ON TWO CONJECTURES OF CHOWLA

Kenneth S. Williams

(received February 7, 1968)

1. Introduction. Let p denote a prime and n a positive integer ≥ 2. Let $N_n(p)$ denote the number of polynomials $x^n + x + a$, $a = 1,2,\ldots,p-1$, which are irreducible (mod p). Chowla [5] has made the following two conjectures:

CONJECTURE 1. *There is a prime* $p_0(n)$, *depending only on* n, *such that for all primes* $p \geq p_0(n)$

$$N_n(p) \geq 1. \tag{1.1}$$

($p_0(n)$ denotes the least such prime.)

CONJECTURE 2.

$$N_n(p) \sim \frac{p}{n}, \; n \text{ fixed}, \; p \to \infty. \tag{1.2}$$

Clearly the truth of conjecture 2 implies the truth of conjecture 1.

Let us begin by noting that both conjectures are true for $n = 2$ and $n = 3$. When $n = 2$ we have

$$N_2(p) = \begin{cases} 1 & , \; p = 2 , \\ \frac{1}{2}(p-1) & , \; p \geq 3 , \end{cases} \tag{1.3}$$

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

so that we can take $p_0(2) = 2$. When $n = 3$ we have [6]

(1.4) $$N_3(p) = \begin{cases} 1 & , \quad p = 2 , \\ 0 & , \quad p = 3 , \\ \frac{1}{3}\left(p - \left(\frac{-3}{p}\right)\right) & , \quad p \geq 5 , \end{cases}$$

so that $p_0(3) = 5$.

In this paper I begin by proving that conjecture 2 (and so conjecture 1) is true when $n = 4$, i.e., $N_4(p) \sim \frac{p}{4}$, as $p \to \infty$. In fact I prove more, namely,

(1.5) $$|N_4(p) - \tfrac{p}{4}| \leq \frac{19}{4} p^{\frac{1}{2}} + 12 , \qquad p > 3 .$$

This is of course a trivial inequality for small values of p, but it does show that $N_4(p) \geq 1$ for $p \geq 457$, so that $p_0(4) \leq 457$. It is very unlikely that there is a simple formula for $N_4(p)$ (not involving character sums) as there is for $N_2(p)$ and $N_3(p)$. In proving (1.5) I use some results of Skolem [9] on the factorization of quartics (mod p) and deep estimates of Perel' muter [8] for certain character sums. The method is not applicable for the estimation of $N_n(p)$ for $n \geq 5$.

It is of interest to estimate the least value of a $(1 \leq a \leq p-1)$ which makes $x^n + x + a$ irreducible (mod p). We denote this least value by $a_n(p)$. $a_2(p)$ exists for all p, $a_3(p)$ exists for all $p \neq 3$ and $a_4(p)$ exists for all $p \geq 457$ (and for other smaller values of p). The existence of $a_n(p)$, for all n and all sufficiently large p, would follow from the truth of conjecture 1.

I conjecture that for each positive integer n there is an infinity of primes p for which $x^n + x + 1$ is irreducible (mod p). This

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

is equivalent to

CONJECTURE 3. *For all* $n \geq 2$

$$\liminf_{p \to \infty} a_n(p) = 1. \tag{1.6}$$

This is easily seen to be true when $n = 2$ (Theorem 3.1) and I also prove that it is true when $n = 3$ (Theorem 3.2). The proof of Theorem 3.2 involves the prime ideal theorem. As regards upper bounds for $a_n(p)$, it is shown that $a_2(p) = O(p^{\frac{1}{4}} \log p)$ (Theorem 4.1) follows from a result of Burgess [3], that $a_3(p) = O(p^{\frac{1}{2}})$ (Theorem 4.2) using a method of Tietäväinen [10], and that $a_4(p) = O(p^{\frac{1}{2}+\varepsilon})$ (Theorem 4.3) using Skolem's results [9] on quartics. Probably the true order of magnitude of these is much smaller, perhaps even $O(p^{\varepsilon})$, for all $\varepsilon > 0$.

Finally I conjecture Chowla's conjecture 2 in the stronger form:

CONJECTURE 4. *Let* $\varepsilon > 0$ *and let* h_p *denote an integer satisfying*

$$p^{\frac{1}{2}+\varepsilon} + 1 \leq h_p \leq p\ . \tag{1.7}$$

Let $N_n(h_p)$ *denote the number of polynomials* $x^n + x + a$, $a = 1,2,\ldots, h_p-1$, *which are irreducible* (mod p). *Then*

$$N_n(h_p) \sim h_p/n, \quad n \text{ fixed}, \quad p \to \infty. \tag{1.8}$$

Conjecture 2 is the special case $h_p = p$. I prove conjecture 4 when $n = 2,3$ and 4.

