(x_2, y_2)$ with integer coefficients, and whose variables range over $\mathbb{Z}$.

Definition 2 *The forms f_1 and f_2 are $\mathbb{Z}$-equivalent if there exists a linear transformation over $\mathbb{Z}$ represented by a 2×2 integer valued matrix A with* $\det A = \pm 1$.

The unimodularity condition ensures that the transformation and its inverse preserve the integrality of the variables.

Let Δ_1 and Δ_2 be the discriminants of f_1 and f_2 respectively. If f_1 and f_2 are $\mathbb{Z}$-equivalent under the transformation A then

$$\Delta_2 = (\det A)^2 \Delta_1 = \Delta_1.$$

We will also consider *rational* binary forms (that is, forms whose variables range over $\mathbb{Q}$). Two rational forms are *$\mathbb{Q}$-equivalent* if there is a non-singular linear transformation over $\mathbb{Q}$ mapping one form to the other. Finally, if a given form f represents a particular integer, then so do all forms $\mathbb{Z}$-equivalent or $\mathbb{Q}$-equivalent to f.

The following theorem ([5] p50) gives necessary conditions on the primitive representation of integers by binary quadratic forms over $\mathbb{Z}$.

Theorem 1 *Let $f_1 = ax_1^2 + bx_1y_1 + cy_1^2$ be a quadratic form over $\mathbb{Z}$ and Δ its discriminant. Then f_1 primitively represents $r \in \mathbb{Z}$ only if there exists some $s \in \mathbb{Z}$ for which*

$$s^2 \equiv \Delta \bmod 4r. \tag{1}$$

Proof: Suppose $f_1(\alpha, \gamma) = r$ for coprime $\alpha, \gamma \in \mathbb{Z}$. Then there exist integers β, δ for which $\alpha\delta - \beta\gamma = 1$. Under the (unimodular) transformation

$$\begin{aligned} x_1 &\mapsto \alpha x_2 + \beta y_2 \\ y_1 &\mapsto \gamma x_2 + \delta y_2 \end{aligned}$$

f_1 is mapped to a $\mathbb{Z}$-equivalent form f_2 with leading coefficient

$$a_2 = a\alpha^2 + b\alpha\gamma + c\gamma^2 = r.$$

Since the discriminant of f_2 is Δ, its remaining coefficients b_2 and c_2 satisfy

$$b_2^2 - 4rc_2 = \Delta.$$

Hence with $s = b_2$ the congruence (1) holds. ∎

As an immediate consequence of Theorem 1 we have

Corollary 1 *Let f be a binary quadratic form over $\mathbb{Z}$ with discriminant Δ, and let p be an odd prime not dividing Δ. If f primitively represents some $r \in \mathbb{Z}$ and $p|r$ then*

$$\left(\frac{\Delta}{p}\right) = 1.$$

In the case $p = 2$ we have

Corollary 2 *Let $f = ax^2 + bxy + cz^2$ be a binary quadratic form with odd discriminant Δ. If f primitively represents some even $r \in \mathbb{Z}$ then at least one of a, c is even.*

Proof: By Theorem 1 we require a solution s to $s^2 \equiv \Delta \bmod 8$. The only odd quadratic residue mod 8 is 1, so we require

$$\Delta \equiv 1 \bmod 8. \tag{2}$$

Clearly Δ is odd if and only if b is odd, so (2) holds only if $4ac \equiv 0 \bmod 8$, which implies a and c are not both odd. ∎

Note also that if b (and therefore Δ) is even, f cannot fail to primitively represent some even r.

In general the converse of Theorem 1 is not quite true, but there is a slightly more general statement that holds. If a solution to (1) exists then some class of forms of discriminant Δ primitively represents r (see [5] p50). We note however, that necessary *and* sufficient conditions on the representation of r by binary *rational* quadratic forms are given by the Hasse-Minkowski Theorem ([4] p61). In fact the representation of r by a binary rational form is equivalent to the representation of zero by a tertiary rational form, so the relevant statement of the Hasse-Minkowski Theorem is the following.

Theorem 2 ([4] p73) *Let a, b and c be rational integers, pairwise coprime and not all the same sign. Then the equation*

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

has a solution in $\mathbb{Q}$ (equivalently, in $\mathbb{Z}$) if and only if the congruences

$$\begin{aligned} x^2 &\equiv -bc \bmod a, \\ x^2 &\equiv -ca \bmod b, \\ x^2 &\equiv -ab \bmod c, \end{aligned}$$

are all solvable.

Theorem 1 can also be derived from the congruence modulo c in Theorem 2. Indeed, suppose $r \in \mathbb{Z}$ such that there exists a rational solution to $f(x, y) = r$.

