On Quadratic Fields Generated by Discriminants of Irreducible Trinomials

IGOR E. SHPARLINSKI*
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

November 8, 2008

Abstract

A. Mukhopadhyay, M. R. Murty and K. Srinivas have recently studied various arithmetic properties of the discriminant $\Delta_n(a, b)$ of the trinomial $f_{n,a,b}(t) = t^n + at + b$, where $n \geq 5$ is a fixed integer. In particular, it is shown that, under the $abc$-conjecture, for every $n \equiv 1 \pmod{4}$, the quadratic fields $\mathbb{Q}\left(\sqrt{\Delta_n(a, b)}\right)$ are pairwise distinct for a positive proportion of such discriminants with integers $a$ and $b$ such that $f_{n,a,b}$ is irreducible over $\mathbb{Q}$ and $|\Delta_n(a, b)| \leq X$, as $X \to \infty$. We use the square-sieve and bounds of character sums to obtain a weaker but unconditional version of this result.

Mathematical Subject Classification (2000): Primary 11R11; Secondary 11L40, 11N36, 11R09

Keywords: Irreducible trinomials, quadratic fields, square sieve, character sums

*This work was supported in part by ARC Grant DP0556431
1 Introduction

For a fixed integer \( n \geq 2 \), we use \( \Delta_n(a, b) \) to denote the discriminant of the trinomial
\[
f_{n,a,b}(t) = t^n + at + b.
\]

A. Mukhopadhyay, M. R. Murty and K. Srinivas [9] have recently studied the arithmetic structure of \( \Delta_n(a, b) \). In particular, it is shown in [9], under the \( abc \)-conjecture, that if \( n \equiv 1 \pmod{4} \) then for a sufficiently large positive \( A \) and \( B \) such that \( B \geq A^{1+\delta} \) with some fixed \( \delta > 0 \), there are at least \( \gamma AB \) integers \( a, b \) with
\[
A \leq |a| \leq 2A \quad \text{and} \quad B \leq |b| \leq 2B
\]
and such that \( f_{n,a,b} \) is irreducible and \( \Delta_n(a, b) \) is square-free, where \( \gamma > 0 \) depends only on \( n \) and \( \delta \).

Then this result is used to derive (still under the \( abc \)-conjecture) that the quadratic fields \( \mathbb{Q}\left(\sqrt{\Delta_n(a, b)}\right) \) are pairwise distinct for a positive proportion of such discriminants with integers \( a \) and \( b \) such that \( f_{n,a,b} \) is irreducible over \( \mathbb{Q} \).

More precisely, for a real \( X \geq 1 \), let \( Q_n(X) \) be the number of distinct fields \( \mathbb{Q}\left(\sqrt{\Delta_n(a, b)}\right) \) taken for all pairs of integers \( a, b \) such that \( f_{n,a,b} \) is irreducible over \( \mathbb{Q} \) and \( |\Delta_n(a, b)| \leq X \).

Throughout the paper, we use \( U = O(V) \), \( U \ll V \), and \( V \gg U \) as equivalents of the inequality \( |U| \leq cV \) with some constant \( c > 0 \), which may depend only on \( n \).

It is shown in [9] that for a fixed \( n \equiv 1 \pmod{4} \),
\begin{equation}
Q(X) \gg X^{\kappa_n},
\end{equation}
where
\[
\kappa_n = \frac{1}{n} + \frac{1}{n-1}
\]
and \( c_0 > 0 \) is a constant depending only on \( n \).

It is also noted in [9] that the Galois groups of irreducible trinomials \( f_{n,a,b} \) have some interesting properties, see also [2, 5, 10]. We remark that, since
\[
\Delta_n(a, b) = (n-1)^{n-1}a^n + n^nb^{n-1}
\]
for \( n \equiv 1 \pmod{4} \), there are \( O \left( X^{\frac{1}{4} + \frac{1}{160}} \right) \) integers \( a \) and \( b \) with \( |\Delta_n(a, b)| \leq X \) and thus indeed (1) means that

\[
Q(X) \gg \# \{(a, b) \in \mathbb{Z}^2 : |\Delta_n(a, b)| \leq X \}.
\]

We use the square-sieve and bounds of character sums to obtain a weaker but unconditional version of this result. We note that, without the irreducibility of \( f_{n,a,b} \) condition, the problem of estimating \( Q(X) \) can be viewed as a bivariate analogue of the question, considered in [8], on the number of distinct quadratic fields of the form \( \mathbb{Q}(\sqrt{F(n)}) \) for \( n = M + 1, \ldots, M + N \), for a nonconstant polynomial \( F(T) \in \mathbb{Z}[T] \). Accordingly we use similar ideas, however we also exploit the specific shape of the polynomial \( \Delta_n(a, b) \) given by (2).

