Glasgow Math. J. 8 (1967), 67-88.

THE DISTRIBUTION OF THE RESIDUES OF A QUARTIC POLYNOMIAL

by K. McCANN AND K. S. WILLIAMS

(Received 17 June, 1966)

1. Introduction. Let $f(x)$ denote a polynomial of degree d defined over a finite field k with $q=p^n$ elements. B. J. Birch and H. P. F. Swinnerton-Dyer [1] have estimated the number $N(f)$ of distinct values of y in k for which at least one of the roots of

$$f(x)=y \tag{1.1}$$

is in k. They prove, using A. Weil's deep results [12] (that is, results depending on the Riemann hypothesis for algebraic function fields over a finite field) on the number of points on a finite number of curves, that

$$N(f)=\lambda q+O(q^{\frac{1}{2}}), \tag{1.2}$$

where λ is a certain constant and the constant implied by the O-symbol depends only on d. In fact, if $G(f)$ denotes the Galois group of the equation (1.1) over $k(y)$ and $G^+(f)$ its Galois group over $k^+(y)$, where k^+ is the algebraic closure of k, then it is shown that λ depends only on $G(f)$, $G^+(f)$ and d. It is pointed out that " in general "

$$\lambda=1-\frac{1}{2!}+\frac{1}{3!}-\ldots-(-1)^d\frac{1}{d!}.$$

It is the purpose of this paper to consider the case of quartic polynomials (mod p) (so that $d=4$ and $q=p$) in greater detail. It is shown, using Skolem's work [9] on the general quartic polynomial (mod p) and Manin's elementary proof [5] of Hasse's result

$$\left|\sum_{x=0}^{p-1}\left(\frac{x^3+ax+b}{p}\right)\right|<2p^{\frac{1}{2}},$$

that (1.2) can be proved in this special case in a completely elementary way, which incidently avoids explicit consideration of $G(f)$ and $G^+(f)$. Further it is shown that the only values of λ which occur are

$$\lambda=\frac{5}{8}\left(=1-\frac{1}{2!}+\frac{1}{3!}-\frac{1}{4!}\right),\ \frac{1}{2},\ \frac{3}{8},\ \frac{1}{4}; \tag{1.3}$$

and moreover it is determined when each of these occurs. For those f having $\lambda=\frac{1}{2}$, $\frac{3}{8}$ or $\frac{1}{4}$, it is proved that the error term in the asymptotic formula for $N(f)$ is in fact $O(1)$. In the case of cubic polynomials [6] the corresponding values of λ are

$$\lambda=1,\quad \tfrac{2}{3}(=1-1/2!+1/3!),\quad \tfrac{1}{3};$$

and in this case the error term is always $O(1)$. We note that for cubic and quartic polynomials, the number of λ-values occurring is the same as the degree of the polynomial under consideration. We also observe that for $d=3$ and 4

$$f^*(x,y)=\frac{f(x)-f(y)}{x-y}$$

is absolutely irreducible $(\bmod p)$ if and only if

$$\lambda=1-\frac{1}{2!}+\frac{1}{3!}-\ldots-(-1)^d\frac{1}{d!}.$$

(For $d=3$ this was first noted by S. Uchiyama [10].)

We also consider the problem of determining the number of residues in an arithmetic progression. If the arithmetic progression has h terms we prove that the number of residues in it is given by

$$\lambda h+O(p^{\frac{1}{2}}\log p), \tag{1.4}$$

where λ is given by (1.3) and the constant implied by the O-symbol is absolute. This proves that any arithmetic progression with $\gg p^{\frac{1}{2}}\log p$ terms contains a residue of $f(x)\ (\bmod p)$, generalizing a result of L. J. Mordell [7] in the case $d=4$. It is shown that it also contains a non-residue (generalizing a result of one of us [14]) and a pair of consecutive residues. (Similar results have been shown to hold in the cubic case [6].) This last result verifies a conjecture of one of us [13] in a special case, namely, that the least pair of consecutive non-negative residues of any polynomial $(\bmod p)$ of degree d is $O(p^{\frac{1}{2}}\log p)$.

Finally we conjecture that (1.4) holds for all polynomials of degree d. The truth of this conjecture would imply that the least non-negative non-residue $(\bmod p)$ of a polynomial of degree d, for which $\lambda \neq 1$, is $O(p^{\frac{1}{2}}\log p)$.

2. Simplification of the problem. Let

$$f_1(x)=a_1x^4+b_1x^3+c_1x^2+d_1x+e_1 \quad (a_1\not\equiv 0)†$$

have the N residues $(\bmod p)$

$$r_1, r_2, \ldots, r_N.$$

Then

$$f_2(x)=x^4+b_2x^3+c_2x^2+d_2x+e_2,$$

where

$$b_2=a_1^{-1}b_1,\quad c_2=a_1^{-1}c_1,\quad d_2=a_1^{-1}d_1,\quad e_2=a_1^{-1}e_1,$$

also has N residues, namely

$$a_1^{-1}r_1, a_1^{-1}r_2, \ldots, a_1^{-1}r_N. \tag{2.1}$$

† Very often we omit $(\bmod p)$ as this is the only modulus occurring.

Now let

$$f_3(x)=f_2(x-4^{-1}b_2)=x^4+c_3x^2+d_3x+e_3,$$

so that

$$c_3=-2^{-3}\,.\,3b_2^2+c_2,\quad d_3=2^{-3}b_2^3-2^{-1}b_2c_2+d_2$$

and

$$e_3=-3.2^{-8}b_2^4+2^{-4}b_2^2c_2-2^{-2}b_2d_2+e_2.$$

Then $f_3(x)$ also has the N residues (2.1). Now set

$$f_4(x)=f_3(x)-e_3.$$

The residues of $f_4(x)$ are

$$a_1^{-1}r_1-e_3,\, a_1^{-1}r_2-e_3,\, \ldots,\, a_1^{-1}r_N-e_3.$$

Hence, without loss of generality, we need only consider the number of residues (mod p) of

$$f(x)=x^4+ax^2+bx. \tag{2.2}$$

When we count the residues (mod p) only if they lie in a certain arithmetic progression, say

$$\{l+ms\}\quad (s=0,1,\ldots,h-1), \tag{2.3}$$

we can still work with (2.2) without any loss of generality, as the formula obtained for the number of its residues in (2.3) is of the form

$$\lambda h+O(p^{\frac{1}{2}}\log p),$$

where λ is the constant discussed in §1 and the constant implied by the O-symbol is absolute† and so does not depend on l and m.

Throughout this paper we will use the following notation. We let N_r ($r=0, 1, 2, \ldots, p-1$) denote the number of incongruent (mod p) solutions x of

$$f(x)\equiv r \pmod p,$$

and set

$$n_i=\sum_{\substack{r\\ N_r=i}} 1 \qquad (i=0,1,2,3,4),$$

where the summation in r is taken over the set $\{0, 1, 2, \ldots, p-1\}$. The number $N(f)$ of residues of $f(x)$ is therefore just

$$\sum_{\substack{r\\ N_r>0}} 1=n_1+n_2+n_3+n_4.$$

For the residues of $f(x)$ (mod p) in the arithmetic progression (2.3), we let $M(f)$ denote their number and introduce

$$m_i=\sum_{\substack{r\\ N_r=i}}{}' 1 \qquad (i=0,1,2,3,4),$$

† Unless otherwise stated, all constants implied by O-symbols are absolute.

where the dash ($'$) denotes that the summation in r is taken over the set (2.3). Hence

$$M(f)=m_1+m_2+m_3+m_4.$$

3. Estimation of n_3. The discriminant of $f(x)-r$ is given by

$$D(r)=-256r^3-128a^2r^2-(16a^4+144ab^2)r-(4a^3b^2+27b^4). \tag{3.1}$$

Hence $D(r)\equiv 0 \pmod p$ has at most three incongruent solutions r, that is $f(x)-r$ has a squared factor $(\operatorname{mod} p)$ for $O(1)$ values of r. But $N_r=3$ implies that $f(x)-r$ has a squared linear factor $(\operatorname{mod} p)$, and so we have

LEMMA 1. $n_3=O(1)$.

