Improved upper bound for the number of cubic polynomials and certain types of trinomials with affect

Project for the PennState-Göttingen International Summer School in Mathematics 2012

Abel Castillo, Alex Henniges, Tanja Schindler

November 30, 2012
1 Galois groups of cubics

We consider a cubic polynomial $ax^3 + bx^2 + cx + d$ with $a, b, c, d \in \mathbb{Z}$. The polynomial is said to be with affect if the Galois group of its splitting field is a proper subgroup of $S_3$, the permutation group with 3 elements. We improve the upper bound for the number of such polynomials with bounded coefficients which is given by Lefton [Lef79]. The improvement is basically done by using a better estimation of the divisor function $\tau$.

**Lemma 1.1.** For integers $m, d$ where $d$ is not a perfect square, the number of integer solutions $(x, y)$ with $x, y \leq M$ satisfying

\[ x^2 - dy^2 = m \]  

is $\ll m^{(2+\epsilon) \log 2 / \log \log m}$ for $d < 0$ and $\ll m^{(2+\epsilon) \log 2 / \log \log m} \log (Md)$ for $d \geq 0$.

**Proof.** We can assume that $d$ is squarefree, otherwise we absorb any squares in $y$. Let $K = \mathbb{Q}(\sqrt{d})$. If $a^2 - db^2 = m$ and

\[ \alpha = a + b\sqrt{d} \]  

then the norm satisfies $N_{K/\mathbb{Q}}(\alpha) = m = \alpha \bar{\alpha}$ where $\bar{\alpha}$ denotes the conjugate of $\alpha$. We want to estimate the number of such ideals.

We observe, as in [Nar90, p. 243] that the number of ideals in $O_K$ with norm $n$, which we denote by $F(n)$, is less than or equal to $d_N(n)$, which denotes the number of factorizations of $n$ into $N$ factors that are not units, taking order into account. This can be estimated by $\tau(n)^N$, where $\tau$ denotes the number of distinct divisors of $n$. In our case, since we are looking at a quadratic extension of $\mathbb{Q}$, we have $N = 2$.

Since the number of the ideals we are looking for is a subset of this, we get that $F(a) \leq \tau(a)^2$. By [Apo98, p.294], and a simple redefinition of $\epsilon$, we have that

\[ d_2(n) < n^{(2+\epsilon) \log 2 / \log \log n} \]

for $n$ sufficiently large. Hence, $F(a) \ll a^{(2+\epsilon) \log 2 / \log \log a}$. In the next steps we will estimate the number of generators in (2) such that $a, b \in \mathbb{Z}$ are bounded by $M$. We consider three cases:

1. $d < 0$: As a consequence of Dirichlet’s unit theorem we have that since $K$ is a imaginary quadratic field the number of units is finite and hence, the number of generators for each principal ideal is also finite.
To be precise, for any primitive $k$-th root of unity, if $k > 3$ and $k \neq 6$, then this primitive root of unity generates an extension of $\mathbb{Q}$ of degree greater than 2, and cannot be contained in our quadratic extension. Therefore, there are at most $\ll \varepsilon^\frac{(2+\varepsilon)\log 2}{\log \log m}$ solutions to (1).

2. $d = 1$: We count the solutions $(x, y)$ for the equation $m = x^2 - y^2 = (x - y)(x + y)$. This is a factorisation of $m$ into two factors, and the number of factorisations of $m$ into two factors equals $d_2(m)$. Therefore, we obtain that the number of solutions is $\ll d_2(m) \ll \varepsilon^\frac{(2+\varepsilon)\log 2}{\log \log m}$. The number of solutions $(x, y)$ satisfying (1) is therefore $\ll \varepsilon^\frac{(2+\varepsilon)\log 2}{\log \log m}$.

3. $d > 1$: Since $\alpha \bar{\alpha} = m$ we have that $|\alpha| \leq M \left(1 + \sqrt{d}\right)$ and $|\bar{\alpha}| \leq M \left(1 + \sqrt{d}\right)$. Since $|\alpha| |\bar{\alpha}| \geq m \geq 1$ it follows that

$$\frac{1}{M \left(1 + \sqrt{d}\right)} \leq |\alpha| \leq M \left(1 + \sqrt{d}\right)$$

and by taking the logarithm

$$|\log |\alpha|| \leq \log \left(M \left(1 + \sqrt{d}\right)\right). \tag{3}$$

If $\alpha_0$ is a generator of (2) then $\alpha_\nu := \eta^\nu \alpha_0$ with $\eta$ a fundamental unit of $K$ is a generator as well. Hence, we get from (3) that

$$|\log |\eta^\nu \alpha_0|| \leq |\nu \log \eta + \log |\alpha_0|| \leq M \left(1 + \sqrt{d}\right)$$
or

$$|\nu + \frac{\log |\alpha_0|}{\log \eta}| \leq \frac{M \left(1 + \sqrt{d}\right)}{\log \eta}.$$

Therefore, $\nu$ belongs to an interval of length $\leq \log(Md)/\log \eta$. By Proposition 1 of [Lef79] $\eta > 1$ and thus we obtain the statement of the lemma.

\[\square\]

**Lemma 1.2.** Let $Q(x, y)$ be a quadratic polynomial with integer coefficients bounded by $N$ and nonsquare discriminant. Then the number of all integer solutions of $Q(x, y) = 0$ such that $|x|, |y| \leq M$ is $\ll \varepsilon^\frac{(8+\varepsilon)\log 2}{\log \log N} \log (MN^4)$. 