This is equivalent (see [4] p393) to there being a representation of zero over $\mathbb{Z}$ by the form

$$q_1 = a_1x_1^2 + b_1x_1y_1 + c_1y_1^2 - rz^2.$$

The linear transformation

$$\begin{array}{rcl} x_1 & \mapsto & x_2 + b_1y_2 \\ y_1 & \mapsto & -2a_1y_2 \end{array}$$

reduces q_1 to the equivalent quadratic form q_2 where

$$q_2 = a_1x_2^2 + a_1(4a_1c_1 - b_1^2)y_2^2 - rz^2.$$

Under the substitution

$$\begin{array}{rcl} a_1x_2 & \mapsto & x_3 \\ a_1y_2 & \mapsto & y_3 \end{array}$$

we now seek integer solutions to the equation

$$x_3^2 - \Delta y_3^2 - a_1rz^2 = 0.$$

The result follows by letting p be an odd prime dividing r but not dividing Δ, and requiring $x_3^2 \equiv \Delta y_3^2 \bmod p$. At this stage we are unable to obtain additional useful information from the sufficient conditions in Thereom 2.

3 Quadratic Residuosity and Smoothness Probabilities

Here we repeat an argument proposed for the MPQS in [3], due to Peter Montgomery, regarding the effect of information about quadratic residuosity on the smoothness probabilities of W-values. Given Corollaries 1 and 2, we are able to extend this argument to quadratic number field sieve polynomials.

Suppose we are to sieve over W-values for some MPQS polynomial W. Recall that the factor base FB consists of all odd primes $p < B$ for which $(N/p) = 1$, and (by the choice of multiplier) the prime 2. Let

$$r_p = \begin{cases} 2 & \text{if } \left(\frac{N}{p}\right) = 1, \\ 0 & \text{if } \left(\frac{N}{p}\right) = -1, \end{cases}$$

where we assume p does not divide N. By the choice of multiplier we define $r_2 = 2$. For all primes $p \in FB$ (including 2) the expected exponent of p in the factorisation of a W-value (that is, the expected *contribution* of p) is

$$p^{r_p\left(\frac{1}{p}+\frac{1}{p^2}+\cdots\right)} = p^{\frac{r_p}{p-1}}.$$

Hence, the estimated sieve array value corresponding to $\log|W(x)|$ after sieving is

$$\log|W(x)| - \sum_{p \leq B} r_p \frac{\log p}{p-1}.$$

The corresponding value for a random integer y of the same size is

$$\log y - \sum_{p \leq B} \frac{\log p}{p-1}.$$

So it is suggested that W-values are about as smooth as random integers of log size $\alpha + \log W(x)$ where

$$\alpha = \sum_{p \leq B} (1 - r_p) \frac{\log p}{p-1}. \tag{3}$$

Hence, if $\alpha < 0$ then W-values are considered more likely to be smooth than random integers of the same size.

Comment: Except in marginal cases, the sign of α is determined by the value of r_p at small p, perhaps even the first three or four values. Clearly it is not necessarily true in general that $\alpha < 0$. A feature of MPQS however is that by choosing an appropriate multiplier, we can ensure that N is a quadratic residue for sufficiently many small odd p, and that (as above) $2 \in FB$. Optimal use of the MPQS therefore tends to the case $\alpha < 0$. Indeed, in [3], values of α are presented for thirty four distinct values of N. In all cases $\alpha < 0$. In fact $\alpha \in [-3.186, -0.5899]$. For values as high as -0.5899, all that saves α from being positive is that $r_2 = 2$ (by the choice of multiplier).

We now adapt the definition of α for quadratic number field sieve polynomials.

For a given binary quadratic form f over $\mathbb{Z}$ and for odd p with $p \not| \Delta$, let

$$q_p = \begin{cases} 2 & \text{if } \left(\frac{\Delta}{p}\right) = 1, \\ 0 & \text{if } \left(\frac{\Delta}{p}\right) = -1. \end{cases}$$

If $p|\Delta$, put $q_p = 0$. Finally, if Δ (equivalently, b) is odd let

$$q_2 = \begin{cases} 2 & \text{if at least one of } a, c \text{ is even,} \\ 0 & \text{otherwise,} \end{cases}$$

and if Δ is even let $q_p = 2$. Then let $\alpha(f)$ be given by

$$\alpha(f) = \sum_{p \leq B} (1 - q_p) \frac{\log p}{p-1}.$$

Now, polynomials f for which $\alpha(f) < 0$, at least heuristically, produce values more likely to be smooth than random integers of the same size. Moreover, suppose we have forms f_1 and f_2 with $\alpha(f_1) < \alpha(f_2)$. Depending on how the *distribution* of smooth values varies with α, we might expect f_1 to be a "better" polynomial than f_2.

In the next section we estimate the effect of varying α on on the yield of smooth f-values. Below though we give a result estimating q_p for a random assignment mod$p$ of the coefficients (a, b, c) of f.

Lemma 1 *For each odd prime p coprime to Δ, the number of non-trivial 3-tuples $(a, b, c) \bmod p$ for which $(\Delta/p) = 1$ is*

$$\frac{1}{2}(p-1)(p^2+p) - 1.$$

Proof: Fix $b \not\equiv 0 \bmod p$. For $\Delta = b^2 - 4ac$ and $(\Delta/p) = 1$ we have

$$ac \equiv (-4)^{-1}(\chi_p - b^2) \bmod p, \tag{4}$$

where χ_p is any of the $(p-1)/2$ quadratic residues mod p. Hence the product ac may take any of $(p-1)/2$ values mod p, exactly one of which will force the right hand side of (4) to be zero because exactly one $\chi_p = b^2$.