2. *Estimation of* $N_4(p)$. As I am only interested in estimating

$N_4(p)$ for large values of p, I assume throughout that $p > 3$. The factorization of $x^4 + x + a \pmod p$, for $p > 3$, depends upon that of $y^3 - 4ay - 1 \pmod p$. These two polynomials have the same discriminant, namely,

$$D(a) = 256a^3 - 27 . \tag{2.1}$$

$D(a) \equiv 0 \pmod p$ is a necessary and sufficient condition for both $x^4 + x + a$ and $y^3 - 4ay - 1$ to have squared factors $\pmod p$. Let n_p denote the number of integers a, $0 \le a \le p-1$, such that $D(a) \equiv 0 \pmod p$. We have

$$n_p = \begin{cases} 0 , & \text{if } p \equiv 1 \pmod 3,\ 2^{(p-1)/3} \not\equiv 1 \pmod p , \\ 1 , & \text{if } p \equiv 2 \pmod 3, \\ 3 , & \text{if } p \equiv 1 \pmod 3,\ 2^{(p-1)/3} \equiv 1 \pmod p . \end{cases} \tag{2.2}$$

Let $M(p)$ denote the number of integers a with $1 \le a \le p-1$ and $D(a) \not\equiv 0 \pmod p$ such that $x^4 + x + a \equiv 0 \pmod p$ has exactly two distinct solutions, and $L(p)$ the number of integers a with $1 \le a \le p-1$ and $D(a) \not\equiv 0 \pmod p$ such that $y^3 - 4ay - 1 \equiv 0 \pmod p$ has exactly one root. By results of Skolem [9] we have

$$N_4(p) + M(p) = L(p) . \tag{2.3}$$

LEMMA 2.1.

$$|L(p) - \tfrac{1}{2}(p-1)| \le p^{\frac{1}{2}} + 1 .$$

<u>Proof</u>. It is well-known that $y^3 - 4ay - 1 \equiv 0 \pmod p$ has exactly one unrepeated solution y if and only if $\left(\frac{D(a)}{p}\right) = -1$. Hence

$$L(p) = \frac{1}{2} \sum_{\substack{a=1 \\ D(a) \not\equiv 0}}^{p-1} \left\{ 1 - \left(\frac{D(a)}{p} \right) \right\}$$

$$= \frac{p-1}{2} - \frac{1}{2} \sum_{a=0}^{p-1} \left(\frac{D(a)}{p} \right) + \frac{1}{2} \left(\frac{-3}{p} \right) - \frac{1}{2} n_p .$$

Now the monic cubic polynomial $2^{-8} D(a)$ is square free (mod p) so (see for example lemma 1 in [2]) we have

$$\left| \sum_{a=0}^{p-1} \left(\frac{D(a)}{p} \right) \right| \leq 2p^{\frac{1}{2}} ,$$

giving

$$\left| L(p) - \tfrac{1}{2}(p-1) \right| \leq p^{\frac{1}{2}} + 1 .$$

LEMMA 2.2. $\quad \left| M(p) - \frac{p}{4} \right| \leq \frac{15}{4} p^{\frac{1}{2}} + \frac{21}{2} .$

<u>Proof</u>. $x^4 + x + a \equiv 0 \pmod p$ has exactly two unrepeated distinct solutions (mod p) if and only if $y^3 - 4ay - 1 \equiv 0 \pmod p$ has exactly one solution, y_1 say, such that $\left(\frac{y_1}{p} \right) = +1$. Now $y^3 - 4ay - 1 \equiv 0 \pmod p$ has exactly one unrepeated root if and only if $\left(\frac{D(a)}{p} \right) = -1$. Hence if $\left(\frac{D(a)}{p} \right) = -1$ then

$$\frac{1}{2} \sum_{\substack{y=1 \\ y^3-4ay-1 \equiv 0}}^{p-1} \left\{ 1 + \left(\frac{y}{p} \right) \right\} = \begin{cases} 1, & \text{if the unique root of } y^3-4ay-1 \equiv 0 \text{ is a quadratic residue,} \\ 0, & \text{if the unique root of } y^3-4ay-1 \equiv 0 \text{ is a quadratic non-residue.} \end{cases}$$

