On the least non-residue of a quartic polynomial

BY KENNETH S. WILLIAMS

University of Manchester

(Received 29 November 1965)

Let \( p \) be a prime and let \( f(x) \) be a quartic polynomial with integral coefficients. I consider the problem of estimating the least non-negative non-residue \( k \) of \( f(x) \pmod{p} \) (I omit the mod \( p \) hereafter), for large primes \( p \), so \( f(x) \equiv r \) has a solution for

\[
    r = 0, 1, \ldots, k-1
\]

but not for \( r = k \). The same problem for cubics has been considered by Mordell (1), who showed that

\[
    k = O(p^{\frac{1}{5}}(\log p)^2), \tag{1}
\]

as \( p \to \infty \), where the constant implied in the \( O \)-symbol is independent of the coefficients of the cubic. In fact a more detailed examination of Mordell's proof gives the better estimate

\[
    k = O(p^{\frac{1}{4}}(\log p)). \tag{2}
\]

It is the purpose of this paper to show that this same estimate also holds for quartic polynomials.

Without any loss of generality we may take \( f(x) \) as

\[
    f(x) = ax^4 + cx^2 + dx + e. \tag{3}
\]

Denote by \( N_r \) the number of solutions of \( f(x) \equiv r \). Then \( N_r = 1, 2, 3, 4 \) for \( 0 \leq r \leq k-1 \) and \( N_k = 0 \). Suppose that \( N_r = 1, 2, 3, 4 \) occurs for \( n_1, n_2, n_3, n_4 \) values of \( r \) respectively. Then

\[
    n_1 + n_2 + n_3 + n_4 = k. \tag{4}
\]

Taking the special case \( n = 4 \) in Mordell's paper (1, equation (8)) we have

\[
    \sum_{r=0}^{k} N_r \leq k + 1 + 4p^{\frac{1}{4}} \log p
\]

and so

\[
    n_1 + 2n_2 + 3n_3 + 4n_4 \leq k + 1 + 4p^{\frac{1}{4}} \log p. \tag{5}
\]

Hence from (4) and (5) we obtain

\[
    k \leq 1 + 4p^{\frac{1}{4}} \log p + n_1. \tag{6}
\]

Thus to obtain an upper bound for \( k \) we require only a suitable estimate for \( n_1 \).

Let \( D(r) \) denote the discriminant of \( f(x) - r \). Then we have

\[
    D(r) = Ar^2 + Br^2 + Cr + D, \tag{7}
\]

where

\[
    A = -256a^3, \\
    B = 128a^2(6ac - c^2), \\
    C = 16a(16ac^2e - c^4 - 48a^2e^2 - 9acd^2), \\
    D = a(256a^2c^3 - 128a^2e^2 + 16c^4e - 27ad^4 + 144acd^2e - 4c^2d^2).
\]
Divide the integers \( r \) satisfying \( 0 \leq r \leq k-1 \) into 2 classes according as \( p \nmid D(r) \) or \( p | D(r) \). We call the second class the exceptional values of \( r \). As \( D(r) \) is a cubic in \( r \) there are at most 3 exceptional integers \( r \). For \( i = 0, 1, 2, 3, 4 \), we let \( l_i \) denote the number of non-exceptional \( r \) such that \( f(x) \equiv r \) has exactly \( i \) solutions and \( m_i \) the number of exceptional \( r \) such that \( f(x) \equiv r \) has exactly \( i \) solutions. Then

\[
\begin{align*}
  n_i &= l_i + m_i \quad (i = 0, 1, 2, 3, 4), \\
  l_0 &= m_0 = 0, \\
  m_4 &= 0, \\
  m_1 + m_2 + m_3 &\leq 3.
\end{align*}
\]

(8)