For each of the $(p-3)/2$ *non-zero* values of the right hand side of (4), there are $p-1$ ordered pairs (a, c) whose product gives the right hand side, since for each non-zero a, c is uniquely determined by $c = a^{-1}(-4)^{-1}(\chi_p - b^2) \bmod p$.

For each single zero value of the right hand side of (4), there are $2p-1$ ordered pairs (a, c) for which at least one of $a \equiv 0 \bmod p$ or $c \equiv 0 \bmod p$ holds.

Hence, for non-zero b, there are

$$\frac{p-3}{2}(p-1) + 2p - 1$$

ordered pairs (a, c) giving $(\Delta/p) = 1$. There are $p-1$ non-zero residue classes for b, so non-zero b account for

$$(p-1)\left[\frac{p-3}{2}(p-1) + 2p - 1\right] = (p-1)\left[\frac{p^2}{2} + \frac{1}{2}\right]$$

tuples $(a, b, c) \bmod p$.

Now, if $b \equiv 0 \bmod p$, we require

$$ac \equiv (-4)^{-1}\chi_p \bmod p \tag{5}$$

where again χ_p is any of the $(p-1)/2$ quadratic residues mod p. Since the right hand side of (5) is always non-zero, there are $p-1$ pairs (a, c) for each χ_q, giving a total of

$$\frac{p-1}{2}(p-1)$$

tuples $(a, b, c) \bmod p$ for $b \equiv 0 \bmod p$.

So, the total number of tuples is

$$(p-1)\left[\frac{p^2}{2} + \frac{1}{2}\right] + \frac{p-1}{2}(p-1) = \frac{p-1}{2}\left[p^2 + p\right],$$

one of which is the trivial tuple $(0, 0, 0) \bmod p$. ∎

Thus, for odd p, the probability that a uniformly random non-trivial selection $(a, b, c) \bmod p$ satisfies $(\Delta/p) = 1$ is given by

$$\begin{aligned} \text{Prob}\left[(\Delta/p) = 1\right] &= \frac{(p-1)(p^2+p)/2 - 1}{p^3 - 1} \\ &< \frac{1}{2}\left[1 - \frac{1}{p^2}\right]. \end{aligned}$$

For odd p not dividing Δ, it is therefore more likely than not that $(\Delta/p) = -1$, and the probability that $(\Delta/p) = 1$ is smallest for smaller p. This highlights the significance of selecting polynomials which do have roots modulo small p.

4 Yield per polynomial

We refer to the number of B-smooth f-values on the sieve interval as the *full yield* of f. For the NFS this is not quite the same as the number of full *relations* per polynomial, since a full relation is required to be a B-smooth value taken by two polynomials with a common root $\bmod N$. We estimate the full yield in section 4.2 by repeating Boender's MPQS calculation for NFS polynomials. In section 4.3 we examine this yield as a function of α.

Relation collection can be sped up considerably by the collection of f-values which are smooth but for up to 2 prime factors between B_1 and B_2 (with $B \leq B_1 < B_2$). We refer to these as *incomplete* f-values. We refer to an incomplete f-value with exactly one so called large prime factor as *partially* (or p-) smooth, and to an incomplete f-value with exactly two large prime factors as *partially partially* (or pp-) smooth. Incomplete f-values are useful only if they lead to relations in which the same large prime occurs at least twice. It is a seperate and open question to estimate (for the NFS) the number of 'useful' relations obtained from a given number of incomplete f-values. In sections 4.4 and 4.5 therefore, we consider only the 'yield', that is, the number of incomplete f-values.

4.1 Smooth integers in an interval

We require an estimate of the number smooth integers amongst an integer interval of a given size. For an integer n let $P_1(n)$ denote the largest prime factor of n. As usual, let

$$\psi(x, y) = \left|\left\{n \in \mathbb{Z}^+ : n \leq x \text{ and } P_1(n) \leq y\right\}\right|.$$

Then

$$\psi(x, y) \approx x\left(\rho(u) + (1-\gamma)\frac{\rho(u-1)}{\log x}\right) \tag{6}$$

where $u = (\log x)/\log y$, γ is Euler's constant and $\rho(u)$ is Dickman's rho function ([3], [8]).

Now, for fixed $\epsilon \in (0,1)$, the number of y-smooth integers in the interval $[x, x+x/z]$ is given by

$$\psi\left(x+\frac{x}{z}, y\right) - \psi(x,y) = \\ \frac{\log(1+y/\log x)}{z\log y}\ \psi(x,y)\left[1+O_\epsilon\left(\frac{1}{z}+\frac{\log\log(1+y)}{\log y}\right)\right] \tag{7}$$

for x, y, z in the range $x \geq 2$ and

$$(\log\log x)^{2/3+\epsilon} < \log y \leq (\log x)^{2/5},\ 1 \leq z \leq R(x,y)^{-1},$$

where $R(x,y)$ is some expression depending on x, y and some fixed constants (see [3] p 48).