4. Estimation of n_1. If $b\equiv 0$, obviously $n_1=O(1)$ so that we may suppose that $b\not\equiv 0$. The cubic resolvent of $f(x)-r$, having the same discriminant as $f(x)-r$, apart from a factor 2^{12}, is

$$g_r(y)=y^3+8ay^2+16(a^2+4r)y-64b^2. \tag{4.1}$$

Now, by a result of Skolem [9], $f(x)-r$ is congruent to the product of a linear polynomial and an irreducible cubic $(\operatorname{mod} p)$ if and only if $g_r(y)$ is irreducible $(\operatorname{mod} p)$. Hence

$$n_1=\sum_{\substack{r\\ g_r \text{ irred} \pmod p}} 1 \quad +O(1),$$

or equivalently

$$n_1=p-\sum_{\substack{r\\ g_r \text{ red} \pmod p}} 1 \quad +O(1).$$

As $\operatorname{discrim} g_r(y)=2^{12}D(r)$, there are at most three values of r for which $g_r(y)$ has a squared factor $(\operatorname{mod} p)$. Let $n^{(1)}$ denote the number of r for which $g_r(y)$ has exactly one linear factor and $n^{(3)}$ the number of r for which $g_r(y)$ has three distinct linear factors $(\operatorname{mod} p)$. Then

$$n_1=p-(n^{(1)}+n^{(3)})+O(1).$$

Now

$$n^{(1)}+3n^{(3)}=p+O(1), \tag{4.2}$$

so that

$$n_1=\tfrac{2}{3}p-\tfrac{2}{3}n^{(1)}+O(1).$$

Now $g_r(y)$ has exactly one linear factor if and only if

$$\left(\frac{\operatorname{discrim} g_r(y)}{p}\right)=-1.$$

This was first proved by L. E. Dickson [4]. Hence

$$\begin{aligned} n^{(1)} &= \tfrac{1}{2}\sum_r \left\{1-\left(\frac{D(r)}{p}\right)\right\}+O(1) \\ &= \tfrac{1}{2}p+O(p^{\frac{1}{2}}), \end{aligned}$$

by Manin's result [5]. Hence we have proved in an elementary way

LEMMA 2.

$$n_1 = \begin{cases} \tfrac{1}{3}p+O(p^{\frac{1}{2}}), & \text{if } b\not\equiv 0, \\ O(1), & \text{if } b\equiv 0. \end{cases}$$

5. Estimation of n_2. In this section we give two different proofs of our estimates for n_2. The first proof appears to be deep but is easily generalized to deal with m_2. The second proof is elementary and completes the elementary proof of the asymptotic formula for $N(f)$. This method does not seem to be easily capable of generalization to m_2. To calculate m_2 by this method would require an asymptotic formula for $m_1+4m_2+9m_3+16m_4$, which, after applying the method of incomplete sums to it, requires an effective estimate for

$$\max_{1\leq v\leq p-1}\left|\sum_{\substack{x,\,y=0\\ f(x)\equiv f(y)}}^{p-1} e(-vf(y))\right|,$$

where, for any real t, $e(t)$ denotes $\exp(2\pi itp^{-1})$. Such an estimate seems difficult to obtain.

First Proof. We consider two cases according as $b\equiv 0$ or $b\not\equiv 0$.

Case (i): $b\equiv 0$. In this case

$$f(x)-r\equiv x^4+ax^2-r$$

is congruent to the product of an irreducible quadratic and two distinct linear factors if and only if

$$\left(\frac{-r}{p}\right)=-1 \quad \text{and} \quad \left(\frac{4r+a^2}{p}\right)=+1.$$

This result is contained in a theorem of Carlitz [2]. (Skolem [9] seems to forget the possibility $a_1^3-4a_1a_2+8a_3\equiv 0$ (his notation) in his paper; in our case we have $a_1=0$, $a_2=a$, $a_3=0$ and $a_4=-r$.) Hence

$$\begin{aligned} n_2 &= \tfrac{1}{4}\sum_r\left\{1-\left(\frac{-r}{p}\right)\right\}\left\{1+\left(\frac{4r+a^2}{p}\right)\right\}+O(1) \\ &= \tfrac{1}{4}\left\{p-\sum_r\left(\frac{-4r^2-a^2r}{p}\right)\right\}+O(1) \\ &= \tfrac{1}{4}\left\{-p\left(\frac{-1}{p}\right)\left[p\left(1-\left(\frac{a^2}{p}\right)\right)-1\right]\right\}+O(1) \\ &= \tfrac{1}{4}\left\{1-\left(\frac{-1}{p}\right)\left[1-\left(\frac{a^2}{p}\right)\right]\right\}p+O(1). \end{aligned}$$

Case (ii): $b \not\equiv 0$. In this case

$$f(x)-r=x^4+ax^2+bx-r$$

is congruent to the product of an irreducible quadratic and two linear distinct factors if and only if

$$g_r(y)\equiv(y-y_1)h_r(y) \quad (y_1\equiv y_1(r)), \tag{5.1}$$

where $h_r(y)$ is an irreducible quadratic and $(y_1 \mid p) = +1$; for convenience we occasionally use this alternative notation for Legendre symbols.

Now $g_r(y)$ is of the form (5.1) if and only if

$$\left(\frac{\operatorname{discrim} g_r(y)}{p}\right)=-1,$$

i.e., if and only if

$$\left(\frac{D(r)}{p}\right)=-1.$$

Hence

$$n_2=\sum_{\substack{r\\(D(r)\mid p)=-1,\,(y_1\mid p)=1,\\ g_r(y_1)\equiv 0}}1+O(1).$$

As $D(r)$ is a cubic in r, the number of r with $(D(r)|p) = -1$ is just

$$\tfrac{1}{2}\sum_r\left\{1-\left(\frac{D(r)}{p}\right)\right\}+O(1)=\tfrac{1}{2}p+O(p^{\frac{1}{2}})>0,$$

for large enough p.

Hence there exists at least one r such that $(D(r)|p) = -1$, say $r = r'$. Let $y_1 = y_1' = y_1(r')$ be the unique solution of

$$g_{r'}(y_1)\equiv 0.$$

Then

$$r'\equiv h(y_1'),$$

where

$$h(y_1)=2^{-6}y_1^{-1}(64b^2-16a^2y_1-8ay_1^2-y_1^3).$$

We note that $y_1 \not\equiv 0$ as $b \not\equiv 0$. Now

$$\begin{aligned}
n_2&=\tfrac{1}{4}\sum_{\substack{r\\ r\equiv h(y_1)}}\sum_{y_1\not\equiv 0}\left\{1-\left(\frac{D(r)}{p}\right)\right\}\left\{1+\left(\frac{y_1}{p}\right)\right\}+O(1)\\
&=\tfrac{1}{4}\sum_{y_1\not\equiv 0}\left\{1-\left(\frac{y_1^4D(h(y_1))}{p}\right)\right\}\left\{1+\left(\frac{y_1}{p}\right)\right\}+O(1)\\
&=\frac{p}{4}+O(p^{\frac{1}{2}})-\tfrac{1}{4}\sum_{y_1\not\equiv 0}\left(\frac{y_1^4D(h(y_1))}{p}\right),
\end{aligned}$$

by a deep result of Perel'muter [8] as

$$y_1^5 D(h(y_1))$$

is a polynomial of odd degree, namely 11. The second sum is also $O(p^{\frac{1}{2}})$ unless

$$y^4 D(h(y)) \equiv \{k(y)\}^2 \pmod p, \tag{5.2}$$

identically in y, where $k(y)$ is a quintic polynomial. (Note that the coefficient of y^{10} on the left-hand side of (5.2) is $2^{-10} = (2^{-5})^2$.) However it is easy to see that this is not so, since on taking $y = y_1'$ we have

$$y_1'^4 D(h(y_1')) \equiv \{k(y_1')\}^2,$$

that is

$$y_1'^4 D(r') \equiv \{k(y_1')\}^2,$$

so that

$$\left(\frac{D(r')}{p}\right) = +1 \quad \text{or} \quad 0,$$

which is a contradiction. Hence we have proved

LEMMA 3.