2 Main result

In fact as in [8] we consider a more general quantity than \( Q(X) \). Namely, for real positive \( A, B, C \) and \( D \) and a square-free integer \( s \), we denote by \( T_n(A, B, C, D; s) \) the number of pairs of integers

\[
(a, b) \in [C, C + A] \times [D, D + B]
\]

such that \( \Delta_n(a, b) = s r^2 \) for some integer \( r \).

We write \( \log x \) for the maximum of the natural logarithm of \( x \) and 1, thus we always have \( \log x \geq 1 \).

**Theorem 1.** For real \( A \geq 1, B \geq 1, C \geq 0 \) and \( D \geq 0 \) and a square-free \( s \), we have

\[
T_n(A, B, C, D; s) \ll (AB)^{2/3} \log(AB) + A \log(AB) + B \log(AB)
\]

\[ + (AB)^{1/3} \left( \frac{\log(ABCD) \log(AB)}{\log \log(ABCD)} \right)^2. \]

Now, for real \( A, B, C \) and \( D \) we denote by \( S_n(A, B, C, D) \) the number of distinct quadratic fields \( \mathbb{Q}(\sqrt{\Delta_n(a, b)}) \) taken for all pairs of integers

\[
(a, b) \in [C, C + A] \times [D, D + B]
\]

such that \( f_{n,a,b} \) is irreducible over \( \mathbb{Q} \). Using that the bound of Theorem 1 is uniform in \( s \), we derive
Theorem 2. For real $A \geq 1$, $B \geq 1$, $C \geq 0$ and $D \geq 0$, we have

$$S_n(A, B, C, D) \gg \min \left\{ \frac{(AB)^{1/3}}{\log(AB)}, \frac{A}{\log(AB)}, \frac{B}{\log(AB)}, \frac{(AB)^{2/3}}{\left( \frac{\log \log(ABCD)}{\log(ABCD)} \right)^2} \right\}.$$ 

The results of Theorems 1 and 2 are nontrivial in a very wide range of parameters $A$, $B$, $C$ and $D$ and apply to very short intervals. In particular, $AB$ could be logarithmically small compared to $CD$. Furthermore, taking

$$A = C = \frac{1}{4(n-1)^{n-1}} X^{1/n} \quad \text{and} \quad B = D = \frac{1}{4n^n} X^{1/(n-1)}$$

we see that

$$Q(X) \gg X^{\kappa / 3} (\log X)^{-1},$$

which, although is weaker than (1), does not depend on any unproven conjectures.

3 Character Sums with the Discriminant

Our proofs rest on some bounds for character sums. For an odd integer $m$ we use $(w/m)$ to denote, as usual, the Jacobi symbol of $w$ modulo $m$. We also put

$$e_m(w) = \exp(2\pi iw/m).$$

Given an odd integer $m \geq 3$ and arbitrary integers $\lambda, \mu$, we consider the double character sums

$$S_n(m; \lambda, \mu) = \sum_{u,v=1}^m \left( \frac{\Delta_n(u,v)}{m} \right) e_m(\lambda u + \mu v).$$

We need bounds of these sums in the case of $m = \ell_1 \ell_2$ being a product of two primes $\ell_1 > \ell_2 \geq n$. However, using the multiplicative property of character sums (see [6, Equation (12.21)] for single sums, double sums behaves exactly the same way) we see that it is enough to estimate $S_n(\ell; \lambda, \mu)$ for primes $\ell$. 

4
We start with evaluating these sums in the special case of $\lambda = \mu = 0$ where we define

$$S_n(\ell) = S_n(\ell; 0, 0).$$

**Lemma 3.** For $n \equiv 1 \pmod{4}$ and a prime $\ell$, we have

$$S_n(\ell) \ll \ell.$$

**Proof.** We can certainly assume that $\ell \geq n$ as otherwise the bound is trivial. Recalling (2), we derive

$$S_n(\ell) = \ell \sum_{u,v=1}^{\ell-1} \left( \frac{(n-1)^{n-1} u^n + n^n v^{n-1}}{\ell} \right) + O(\ell).$$

