PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 10, October 2009, Pages 3219–3226
S 0002-9939(09)09831-1
Article electronically published on June 8, 2009

COUNTING SQUAREFREE DISCRIMINANTS OF TRINOMIALS UNDER ABC

ANIRBAN MUKHOPADHYAY, M. RAM MURTY, AND KOTYADA SRINIVAS

(Communicated by Wen-Ching Winnie Li)

Abstract. For an odd positive integer $n \geq 5$, assuming the truth of the *abc* conjecture, we show that for a positive proportion of pairs (a, b) of integers the trinomials of the form $t^n + at + b \quad (a, b \in \mathbb{Z})$ are irreducible and their discriminants are squarefree.

1. Introduction

Let D_f be the discriminant of the trinomial

$$f(t) = t^n + at + b \quad (a, b \in \mathbb{Z}), \tag{1}$$

where $\mathbb{Z}$ denotes the set of integers. For positive integers $A > 1, B > 1$ we define $\mathcal{M}_n(A, B)$ to be the set of (a, b) with $A \leq |a| \leq 2A$, $B \leq |b| \leq 2B$ such that $f(t)$ is irreducible and D_f is squarefree. Let $M_n(A, B) = \#\mathcal{M}_n(A, B)$. It is reasonable to expect that for A, B tending to infinity,

$$M_n(A, B) \sim c_n AB,$$

for some positive constant c_n. This is probably very difficult to prove. We will apply the *abc* conjecture to show that $M_n(A, B) \gg AB$. Recall that the *abc* conjecture, first formulated in 1985 by Oesterlé and Masser, is the following statement.

Fix $\epsilon > 0$. If a, b and c are coprime positive integers satisfying $a + b = c$, then

$$c \ll_\epsilon N(a, b, c)^{1+\epsilon},$$

where $N(a, b, c)$ is the product of distinct primes dividing abc.

Our main theorem is as follows:

Theorem 1. *Assume the truth of the abc conjecture. Let $n \geq 5$ be odd and $n \equiv 1 \bmod 4$. Let A be sufficiently large and $B > A^{1+\delta_0}$ for some fixed $\delta_0 > 0$. Then*

$$M_n(A, B) \gg AB,$$

where the implied constants may depend on n.

Received by the editors August 5, 2008.

2000 *Mathematics Subject Classification.* Primary 11R09; Secondary 11C08.

Key words and phrases. Irreducible polynomials, squarefree discriminants, quadratic extensions.

Remark. The cases $n = 2$ and $n = 3$ of the theorem can be treated without the use of the *abc* conjecture. Indeed, the case $n = 2$ reduces to counting the number of a, b with $a^2 - 4b$ squarefree. This question is answered in [6] as Theorem 3. The case $n = 3$ can be dealt with along the same lines. Indeed, first, one counts the number of such pairs (a, b) such that $4a^3 + 27b^2$ is squarefree. This is easily done by fixing a, using Theorem 3 of [6] and then summing over a. A cognate result is derived in [3]. The case $n = 4$ can be treated using the simple asymptotic sieve as in [5]. In this case, we essentially need to count how often $27a^4 + 256b^3$ is squarefree. Fixing a, we are reduced to determining how often the value of a cubic polynomial is squarefree. Following the method of Chapter 4 of [5], we easily derive the required result. An appropriate modification of this leads to an answer to the question under consideration. We leave the details to the reader.

Now we describe an application of the theorem. In [7], Osada showed that the Galois group of (1) is isomorphic to S_n provided

(1) $f(t)$ is irreducible over $\mathbb{Q}$,
(2) $((n-1)a, nb) = 1$.

Moreover, if K_f is the splitting field of $f(t)$ over $\mathbb{Q}$, then K_f is unramified at all finite primes over $\mathbb{Q}(\sqrt{D_f})$ with the alternating group A_n of degree n as the Galois group.

Using Theorem 1, we prove the following quantitative version of Osada's result.

Corollary 1. *Assume the truth of the abc conjecture. Let $n \geq 5$ be odd and $n \equiv 1 \bmod 4$. Also, let $\mathcal{N}_n(X)$ be the number of quadratic number fields of the form $\mathbb{Q}(\sqrt{D_f})$ with $|D_f| \leq X$ which has a Galois extension with Galois group A_n and is unramified at all finite primes. Then for large X,*

$$\mathcal{N}_n(X) \gg X^{\frac{1}{n}+\frac{1}{n-1}},$$

where the implied constant may depend on n.