$$n_2 = \begin{cases} \dfrac{1}{4}\left[1-\left(\dfrac{-1}{p}\right)\left\{1-\left(\dfrac{a^2}{p}\right)\right\}\right]p+O(1), & \text{if } b\equiv 0, \\ \frac{1}{4}p+O(p^{\frac{1}{2}}), & \text{if } b\not\equiv 0. \end{cases}$$

Second proof. We note the obvious relation

$$n_1+2n_2+3n_3+4n_4=p. \tag{5.3}$$

As we have evaluated n_1 and n_3, to determine n_2 (and n_4) it suffices to estimate

$$n_1+4n_2+9n_3+16n_4.$$

We prove in an elementary way

LEMMA 3′.

$$n_1+4n_2+9n_3+16n_4 = \begin{cases} \left[3+\left(\dfrac{-1}{p}\right)-\left(\dfrac{-a^2}{p}\right)\right]p+O(1), & \text{if } b\equiv 0, \\ 2p+O(p^{\frac{1}{2}}), & \text{if } b\not\equiv 0. \end{cases}$$

Proof.

$$\sum_{i=1}^{4} i^2 n_i = \sum_{i=0}^{4} \sum_{\substack{j=0 \\ N_j=i}}^{p-1} i^2 = \sum_{i=0}^{4} \sum_{\substack{j=0 \\ N_j=i}}^{p-1} N_j^2$$

$$= \sum_{j=0}^{p-1} N_j^2 = N_f,$$

where N_f denotes the number of solutions (x, y) of

$$f(x) \equiv f(y). \tag{5.4}$$

Let N'_f denote the number of such solutions with $x \not\equiv y$; then

$$n_1 + 4n_2 + 9n_3 + 16n_4 = p + N'_f.$$

After cancelling the factor $x - y$ in (5.4) we find that solutions with $x \not\equiv y$ satisfy

$$(x+y)(x^2+y^2+a) \equiv -b. \tag{5.5}$$

As there are at most three solutions of this with $x \equiv y$ we have

$$N'_f = N''_f + O(1),$$

where N''_f denotes the number of solutions (x, y) of (5.5). We now consider two cases according as $b \equiv 0$ or $b \not\equiv 0$.

Case (i): $b \equiv 0$. Then (5.5) becomes

$$(x+y)(x^2+y^2+a) \equiv 0$$

and the number N''_f of solutions (x, y) of this is

$$p + \left\{\left[1 + \left(\frac{-1}{p}\right) - \left(\frac{-a^2}{p}\right)\right] p - \left(\frac{-1}{p}\right)\right\} - \left\{1 + \left(\frac{-2a}{p}\right)\right\} = \left\{2 + \left(\frac{-1}{p}\right) - \left(\frac{-a^2}{p}\right)\right\} p + O(1).$$

Case (ii): $b \not\equiv 0$. Let $N''_k (1 \leqq k \leqq p-1)$ denote the number of solutions (x, y) of the pair of congruences

$$x^2 + y^2 + a \equiv k, \quad x + y \equiv -bk^{-1}. \tag{5.6}$$

Then

$$N''_f = \sum_{k=1}^{p-1} N''_k.$$

Eliminating y from the pair (5.6), we find that N''_k is just the number of solutions x of

$$x^2 + bk^{-1}x + 2^{-1}(b^2k^{-2} - k + a) \equiv 0.$$

Hence

$$N''_k = 1 + \left(\frac{b^2k^{-2} - 4.2^{-1}(b^2k^{-2} - k + a)}{p}\right) = 1 + \left(\frac{2k^3 - 2ak^2 - b^2}{p}\right),$$

and so

$$N''_f = p - 1 + \sum_{k \neq 0} \left(\frac{2k^3 - 2ak^2 - b^2}{p}\right).$$

As $b \not\equiv 0$, by Manin's results [5],

$$N''_f = p + O(p^{\frac{1}{2}}).$$

This completes the proof of the lemma.

6. Estimation of n_4. This follows at once from Lemmas 1, 2 and 3, or 3′ and (5.3). We have

LEMMA 4.

$$n_4 = \begin{cases} \dfrac{p}{24} + O(p^{\frac{1}{2}}), & \text{if} \quad b \not\equiv 0, \\[2ex] \dfrac{1}{8}\left[1+\left(\dfrac{-1}{p}\right)\left\{1-\left(\dfrac{a^2}{p}\right)\right\}\right]p + O(1), & \text{if} \quad b \equiv 0. \end{cases}$$

7. The number of residues in a complete residue system. The number of residues $N(f) = n_1+n_2+n_3+n_4$ of the quartic polynomial (2.2) (and so of $f_1(x)$) is given by

THEOREM 1.

$$N(f) = \begin{cases} \frac{1}{4}p + O(1), & \text{if} \quad a, b \equiv 0,\ p \equiv 1 \pmod 4, \\ \frac{1}{2}p + O(1), & \text{if} \quad a, b \equiv 0,\ p \equiv 3 \pmod 4, \\ \frac{3}{8}p + O(1), & \text{if} \quad a \not\equiv 0,\ b \equiv 0, \\ \frac{5}{8}p + O(p^{\frac{1}{2}}), & \text{if} \quad b \not\equiv 0. \end{cases}$$

In the cases where the error terms are $O(1)$, it would be very easy to prove exact results. In fact, quoting some results of R. D. von Sterneck [11], we have in these cases

$$N(f) = \begin{cases} \dfrac{p+3}{4} & \text{for} \quad a, b \equiv 0,\ p \equiv 1 \pmod 4, \\[2ex] \dfrac{p+1}{2} & \text{for} \quad a, b \equiv 0,\ p \equiv 3 \pmod 4, \\[2ex] \dfrac{1}{8}\left(3p+4-2\left(\dfrac{-a}{p}\right)+\left(\dfrac{-1}{p}\right)+2\left(\dfrac{-2a}{p}\right)\right) & \text{for} \quad a \not\equiv 0,\ b \equiv 0. \end{cases}$$

8. Estimation of m_3. As $m_3 \leqq n_3$ we have, from Lemma 1,

LEMMA 5.