Substituting $uv$ instead of $u$, we obtain

$$S_n(\ell) = \ell \sum_{u=1}^{\ell-1} \sum_{v=1}^{\ell-1} \left( \frac{(n-1)^{n-1} u^n + n^n v^{n-1}}{\ell} \right) + O(\ell)$$

since $n-1$ is even. We now rewrite it in a slightly more convenient form as

$$S_n(\ell) = \ell \sum_{u=1}^{\ell-1} \sum_{v=1}^{\ell-1} \left( \frac{(n-1)^{n-1} u^n v + n^n}{\ell} \right) + O(\ell).$$

As $\gcd(\ell, n-1) = 1$, making the change of variables $(n-1)^{n-1} u^n v + n^n = w$, we note that for every $u = 1, \ldots, \ell-1$ if $v = 1, \ldots, \ell$, then $w$ runs through the complete residue system modulo $\ell$. Hence,

$$S_n(\ell) = (\ell - 1) \sum_{w=1}^{\ell} \left( \frac{w}{\ell} \right) + O(\ell) = O(\ell),$$

which concludes the proof. 

\[\Box\]
The following result can be derived from [3, Theorem 1.1], however we give a self-contained and more elementary proof.

**Lemma 4.** For \( n \equiv 1 \pmod{4} \), a prime \( \ell \) and arbitrary integers \( \lambda, \mu \) with \( \gcd(\lambda, \mu, \ell) = 1 \), we have
\[
|S_n(\ell; \lambda, \mu)| \ll \ell.
\]

**Proof.** As in the proof of Lemma 3, we can certainly assume that \( \ell \geq n \) as otherwise the bound is trivial.

Also as in the proof of Lemma 3 we obtain
\[
S_n(\ell; \lambda, \mu) = \sum_{u=1}^{\ell-1} \sum_{w=1}^{\ell} \left( \frac{(n-1)^{n-1}u^n v + n^n}{\ell} \right) e_{\ell}((\lambda u + \mu)v) + O(\ell).
\]

As \( \gcd(\ell, n-1) = 1 \), making the change of variables \((n-1)^{n-1}u^n v + n^n = w\), we obtain
\[
S_n(\ell; \lambda, \mu) = \sum_{u=1}^{\ell-1} \sum_{w=1}^{\ell} \left( \frac{w}{\ell} \right) e_{\ell}((n-1)^{-n+1}u^{-n}(\lambda u + \mu)(w-n^n)) + O(\ell)
\]
\[
= \sum_{u=1}^{\ell-1} e_{\ell}(-(n-1)^{-n+1}n^{-n}(\lambda u + \mu))
\]
\[
\sum_{w=1}^{\ell} \left( \frac{w}{\ell} \right) e_{\ell}((n-1)^{-n+1}u^{-n}(\lambda u + \mu)w) + O(\ell).
\]

The sums over \( w \) is the Gauss sum, thus
\[
\sum_{w=1}^{\ell} \left( \frac{w}{\ell} \right) e_{\ell}((n-1)^{-n+1}u^{-n}(\lambda u + \mu)w)
\]
\[
= \left( \frac{(n-1)^{-n+1}u^{-n}(\lambda u + \mu)}{\ell} \right) \vartheta_{\ell^{1/2}},
\]
for some complex \( \vartheta_{\ell} \) with \( |\vartheta_{\ell}| = 1 \) (which depends only on the residue class of \( \ell \) modulo 4), we refer to [3, 7] for details.

Since \( n \equiv 1 \pmod{4} \) we have
\[
\left( \frac{u^{-n}}{\ell} \right) = \left( \frac{u^{-1}}{\ell} \right).
\]
Thus, combining the above identities we obtain

\[ S_n(\ell; \lambda, \mu) = \psi_\ell \ell^{1/2} \sum_{u=1}^{\ell-1} \left( \frac{(n-1)^{-n+1}(\lambda + \mu u^{-1})}{\ell} \right) e_\ell \left( -(n-1)^{-n+1}n^u(\lambda u + \mu) \right) + O(\ell). \]

Since \( \gcd(\lambda, \mu, \ell) = 1 \), the Weil bound (see [6, Bound (12.23)]) applies and implies that the sum over \( u \) is \( O(\ell^{1/2}) \) which concludes the proof. \( \square \)

Combining Lemmas 3 and 4 and using the aforementioned multiplicativity property, we obtain

**Lemma 5.** For \( n \equiv 1 \pmod{4} \), an integer \( m = \ell_1\ell_2 \) which is a product of two distinct primes \( \ell_1 \neq \ell_2 \) and arbitrary integers \( \lambda, \mu \), we have

\[ |S_n(m; \lambda, \mu)| \ll m. \]