In order to prove the theorem we need to count irreducible polynomials with squarefree discriminants. In section 2, we show that almost all polynomials of the specific form under consideration are irreducible. In section 3, we show that a positive proportion of the polynomials have squarefree discriminants. Sections 4 and 5 provide the technical details needed in section 3. The last section contains the conclusion of the proof.

2. Counting irreducible polynomials

We start with a result due to S. D. Cohen [4] regarding the number of irreducible polynomials of a certain form over finite fields. Before stating it we need to introduce some notation. For a fixed prime p, let $g(t), h(t)$ be monic, relatively prime polynomials in $\mathbb{F}_p[t]$ satisfying

$$n = \deg g > \deg h \geq 0$$

and

$$g(t)/h(t) \neq g_1(t^p)/h_1(t^p), \text{ for any } g_1(t), h_1(t) \in \mathbb{F}_p[t].$$

Let L be the splitting field of $Q(y) = g(t) - yh(t) \in \mathbb{F}_p[t][y]$ over $\mathbb{F}_p(y)$ and G be its Galois group. Let $\mathbb{F}_{p^f}$ be the maximal algebraic extension of $\mathbb{F}_p$ in L. For any $\sigma \in G$, let L_σ denote the subfield of L fixed by σ. We define

$$G^* = \left\{\sigma \in G \mid L_\sigma \cap \mathbb{F}_{p^f} = \mathbb{F}_p\right\}.$$

We consider G to be a subgroup of S_n. Let $G_n = \{\sigma \in G \mid \sigma \text{ is an } n\text{-cycle}\}$ and $G_n^* = G^* \cap G_n$. We define $\pi(g,h)$ to be the number of irreducible polynomials of the form $hP(g/h)$, where P is a linear monic polynomial in $\mathbb{F}_p[t]$. Now we state a particular case of Theorem 3 in [4].

Lemma 1.

$$\pi(g,h) = \frac{|G_n^*|}{|G^*|}p + O(\sqrt{p}).$$

For a fixed $a \in \mathbb{F}_p$, let $g_a(t) = t^n + at$. For $g = g_a$ and $h = 1$, we get from [1] that

$$G = G^* = S_n$$

whenever $(p, 2n(n-1)) = 1$. Also

$$\frac{|G_n^*|}{|G^*|} = \frac{1}{n}.$$

Hence from Lemma 1, we have

$$\pi(g_a, 1) = \frac{p}{n} + O(\sqrt{p}). \tag{2}$$

Clearly, for a fixed $a \in \mathbb{F}_p$, $\pi(g_a, 1)$ is the number of irreducible polynomials of the form $t^n + at + b$ with $b \in \mathbb{F}_p$.

For a prime p we define $\mathcal{S}_p$ and $\mathcal{T}_p$ as follows:

$$\mathcal{S}_p = \left\{(a,b) \in (\mathbb{F}_p)^2 \mid t^n + at + b \text{ is reducible over } \mathbb{F}_p\right\},$$
$$\mathcal{T}_p = \left\{(a,b) \in (\mathbb{F}_p)^2 \mid t^n + at + b \text{ is irreducible over } \mathbb{F}_p\right\},$$

and let $s_p = |\mathcal{S}_p|$ and $t_p = |\mathcal{T}_p|$. From (2), varying over $a \in \mathbb{F}_p$, we get the following lemma estimating t_p.

Lemma 2. *If p does not divide $2n(n-1)$, then*

$$t_p = \frac{p^2}{n} + O(p^{3/2}).$$

Now we introduce the following notation:

$$\mathcal{T}(A,B) = \left\{(a,b) \in \mathbb{Z}^2 \mid t^n + at + b \text{ is irreducible}, \ A \le |a| \le 2A, B \le |b| \le 2B\right\}.$$

The proof of the following proposition estimating the cardinality of $\mathcal{T}(A,B)$, closely follows the method outlined in exercise no. 12, page 169 of [2].