$$m_3 = O(1).$$

9. Estimation of m_1. If $b \equiv 0$, obviously $m_1 = O(1)$, and so we may suppose that $b \not\equiv 0$. As in §4 we have

$$m_1 = \sum_{\substack{r \\ g_r \text{ irred} \pmod p}}{}' 1 \quad + O(1),$$

or equivalently

$$m_1 = h - \sum_{\substack{r \\ g_r \text{ red} \pmod p}}{}' 1 \quad + O(1).$$

Define $m^{(i)}$ $(i = 0, 1, 2, 3)$ by

$$m^{(i)} = \sum_{\substack{r \\ \tilde{N}_r = i}} 1,$$

where $\tilde{N}_r$ denotes the number of solutions y of $g_r(y) \equiv 0$, so that

$$m_1 = h - (m^{(1)} + m^{(3)}) + O(1). \tag{9.1}$$

Corresponding to (4.2) we prove that

$$m^{(1)} + 3m^{(3)} = h + O(p^{1/2} \log p). \tag{9.2}$$

We have

$$\begin{aligned}
\sum_{i=1}^{3} im^{(i)} &= \sum_{i=0}^{3} \sum_{\substack{r \\ \tilde{N}_r = i}}' i = \sum_{i=0}^{3} \sum_{\substack{r \\ \tilde{N}_r = i}}' \tilde{N}_r = \sum_r{}' \tilde{N}_r \\
&= (1/p) \sum_r{}' \sum_y \sum_t e(tg_r(y)) \\
&= h + (1/p) \sum_{t \neq 0} \{ \sum_y e(t(y^3 + 8ay^2 + 16a^2y - 64b^2)) \sum_r{}' e(64tyr) \} \\
&= h + (1/p) \sum_{t \neq 0} \{ \sum_{y \neq 0} e(t(y^3 + 8ay^2 + 16a^2y - 64b^2)) \sum_r{}' e(64tyr) \} + O(1),
\end{aligned}$$

as $b \not\equiv 0$. Now change the summation in y to summation in z defined by $z \equiv ty$, for fixed t. Then

$$\begin{aligned}
\sum_{i=1}^{3} im^{(i)} - h &= (1/p) \sum_{t \neq 0} \{ \sum_{z \neq 0} e(t^{-2}z^3 + 8at^{-1}z^2 + 16a^2z - 64b^2t) \sum_r{}' e(64zr) \} + O(1) \\
&= (1/p) \sum_{z \neq 0} e(16a^2z) \{ \sum_{t \neq 0} e(t^{-2}z^3 + 8at^{-1}z^2 - 64b^2t) \} \{ \sum_r{}' e(64zr) \} + O(1),
\end{aligned}$$

and so

$$\begin{aligned}
\left| \sum_{i=1}^{3} im^{(i)} - h \right| &\leq (1/p) \sum_{z \neq 0} \left| \sum_{t \neq 0} e(t^{-2}z^3 + 8at^{-1}z^2 - 64b^2t) \right| \left| \sum_r{}' e(64zr) \right| + O(1) \\
&\leq (1/p) \max_{1 \leq z \leq p-1} \left| \sum_{t \neq 0} e(z^3t^{-2} + 8az^2t^{-1} - 64b^2t) \right| \sum_{z \neq 0} \left| \sum_r e(64zr) \right| + O(1).
\end{aligned}$$

Now

$$\left| \sum_r{}' e(64zr) \right| = \left| \frac{1 - e(64zhm)}{1 - e(64zm)} \right| \leq \frac{1}{|\sin(64\pi zm/p)|}$$

and so

$$\begin{aligned}
\sum_{z \neq 0} \left| \sum_r{}' e(64zr) \right| &\leq \sum_{z=1}^{p-1} \frac{1}{|\sin(64\pi zm/p)|} = \sum_{u=1}^{p-1} \frac{1}{\sin(\pi u/p)} \\
&= 2 \sum_{u=1}^{\frac{1}{2}(p-1)} \frac{1}{\sin(\pi u/p)} \leq p \sum_{u=1}^{\frac{1}{2}(p-1)} (1/u) \\
&\leq p \log p,
\end{aligned}$$

for p large enough. Hence

$$\left|\sum_{i=1}^{3} im^{(i)}-h\right| \leqq \log p.\max_{1\leqq z\leqq p-1}\left|\sum_{t\neq 0} e\left\{\frac{z^3+8az^2t-64b^2t^3}{t^2}\right\}\right|+O(1) = O(p^{1/2}\log p),$$

by a deep result of Perel'muter [8]. Now $m^{(2)} = O(1)$, so that

$$m^{(1)}+3m^{(3)} = h+O(p^{1/2}\log p).$$

Hence from (9.1) and (9.2) we have

$$m_1 = \tfrac{2}{3}h-\tfrac{2}{3}m^{(1)}+O(p^{1/2}\log p).$$

Now $g_r(y)$ has exactly one linear factor if and only if $(D(r)\,|\,p) = -1$. Hence

$$m^{(1)} = \tfrac{1}{2}{\sum_r}'\left\{1-\left(\frac{D(r)}{p}\right)\right\}+O(1).$$

It is well-known that the above incomplete sum is $O(p^{1/2}\log p)$, so that

$$m^{(1)} = \tfrac{1}{2}h+O(p^{1/2}\log p),$$

giving

LEMMA 6.

$$m_1 = \begin{cases} \tfrac{1}{3}h+O(p^{1/2}\log p), & \textit{if} \quad b\not\equiv 0,\\ O(1), & \textit{if} \quad b\equiv 0.\end{cases}$$

10. Estimation of m_2. We consider two cases according as $b \equiv 0$ or $b \not\equiv 0$.

Case (*i*), $b \equiv 0$. In this case, from §5, we have

$$\begin{aligned} m_2 &= \tfrac{1}{4}{\sum_r}'\left\{1-\left(\frac{-r}{p}\right)\right\}\left\{1+\left(\frac{4r+a^2}{p}\right)\right\}+O(1)\\ &= \tfrac{1}{4}\left\{h+{\sum_r}'\left(\frac{4r+a^2}{p}\right)-\left(\frac{-1}{p}\right){\sum_r}'\left(\frac{r}{p}\right)-\left(\frac{-1}{p}\right){\sum_r}'\left(\frac{4r^2+a^2r}{p}\right)\right\}+O(1).\end{aligned}$$

The first two incomplete sums in r are $O(p^{1/2}\log p)$ and the third one is also, unless $a\equiv 0$, when its sum is h. Hence

$$m_2 = \tfrac{1}{4}\left\{1-\left(\frac{-1}{p}\right)\left[1-\left(\frac{a^2}{p}\right)\right]\right\}h+O(p^{1/2}\log p).$$

Case (ii), $b \not\equiv 0$. Again from §5 we have

$$m_2 = \sum_{\substack{r \\ (D(r)\mid p)=-1,\ (y_1\mid p)=1, \\ g_r(y_1)\equiv 0}}' 1 + O(1)$$

$$= \tfrac{1}{4} \sum_{\substack{r \\ r\equiv h(y_1)}}' \sum_{y_1\neq 0} \left\{1+\left(\frac{D(r)}{p}\right)\right\}\left\{1+\left(\frac{y_1}{p}\right)\right\} + O(1)$$

$$= \frac{1}{4p} \sum_{\substack{r \\ r\equiv h(y_1)}} \sum_{y_1\neq 0} \left\{1-\left(\frac{D(r)}{p}\right)\right\}\left\{1+\left(\frac{y_1}{p}\right)\right\} \sum_s{}' \sum_t e(t(r-s)) + O(1)$$

$$= \frac{h}{4p} \sum_{\substack{r \\ r\equiv h(y_1)}} \sum_{y_1\neq 0} \left\{1-\left(\frac{D(r)}{p}\right)\right\}\left\{1+\left(\frac{y_1}{p}\right)\right\}$$

$$+ \frac{1}{4p}\sum_{t\neq 0}\left\{ \sum_{\substack{r \\ r\equiv h(y_1)}} \sum_{y_1\neq 0} \left\{1-\left(\frac{D(r)}{p}\right)\right\}\left\{1+\left(\frac{y_1}{p}\right)\right\} e(tr) \sum_s{}' e(-st)\right\} + O(1).$$