Finally, using the standard reduction between complete and incomplete sums (see [6, Section 12.2]), we derive from Lemma 5

**Lemma 6.** For \( n \equiv 1 \pmod{4} \), an integer \( m = \ell_1\ell_2 \) which is a product of two distinct primes \( \ell_1 \neq \ell_2 \) and real positive \( A, B, C \) and \( D \), we have

\[ \sum_{C \leq a \leq C+A} \sum_{D \leq b \leq D+B} \left( \frac{\Delta_n(a,b)}{m} \right) \ll \left( \frac{A}{m} + 1 \right) \left( \frac{B}{m} + 1 \right) m \log m. \]

4 Irreducibility

As in [9] we recall a very special case of a results of S. D. Cohen [1] about the distribution of irreducible polynomials over a finite field \( \mathbb{F}_q \) of \( q \) elements.

**Lemma 7.** For any prime \( p \), there are \( p^2/n + O(p^{3/2}) \) irreducible trinomials \( t^n + \alpha t + \beta \in \mathbb{F}_p[t] \).

5 Proof of Theorem 1

For a real number \( z \geq 1 \) we let \( \mathcal{L}_z \) be the set of primes \( \ell \in [z, 2z] \). For a positive integer \( k \) we write \( \omega(k) \) for the number of prime factors of \( k \).
We note that if \( k \geq 1 \) is a perfect square, then for \( z \geq 3 \),
\[
\sum_{\ell \in \mathcal{L}_z} \left( \frac{k}{\ell} \right) \geq \#\mathcal{L}_z - \omega(k),
\]
For each pair \((a, b)\), counted in \( T_n(A, B, C, D; s) \), we see that \( s\Delta_n(a, b) \) is a perfect square and that \( s \mid \Delta_n(a, b) \). Hence,
\[
\omega(s\Delta_n(a, b)) = \omega(\Delta_n(a, b)).
\]
Thus, for such \((a, b)\) we have
\[
\sum_{\ell \in \mathcal{L}_z} \left( \frac{s\Delta_n(a, b)}{\ell} \right) \geq \#\mathcal{L}_z - \omega_z(s\Delta_n(a, b)) = \#\mathcal{L}_z - \omega(\Delta_n(a, b)).
\]
Since \( \omega(k)! \leq k \), we see from the Stirling formula that
\[
\omega(k) \ll \frac{\log k}{\log \log k}.
\]
Thus
\[
\omega(\Delta_n(a, b)) \ll \frac{\log(A + B + C + D)}{\log \log(A + B + C + D)} \ll \frac{\log(ABCD)}{\log \log(ABCD)}.
\]
In particular, by the Cauchy inequality,
\[
(#\mathcal{L}_z)^2 T_n(A, B, C, D; s) \ll \sum_{C \leq a \leq C + A} \sum_{D \leq b \leq D + B} \left( \sum_{\ell \in \mathcal{L}_z} \left( \frac{s\Delta_n(a, b)}{\ell} + \omega(\Delta_n(a, b)) \right) \right)^2
\]
\[
\ll \sum_{C \leq a \leq C + A} \sum_{D \leq b \leq D + B} \left( \sum_{\ell \in \mathcal{L}_z} \left( \frac{s\Delta_n(a, b)}{\ell} \right) \right)^2 + AB \left( \frac{\log(ABCD)}{\log \log(ABCD)} \right)^2.
\]
We note that

\[
\sum_{C \leq a \leq C + A} \sum_{D \leq b \leq D + B} \left( \sum_{\ell \in \mathcal{L}_z} \left( \frac{s \Delta_n(a, b)}{\ell} \right) \right)^2
\]

\[
= \sum_{C \leq a \leq C + A} \sum_{D \leq b \leq D + B} \left( \frac{s}{\ell} \sum_{\ell \in \mathcal{L}_z} \left( \frac{\Delta_n(a, b)}{\ell} \right) \right)^2
\]

\[
\leq \sum_{C \leq a \leq C + A} \sum_{D \leq b \leq D + B} \left( \sum_{\ell \in \mathcal{L}_z} \left( \frac{\Delta_n(a, b)}{\ell} \right) \right)^2.
\]