Proposition 1.

$$|\mathcal{T}(A,B)| = AB + o(AB).$$

Proof. We observe that $s_p + t_p = p^2$. So, from Lemma 2, we get

$$s_p = p^2\left(1 - \frac{1}{n}\right) + O(p^{3/2}).$$

For a squarefree integer d, let

$$\phi_d : \mathbb{Z}^2 \to (\mathbb{Z}/d\mathbb{Z})^2$$

be the reduction modulo d. Let

$$H \subset \left\{(a,b) \in \mathbb{Z}^2 \mid A \le |a| \le 2A, \ B \le |b| \le 2B\right\}$$

and H_d be the image of H under ϕ_d. The number of elements of H which are mapped to the same element of $(\mathbb{Z}/d\mathbb{Z})^2$ under ϕ_d does not exceed $([2A/d]+1)([2B/d]+1)$. We deduce

$$\begin{aligned} |H| &\leq |H_d|([2A/d]+1)([2B/d]+1) \\ &\ll \frac{|H_d|}{d^2}AB \\ &\ll \left(\prod_{p|d}\frac{|H_p|}{p^2}\right)AB. \end{aligned}$$

Now we set

$$H=\left\{(a,b)\in\mathbb{Z}^2|\ t^n+at+b \text{ is reducible, with } A\leq|a|\leq 2A, B\leq|b|\leq 2B\right\}.$$

Then $H_p\subset\mathcal{S}_p$ for each prime p. From above, we have

$$|H|\ll\left(\prod_{p|d}\frac{s_p}{p^2}\right)AB\ll\prod_{p|d}\left(1-\frac{1}{n}\right)AB.$$

For $\epsilon>0$, we choose $m>1$ such that

$$\left(1-\frac{1}{n}\right)^m<\epsilon.$$

Let $p_1,p_2,\ldots,p_m$ be the first m primes not dividing $2n(n-1)$. By choosing $d=p_1\cdots p_m$, we get

$$|H|\ll\epsilon AB.$$

Hence the proposition follows. □

Corollary 1 is the quantitative version of the following result due to Osada (see Corollary 2, [7]).

Let K_f be the splitting field of $f(t)$ over $\mathbb{Q}$ and G be the Galois group $Gal(K_f/\mathbb{Q})$.

Lemma 3. *Let $f(t)=t^n+at+b$ be a polynomial in $\mathbb{Z}[t]$, where $a=a_0c^n$ and $b=b_0c^n$ for some integer c. Then the Galois group G is isomorphic to S_n if the following conditions are satisfied:*

(1) *$f(t)$ is irreducible over $\mathbb{Q}$;*
(2) *$(a_0c(n-1),nb_0)=1$.*

Moreover, $K/\mathbb{Q}(\sqrt{D_f})$ is unramified at all finite places.

3. Counting squarefree discriminants

Let $T(a,b)=(n-1)^{n-1}a^n+n^nb^{n-1}$ for integers a,b. For $n\equiv 1 \bmod 4$, we observe that discriminant $D_f=T(a,b)$. For sufficiently large positive real numbers A,B, let $D(A,B)$ be the number of squarefree integers d with at least one solution to

$$d=T(a,b),\ \text{where } A\leq|a|\leq 2A, B\leq|b|\leq 2B \tag{3}$$

and $((n-1)a,nb)=1$. Using ideas from [8] we now find a lower bound for $D(A,B)$. For a squarefree number d, let $R_0(d)$ denote the number of solutions to (3). We have

Lemma 4.

$$\sum_d R_0(d) \gg AB.$$

Lemma 5.

$$\sum_d R_0(d)^2 \ll AB.$$

The proofs of these two lemmas will be presented in the next section. Assuming them, we are ready to prove the following result giving a lower bound for $D(A,B)$.

Proposition 2.

$$D(A,B) \gg AB.$$

Proof. By the Cauchy-Schwarz inequality,

$$D(A,B) \geq \left(\sum_d R_0(d)\right)^2 \left(\sum_d R_0(d)^2\right)^{-1}.$$

Hence the result follows by Lemmas 4 and 5. □

4. Proof of Lemma 4

We define a new polynomial $H(a,b) = T(a,b)T(-a,b)$. Let $\mathcal{M}_1$ be the set of pairs (a,b) of integers with $A \leq a \leq 2A$ and $B \leq |b| \leq 2B$ such that $H(a,b)$ is not divisible by the square of any prime $p \leq \log B$. We put $M_1 = \#\mathcal{M}_1$ and $P = \prod_{p \leq \log B} p$. We observe that $\sum_{l^2 | (\alpha, P^2)} \mu(l) = 1$ or 0 depending on whether $p^2 \nmid \alpha$ for all $p \leq \log B$ or not. Thus

$$M_1 = \sum_{A \leq a \leq 2A} \sum_{B \leq |b| \leq 2B} \sum_{l^2 | (H(a,b), P^2)} \mu(l) = \sum_{A \leq a \leq 2A} \sum_{l | P} \mu(l) \sum_{\substack{B \leq |b| \leq 2B \\ H(a,b) \equiv 0 \bmod l^2}} 1. \tag{4}$$