Combining (6) and (7) and approximating some of the logarithms gives

$$\frac{z}{x}\left\{\psi\left(x+\frac{x}{z}, y\right)\right\} \approx \\ \left(1-\frac{\log\log x}{\log y}\right)\sigma(x,y,z)\left(1+c_1(\epsilon)\frac{1}{z}+c_2(\epsilon)\frac{\log\log y}{\log y}\right), \tag{8}$$

where $\sigma(x,y,z)$ is given by

$$\sigma(x,y,z) = \rho(u) + (1-\gamma)\frac{\rho(u-1)}{\log x}$$

and the $c_i(\epsilon)$ are constants depending on ϵ ([3] p 49). Boender notes that the range of interest for x, y, z is slightly outside that for which (7) is proven to hold. Empirically however, (7) still provides a good approximation in the range of interest.

4.2 Estimating the yield

In the implementation described in [9] sieving is performed using a method known as line sieving. During line sieving, only values $f(x,1)$ are considered. Hence we now consider only quadratic polynomials $f(x)$. Suppose then, that we are to sieve for B-smooth values of $|f(x)|$ with x in the range $[a_1, a_2]$.

Care is required in the calculations below when f (considered as a continuous curve on the real interval $[a_1, a_2]$) contains a stationary point or roots in $[a_1, a_2]$. In our circumstances this is always the case. Clearly each curve f can be cut into segments which exclude roots and turning points (we require at most four segments). We call the segment so obtained which occupies the largest portion of $[a_1, a_2]$ the *principal segment.* For each curve below we have repeated our calculations on every segment of the curve, and obtained almost identical results on each segment. Hence we report only the results on the principal segment.

Let I be the real x-interval defining the principal segment, and let Γ be the continous curve defined by f on I. Since Γ contains no turning point in I, we can assume either $f'(x) < 0$ or $f'(x) > 0$ for all $x \in I$. We assume the latter, the former only requires sign changes in the arguments below. Similarly, we assume $f(x) > 0$ for all $x \in I$. The question now is 'how many integer points on Γ are B-smooth?'.

We approximate the number of B-smooth f-values on Γ by examining Γ in short intervals. Let S_1 and S_2 be the minimum and maximum values respectively, taken by Γ on I. We cut $[S_1, S_2]$ into K subintervals $[y_i, y_{i+1}]$ for $i = 0, \ldots, K-1$ by taking

$$h = \frac{\log S_2 - \log S_1}{K},$$

so $y_i = S_1 e^{ih}$. In accordance with our notation for estimating the number of smooth integers in an interval, we write $y_{i+1} = y_i + y_i/z$ where $1/z = e^h - 1$.

Now, for each y_i, let $x_i \in \mathbb{R}$ be such that $(x_i, y_i) \in \Gamma$. Let

$$s_i = \frac{y_{i+1} - y_i}{x_{i+1} - x_i}$$

denote the slope of Γ on $[x_i, x_{i+1}]$, and let $t(y_i)$ denote the number of B-smooth f-values on Γ with $y \leq y_i$. Clearly the yield on the whole of Γ, X_f, is given by

$$X_f = \sum_{i=0}^{K-1} \left(t(y_{i+1}) - t(y_i) \right). \tag{9}$$

For $y \in [y_i, y_{i+1}]$ the probability that a randomly chosen $(x, y) \in \Gamma$ has $x \in \mathbb{Z}$ is approximately $1/s_i$. So we have

$$t(y_{i+1}) - t(y_i) \;\approx\; \frac{y_{i+1} - y_i}{s_i} P \;=\; (x_{i+1} - x_i) P$$

where P is the probability that an integer f-value in $[y_i, y_{i+1}]$ is B-smooth.

Recall that we consider f-values $f(x)$ to be as likely to be B-smooth as random integers of logarithm $\log(f(x)) + \alpha(f)$ where

$$\alpha(f) = \sum_{p \leq B} (1 - q_p) \frac{\log p}{p - 1}.$$

So, if $g_i = \log y_i + \alpha = S_1 + ih + \alpha$, and if $v_i = g_i / \log B$, approximation (8) yields

$$\begin{aligned} t(y_{i+1}) - t(y_i) \approx & \\ & (x_{i+1} - x_i) \left(1 - \frac{\log g_i}{\log B} \right) \left(\rho(v_i) + (1 - \gamma) \frac{\rho(v_i - 1)}{g_i} \right) \\ & \times \left(1 + \frac{c_1}{z} + \frac{c_2 \log \log B}{\log B} \right). \end{aligned} \tag{10}$$

Approximation (10) and equation (9) give an approximation to X_f.

4.3 Full yield as a function of α

We now consider the yield per polynomial as a function of α. For B fixed, $\alpha(f)$ is bounded, in fact for $B = 5 \cdot 10^6$ we have approximately $|\alpha| \leq 14.16$. However for the quadratic NFS polynomials investigated, typically $\alpha \in [-2, 2]$, a range of 4. So we consider $\alpha \in [-4, 0]$ and refer to this as the *practical range* for α. We approximate X_f, with appropriate parameter choices, as α varies in the practical range. In fact we calculate

$$\begin{aligned} Q(\alpha) &= \frac{X_f(\alpha)}{X_f(0)} \\ &\approx \frac{\sum_{i=0}^{K-1}(x_{i+1} - x_i)\left(1 - \frac{\log g_i(\alpha)}{\log B}\right)\left(\rho(v_i(\alpha)) + (1-\gamma)\frac{\rho(v_i(\alpha)-1)}{g_i(\alpha)}\right)}{\sum_{i=0}^{K-1}(x_{i+1} - x_i)\left(1 - \frac{\log g_i}{\log B}\right)\left(\rho(v_i) + (1-\gamma)\frac{\rho(v_i-1)}{g_i}\right)}, \end{aligned}$$

where the terms in the denominator are understood to be evaluated at $\alpha = 0$. The quantity $Q(\alpha)$ approximates the relative increase in full yield we might expect as α decreases in the practical range.