Squaring out and changing the order of summation, we obtain

\[\left( \# \mathcal{L}_z \right)^2 T_n(A, B, C, D; s) \ll \sum_{\ell_1, \ell_2 \in \mathcal{L}_z} \sum_{C \leq a \leq C + A} \sum_{D \leq b \leq D + B} \left( \frac{\Delta_n(a, b)}{\ell_1 \ell_2} \right)\]

\[+ AB \left( \frac{\log(ABCD)}{\log \log(ABCD)} \right)^2.\]

We now estimate the double sum over \(a\) and \(b\) trivially as \(O(AB)\) on the “diagonal” \(\ell_1 = \ell_2\) and use Lemma 6 otherwise, getting

\[\left( \# \mathcal{L}_z \right)^2 T_n(A, B, C, D; s) \ll \# \mathcal{L}_z AB + \left( \# \mathcal{L}_z \right)^2 \left( \frac{A}{z^2} + 1 \right) \left( \frac{B}{z^2} + 1 \right) z^2 \log z\]

\[+ AB \left( \frac{\log(ABCD)}{\log \log(ABCD)} \right)^2.\]

By the prime number theorem we have \(\# \mathcal{L}_z \gg z/\log z\) so we derive from (3) that

\[T_n(A, B, C, D; s) \ll ABz^{-1} \log z + ABz^{-2} + A \log z + B \log z\]

\[+ z^2 \log z + ABz^{-2} \left( \frac{\log(ABCD)}{\log \log(ABCD)} \right)^2.\]

Clear the first term always dominates the second one, so the second term can be simply dropped. Thus taking \(z = (AB)^{1/3}\) to balance the terms \(ABz^{-1} \log z\) and \(z^2 \log z\), we obtain the desired estimate.
6 Proof of Theorem 2

Let $p_0$ be smallest prime for which there exists an irreducible trinomial

$$t^n + \alpha_0 t + \beta_0 \in \mathbb{F}_{p_0}[t]$$

($p_0$ exists by Lemma 7).

We now define the sets of integers

$$A = \{a \in [C, C + A] \cap \mathbb{Z} : a \equiv \alpha_0 \pmod{p_0}\};$$
$$B = \{b \in [D, D + B] \cap \mathbb{Z} : b \equiv \beta_0 \pmod{p_0}\}$$

(4)

Clearly

$$\#A \gg A \quad \text{and} \quad \#B \gg B$$

(5)

and every trinomials $t^n + at + b$ with $a \in A$, $b \in B$ is irreducible over $\mathbb{Z}$.

Using Theorem 1 to estimate the number of pairs $(a, b) \in A \times B$ for which $
\mathbb{Q}(\sqrt{-\Delta_n(a, b)})$ is a given quadratic field, we obtain the desired result.

7 Remarks

Similar results can be obtained for more general trinomials $t^n + at^m + b$ with fixed integers $n > m \geq 1$. Some properties of the Galois group of these trinomials have been studied in [2, 5, 10] where one can also find an explicit formula for their discriminant (which generalises (2)). In the case of $a = b = 1$ it becomes $(-1)^{(n-1)/2} (n^n - (-1)^n m^m (n - m)^{n-m})$. Studying arithmetic properties of this expression, for example, its square-free part, when $n$ and $m$ vary in the region $N \geq n > m \geq 1$ for a sufficiently large $N$, is a very challenging question.

References

[1] S. D. Cohen, ‘The distribution of polynomials over finite fields’, Acta Arith., 17 (1970), 255–271.

[2] S. D. Cohen, A. Movahhedi and A. Salinier, ‘Galois groups of trinomials’, J. Algebra, 222 (1999), 561–573.
[3] E. Fouvry and N. Katz, ‘A general stratification theorem for exponential sums, and applications’, *J. Reine Angew. Math.*, **540** (2001), 115-166.

[4] D. R. Heath-Brown, ‘The square sieve and consecutive squarefree numbers’, *Math. Ann.*, **266** (1984), 251–259.

[5] A. Hermez and A. Salinier, ‘Rational trinomials with the alternating group as Galois group’, *J. Number Theory*, **90** (2001), 113–129.

[6] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[7] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[8] F. Luca and I. E. Shparlinski, ‘Quadratic fields generated by polynomials’, *Archiv Math.*, (to appear).

[9] A. Mukhopadhyay, M. R. Murty and K. Srinivas, ‘Counting squarefree discriminants of trinomials under abc’, *Preprint*, 2008, (available from [http://arxiv.org/abs/0808.0418](http://arxiv.org/abs/0808.0418)).

[10] B. Plans and N. Vila, ‘Trinomial extensions of $\mathbb{Q}$ with ramification conditions’, *J. Number Theory*, **105** (2004), 387–400.