Let

$$\rho_a(p) = |\{b \bmod p \mid H(a,b) \equiv 0 \bmod p\}|.$$

Clearly $\rho_a(l)$ is a multiplicative function of l. For a prime $p \nmid an(n-1)$ and an integer $\alpha \geq 1$,

$$\rho_a(p^\alpha) = \rho_a(p) \leq 2n-2.$$

We divide the sum over b in (4) into intervals of length l^2. We see that this sum is

$$2B\rho_a(l^2)/l^2 + O(\rho_a(l^2)).$$

Thus,

$$\begin{aligned}
&\sum_{l|P}\mu(l) \sum_{\substack{B\le|b|\le 2B\\ H(a,b)\equiv 0 \bmod l^2}} 1\\
&= 2B\sum_{l|P}\mu(l)\frac{\rho_a(l^2)}{l^2} + O(\sum_{l|P}\mu(l)\rho_a(l^2))\\
&= 2B\prod_{p|P}\left(1-\frac{\rho_a(p)}{p^2}\right) + O(\tau(P))\\
&= 2B\exp\left(-\sum_{p}\frac{\rho_a(p)}{p^2} + O\left(\sum_{p>\log B}\frac{1}{p^2}\right)\right) + O(B^{\epsilon})\\
&= 2cB + o(B) \text{ (for some constant } c>0),
\end{aligned}$$

where $\tau(\alpha)$ denotes the divisor function, and we use the observation that $P \asymp B$. Summing over all choices of a, we get from (4):

$$M_1 = 2cAB + o(AB) \text{ (for some constant } c > 0).$$

Let $\mathcal{M}_2$ be the set of pairs (a,b), $A \le a \le 2A$ and $B \le |b| \le 2B$ such that $H(a,b)$ is divisible by the square of a prime $p \in (\log B, B]$. Also let $M_2 = \#\mathcal{M}_2$. Then

$$\begin{aligned}
M_2 &= \sum_{A\le a\le 2A}\sum_{\log B<p\le B}\sum_{\substack{B\le|b|\le 2B\\ H(a,b)\equiv 0 \bmod p^2}} 1\\
&= 2B\sum_{A\le a\le 2A}\sum_{\log B<p\le B}\frac{\rho_a(p^2)}{p^2} + O\left(\sum_{A\le a\le 2A}\sum_{\log B<p\le B}\rho_a(p^2)\right).
\end{aligned}$$

The first term is

$$\ll AB\sum_{p>\log B}\frac{1}{p^2} \ll \frac{AB}{\log B} = o(AB).$$

The O-term is estimated as

$$\ll A\sum_{\log B<p\le B} 1 \ll \frac{AB}{\log B} = o(AB).$$

Then $\mathcal{M}_1 \setminus \mathcal{M}_2$ is the set of pairs (a,b), $A \le a \le 2A$ and $B \le |b| \le 2B$, such that both $T(a,b)$ and $T(-a,b)$ are not divisible by the square of a prime $p \le B$. We observe that $\#(\mathcal{M}_1 \setminus \mathcal{M}_2) \ge M_1 - M_2$.

We call a pair (a,b) "good" if $T(a,b)$ is not divisible by the square of a prime $p > B$; otherwise (a,b) is called "bad".

Now we claim that (a,b) and $(-a,b)$ cannot both be bad. Suppose both are bad. Then there are primes $p, q > B$ such that

$$T(a,b) = p^2 d_1, \quad T(-a,b) = q^2 d_2.$$

Since n is odd we get by multiplying that

$$T(a,b)T(-a,b) = n^{2n}b^{2(n-1)} - (n-1)^{2(n-1)}a^{2n} = p^2q^2d_1d_2. \tag{5}$$

If $p = q$, then p divides $T(a, b) + T(-a, b)$ implying $p \leq B$, a contradiction. Thus p, q are distinct. Using the *abc* conjecture on the equation (5), we get for any $\epsilon > 0$,

$$pq \ll (AB)^{1+\epsilon},$$

which is a contradiction, as p, q both are $> B$ and $B > A^{1+\delta_0}$ for a fixed $\delta_0 > 0$.

