ON THE RESIDUES OF A CUBIC POLYNOMIAL (Mod p)

K. McCann and K. S. Williams

(received November 18, 1966)

If \( f(x) \) is a polynomial with integral coefficients then the integer \( r \) is said to be a residue of \( f(x) \) modulo an integer \( m \) if the congruence

\[
f(x) \equiv r \pmod{m}
\]

is soluble for \( x \); otherwise \( r \) is termed a non-residue. When \( m \) is a prime \( p \), Mordell [4] has shown that the least non-negative residue \( l \) of \( f(x) \) (mod \( p \)) satisfies

\[
l \leq d \cdot p^{1/2} \log p,
\]

where \( d \) is the degree of \( f(x) \). When \( f(x) \) is a cubic he has also shown that the least non-negative non-residue \( k \) of \( f(x) \) (mod \( p \)) is* \( 0(p^{1/2} \log p) \). It is the purpose of this note to discuss the distribution of the residues of the cubic \( f(x) \) (mod \( p \)) in greater detail. To keep the notation simple we take \( f(x) \) in the form \( x^3 + ax \); no real loss of generality is involved, everything we do for \( x^3 + ax \) can be done for \( Ax^3 + Bx^2 + Cx + D \) but at the cost of complicating the notation. When \( a \equiv 0 \pmod{p} \), \( f(x) = x^3 \) and our results are well-known in this case. Henceforth we assume that \( a \neq 0 \pmod{p} \). Let

\[
\begin{align*}
(1) \quad n_i &= \sum_{r=1}^{p} 1, \quad (i = 0, 1, 2, 3) \\
N_i &= i \\
\end{align*}
\]

* Unless otherwise stated all constants implied by \( 0 \)-symbols are absolute.
where $N_r$ denotes the number of solutions $x$ of

(2) \[ x^3 + ax \equiv r \pmod{p}. \]

It is well-known that for $p > 3$

(3) \[ n_1 = \frac{1}{2} \left\{ p + \left( \frac{-3}{p} \right) - \left( \frac{-3a}{p} \right) - 1 \right\}, \]

(4) \[ n_2 = \left( \frac{-3a}{p} \right) + 1 \]

and

(5) \[ n_3 = \frac{1}{6} \left\{ p - \left( \frac{-3}{p} \right) - 3 \left( \frac{-3a}{p} \right) - 3 \right\}. \]

Hence the number of residues of $x^3 + ax \pmod{p}$, which is just $n_1 + n_2 + n_3$, is

(6) \[ \frac{1}{3} \left\{ 2p + \left( \frac{-3}{p} \right) \right\} = \frac{2}{3} p + O(1), \quad \text{as } p \to \infty. \]

This tells us that, for large $p$, approximately two-thirds of the integers

(7) \[ 1, 2, 3, \ldots, p \]

are residues of $x^3 + ax$. We show that this is also true for

(8) \[ 1, 2, 3, \ldots, h \]

provided $h$ is sufficiently large. More precisely we show that the number of residues of $x^3 + ax$ in (8) is

(9) \[ \frac{2}{3} h + O(p^{1/2} \log p). \]

A consequence of this is Mordell's estimate for $k$. In addition, as $\frac{2}{3} > \frac{1}{2}$, it shows that the least pair of consecutive positive
residues is also $O(p^{1/2} \log p)$.

In the proof of (9) (and later) we use Vinogradov's method for incomplete character and exponential sums. This requires the familiar Polya-Vinogradov inequality, namely,

$$\sum_{y=1}^{p-1} \sum_{x=1}^{h} e(yx) \leq p \log p,$$

(10)

for $p \geq 61$, where $e(t)$ denotes $\exp(2\pi i tp^{-1})$. For the complete sums involved we appeal to the general estimates of Perel'mut' [5]. These include the estimate of Carlitz and Uchiyama [2], used by Mordell in [4], namely

$$\sum_{x=1}^{p} e(f(x)) \leq (d-1)p^{1/2},$$

(11)

where $d$ denotes the degree of the polynomial $f$, and Weil's estimate [6] for the Kloosterman sum, i.e.,

$$\sum_{x=1}^{p-1} e(ax + bx^{-1}) \leq 2p^{1/2},$$

(12)

where $x^{-1}$ denotes the inverse of $x \pmod{p}$ and $a, b \not\equiv 0 \pmod{p}$. All these estimates are consequences of Weil's proof of the Riemann hypothesis for algebraic function fields over a finite field.