Hence

$$\left| m_2 - \frac{h}{p} n_2 \right| \leqq \frac{1}{4p} \max_{1\leqq t\leqq p-1} \left| \sum_{y_1\neq 0} \left\{1-\left(\frac{D(h(y_1))}{p}\right)\right\}\left\{1+\left(\frac{y_1}{p}\right)\right\} e(th(y_1)) \right| \sum_{t\neq 0} \left| \sum_s{}' e(-st) \right| + O(1)$$

and so from a deep result of Perel'muter [8]

$$m_2 = \frac{hn_2}{p} + O(p^{\frac{1}{2}}\log p) = \frac{h}{4} + O(p^{\frac{1}{2}}\log p).$$

We have proved

LEMMA 7.

$$m_2 = \begin{cases} \tfrac{1}{4}\left\{1-\left(\frac{-1}{p}\right)\left[1-\left(\frac{a^2}{p}\right)\right]\right\} h + O(p^{\frac{1}{2}}\log p), & \text{if } b\equiv 0, \\ \frac{h}{4} + O(p^{\frac{1}{2}}\log p), & \text{if } b\not\equiv 0. \end{cases}$$

11. Estimation of m_4. It is easy to show in a similar (but easier) way to that used in the proof of

$$m^{(1)} + 2m^{(2)} + 3m^{(3)} = h + O(p^{\frac{1}{2}}\log p)$$

in §9, that

$$m_1 + 2m_2 + 3m_3 + 4m_4 = h + O(p^{\frac{1}{2}}\log p). \tag{11.1}$$

Hence, from Lemmas 5, 6 and 7, we have

LEMMA 8.

$$m_4 = \begin{cases} \dfrac{h}{24} + O(p^{\frac{1}{2}} \log p), & \textit{if} \quad b \not\equiv 0 \\ \dfrac{1}{8}\left\{1 + \left(\dfrac{-1}{p}\right)\left[1 - \left(\dfrac{a^2}{p}\right)\right]\right\} h + O(p^{\frac{1}{2}} \log p), & \textit{if} \quad b \equiv 0. \end{cases}$$

12. The number of residues in an arithmetic progression. The number of residues $M(f) = m_1 + m_2 + m_3 + m_4$ of the quartic polynomial (2.11), and so of (2.1), in the arithmetic progression (2.12) is given by

THEOREM 2.

$$M(f) = \begin{cases} \tfrac{1}{4}h + O(p^{\frac{1}{2}} \log p), & \textit{if} \quad a, b \equiv 0, \ p \equiv 1 \pmod 4, \\ \tfrac{1}{2}h + O(p^{\frac{1}{2}} \log p), & \textit{if} \quad a, b \equiv 0, \ p \equiv 3 \pmod 4, \\ \tfrac{3}{8}h + O(p^{\frac{1}{2}} \log p), & \textit{if} \quad a \not\equiv 0, \ b \equiv 0, \\ \tfrac{5}{8}h + O(p^{\frac{1}{2}} \log p), & \textit{if} \quad b \not\equiv 0. \end{cases}$$

13. Some corollaries of Theorem 2. By choosing h large enough in the asymptotic formulae of Theorem 2 we can guarantee that $M(f) > 0$. This proves

THEOREM 3. *Any arithmetic progression with* $\gg p^{\frac{1}{2}} \log p$ *terms contains a residue and non-residue* (mod p) *of* $f(x)$.

We also note that Theorem 2 implies

THEOREM 4. *If* $b \not\equiv 0$, *any arithmetic progression with* $\gg p^{\frac{1}{2}} \log p$ *terms contains a pair of consecutive residues* (mod p) *of* $f(x)$.

Proof. As $b \not\equiv 0$, by Theorem 2,

$$M(f) = \tfrac{5}{8}h + O(p^{\frac{1}{2}} \log p).$$

Hence, for all $p \geqq p_0$, there exists a constant $k > 0$ such that

$$M(f) > \tfrac{5}{8}h - kp^{\frac{1}{2}} \log p.$$

Choose

$$h = [9kp^{\frac{1}{2}} \log p] + 1,$$

so that

$$M(f) > \frac{37}{8} kp^{\frac{1}{2}} \log p > 0.$$

We show that

$$l, l+m, l+2m, \ldots, l+(h-1)m,$$

with this value of h, always contains a pair of consecutive residues. For suppose not; then

$$M(f) \leqq \left[\frac{h}{2}\right]+1$$

and so, for $p \geqq p_0$,

$$\tfrac{5}{8}h-kp^{\frac{1}{2}}\log p \leqq \tfrac{1}{2}h+1,$$

which implies, for large enough p, the contradiction

$$h \leqq 8kp^{\frac{1}{2}}\log p+8.$$

We remark that a number of other results, similar to Theorems 3 and 4, can be obtained in much the same way and that most of the results of this paper, with only slight modifications, go over to quartics over a general finite field.

14. The least pair of consecutive residues when $b \equiv 0$. When $b \equiv 0$, the asymptotic formulae of Theorem 2 tell us that there are far fewer residues of $f(x)$ (mod p), and we do not have enough information to guarantee the existence of a pair of consecutive ones in this case. To overcome this difficulty we determine asymptotic formulae for the number $\mathfrak{M}$ of pairs of consecutive residues in the arithmetic progression (2.3). To do this we set

$$m_{ij} = \sum_{\substack{r \\ N_r=i,\, N_{r+m}=j}}{}' 1 \qquad (i,j=0,1,2,3,4), \tag{14.1}$$

so that

$$\mathfrak{M} = \sum_{i,j=1}^{4} m_{ij}. \tag{14.2}$$

Now it is clear that

$$m_{13}, m_{23}, m_{31}, m_{32}, m_{33}, m_{34}, m_{43} \leqq m_3$$

and

$$m_{11}, m_{12}, m_{14}, m_{24}, m_{41} \leqq m_1;$$

hence by Lemmas 5 and 6 we have

LEMMA 9. *When $b \equiv 0$, each of $m_{11}, m_{12}, m_{13}, m_{14}, m_{21}, m_{23}, m_{31}, m_{32}, m_{33}, m_{34}, m_{43}$ is $O(1)$.*

Thus (14.2) becomes

$$\mathfrak{M} = m_{22}+m_{24}+m_{42}+m_{44}+O(1), \tag{14.3}$$

so that we are left with the problem of estimating m_{22}, m_{24}, m_{42} and m_{44}. We begin with m_{22}.

LEMMA 10. *When* $b \equiv 0$,

$$m_{22} = \begin{cases} \frac{1}{8}\left\{1-\left(\frac{-1}{p}\right)\right\}h + O(p^{\frac{3}{4}}\log p), & \textit{if} \quad a \equiv 0, \\ \frac{1}{16}\left\{1-\left(\frac{-1}{p}\right)\right\}h + O(p^{\frac{3}{4}}\log p), & \textit{if} \quad a^2 \equiv \pm 4m, \\ \frac{1}{16}h + O(p^{\frac{3}{4}}\log p), & \textit{otherwise}. \end{cases}$$

Proof. Appealing to Carlitz's results [2] we see that

$$x^4 + ax^2 - r$$

is congruent (mod p) to the product of two distinct linear factors and an irreducible quadratic if and only if

$$\left(\frac{-r}{p}\right) = -1 \quad \text{and} \quad \left(\frac{4r+a^2}{p}\right) = +1. \tag{14.4}$$

For convenience we set $a \equiv 2c$ so that the second condition of (14.4) becomes $(r+c^2 \,|\, p) = +1$. Hence

$$m_{22} = \sum_r{}' 1 + O(1),$$

where, in the summation,

$$\left(\frac{-r}{p}\right) = -1, \quad \left(\frac{r+c^2}{p}\right) = +1, \quad \left(\frac{-(r+m)}{p}\right) = -1, \quad \left(\frac{r+(m+c^2)}{p}\right) = +1.$$

Hence

$$m_{22} = \frac{1}{16}\sum_r{}'\left\{1-\left(\frac{-r}{p}\right)\right\}\left\{1-\left(\frac{-(r+m)}{p}\right)\right\}\left\{1+\left(\frac{r+c^2}{p}\right)\right\}\left\{1+\left(\frac{r+(m+c^2)}{p}\right)\right\} + O(1).$$

Now unless, after multiplying the expressions in the four brackets together, we obtain squares in the Legendre symbols, this gives

$$m_{22} = \frac{1}{16}h + O(p^{\frac{3}{4}} \log p).$$

Now squares occur if and only if one of the following three possibilities holds: (i) $c \equiv 0$, (ii) $c^2 \equiv m$, (iii) $c^2 \equiv -m$.