Hence

$$M(p) = \frac{1}{2} \sum_{a=1}^{p-1} \sum_{\substack{y=1 \\ \left(\frac{D(a)}{p}\right)=-1 \quad y^3-4ay-1 \equiv 0}}^{p-1} \left\{ 1 + \left(\frac{y}{p}\right) \right\}$$

$$= \frac{1}{4} \sum_{y=1}^{p-1} \sum_{\substack{a=1 \\ a \equiv (y^3-1)/4y \\ D(a) \not\equiv 0}}^{p-1} \left\{ 1 - \left(\frac{D(a)}{p}\right) \right\} \left\{ 1 + \left(\frac{y}{p}\right) \right\}$$

$$= \frac{1}{4} \sum_{\substack{y=1 \\ y^3 \not\equiv 1 \\ D((y^3-1)/4y) \not\equiv 0}}^{p-1} \left\{ 1 - \left(\frac{y^4 D((y^3-1)/4y)}{p}\right) \right\} \left\{ 1 + \left(\frac{y}{p}\right) \right\}$$

$$= \frac{1}{4} \sum_{y=0}^{p-1} \left\{ 1 - \left(\frac{y^4 D((y^3-1)/4y)}{p}\right) \right\} \left\{ 1 + \left(\frac{y}{p}\right) \right\} + A \ ,$$

where $|A| \leq 8$. Now as $\sum_{y=0}^{p-1} \left(\frac{y}{p}\right) = 0$,

$$\sum_{y=0}^{p-1} \left\{ 1 - \left(\frac{y^4 D((y^3-1)/4y)}{p}\right) \right\} \left\{ 1 + \left(\frac{y}{p}\right) \right\} = p - S_o - S_1 \ ,$$

where

(2.4) $$S_i = \sum_{y=0}^{p-1} \left(\frac{y^{4+i} D((y^3-1)/4y)}{p}\right) , \quad i = 0,1,$$

so

(2.5) $$M(p) = \frac{1}{4}(p - S_o - S_1) + A \ .$$

Suppose that

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

$$2^{-2}y^4D((y^3-1)/4y) \equiv (y^9-3y^6-2^{-2}.15y^3-1)y \equiv \{f(y)\}^2 \; g(y) \pmod p ,$$

where $f(y)$ is a polynomial of degree d $(0 \le d \le 5)$ and $g(y)$ is a square-free polynomial of degree e $(0 \le e \le 10)$. Clearly $2d + e = 10$. As $y \mid \{f(y)\}^2 g(y)$, $y^2 \nmid \{f(y)\}^2 g(y)$ we have $y \nmid f(y)$, $y \mid g(y)$ so that $e \neq 0$. Hence $e = 2,4,6,8$ or 10.

Now

$$S_o = \sum_{y=0}^{p-1} \left(\frac{\{f(y)\}^2 \; g(y)}{p}\right)$$

$$= \sum_{y=0}^{p-1} \left(\frac{g(y)}{p}\right) - \sum_{\substack{y=0 \\ f(y) \equiv 0}}^{p-1} \left(\frac{g(y)}{p}\right) .$$

Clearly

$$\left| \sum_{\substack{y=0 \\ f(y) \equiv 0}}^{p-1} \left(\frac{g(y)}{p}\right) \right| \le d \le 4$$

and by Perel' muter's results [8]

$$\left| \sum_{y=0}^{p-1} \left(\frac{g(y)}{p}\right) \right| \le (e-2)p^{\frac{1}{2}} + 1 \le 8p^{\frac{1}{2}} + 1 .$$

Hence

(2.6) $$|S_o| \le 8p^{\frac{1}{2}} + 5 .$$

Similarly

(2.7) $$|S_1| \le 7p^{\frac{1}{2}} + 5 .$$

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

Putting (2.5), (2.6) and (2.7) together we obtain

$$|M(p) - p/4| \leq \frac{15}{4}p^{\frac{1}{2}} + \frac{21}{2} .$$

From (2.3) and lemmas 2.1 and 2.2 we have

THEOREM 2.3. $\quad |N_4(p) - \frac{p}{4}| < \frac{19}{4}p^{\frac{1}{2}} + 12 .$

3. <u>Calculation of</u> $\liminf_{p \to\infty} a_n(p)$ <u>for</u> $n = 2$ <u>and</u> 3.