2
Proof. We can write $Q(x, y) := ax^2 + bxy + cy^2 + dx + ey + f$. If we substitute $x' := -Dy + 2ae - bd$ and $y' := 2ax + by + d$ with $D := b^2 - 4ac$ and $m' := -D(d^2 - 4af) + (2ae + bd)^2$ then the condition $Q(x, y) = 0$ is equivalent to

$$x'^2 - Dy'^2 = m'. \quad (4)$$

Each solution $(x, y)$ with $|x|, |y| \leq M$ gives a solution $(x', y')$ for (4) such that $|x'|, |y'| \ll MN^2$. This follows from the definition of $x', y'$ and the boundedness of the coefficients. By Lemma 1.1 (note that $D$ is not a perfect square by assumption), the number of such integer solutions of (4) is $\ll m \left( 2 + \epsilon \right) \frac{\log 2}{\log \log m} \log (MN^2 D)$. Furthermore, $D \ll N^2$ and $m \ll N^4$. Hence, the number of integer solutions of (4) is $\ll \epsilon N \left( \frac{8+\epsilon}{\log \log N} \log (M N^2) \right) \log (M N^4)$. Redefining $\epsilon$ this is $\ll \epsilon N \left( \frac{8+\epsilon}{\log \log N} \log (M N) \right)$. \hfill \Box

**Theorem 1.3.** Let $I(N)$ be the number of irreducible polynomials $f(x) = ax^3 + bx^2 + cx + d$ with integer coefficients, bounded in absolute value by $N$, $N \geq 1$, with affect. Then

$$I(N) \ll N^{3+\left(\frac{8+\epsilon}{\log \log N}\right)}.$$

Proof. Following the considerations of Theorem 1 in [Lef79] it suffices to count the solutions in $a, b, c, d$ and $z$ fulfilling the equation

$$27a^2d^2 + (4b^3 - 18abc) d + 4ac^3 - b^2c^2 + z^2 = 0 \quad (5)$$

where $|a|, |b|, |c|, |d| < N$ If we fix $a, b, c$, then (5) is a quadratic equation in $d$ and $z$. Since $a, b, c$ are bounded by $N$ the coefficients of that quadratic equation are bounded by $N^4$. Furthermore, $|d| \leq N$ implies $z^2 \ll N^4$ and hence $z \ll N^2$. In addition, $D = 0 - 4(27a^2)$ is not a square. By Lemma 1.2 the number of integers $(d, z)$ satisfying (5) is $\ll \epsilon N \left( \frac{8+\epsilon}{\log \log N} \log (N \cdot N^2) \right) \ll \epsilon N \left( \frac{8+\epsilon}{\log \log N} \log N \log N \right) \ll \epsilon N \left( \frac{8+\epsilon}{\log \log N} \log N \right)$ A redefinition of $\epsilon$ gives $\ll \epsilon N \left( \frac{8+\epsilon}{\log \log N} \log N \right)$. Summing over $|a|, |b|, |c|$ we get

$$I(N) \ll \epsilon \sum_{|a|, |b|, |c| \leq N} N \left( \frac{8+\epsilon}{\log \log N} \log N \right) = N^{3+\left(\frac{8+\epsilon}{\log \log N}\right)}.$$

\hfill \Box

**Theorem 1.4.** Let $E_n$ denote the number of monic $n$th degree polynomials with affect with integer coefficients bounded in absolute value by $N$. Then for each $\epsilon > 0$ we have

$$E_3(N) \ll \epsilon N^{2+\left(\frac{8+\epsilon}{\log \log N}\right)}.$$
Proof. By [vdW36] we have that the number of reducible polynomials with coefficients bounded in absolute value by \(N\) is \(\ll N^2\). Hence, the number of these polynomials is negligible. With the same argumentation as in Theorem 1.3 the Galois group of the splitting field of the polynomial is a subgroup of \(A_3\).

Setting \(a = 1\) in the proof of Theorem 1.3 we get the result.

\[\Box\]

2 Galois groups of Trinomials of the form \(ax^n + bx^k + c\)

In the following section we consider polynomials \(f(x) = ax^n + bx^k + c\) with \(a \neq 0\) and \(n > k > 0\) which fulfill the following properties:

1. \(a, b, c \in \mathbb{Z}\) and \(|a|, |b|, |c| \leq M\) for \(M \geq 1\).

2. The Galois group of the splitting field of \(f(x)\) is a proper subgroup of the alternating group of degree \(n\).

We define \(J_{n,k}\) as the number of polynomials fulfilling the above properties. Using the same techniques as for the cubics we can derive the following statement:

**Theorem 2.1.**

\[J_{n,k} \ll N, \epsilon M^{2+ \frac{(N+1)(1+\epsilon) \log 2}{\log \log d}}\]

where \(N := n/(k,n)\).