Remark: In practice $Q(\alpha)$ is approximately independent of K, so we use $K = 100$ in accordance with [3]. Also, we calculate the Dickman function using the Taylor series method described in [1].

We calculate values of $Q(\alpha)$ for five sets of parameters, labelled C87, C97, C105, C106 and C107. We use the parameters reported in [9] for factorisations of integers of the same labels. Moreover, we use the polynomials $f_1(x)$ of [9] for each integer, to determine our values x_i, y_i and s_i. We claim therefore, only that the parameters Cs are typical for quadratic NFS polynomials with integers of s decimal digits. So the values $Q(\alpha)$ approximate the relative range of yields we can expect from typical quadratic polynomials for integers of size s. In any event $Q(\alpha)$ seems more dependent on the rate at which the Dickman function is decreasing than it does on minor parameter changes.

Table 1 contains the relevant parameters.

	C87	C97	C105	C106	C107
divides	$72^{99} + 1$	$12^{441} + 1$	$3^{367} - 1$	$12^{157} + 1$	$6^{223} + 1$
B	$1.0 \cdot 10^6$	$2.2 \cdot 10^6$	$1.6 \cdot 10^6$	$2.7 \cdot 10^6$	$2.9 \cdot 10^6$
$\lvert x\rvert \leq$	$7.5 \cdot 10^{12}$	$25 \cdot 10^{12}$	$7.5 \cdot 10^{14}$	$1.0 \cdot 10^{15}$	$1.0 \cdot 10^{15}$
$I \approx$	$[3.0 \cdot 10^{12}, 7.5 \cdot 10^{12}]$	$[-2.5 \cdot 10^{13}, -5.8 \cdot 10^{12}]$	$[-1.3 \cdot 10^{13}, 7.5 \cdot 10^{14}]$	$[-1.0 \cdot 10^{15}, -2.2 \cdot 10^{14}]$	$[-1.3 \cdot 10^{14}, 1.0 \cdot 10^{15}]$

Table 1: Parameters for Table 2

Table 2 contains values of $Q(\alpha)$ for these parameters, at several values of α.

$-\alpha$	$Q(\alpha)$				
	$C87$	$C97$	$C105$	$C106$	$C107$
0.05	1.01	1.01	1.01	1.01	1.01
0.50	1.11	1.11	1.12	1.11	1.11
1.00	1.24	1.22	1.24	1.23	1.23
1.50	1.37	1.35	1.39	1.37	1.36
2.00	1.53	1.50	1.54	1.51	1.51
2.50	1.69	1.66	1.72	1.68	1.68
3.00	1.88	1.83	1.92	1.86	1.86
3.50	2.09	2.02	2.13	2.06	2.06
4.00	2.32	2.23	2.38	2.28	2.28

Table 2: $Q(\alpha)$ vs α

The complete results on C107 for $\alpha \in [-4, 0]$ are shown in Figure 1 below. The complete results for the other parameters are similar.

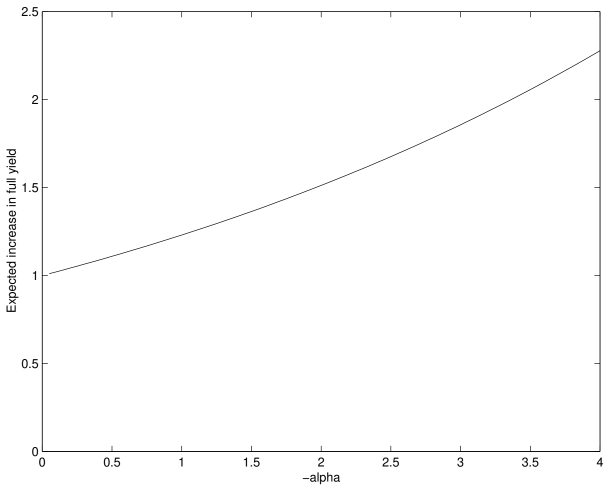

Figure 1: $Q(\alpha)$ for C107

We see from Table 2 that, heuristically, we might expect the difference in yield between polynomials with values of α at the extremes of the practical range to be as much as a factor of 2. This would be a significant increase.