THEOREM 3.1. $\quad \liminf_{p \to\infty} a_2(p) = 1 .$

<u>Proof</u>. $x^2 + x + 1$ is irreducible (mod p) if and only if $\left(\frac{-3}{p}\right) = -1$, that is, for all primes $p \equiv 2 \pmod 3$.

THEOREM 3.2. $\quad \liminf_{p \to\infty} a_3(p) = 1 .$

<u>Proof</u>. We suppose that $\liminf a_3(p) \neq 1$. Hence there are only a finite number of primes such that $x^3 + x + 1$ is irreducible (mod p). Thus there is a prime p_o such that for all primes $p > p_o$, $x^3 + x + 1$ is reducible (mod p). The discriminant of $x^3 + x + 1$ is -31, so $x^3 + x + 1$ has a squared factor (mod p) if and only if $p = 31$. Hence for all $p > p_1 = \max(p_o, 31)$, $x^3 + x + 1$ is reducible (mod p) into distinct factors. Let $\nu(p)$ denote the number of incongruent solutions $x \pmod p$ of $x^3 + x + 1 \equiv 0 \pmod p$. Then

(3.1) $$\nu(p) = 1 \text{ or } 3 \text{ for all } p > p_1 .$$

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

Let

$$(3.2)\qquad P_i(x) = \left\{p \mid p_1 < p \leq x\ ,\ \nu(p) = i\right\} \qquad (i = 1 \text{ or } 3)$$

so that

$$P_1(x) \cap P_3(x) = \emptyset$$

and

$$P_1(x) \cup P_3(x) = \left\{p \mid p_1 < p \leq x\right\}\ .$$

Let $n\ (P_i(x))$ $(i = 1$ or $3)$ denote the number of primes in $P_i(x)$ so

$$(3.3)\qquad n\ (P_1(x)) + n\ (P_3(x)) = \pi(x) - \pi(p_1)\ ,$$

where $\pi(t)$ denotes the number of primes $\leq t$. Hence

$$(3.4)\qquad \lim_{x\to\infty} \frac{\ln x}{x}\ (n\ (P_1(x)) + n\ (P_3(x))) = 1\ ,$$

by the prime number theorem. Now

$$\sum_{p_1 < p \leq x} \nu(p) = \sum_{\substack{p_1 < p \leq x \\ \nu(p) = 1}} \nu(p) + \sum_{\substack{p_1 < p \leq x \\ \nu(p) = 3}} \nu(p)$$

$$= n\ (P_1(x)) + 3n\ (P_3(x))$$

so that

$$(3.5)\qquad \lim_{x\to\infty} \frac{\ln x}{x} \left\{n\ (P_1(x)) + 3n\ (P_3(x))\right\}$$

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

$$= \lim_{x \to \infty} \frac{\ln x}{x} \sum_{p_1 < p \leq x} \nu(p)$$

$$= \lim_{x \to \infty} \frac{\ln x}{x} \sum_{p \leq x} \nu(p)$$

$$= 1 ,$$

by the prime ideal theorem, as $x^3 + x + 1$ is irreducible over the integers. Hence from (3.4) and (3.5) we have

$$\lim_{x \to \infty} \frac{\ln x}{x} n\, (P_1(x)) = 1 . \tag{3.6}$$

Now $x^3 + x + 1 \equiv 0 \pmod p$ has exactly one distinct root if and only if $\left(\frac{-31}{p}\right) = -1$ so

$$n(P_1(x)) = \sum_{\substack{p_1 < p \leq x \\ \left(\frac{-31}{p}\right) = -1}} 1$$

$$= \frac{1}{2} \sum_{p_1 < p \leq x} \left\{1 + \left(\frac{-31}{p}\right)\right\}$$

$$+ \frac{1}{2}\left\{\pi(x) - \pi(p_1)\right\} + \frac{1}{2} \sum_{p_1 < p \leq x} \left(\frac{-31}{p}\right)$$

giving

$$\lim_{x \to \infty} \frac{\ln x}{x} n(P_1(x)) = \frac{1}{2} , \tag{3.7}$$

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

as

$$\sum_{p_1 < p \le x} \left(\frac{-31}{p}\right) = o(x/\ln x) .$$

(3.6) and (3.7) give the required contradiction.

4. Upper bounds for $a_n(p)$, $n = 2,3,4$.

We now obtain upper bounds for $a_2(p)$, $a_3(p)$ and $a_4(p)$.