Analogous to (1) we set

$$m_i = \sum_{r=1}^{h} 1,$$

(13)

$$N = i,$$

so that we require $m_4 + m_2 + m_3$. From [4] we have

$$m_2 = O(1),$$

(14)

and from Mordell's paper [4]

31
(15) \[ m_1 + 2m_2 + 3m_3 = h + 0(p^{1/2} \log p), \]

so that it suffices to determine \( m_1 \). Now (2) has one solution if and only if

\[ \left( \frac{-4a^3 - 27r^2}{p} \right) = -1 \]

so

\[ m_1 = \frac{1}{2} \sum_{r=1}^{h} \left\{ 1 - \left( \frac{-4a^3 - 27r^2}{p} \right) \right\} + O(1). \]

Applying Vinogradov's method and appealing to Perel'muter's results [5] (or to Weil's estimate (12) for the Kloosterman sum) we have

\[ \sum_{r=1}^{h} \left( \frac{-4a^3 - 27r^2}{p} \right) = O(p^{1/2} \log p) \]

so that

(16) \[ m_1 = \frac{1}{2} h + O(p^{1/2} \log p). \]

We now consider pairs of consecutive residues of \( x^3 + ax \pmod{p} \). Define \( n_{ij} \) \( (0 \leq i, j \leq 3) \) by

(17) \[ n_{ij} = \sum_{r=1}^{p} 1 \quad N_r = i, \quad N_{r+1} = j \]

so that the number of such pairs is just

(18) \[ \sum_{1 \leq i, j \leq 3} n_{ij}. \]

From (4) \( n_{12}, n_{2j} = O(1) \) for \( 0 \leq i, j \leq 3 \). Also it is easy to
show that \( n_{13} = n_{34} \) so it suffices to evaluate \( n_{14}, n_{43} \) and \( n_{33} \). We begin by showing that

\[
n_{14} = \frac{p}{4} + O(p^{1/2}).
\]

We have

\[
n_{14} = \sum_{r=1}^{p} 1
\]

\[
\left( \frac{-4a^3 - 27r^2}{p} \right) = -1, \quad \left( \frac{-4a^3 - 27(r+1)^2}{p} \right) = -1
\]

\[
= \frac{1}{4} \sum_{r=1}^{p} \left\{ 1 - \left( \frac{-4a^3 - 27r^2}{p} \right) \right\} \left\{ 1 - \left( \frac{-4a^3 - 27(r+1)^2}{p} \right) \right\} + O(1)
\]

\[
= \frac{p}{4} - \frac{1}{4} \sum_{r=1}^{p} \left( \frac{-4a^3 - 27r^2}{p} \right) - \frac{1}{4} \sum_{r=1}^{p} \left( \frac{-4a^3 - 27(r+1)^2}{p} \right)
\]

\[
+ \frac{1}{4} \sum_{r=1}^{p} \left( \frac{-4a^3 - 27r^2}{p} \right) \left( \frac{-4a^3 - 27(r+1)^2}{p} \right) + O(1).
\]

The first two character sums are \( O(1) \) and the last one by Perel'muter's results is \( \leq 3p^{1/2} \) in absolute value, since \(( -4a^3 - 27r^2)( -4a^3 - 27(r+1)^2) \) is not identically \((\text{mod } p)\) a square in \( r \).

We next prove that

\[
n_{13} = \frac{p}{12} + O(p^{1/2}).
\]

We do this by showing that

\[
n_{14} + 2n_{12} + 3n_{43} = \frac{p}{2} + O(p^{1/2}).
\]

(20) follows since we know \( n_{11} \) and \( n_{12} \). We have
\[
\begin{align*}
3 \sum_{j=0}^{\frac{p}{r+1}} - 2 & = \sum_{j=0}^{\frac{p}{r+1}} j \sum_{r=1}^{N_r} 1 = \sum_{r=1}^{N_r} \frac{p}{r+1} \\
& = \sum_{r=1}^{\frac{p}{N_r+1}} \sum_{x=1}^{\frac{p}{r+1}} 1 \\
& = \frac{1}{2} \sum_{x=1}^{\frac{p}{2}} \left( 1 - \left( -\frac{4a^3 - 27x^2}{p} \right) \right) + O(1) \\
& = \frac{p}{2} - \frac{1}{2} \sum_{x=1}^{\frac{p}{2}} \left( -\frac{4a^3 - 27(x^3 + ax - 1)^2}{p} \right) + O(1). \end{align*}
\]

Now \(27^2(x^3 + ax - 1)^2 + 108a^3\) is not identically \((\text{mod } p)\) a square in \(x\) as \(a \neq 0 \pmod{p}\). Hence Perel'muter's work tells us that the character sum is \(O(p^{1/2})\). This proves (21).