4.4 Partial yield as a function of α

Let Y_f be the number of partially smooth f values on Γ. Let $t_1(y_i)$ be the number of partially smooth f-values on Γ with $y \leq y_i$. Clearly

$$Y_f = \sum_{i=0}^{K-1} (t_1(y_{i+1}) - t_1(y_i)). \tag{11}$$

For each large prime p, let $g_{i,p} = g_i - \log p = \log S_1 + ih + \alpha - \log p$, and $v_{i,p} = g_{i,p}/\log B$. Where necessary we indicate the dependence on α by writing $g_{i,p}(\alpha)$ and $v_{i,p}(\alpha)$. Then

$$\begin{aligned}
t_1(y_{i+1}) - t_1(y_i) &\approx \sum_{B_1<p<B_2} \frac{q_p}{p} (t(y_{i+1}/p) - t(y_i/p)) \\
&\approx \quad (x_{i+1} - x_i) \sum_{B_1<p<B_2} \frac{q_p}{p} \left(1 - \frac{\log g_{i,p}}{\log B}\right) \left(\rho(v_{i,p}) + (1-\gamma)\frac{\rho(v_{i,p}-1)}{g_{i,p}}\right) \\
&\quad \times \left(1 + \frac{c_1}{z} + \frac{c_2 \log\log B}{\log B}\right),
\end{aligned} \tag{12}$$

which, with (11) gives an approximation to Y_f (see [3] p 52) .

We are interested in the relative increase in p-yield as a function of α, that is, the ratio

$$\frac{Y_f(\alpha)}{Y_f(0)}. \tag{13}$$

Calculating (13) directly is time-consuming. Since we are interested only in checking that practical changes in α can bring significant increases in yield, we instead obtain upper and lower bounds on (13) in intervals along along f. The bounds suffice to show a significant increase in yield. For $i = 1 \dots K-1$ let $Y_{f,i}(\alpha) = t_1(y_{i+1}) - t_1(y_i)$ be the partial yield in the i-th interval only. We bound

$$R_i(\alpha) = \frac{Y_{f,i}(\alpha)}{Y_{f,i}(0)}$$

for $i = 1 \dots K-1$.

Let

$$LP = \{p : p \text{ prime }, \ B_1 < p < B_2, \ (\Delta/p) = 1\},$$

and let p_1, p_2 be the minimum and maximum elements (respectively) in LP. Then

$$\begin{aligned}
g_{i,1}(\alpha) &= \log x_i + ih + \alpha - \log p_2, \text{ and} \\
g_{i,2}(\alpha) &= \log x_i + ih + \alpha - \log p_1
\end{aligned}$$

are the minimum and maximum values (respectively) of $g_{i,p}$ on (x_i, x_{i+1}). Also,

$$\begin{aligned}
v_{i,1}(\alpha) &= g_{i,1}(\alpha)/\log B, \text{ and} \\
v_{i,2}(\alpha) &= g_{i,2}(\alpha)/\log B
\end{aligned}$$

are the minimum and maximum values (respectively) of $v_{i,p}$ on (x_i, x_{i+1}). Finally, let

$$\begin{aligned}
\mathcal{L}_i(\alpha) &= \frac{2}{p_2}\left(1-\frac{\log g_{i,2}(\alpha)}{\log B}\right)\left(\rho(v_{i,2}(\alpha)) + (1-\gamma)\frac{\rho(v_{i,2}(\alpha)-1)}{g_{i,2}(\alpha)}\right), \\
\mathcal{U}_i(\alpha) &= \frac{2}{p_1}\left(1-\frac{\log g_{i,1}(\alpha)}{\log B}\right)\left(\rho(v_{i,1}(\alpha)) + (1-\gamma)\frac{\rho(v_{i,1}(\alpha)-1)}{g_{i,1}(\alpha)}\right).
\end{aligned}$$

Then

$$Y_{f,i}(\alpha) < (x_{i+1} - x_i) \cdot |LP| \cdot \mathcal{U}_i(\alpha).$$

Similarly, $Y_{f,i}(\alpha) > (x_{i+1} - x_i) \cdot |LP| \cdot \mathcal{L}_i(\alpha)$. Since we are varying only α,

$$\frac{\mathcal{L}_i(\alpha)}{\mathcal{U}_i(0)} < R_i(\alpha) < \frac{\mathcal{U}_i(\alpha)}{\mathcal{L}_i(0)}. \tag{14}$$

To calculate $R_i(\alpha)$ we use the following additional parameters from [9].

	C87	C97	C105	C106	C107
B_1	$1.0 \cdot 10^6$	$10 \cdot 10^6$	$23 \cdot 10^6$	$27 \cdot 10^6$	$27.2 \cdot 10^6$
B_2	$2.346 \cdot 10^6$	$24 \cdot 10^6$	$30 \cdot 10^6$	$30 \cdot 10^6$	$30 \cdot 10^7$

Table 3: Large prime bounds

We give values of the bounds on $R_i(\alpha)$ evaluated at $\alpha = -4$, for several i, in Table 4.