THEOREM 4.1. $a_2(p) = 0(p^{\frac{1}{4}} \ln p)$.

Proof. $x^2 + x + a$ is irreducible (mod p) if and only if $\left(\frac{1-4a}{p}\right) = -1$. Hence, as $a_2(p)$ is the least such positive a, $\left(\frac{1-4a}{p}\right) = +1$, for $a = 1,2,\ldots, a_2(p) - 1$, except if smallest positive solution b of $4b \equiv 1 \pmod p$ satisfies $1 \le b < a_2(p)$, in which case the Legendre symbol corresponding to $a = b$ is zero. We consider two cases, according as $b \ge a_2(p)$ or $1 \le b < a_2(p)$. If $b \ge a_2(p)$

$$(4.1) \qquad \left(\frac{-b+a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4b-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{1-4a}{p}\right) = \left(\frac{-1}{p}\right)$$

for $a = 1,2,\ldots, a_2(p) - 1$ so that

$$(4.2) \qquad \left\{-b+1, -b+2, \ldots, -b+a_2(p) - 1\right\}$$

is a sequence of $a_2(p) - 1$ consecutive quadratic residues (mod p) if $p \equiv 1 \pmod 4$ and a sequence of $a_2(p) - 1$ quadratic non-residues if $p \equiv 3 \pmod 4$. Burgess [3] has proved that the maximum number of consecutive quadratic residues or non-residues (mod p) is $0(p^{\frac{1}{4}} \ln p)$. Hence $a_2(p) - 1 = 0(p^{\frac{1}{4}} \ln p)$, that is, $a_2(p) = 0(p^{\frac{1}{4}} \ln p)$, as required.

If $1 \leq b < a_2(p)$, we consider in place of (4.2) the longer of the two sequences $-b+1, -b+2, \ldots, -1$ and $1, 2, \ldots, -b+a_2(p)-1$; it contains at least $\frac{a_2(p)}{2} - 1$ terms.

THEOREM 4.2. $a_3(p) = O(p^{\frac{1}{2}})$.

Proof. Let $N(a)$ denote the number of solutions x of the congruence

$$x^3 + x + a \equiv 0 \pmod p .$$

Clearly $N(a) = 0, 1, 2$ or 3. Set

$$\phi(a) = \frac{1}{3}\left\{1 - N(a)\right\}\left\{3 - N(a)\right\} . \tag{4.3}$$

Now $N(a) = 2$ if and only if $-4-27a^2 \equiv 0 \pmod p$ hence

$$\phi(a) = \begin{cases} 1, & \text{if } x^3 + x + a \text{ is irreducible } (\mathrm{mod}\ p), \\ 0, & \text{if } x^3 + x + a \text{ is reducible } (\mathrm{mod}\ p),\ -4-27a^2 \not\equiv 0, \\ -\frac{1}{3}, & \text{if } x^3 + x + a \text{ is reducible } (\mathrm{mod}\ p),\ -4-27a^2 \equiv 0. \end{cases} \tag{4.4}$$

Let h denote an integer such that $1 \leq h \leq \frac{1}{2}(p+1)$, so that $0 \leq h-1 \leq \frac{1}{2}(p-1)$. Set $H = \{0, 1, 2, \ldots, h-1\}$ and write $H(a)$, $(a = 0, 1, 2, \ldots, p-1)$, for the number of solutions of

$$x + y \equiv a \pmod p \quad , \quad x \in H \ , \ y \in H .$$

We set

$$A(p) = \sum_{\substack{a=0 \\ -4-27a^2 \not\equiv 0}}^{p-1} \phi(a) H(a) . \tag{4.5}$$

Now

(4.6) $$pH(a) = \sum_{t=0}^{p-1} \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} e\{t(x+y-a)\}$$

where $e(\nu) = \exp(2\pi i\nu/p)$. Hence

(4.7) $$pA(p) = \sum_{t=0}^{p-1} \left\{ \sum_{\substack{a=0 \\ -4-27a^2 \not\equiv 0}}^{p-1} \phi(a)e(-at) \right\} \left\{ \sum_{x=0}^{h-1} e(tx) \right\}^2 ,$$

which gives, on picking out the term with $t = 0$,

(4.8) $$\left| pA(p) - h^2 \sum_{\substack{a=0 \\ -4-27a^2 \not\equiv 0}}^{p-1} \phi(a) \right|$$

$$= \left| \sum_{t=1}^{p-1} \left\{ \sum_{\substack{a=0 \\ -4-27a^2 \not\equiv 0}}^{p-1} \phi(a)e(-at) \right\} \left\{ \sum_{x=0}^{h-1} e(tx) \right\}^2 \right|$$

$$\leq \sum_{t=1}^{p-1} \left| \sum_{\substack{a=0 \\ -4-27a^2 \not\equiv 0}}^{p-1} \phi(a)e(-at) \right| \left| \sum_{x=0}^{h-1} e(tx) \right|^2 .$$