Hence among the pairs in $\mathcal{M}_1 \setminus \mathcal{M}_2$, half of them are good, and hence squarefree, as they are not divisible by the square of a prime $\leq B$. Thus

$$\sum_{d \leq X} R_0(d) \geq \frac{1}{2}(M_1 - M_2) \gg AB.$$

This completes the proof. □

5. Proof of Lemma 5

Let a_1, a_2 be in $[-2A, -A] \cup [A, 2A]$ and b_1, b_2 be in $[-2B, -B] \cup [B, 2B]$. Then $\sum_{d \leq X} R_0(d)(R_0(d) - 1)$ is bounded by the number of (a_1, a_2, b_1, b_2) with $(a_1, b_1) \neq (a_2, b_2)$ and $T(a_1, b_1) = T(a_2, b_2)$. Then

$$(n-1)^{n-1} a_1^n + n^n b_1^{n-1} = (n-1)^{n-1} a_2^n + n^n b_2^{n-1},$$

which implies that

$$(n-1)^{n-1}(a_1^n - a_2^n) = n^n (b_2^{n-1} - b_1^{n-1}).$$

Thus, for fixed (a_1, a_2), the number of possible b_1 and b_2 is $\ll X^\epsilon$. Hence

$$\sum_{d \leq X} R_0(d)(R_0(d) - 1) \ll X^\epsilon A^2.$$

Therefore, we have

$$\sum_{d \leq X} R_0(d)^2 \ll X^\epsilon A^2 + AB \ll AB,$$

completing the proof of Lemma 5.

6. Proof of the theorem and the corollary

Let $\mathcal{D}(A, B)$ be the set of (a, b)'s chosen exactly one for each d counted in $D(A, B)$. Thus $D(A, B) = |\mathcal{D}(A, B)|$. Clearly

$$\mathcal{T}(A, B) \cap \mathcal{D}(A, B) \subset \mathcal{M}(A, B).$$

Hence the theorem follows from Propositions 1 and 2.

The corollary is a direct consequence of the theorem with $A = X^{1/n}/(4n)$ and $B = X^{1/(n-1)}/(4n^2)$ and Lemma 3 with $c = 1$.

Acknowledgements

We thank D. Suryaramana for indicating the proof of Proposition 1. We also thank R. Balasubramanian for some useful discussions. Finally, we thank the referee for carefully reading the manuscript.

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer: Note on a problem of Chowla, *Acta Arith.*, **5** (1959), 417-423. MR0113844 (22:4675)

[2] N. Bourbaki: *Algebra II*, Chapter 5, Springer-Verlag, Berlin, 2003. MR1994218

[3] K. Chakraborty and M. Ram Murty, On the number of real quadratic fields with class number divisible by 3, *Proc. Amer. Math. Soc.*, **131** (2003), no. 1, 41-44. MR1929021 (2003m:11184)

[4] S. D. Cohen: The distribution of polynomials over finite fields, *Acta Arith.*, **17** (1970), 255-271. MR0277501 (43:3234)

[5] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge University Press, 1976. MR0404173 (53:7976)

[6] M. Ram Murty: Exponents of class groups of quadratic fields, *Topics in Number Theory* (University Park, PA, 1997), Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999, 229–239. MR1691322 (2000b:11123)

[7] H. Osada: The Galois groups of the polynomials $X^n + aX^l + b$, *J. Number Theory*, **25** (1987), 230–238. MR873881 (88c:11059)

[8] K. Soundararajan: Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc.*, **61** (2000), no. 2, 681–690. MR1766097 (2001i:11128)

Institute of Mathematical Sciences, CIT Campus, Tharamani, Chennai 600 113, India
E-mail address: anirban@imsc.res.in

Department of Mathematics and Statistics, Jeffery Hall, Queen's University, Kingston, Ontario, K7L 3N6, Canada
E-mail address: murty@mast.queensu.ca

Institute of Mathematical Sciences, CIT Campus, Tharamani, Chennai 600 113, India
E-mail address: srini@imsc.res.in