$\frac{\mathcal{L}_i(-4)}{\mathcal{U}_i(0)}, \frac{\mathcal{U}_i(-4)}{\mathcal{L}_i(0)}$	C87	C97	C105	C106	C107
$i = 1$	$0.64, 4.42$	$0.61, 4.39$	$1.52, 1.93$	$1.51, 1.93$	$1.54, 1.92$
$i = 25$	$0.69, 4.98$	$0.65, 4.82$	$1.62, 2.05$	$1, 62, 2.06$	$1.62, 2.05$
$i = 50$	$0.72, 5.36$	$0.68, 5.18$	$1.72, 2.18$	$1.72, 2.20$	$1.72, 2.18$
$i = 75$	$0.75, 5.74$	$0.71, 5.53$	$1.81, 2.29$	$1.83, 2.32$	$1.81, 2.30$
$i = 99$	$0.78, 5.97$	$0.73, 5.85$	$1.87, 2.40$	$1.88, 2.42$	$1.90, 2.40$

Table 4: Upper and lower bounds on $R_i(-4)$

The values for C87 and C97 are inconclusive, but the values for C105, C106 and C107 (in particular the lower bounds) are useful. We illustrate in Figure 2 the complete results for C107. The results for C105 and C106 are similar. The region between the lines represents the expected increase in the p-yield of f.

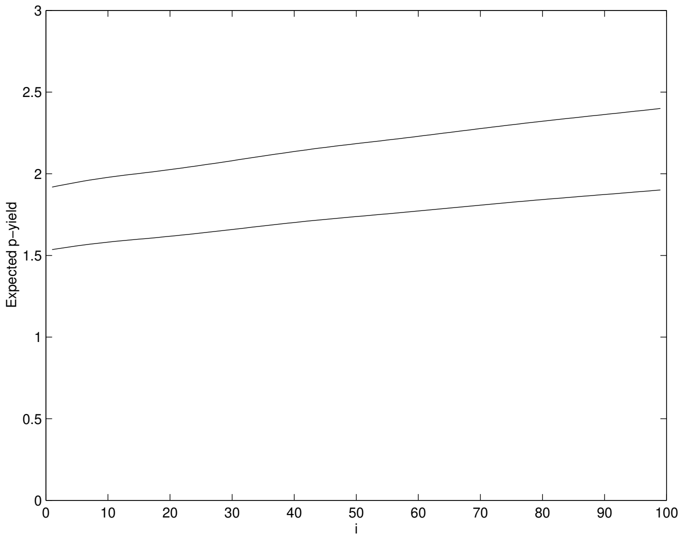

Figure 2: $R_i(-4)$ for C107

We conclude that for sufficiently large integers, practical changes in α might bring significant increases in the partial yield.

4.5 Partial-partial yield as a function of α

Let Z_f be the number of pp-smooth f values on Γ. Let $t_2(y_i)$ be the number of pp-smooth f-values on Γ with $y \leq y_i$. Then

$$Z_f = \sum_{i=0}^{K-1} (t_2(y_{i+1}) - t_2(y_i)). \tag{15}$$

For the large prime pair $\{p, q\}$ let $g_{i,pq} = g_i(\alpha) - \log p - \log q$ and $v_{i,pq} = g_{i,pq}/\log B$. Then, assuming that the appearance of p and q in the factorisations of f-values is independent,

$$\begin{aligned} t_2(y_{i+1}) - t_2(y_i) &\approx \sum_{\{p,q\}\in LP} \frac{4}{pq}\left(t(y_{i+1}/pq) - t(y_i/pq)\right) \\ \approx \quad (x_{i+1} - x_i) &\sum_{\{p,q\}\in LP} \frac{4}{pq}\left(1 - \frac{\log g_{i,pq}}{\log B}\right)\left(\rho(v_{i,pq}) + (1-\gamma)\frac{\rho(v_{i,pq}-1)}{g_{i,pq}}\right) \\ \times &\left(1 + \frac{c_1}{z} + \frac{c_2 \log\log B}{\log B}\right). \end{aligned} \tag{16}$$

Equation (15) and approximation (16) give an approximation to Z_f.

Again we present bounds on the relative increase in Z_f in intervals along Γ, as α varies in the practical range. Let $Z_{f,i} = t_2(y_{i+1}) - t_2(y_i)$ be the pp-yield in the i-th interval, and let

$$T_i(\alpha) = \frac{Z_{f,i}(\alpha)}{Z_{f,i}(0)}.$$

We calculate bounds on T_i for $i = 1 \ldots K-1$ by repeating the calculations of the previous section. Thus, let p_1, p_2 and p_3, p_4 be the two least and two greatest elements (respectively) of LP. Let

$$\begin{aligned}
g_{i,1}(\alpha) &= \log x_i + \alpha - \log p_3 - \log p_4, \\
g_{i,2}(\alpha) &= \log x_i + \alpha - \log p_1 - \log p_2, \\
v_{i,1}(\alpha) &= g_{i,1}(\alpha)/\log B, \text{ and} \\
v_{i,2}(\alpha) &= g_{i,2}(\alpha)/\log B.
\end{aligned}$$

Then if

$$\begin{aligned}
\mathcal{L}_i(\alpha) &= \frac{4}{p_3 p_4}\left(1 - \frac{\log g_{i,2}(\alpha)}{\log B}\right)\left(\rho(v_{i,2}(\alpha)) + (1-\gamma)\frac{\rho(v_{i,2}(\alpha)-1)}{g_{i,2}(\alpha)}\right), \text{ and} \\
\mathcal{U}_i(\alpha) &= \frac{4}{p_1 p_2}\left(1 - \frac{\log g_{i,1}(\alpha)}{\log B}\right)\left(\rho(v_{i,1}(\alpha)) + (1-\gamma)\frac{\rho(v_{i,1}(\alpha)-1)}{g_{i,1}(\alpha)}\right)
\end{aligned}$$

we have

$$\frac{\mathcal{L}_i(\alpha)}{\mathcal{U}_i(0)} < T_i(\alpha) < \frac{\mathcal{U}_i(\alpha)}{\mathcal{L}_i(0)}. \tag{17}$$

Table 5 contains values of the bounds on $T_i(-4)$ given by (17), for several i.