We note that from (4.4) and (1.4) we have

(4.9) $$\sum_{\substack{a=0 \\ -4-27a^2 \not\equiv 0}}^{p-1} \phi(a) = N_3(p) = \frac{1}{3}\left\{p - \left(\frac{-3}{p}\right)\right\} .$$

Now

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

$$\left|\sum_{\substack{a=0\\ -4-27a^2\not\equiv 0}}^{p-1} \phi(a)e(-at)\right| = \left|\sum_{a=0}^{p-1} \phi(a)e(-at) - \sum_{\substack{a=0\\ -4-27a^2\equiv 0}}^{p-1} \phi(a)e(-at)\right|$$

$$\leq \left|\sum_{a=0}^{p-1} \phi(a)e(-at)\right| + \frac{2}{3} .$$

For $t = 1,2,\ldots, p-1$

$$\sum_{a=0}^{p-1} \phi(a)e(-at) = \sum_{a=0}^{p-1} \frac{1}{3}\left\{1-N(a)\right\}\left\{3-N(a)\right\} e(-at)$$

$$= \sum_{a=0}^{p-1} e(-at) - \frac{4}{3}\sum_{a=0}^{p-1} N(a)e(-at)+\frac{1}{3}\sum_{a=0}^{p-1}\left\{N(a)\right\}^2 e(-at)$$

$$= \frac{1}{3}\sum_{a=0}^{p-1}\left\{N(a)\right\}^2 e(-at) - \frac{4}{3}\sum_{a=0}^{p-1} N(a)e(-at) ,$$

as $\sum_{a=0}^{p-1} e(-at) = 0$, when $t \not\equiv 0 \pmod p$. Now

$$\left|\sum_{a=0}^{p-1} N(a)e(-at)\right| = \left|\sum_{a=0}^{p-1}\left\{\frac{1}{p}\sum_{x,u=0}^{p-1} e\left(u\left(x^3+x+a\right)\right)\right\} e(-at)\right|$$

$$= \left|\frac{1}{p}\sum_{x,u=0}^{p-1} e\left(u\left(x^3+x\right)\right)\sum_{a=0}^{p-1} e(a(u-t))\right|$$

$$= \left|\sum_{x=0}^{p-1} e\left(t\left(x^3+x\right)\right)\right|$$

$$\leq 2p^{\frac{1}{2}} ,$$

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

by a result of Carlitz and Uchiyama [4]. Similarly

$$\left|\sum_{a=0}^{p-1}\{N(a)\}^2 e(-at)\right| = \left|\sum_{\substack{x,y=0\\ x^3+x-y^3-y\equiv 0}}^{p-1} e(t(y^3+y))\right|$$

$$\leq \left|\sum_{x=0}^{p-1} e(t(x^3+x))\right| + \left|\sum_{\substack{x,y=0\\ x\not\equiv y\\ x^2+xy+y^2+1\equiv 0}}^{p-1} e(t(y^3+y))\right|$$

$$\leq 2p^{\frac{1}{2}} + \left|\sum_{\substack{x,y=0\\ x^2+xy+y^2+1\equiv 0}}^{p-1} e(t(y^3+y))\right| + \left|\sum_{\substack{y=0\\ 3y^2+1\equiv 0}}^{p-1} e(t(y^3+y))\right|$$

By a result of Bombieri and Davenport [1] the middle term is less than or equal to $18p^{\frac{1}{2}} + 9$ and the last term is clearly less than or equal to 2. Putting these estimates together we have

$$\left|\sum_{\substack{a=0\\ -4-27a^2\not\equiv 0}}^{p-1} \phi(a)e(-at)\right| \leq \frac{1}{3}(28p^{\frac{1}{2}} + 13) .$$