By a result of Stickelberger (3), for non-exceptional \( r \),

\[
\left( \frac{D(r)}{p} \right) = (-1)^{4-v_r},
\]

where \( v_r \) denotes the number of irreducible factors \( \text{mod} \ p \) of \( f(x) - r \). Hence \( f(x) \equiv r \), for any non-exceptional \( r \), has exactly 1 or 4 solutions if and only if

\[
\left( \frac{D(r)}{p} \right) = +1.
\]

(9)

Hence

\[
l_1 + l_4 = \text{number of non-exceptional } r \text{ with } \left( \frac{D(r)}{p} \right) = 1
\]

\[
= \text{number of } r \text{ with } \left( \frac{D(r)}{p} \right) = 1,
\]

and so using (8) we have

\[
n_1 \leq m + 3,
\]

(10)

where \( m \) denotes the number of \( r \) satisfying \( 0 \leq r \leq k-1 \) with \( (D(r)/p) = +1 \). As \( (D(r)/p) = +1 \) or \(-1\) except for at most three values of \( r \) we have

\[
m = \frac{1}{2} \left[ \sum_{r=0}^{k-1} \left( \frac{D(r)}{p} \right) + 1 \right] \frac{1}{2} z,
\]

(11)

where

\[
0 \leq z \leq 3.
\]

(12)

Let

\[
A = \sum_{r=0}^{k-1} \left( \frac{D(r)}{p} \right).
\]

(13)

Following the usual procedure for incomplete sums we write

\[
pA = \sum_{r=0}^{k-1} \sum_{s=0}^{p-1} \left( \frac{D(s)}{p} \right) \sum_{t=0}^{p-1} e(t(r-s))
\]

(the inner sum is zero if \( r \neq s \) and \( p \) if \( r = s \)) and isolate the term with \( t = 0 \). We obtain

\[
pA = k \sum_{s=0}^{p-1} \left( \frac{D(s)}{p} \right) + \sum_{t=1}^{p-1} \left[ \sum_{s=0}^{p-1} \left( \frac{D(s)}{p} \right) e(-st) \right] \sum_{r=0}^{k-1} e(rt).
\]

Hence as

\[
\sum_{t=1}^{p-1} \left| \sum_{r=0}^{k-1} e(rt) \right| < p \log p
\]

(14)
for large $p$, we have

$$p | A | \leq k \Phi + \Phi p \log p, \quad (15)$$

where $\Phi$ is any upper bound for

$$\left| \sum_{s=0}^{p-1} \left( \frac{D(s)}{p} \right) e(-st) \right|,$$

which is independent of $t = 0, 1, 2, \ldots, p - 1$. Suppose that $D_1(s)$ denotes the square-free part of $D(s)$, i.e.

$$D(s) \equiv D_1(s) (D_2(s))^2 \pmod{p} \quad (16)$$

for some polynomial $D_2(s)$ with integral coefficients. As $D(s)$ is a cubic, $D_2(s) \equiv 0$ has at most one solution. Thus we have

$$\left| \sum_{s=0}^{p-1} \left( \frac{D(s)}{p} \right) e(-st) \right| \leq \left| \sum_{s=0}^{p-1} \left( \frac{D_1(s)}{p} \right) e(-st) \right| + 1 \quad (17)$$

for $t = 0, 1, 2, \ldots, p - 1$. As $D_1(s)$ is square-free $\pmod{p}$ by a result of Perel'muter (Перельмутер (2)), this last sum is $O(p^{\frac{1}{2}})$, where the implied constant is absolute. Hence we may take

$$\Phi = O(p^{\frac{1}{2}}), \quad (18)$$

where the implied constant is absolute. Thus as $k < p$ we have from (15) and (18)

$$A = O(p^{\frac{1}{2}} \log p). \quad (19)$$

From (11), (12), (13) and (19) we obtain

$$m = \frac{k}{2} + O(p^{\frac{1}{2}} \log p). \quad (20)$$

The required result then follows from (6), (10) and (20).

REFERENCES


(2) Перельмутер, Г. И. О некоторых суммах с характерами. *Успехи математических наук*, 18 (1963), 145–149.