If (i) holds,

$$\begin{aligned} m_{22} &= \frac{1}{16}\sum_r{}'\left\{1-\left(\frac{-r}{p}\right)\right\}\left\{1+\left(\frac{r}{p}\right)\right\}\left\{1-\left(\frac{-(r+m)}{p}\right)\right\}\left\{1+\left(\frac{r+m}{p}\right)\right\} + O(1) \\ &= \frac{1}{16}\sum_r{}'\left\{1-\left(\frac{-1}{p}\right)\right\}\left\{1+\left(\frac{r}{p}\right)\right\}\left\{1-\left(\frac{-1}{p}\right)\right\}\left\{1+\left(\frac{r+m}{p}\right)\right\} + O(1) \\ &= \frac{1}{16}\left\{1-\left(\frac{-1}{p}\right)\right\}^2 \sum_r{}'\left\{1+\left(\frac{r}{p}\right)\right\}\left\{1+\left(\frac{r+m}{p}\right)\right\} + O(1) \\ &= \frac{1}{8}\left\{1-\left(\frac{-1}{p}\right)\right\}h + O(p^{\frac{3}{4}}\log p). \end{aligned}$$

Similarly if (ii) or (iii) holds we have

$$m_{22} = \frac{1}{16}\left\{1-\left(\frac{-1}{p}\right)\right\} h+O(p^{\frac{1}{2}}\log p).$$

This completes the proof of Lemma 10.

LEMMA 11. *When* $b \equiv 0$,

$$m_{24} = \begin{cases} O(1), & \text{if } a \equiv 0, \\ \left\{1+\left(\frac{-1}{p}\right)\right\}\frac{h}{32}+O(p^{\frac{1}{2}}\log p), & \text{if } a^2 \equiv 4m, \\ \left\{1-\left(\frac{-1}{p}\right)\right\}\frac{h}{32}+O(p^{\frac{1}{2}}\log p), & \text{if } a^2 \equiv -4m, \\ \frac{h}{32}+O(p^{\frac{1}{2}}\log p), & \text{otherwise.} \end{cases}$$

Proof. From Lemma 3, when $a, b \equiv 0$ and $p \equiv 1 \pmod 4$,

$$n_2 = O(1).$$

As $m_{24} \leqq m_2 \leqq n_2$, we have $m_{24} = O(1)$. From Lemma 4 when $a, b \equiv 0$ and $p \equiv 3 \pmod 4$,

$$n_4 = O(1).$$

As $m_{24} \leqq m_4 \leqq n_4$, we have $m_{24} = O(1)$.

Hence we may suppose that $a \not\equiv 0$. From Carlitz's result we have that x^4+ax^2-r is congruent $(\mathrm{mod}\, p)$ to the product of two distinct linear factors and an irreducible quadratic if and only if

$$\left(\frac{-r}{p}\right) = -1 \quad \text{and} \quad \left(\frac{r+c^2}{p}\right) = +1,$$

where $a \equiv 2c$; also

$$y^4+ay^2-(r+m)$$

is congruent $(\mathrm{mod}\, p)$ to the product of four distinct linear factors if and only if

$$\left(\frac{-(r+m)}{p}\right) = +1, \quad \text{say} \quad r+m \equiv -s^2,$$

and

$$\left(\frac{c^2-s^2}{p}\right) = +1, \quad \left(\frac{-2(c+s)}{p}\right) = +1.$$

Hence

$$m_{24} = \sum_{s=1}^{\frac{1}{2}(p-1)} \sum_{r}{}' 1+O(1),$$

where, in the summations, $r+m \equiv -s^2$ and

$$\left(\frac{-r}{p}\right) = -1, \quad \left(\frac{r+c^2}{p}\right) = +1, \quad \left(\frac{-2(c+s)}{p}\right) = +1, \quad \left(\frac{c^2-s^2}{p}\right) = +1.$$

Setting

$$A(r,s) = \left\{1-\left(\frac{-r}{p}\right)\right\}\left\{1+\left(\frac{r+c^2}{p}\right)\right\}\left\{1+\left(\frac{-2(c+s)}{p}\right)\right\}\left\{1+\left(\frac{c^2-s^2}{p}\right)\right\}$$

and

$$B(s) = A(-s^2-m, s)$$

for convenience, we have

$$\begin{aligned} m_{24} &= \frac{1}{16}\sum_{s=1}^{\frac{1}{2}(p-1)}\sum_{\substack{r \\ r+m\equiv -s^2}}{}' A(r,s) + O(1) \\ &= \frac{1}{32}\sum_{s}\sum_{\substack{r \\ r+m\equiv -s^2}}{}' A(r,s) + O(1) \\ &= \frac{1}{32}\sum_{s}\sum_{\substack{r \\ r+m\equiv -s^2}}{}' A(r,s)\sum_{u}{}'\sum_{t} e(t(u-r)) + O(1) \\ &= \frac{h}{32p}\sum_{\substack{s,r \\ r+m\equiv -s^2}} A(r,s) + \frac{1}{32p}\sum_{t\neq 0}\left\{\sum_{\substack{s,r \\ r+m\equiv -s^2}} A(r,s)e(-tr)\right\}\left\{\sum_{u}{}' e(tu)\right\} + O(1) \\ &= \frac{h}{32p}\sum_{s} B(s) + \frac{1}{32p}\sum_{t\neq 0}\left\{\sum_{s} B(s)e((s^2+m)t)\right\}\left\{\sum_{u}{}' e(tu)\right\} + O(1). \end{aligned}$$

Hence

$$\begin{aligned} \left| m_{24} - \frac{h}{32p}\sum_{s} B(s)\right| &\leq \frac{1}{32p}\max_{1\leq t\leq p-1}\left|\sum_{s} B(s)e((s^2+m)t)\right|\sum_{t\neq 0}\left|\sum_{u}{}' e(tu)\right| + O(1) \\ &= O(p^{\frac{1}{2}}\log p), \end{aligned}$$

by a result of Perel'muter [8]. We now consider

$$\sum_{s}\left\{1-\left(\frac{s^2+m}{p}\right)\right\}\left\{1+\left(\frac{-s^2+(c^2-m)}{p}\right)\right\}\left\{1+\left(\frac{-2(s+c)}{p}\right)\right\}\left\{1+\left(\frac{-s^2+c^2}{p}\right)\right\}. \quad (14.5)$$