$\frac{\mathcal{L}_i(-4)}{\mathcal{U}_i(0)}, \frac{\mathcal{U}_i(-4)}{\mathcal{L}_i(0)}$	C87	C97	C105	C106	C107
$i = 1$	$0.25, 11.60$	$0.23, 11.53$	$1.26, 2.02$	$1.26, 2.02$	$1.28, 1.99$
$i = 25$	$0.25, 12.32$	$0.65, 4.82$	$1.33, 2.12$	$1.33, 2.13$	$1.36, 2.09$
$i = 50$	$0.26, 13.13$	$0.24, 13.00$	$1.40, 2.26$	$1.41, 2.27$	$1.43, 2.23$
$i = 75$	$0.26, 13.68$	$0.24, 13.64$	$1.46, 2.36$	$1.47, 2.38$	$1.50, 2.34$
$i = 99$	$0.27, 14.36$	$0.25, 14.24$	$1.51, 2.47$	$1.53, 2.50$	$1.56, 2.46$

Table 5: Upper and lower bounds on $T_i(-4)$

Again the results for C87 and C97 are inconclusive, whilst those for C105, C106 and C107 are useful. In Figure 3 we plot the complete results for C107. The plots for C105 and C106 are similar.

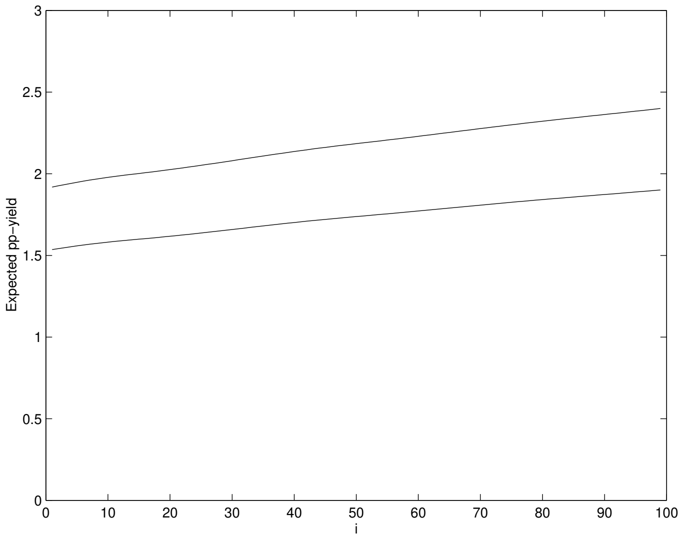

Figure 3: $T_i(-4)$ for C107

We conclude again, that for sufficiently large integers, practical changes in α might bring significant increases in the pp-yield.

5 Conclusion

We have given necessary conditions on the existence of roots mod p for quadratic NFS polynomials f. Using the measure α capturing these conditions and adapted from the MPQS calculations in [3], we are able to quantify the extent to which these conditions may affect the yield and incomplete yield of f. We conclude that, heuristically, varying α within practically attainable values can bring significant changes in the yield of smooth values of quadratic number field sieve polynomials.

References

[1] E Bach and R Peralta, "Asymptotic Semismoothness Probabilities" *Math. Comp.* **65** (1996), pp 1717–1735.

[2] D J Bernstein and A K Lenstra, "A General Number Field Sieve Implementation", *The Development of the Number Field Sieve, LNM* **1554** (1993) pp 103–125.

[3] H Boender, "The Number of Relations in the Quadratic Sieve Algorithm", *Chapter 4, PhD Thesis*, University of Leiden, 1997.

[4] Z I Borevich and I R Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[5] D A Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations*, Springer-Verlag, New York, 1989.

[6] J P Buhler, H W Lenstra Jr, C Pomerance, "Factoring Integers with the Number Field Sieve", *The Development of the Number Field Sieve, LNM* **1554** (1993) pp 50–94.

[7] J Cowie, B Dodson, R M Elkenbracht-Huizing, A K Lenstra. P Montgomery, J Zayer, "A World Wide Number Field Sieve Factoring Record: On to 512 Bits", *Advances in Cryptology - ASIACRYPT 1996, LNCS* **1163** (1997) pp 382–394

[8] K Dickman, "On the Frequency of Numbers Containing Prime Factors of a Certain Relative Magnitude", *Ark. Mat., Astronomi och Fysik* **22A** 10 (1930), pp 1–14.

[9] M Elkenbracht-Huizing, "An Implementation of the Number Field Sieve", *Experimental Mathematics* **5**(3) (1996) pp 375–389.

[10] R D Silverman, "The Multiple Polynomial Quadratic Sieve", *Math. Comp.* **48** (1987) pp 329–339.