Finally consider
\[
\begin{align*}
n_{11} + 2(n_{12} + n_{21}) + 3(n_{13} + n_{31}) + 4n_{22} + 6(n_{23} + n_{32}) + 9n_{33}. \end{align*}
\]
This is just the number of solutions \((x, y)\) of
\[
(x^3 + ax) - (y^3 + ay) - 1 \equiv 0 \pmod{p}.
\]
By a result of Lang and Weil [3] this number is
\[
p + O(p^{1/2}).
\]
Hence
\[
(22) \quad n_{33} = \frac{p}{36} + O(p^{1/2}).
\]
Thus the number of pairs of consecutive residues is
\begin{equation}
\frac{4}{9} p + O(p^{1/2}).
\end{equation}

We conclude by calculating the number of pairs of residues of \( x^3 + ax \mod p \) in (8). We define \( m_{ij} \) \((0 \leq i, j \leq 3)\) by
\begin{equation}
m_{ij} = \sum_{r=1}^{p} 1, \quad N_r = i, \quad N_{r+1} = j
\end{equation}

From (4) we have \( m_{12}, m_{2j} = O(1) \) \((0 \leq i, j \leq 3)\) and, much as before, we can show that
\begin{equation}
m_{11} = \frac{h}{4} + O(p^{1/2} \log p)
\end{equation}
and
\begin{equation}
m_{13} = m_{31} = \frac{h}{12} + O(p^{1/2} \log p).
\end{equation}

The only difficulty is the estimation of \( m_{33} \). We find it necessary to appeal to a recent deep estimate of Bombieri and Davenport [1] for an exponential sum of the type
\begin{equation}
\sum_{x, y=1}^{p} e(f(x))
\end{equation}
\( \varnothing(x, y) \equiv 0 \mod p \)

where \( \varnothing(x, y) \) is absolutely irreducible \( \mod p \). We have
\begin{equation}
m_{11} + 2(m_{12} + m_{21}) + 3(m_{13} + m_{31}) + 4m_{22} + 6(m_{23} + m_{32}) + 9m_{33}
\end{equation}
\begin{equation}
= \sum_{r=1}^{h} N_r N_{r+1}
\end{equation}
\[
= \frac{1}{p} \sum_{\rho} \sum_{\nu} \sum_{\pi} N_{r} N_{r+1} e(t(r-s)) \\
= \frac{1}{p} \sum_{\rho} \sum_{\nu} N_{r} N_{r+1} + \frac{1}{p} \sum_{\rho} \sum_{t=1}^{\rho-1} N_{r} N_{r+1} e(tr) \quad \{ \sum_{s=1}^{h} e(-st) \} \\
\]

Hence
\[
|m_{11} + 2(m_{12} + m_{21}) + \ldots + 9m_{33} - \frac{h}{p} (p + 0(p^{1/2}))| \leq \max_{1 \leq t \leq p-1} \left| \sum_{r=1}^{p} N_{r} N_{r+1} e(tr) \right| \log p.
\]

Now
\[
\sum_{r=1}^{p} N_{r} N_{r+1} e(tr) \\
= \frac{1}{2} \sum_{r=1}^{p} \sum_{x=1}^{p} \sum_{u=1}^{p} e\{u(f(x)-r)\} \sum_{y=1}^{p} \sum_{v=1}^{p} e\{v(f(y)-r-1)\} e(tr). \\
= \frac{1}{2} \sum_{r=1}^{p} e\{uf(x) + vf(y) - v\} \sum_{r=1}^{p} e\{(t-u-v)r\} \\
= \frac{1}{p} \sum_{x, y, u, v = 1}^{p} e\{(t-v)f(x) + vf(y) - v\} \\
= \frac{1}{p} \sum_{x, y = 1}^{p} e\{tf(x)\} \sum_{y=1}^{p} e\{v(f(y) - f(x) - 1)\} \\
= \sum_{x, y = 1}^{p} e(tf(x)).
\]

\[f(y) - f(x) - 1 \equiv 0\]
As \( f(y) - f(x) - 1 \) is absolutely irreducible \((\text{mod } p)\), by the mentioned result of Davenport and Bombieri, this sum in absolute value is less than \( 18p^{1/2} + 9 \). Hence

\[
m_{33} = \frac{h}{36} + o(p^{1/2} \log p)
\]

and the number of pairs of consecutive residues in (8) is

\[
\frac{4h}{9} + o(p^{1/2} \log p)
\]

This implies that the least triple of consecutive positive residues of \( x^3 + ax \pmod p \) is also \( o(p^{1/2} \log p) \).

In conclusion we would like to say that a number of modifications of this work are possible; for example the results obtained can be extended to arbitrary arithmetic progressions without difficulty and also to quartic polynomials. Finally we offer the following

CONJECTURE: For a fixed positive integer \( k \) the number \( N_k(a) \) of blocks of \( k \) consecutive residues of \( x^3 + ax \pmod p \) satisfies

\[
\lim_{p \to \infty} \frac{N_k(a)}{p} = \left( \frac{2}{3} \right)^k
\]

for each \( k \), uniformly in \( a \neq 0 \pmod p \).

This has been verified for \( k = 1 \) and 2.

REFERENCES


Manchester University
Manchester, England

Carleton University
Ottawa, Canada