By Perel'muter's results this is

$$p + O(p^{\frac{1}{2}})$$

except in a few special cases. Thus in general

$$m_{24} = \frac{h}{32} + O(p^{\frac{1}{2}}\log p).$$

F

As $c, m \not\equiv 0$ the special cases are easily seen to arise when

$$c^2 \equiv m \quad \text{or} \quad c^2 \equiv -m.$$

When $c^2 \equiv m$, (14.5) becomes

$$\sum_s \left\{1-\left(\frac{s^2+c^2}{p}\right)\right\}\left\{1+\left(\frac{-s^2}{p}\right)\right\}\left\{1+\left(\frac{-2(s+c)}{p}\right)\right\}\left\{1+\left(\frac{-s^2+c^2}{p}\right)\right\}$$

$$= \sum_s \left\{1+\left(\frac{-1}{p}\right)\right\}\left\{1-\left(\frac{s^2+c^2}{p}\right)\right\}\left\{1+\left(\frac{-2(s+c)}{p}\right)\right\}\left\{1+\left(\frac{-s^2+c^2}{p}\right)\right\}+O(1)$$

$$= \left\{1+\left(\frac{-1}{p}\right)\right\}p+O(p^{\frac{1}{2}}),$$

giving

$$m_{24} = \left\{1+\left(\frac{-1}{p}\right)\right\}\frac{h}{32}+O(p^{\frac{1}{2}}\log p).$$

Similarly, when $c^2 \equiv -m$, we obtain

$$m_{24} = \left\{1-\left(\frac{-1}{p}\right)\right\}\frac{h}{32}+O(p^{\frac{1}{2}}\log p).$$

This completes the proof of Lemma 11. In an almost identical way we can prove

LEMMA 12. *When* $b \equiv 0$,

$$m_{42} = \begin{cases} O(1), & \text{if } a \equiv 0, \\ \left\{1-\left(\frac{-1}{p}\right)\right\}\frac{h}{32}+O(p^{\frac{1}{2}}\log p), & \text{if } a^2 \equiv 4m, \\ \left\{1+\left(\frac{-1}{p}\right)\right\}\frac{h}{32}+O(p^{\frac{1}{2}}\log p), & \text{if } a^2 \equiv -4m, \\ \frac{h}{32}+O(p^{\frac{1}{2}}\log p), & \text{otherwise.} \end{cases}$$

Finally we evaluate m_{44}.

LEMMA 13. *When* $b \equiv 0$,

$$m_{44} = \begin{cases} \left\{1+\left(\frac{-1}{p}\right)\right\}\frac{h}{32}+O(p^{\frac{1}{2}}\log p), & \text{if } a \equiv 0, \\ \left\{1+\left(\frac{-1}{p}\right)\right\}\frac{h}{64}+O(p^{\frac{1}{2}}\log p), & \text{if } a^2 \equiv \pm 4m, \\ \frac{h}{64}+O(p^{\frac{1}{2}}\log p), & \text{otherwise.} \end{cases}$$

Proof. As x^4+ax^2-r is congruent (mod p) to the product of four distinct linear factors if and only if

$$\left(\frac{-r}{p}\right)=+1, \quad \text{say} \quad r\equiv -s^2,$$

and

$$\left(\frac{c^2-s^2}{p}\right)=+1, \quad \left(\frac{-2(c+s)}{p}\right)=+1,$$

we have

$$m_{44}=\sum_{t=1}^{\frac{1}{2}(p-1)}\sum_{s=1}^{\frac{1}{2}(p-1)}\sum_r{}' 1,$$

where, in the summations, $r\equiv -s^2$, $r+m\equiv -t^2$, and

$$\left(\frac{c^2-s^2}{p}\right)=+1, \quad \left(\frac{-2(c+s)}{p}\right)=+1, \quad \left(\frac{c^2-t^2}{p}\right)=+1, \quad \left(\frac{-2(c+t)}{p}\right)=+1.$$

Hence

$$m_{44}=\frac{1}{16}\sum_{\substack{t=1\\ r\equiv -s^2,\, s^2-t^2\equiv m}}^{\frac{1}{2}(p-1)}\sum_{s=1}^{\frac{1}{2}(p-1)}\sum_r{}'\left\{1+\left(\frac{c^2-s^2}{p}\right)\right\}\left\{1+\left(\frac{-2(c+s)}{p}\right)\right\}\left\{1+\left(\frac{c^2-t^2}{p}\right)\right\}$$
$$\times\left\{1+\left(\frac{-2(c+t)}{p}\right)\right\}+O(1).$$
$$=\frac{1}{64}\sum_{\substack{t,s\\ r\equiv -s^2,\, s^2-t^2\equiv m}}\sum_r{}'\left\{1+\left(\frac{c^2-s^2}{p}\right)\right\}\left\{1+\left(\frac{-2(c+s)}{p}\right)\right\}\left\{1+\left(\frac{c^2-t^2}{p}\right)\right\}$$
$$\times\left\{1+\left(\frac{-2(c+t)}{p}\right)\right\}+O(1).$$

Now change the summation over s and t to one over u and t, where u is defined by

$$s\equiv t+u.$$

Hence

$$m_{44}=\frac{1}{64}\sum_{\substack{u,t\\ r\equiv -(t+u)^2,\\ u^2+2ut-m\equiv 0}}\sum_r{}'\left\{1+\left(\frac{c^2-(t+u)^2}{p}\right)\right\}\left\{1+\left(\frac{-2(c+t+u)}{p}\right)\right\}\left\{1+\left(\frac{c^2-t^2}{p}\right)\right\}$$
$$\times\left\{1+\left(\frac{-2(c+t)}{p}\right)\right\}+O(1)$$
$$=\frac{1}{64}\sum_{\substack{u\neq 0\\ 4u^2r\equiv -(m+u^2)^2}}\sum_r{}'\left\{1+\left(\frac{c^2-(m+u^2)^2/4u^2}{p}\right)\right\}\left\{1+\left(\frac{-2(c+(m+u^2)/2u)}{p}\right)\right\}$$
$$\times\left\{1+\left(\frac{c^2-(m-u^2)^2/4u^2}{p}\right)\right\}\left\{1+\left(\frac{-2(c+(m-u^2)/2u)}{p}\right)\right\}+O(1)$$
$$=\frac{1}{64}\sum_{\substack{u\neq 0\\ 4u^2r\equiv -(m+u^2)^2}}\sum_r{}' C(u)+O(1),$$

where

$$C(u)=\left\{1+\left(\frac{-u^4+(4c^2-2m)u^2-m^2}{p}\right)\right\}\left\{1+\left(\frac{-u^3-2cu^2-mu}{p}\right)\right\}$$
$$\times\left\{1+\left(\frac{-u^4+(4c^2+2m)u^2-m^2}{p}\right)\right\}\left\{1+\left(\frac{u^3-2cu^2-mu}{p}\right)\right\}.$$

Thus

$$m_{44}=\frac{1}{64p}\sum_{\substack{u\neq 0\\ 4u^2r\equiv-(m+u^2)^2}}\sum_{r} C(u)\sum_w{}'\sum_t e(t(w-r)+O(1)$$
$$=\frac{h}{64p}\sum_{\substack{u\neq 0\\ 4u^2r\equiv-(m+u^2)^2}}\sum_{r} C(u)+\frac{1}{64p}\sum_{t\neq 0}\left\{\sum_{\substack{u\neq 0\\ 4u^2r\equiv-(m+u^2)^2}}\sum_{r} C(u)e(-rt)\right\}\left\{\sum_w{}' e(tw)\right\}+O(1)$$
$$=\frac{h}{64p}\sum_{u\neq 0} C(u)+\frac{1}{64p}\sum_{t\neq 0}\left\{\sum_{u\neq 0} C(u)e\{t(m+u^2)^2/4u^2\}\right\}\left\{\sum_w{}' e(tw)\right\}+O(1)$$

and so

$$\left|m_{44}-\frac{h}{64p}\sum_{u\neq 0}C(u)\right|\leq\left|\frac{1}{64p}\max_{1\leq t\leq p-1}\left|\sum_{u\neq 0}C(u)e\{t(m+u^2)^2/4u^2\}\right|\sum_{t\neq 0}\sum_w{}' e(tw)\right|+O(1)$$
$$=O(p^{\frac{1}{2}}\log p),$$

by Perel'muter's results [8]. We must therefore consider

$$\sum_{u\neq 0}\left\{1+\left(\frac{-u^4+(4c^2-2m)u^2-m^2}{p}\right)\right\}\left\{1+\left(\frac{-u^3-2cu^2-mu}{p}\right)\right\}$$
$$\times\left\{1+\left(\frac{-u^4+(4c^2+2m)u^2-m^2}{p}\right)\right\}\left\{1+\left(\frac{+u^3-2cu^2-mu}{p}\right)\right\}. \quad (14.6)$$

In general this is $p+O(p^{\frac{1}{2}})$ except for a few special cases, and so

$$m_{44}=\frac{h}{64}+O(p^{\frac{1}{2}}\log p).$$

It is easy to check that the special cases only occur if $c\equiv 0$, $c^2\equiv m$ or $c^2\equiv -m$.