**Proof.** We first assume that neither \(a\), \(b\) nor \(c\) equal zero since the number of such trinomials with at least one of the coefficients equal to zero is \(\ll M^2\). We use as in Lefton [Lef79, 3.1] the discriminant formula for the above trinomial with \(a \neq 0\), \(n > k > 0\):

\[D_f = (-1)^{\frac{1}{2}(n(n-1))} a^{n-k-1} c^{k-1} \left( n^N a^K c^{N-K} + (-1)^{N-1} (n-k)^{N-K} k^K b^N \right)^d\]

where \(d := (n,k), N := n/d\), and \(K := k/d\). We can summarize this formula as

\[D_f = (-1)^{\frac{1}{2}(n(n-1))} a^{n-k-1} c^{k-1} E^d\]

with

\[E := n^N a^K c^{N-K} + (-1)^{N-1} (n-k)^{N-K} k^K b^N.\]

We consider two cases:
1. \(d\) odd. In that case there exists \(F \in \mathbb{Z}[a, b, c]\) such that
\[
F^{-2}D_f = \pm a^{N-K-1}c^{K-1}E. \tag{8}
\]
Since under the hypothesis that the Galois group of \(f(x) = 0\) is a subgroup of the alternating group it follows that \(D_f\) is the square of a rational integer, see [Jac51, p. 91]. Hence, the right hand side of (8) is also a square.

(a) \(n\) even, \(k\) odd: Hence, \(N\) even and \(K\) odd. It follows that there exists \(F \in \mathbb{Z}[a, b, c]\) such that \(E = \pm z^2\) for some \(z \in \mathbb{Z}\). Applying (7) this becomes
\[
\pm n^N a^K c^{N-K} = z^2 \pm (n - k)^{N-K} k^K \left(\frac{b^{N/2}}{2}\right)^2.
\]
with \(\pm = (1/N)\). If we fix \(a\) and \(c\) we can apply Lemma 1.1, since \(x = z\) and \(y = b^{N/2}\) are integer solutions of \(m = x^2 - dy^2\) where \(m = \pm n^N a^K c^{N-K}\) and \(d = \mp (n - k)^{N-K} k^K\). The number of such integers is \(\ll N, \varepsilon M^{N(1+\varepsilon) \log 2 \log \log M} N \log M\), i.e. \(\ll N, \varepsilon M^{N(1+\varepsilon) \log 2 \log \log M} \) for some \(\varepsilon' > \varepsilon\). Hence, there are \(\ll N, \varepsilon M^{N(1+\varepsilon) \log 2 \log \log M} \) solutions for the triple \((a, b, c)\).

(b) \(n\) odd, \(k\) even: Hence, \(N\) odd and \(K\) even. Analogously to (a) it follows that \(\pm cE = z^2\) for some \(z \in \mathbb{Z}\). By (7) this can also be written as
\[
\pm (n - k)^{N-K} k^K b^N c = z^2 \mp n^N c^{N-K+1} \left(\frac{a^{K/2}}{2}\right)^2
\]
where \(\pm = (1/N-1)\). If we fix \(b\) and \(c\) we can see that \(x = z\) and \(y = a^{K/2}\) are integer solutions of \(m = x^2 - dy^2\) with \(m = \pm (n - k)^{N-K} k^K b^N c\) and \(d = \mp n^N c^{N-K+1}\). By Lemma 1.1 we obtain analogously as in (a) that the number of integer solutions is \(\ll N, \varepsilon M^{N(1+\varepsilon) \log 2 \log \log M} \).

(c) \(n\) odd, \(k\) odd: We can conclude from (6) that the discriminants of \(f(x) = ax^n + bx^k + c\) and \(g(x) = cx^n + bx^{n-k} + a\) are equal. In that case \(n - k\) is odd and we can apply (b) to \(g(x)\).

2. \(d\) even. In that case there exists \(F \in \mathbb{Z}[a, b, c]\) such that
\[
F^{-2}D_f = \pm ac.
\]
since in that case \( n - k - 1 \) and \( k - 1 \) are even. With an analogous argumentation as in case 1 we get that

\[
(a + c)^2 - (a - c)^2 = 4ac = \pm 4z^2.
\]

Fixing \( a - c \) we can apply Lemma 1.1: \( a + c \) and \( a - c \) are bounded by \( 2M \) and since \( z^2 = ac \) we conclude that \( z \) is also bounded by \( M \). Hence, there \( \ll \epsilon M^{\frac{2(1+\epsilon)\log 2}{\log \log M}} \) values for \( a - c \). Hence, there are \( \ll \epsilon M^{1+\frac{2(1+\epsilon)\log 2}{\log \log M}} \) values for the tuple \( (a, c) \) and \( \ll \epsilon M^{2+\frac{2(1+\epsilon)\log 2}{\log \log M}} \) values for the triple \( (a, b, c) \).

The maximal bound for \( J_{n,k} \) of these cases is \( \ll \epsilon, N M^{2+\frac{N+1}{2}(1+\epsilon)\log 2}{\log \log M} \).

\[ \square \]

References