If $c\equiv 0$, (14.6) becomes

$$\sum_{u\neq 0}\left\{1+\left(\frac{-(u^2+m)^2}{p}\right)\right\}\left\{1+\left(\frac{-u(u^2+m)}{p}\right)\right\}\left\{1+\left(\frac{-(u^2-m)^2}{p}\right)\right\}\left\{1+\left(\frac{u(u^2-m)}{p}\right)\right\}$$
$$=\sum_{u\neq 0}\left\{1+\left(\frac{-1}{p}\right)\right\}^2\left\{1+\left(\frac{-u(u^2+m)}{p}\right)\right\}\left\{1+\left(\frac{u(u^2-m)}{p}\right)\right\}+O(1)$$
$$=2\left\{1+\left(\frac{-1}{p}\right)\right\}\{p+O(p^{\frac{1}{2}})\},$$

so that

$$m_{44}=\left\{1+\left(\frac{-1}{p}\right)\right\}\frac{h}{32}+O(p^{\frac{1}{2}}\log p).$$

If $c^2 \equiv m$, (14.6) becomes

$$\sum_{u\neq 0}\left\{1+\left(\frac{-(u^2-c^2)^2}{p}\right)\right\}\left\{1+\left(\frac{-u(u+c)^2}{p}\right)\right\}\left\{1+\left(\frac{-u^4+6c^2u^2-m^2}{p}\right)\right\}\left\{1+\left(\frac{u(u^2-2cu-c^2)}{p}\right)\right\}$$

$$=\sum_{u\neq 0}\left\{1+\left(\frac{-1}{p}\right)\right\}\left\{1+\left(\frac{-u(u+c)^2}{p}\right)\right\}\left\{1+\left(\frac{-u^4+6c^2u^2-m^2}{p}\right)\right\}$$

$$\times\left\{1+\left(\frac{u(u^2-2cu-c^2)}{p}\right)\right\}+O(1)$$

$$=\left\{1+\left(\frac{-1}{p}\right)\right\}p+O(p^{\frac{1}{2}}),$$

and therefore

$$m_{44}=\left\{1+\left(\frac{-1}{p}\right)\right\}\frac{h}{64}+O(p^{\frac{1}{2}}\log p).$$

The case $c^2 \equiv -m$ is exactly similar. This completes the proof of Lemma 13. Putting together the results of Lemmas 10, 11, 12 and 13 we obtain (using 14.3)

THEOREM 5. *If* $b \equiv 0$,

$$\mathfrak{M}=\begin{cases}\dfrac{h}{16}+O(p^{\frac{1}{2}}\log p), & \textit{if}\quad a\equiv 0,\quad p\equiv 1\,(\mathrm{mod}\,4),\\[2mm] \dfrac{h}{4}+O(p^{\frac{1}{2}}\log p), & \textit{if}\quad a\equiv 0,\quad p\equiv 3\,(\mathrm{mod}\,4),\\[2mm] \dfrac{3h}{32}+O(p^{\frac{1}{2}}\log p), & \textit{if}\quad a^2\equiv 4m,\quad p\equiv 1\,(\mathrm{mod}\,4),\\[2mm] \dfrac{3h}{16}+O(p^{\frac{1}{2}}\log p), & \textit{if}\quad a^2\equiv 4m,\quad p\equiv 3\,(\mathrm{mod}\,4),\\[2mm] \dfrac{3h}{32}+O(p^{\frac{1}{2}}\log p), & \textit{if}\quad a^2\equiv -4m,\quad p\equiv 1\,(\mathrm{mod}\,4),\\[2mm] \dfrac{3h}{16}+O(p^{\frac{1}{2}}\log p), & \textit{if}\quad a^2\equiv -4m,\quad p\equiv 3\,(\mathrm{mod}\,4),\\[2mm] \dfrac{9h}{64}+O(p^{\frac{1}{2}}\log p), & \textit{otherwise.}\end{cases}$$

An immediate corollary of this is

THEOREM 6. *If* $b \equiv 0$, *any arithmetic progression with* $\gg p^{\frac{1}{2}} \log p$ *terms contains a pair of consecutive residues* $(\bmod p)$ *of* $f(x)$.

15. A conjecture. We conclude this paper by making the following

Conjecture. The number $M(f)$ of residues $(\bmod p)$ of a general polynomial $f(x)$ of degree d in an arithmetic progression of h terms is given by

$$M(f) = \lambda h + O(p^{\frac{1}{2}} \log p),$$

where λ is the constant given by Birch and Swinnerton-Dyer [1] and the constant implied by the O-symbol depends only on d.

We remark that it is true when $d = 2$, 3 or 4.

REFERENCES

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

2. L. Carlitz, Note on a quartic congruence, *Amer. Math. Monthly* **63** (1956), 569–571.

3. L. Carlitz and S. Uchiyama, Bounds for exponential sums, *Duke Math. J.* **24** (1957), 37–41.

4. L. E. Dickson, Criteria for the irreducibility of functions in a finite field, *Bull. Amer. Math. Soc.* **13** (1906), 1–8.

5. Yu. I. Manin, On a cubic congruence to a prime modulus, *Amer. Math. Soc. Transl.* **13** (1960), 1–7.

6. K. McCann and K. S. Williams, On the residues of a cubic polynomial, *Canad. Math. Bull.* **10** (1967), 29–38.

7. L. J. Mordell, On the least residue and non-residue of a polynomial, *J. Lond. Math. Soc.* **38** (1963), 451–453.

8. G. I. Perel'muter, On certain sums of characters, *Uspehi Mat. Nauk.* **18** (1963), 145–149.

9. Th. Skolem, The general congruence of 4th degree modulo *p*, *p* prime, *Norske Mat. Tidsskr.* **34** (1952), 73–80.

10. S. Uchiyama, Sur le nombre des valeurs distinctes d'un polynôme à coefficients dans un corps fini, *Proc. Japan Acad.* **30** (1954), 930–933.

11. R. D. Von Sterneck, Über die Anzahl inkongruenter Werte die eine ganze Function dritte Grades annimont, *S.-B. Akad. Wiss. Wien. Math. Kl.* **116** (1907), 895–904.

12. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. et Ind. **1041** (Paris, 1948).

13. K. S. Williams, Pairs of consecutive residues of polynomials, *Canad. J. Math.* **19** (1967), 655–666.

14. K. S. Williams, On the least non-residue of a quartic polynomial, *Proc. Cambridge Phil. Soc.* **62** (1966), 429–431.

MANCHESTER UNIVERSITY
MANCHESTER, ENGLAND

CARLETON UNIVERSITY
OTTAWA, CANADA