Hence from (4.8) and (4.9) we have

$$\left|pA(p) - \frac{h^2}{3}\left(p-\left(-3/p\right)\right)\right|$$

$$\leq \frac{1}{3}(28p^{\frac{1}{2}} + 13)\sum_{t=1}^{p-1}\left|\sum_{x=0}^{h-1} e(tx)\right|^2$$

$$= \frac{1}{3}(28p^{\frac{1}{2}} + 13)h(p-h)$$

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

giving

$$pA(p) \geq \frac{h^2}{3}\left(p-\left(\frac{-3}{p}\right)\right) - \frac{1}{3}(28p^{\frac{1}{2}} + 13)h(p-h)$$

$$\geq \frac{h^2 p}{6} - 14hp^{3/2}$$

$$= \frac{ph}{6}\left\{h - 84p^{\frac{1}{2}}\right\} .$$

Choose $h = [84p^{\frac{1}{2}}] + 1$, so that $A(p) > 0$ i.e.,

$$\sum_{\substack{a=0 \\ -4-27a^2 \neq 0}}^{p-1} \phi(a)H(a) > 0 .$$

Hence there exists a, $0 \leq a \leq p-1$, for which

$$-4-27a^2 \neq 0 , \quad \phi(a) > 0 , \quad H(a) > 0 ,$$

i.e., for which x^3+x+a is irreducible $\pmod p$ and moreover

$$a = x+y , \quad x,y \in H ,$$

so that

$$0 \leq a \leq 2(h-1) = 2[84p^{\frac{1}{2}}] .$$

Hence

$$a_3(p) \leq 168p^{\frac{1}{2}}$$

as required.

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

THEOREM 5.1. *If* $p^{\frac{1}{4}+\varepsilon} < h_p \leq p$,

(5.1) $$N_2(h_p) \sim \frac{1}{2} h_p \quad , \quad \text{as} \quad p \to \infty .$$

Proof. x^2+x+a is irreducible (mod p) if and only if

$$\left(\frac{1-4a}{p}\right) = -1 .$$

Hence

$$N_2(h_p) = \sum_{\substack{a=1 \\ \left(\frac{1-4a}{p}\right) = -1}}^{h_p-1} 1$$

$$= \frac{1}{2} \sum_{a=0}^{h_p-1} \left\{1 - \left(\frac{1-4a}{p}\right)\right\} - \frac{1}{2} \ell_p \quad ,$$

where

$$\ell_p = \begin{cases} 1, & \text{if there exists a such that } 1 \leq a \leq h_p-1,\ 4a \equiv 1 \pmod p), \\ 0, & \text{otherwise.} \end{cases}$$

Thus

$$\left|\frac{1}{h_p} (2N_2(h_p) + \ell_p) - 1\right| = \frac{1}{h_p}\left|\sum_{a=0}^{h_p-1} \left(\frac{1-4a}{p}\right)\right| .$$

As $h_p > p^{\frac{1}{4}+\varepsilon}$, by a result of Burgess [2], for any $\delta > 0$ there exists $p_0(\delta,\varepsilon)$ such that for all $p \geq p_0$ we have

$$\left|\frac{1}{h_p} \sum_{a=0}^{h_p-1} \left(\frac{1-4a}{p}\right)\right| < \delta ,$$

giving

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

THEOREM 4.3. $a_4(p) = O(p^{\frac{1}{2}+\varepsilon})$.

Proof. Let $M(h_p)$ denote the number of integers a with $1 \le a \le h_p-1$, where $p^{\frac{1}{2}+\varepsilon} \le h_p \le p$ and $D(a) \not\equiv 0 \pmod p$, such that $x^4+x+a \equiv 0 \pmod p$ has exactly two distinct solutions; let $L(h_p)$ the number of integers a with $1 \le a \le h_p-1$ and $D(a) \not\equiv 0 \pmod p$ such that $y^3-4ay-1 \equiv 0 \pmod p$ has exactly one root. We have [9]

$$N_4(h_p) + M(h_p) = L(h_p) \quad . \tag{4.10}$$

Similarly to lemmas 2.1 and 2.2, using incomplete character sums in place of complete ones, we can show that

$$L(h_p) = \frac{1}{2} h_p + O(p^{\frac{1}{2}}\ln p) \tag{4.11}$$

and

$$M(h_p) = \frac{1}{4} h_p + O(p^{\frac{1}{2}}\ln p) \quad . \tag{4.12}$$

(The method is illustrated in [7]). Hence

$$N_4(h_p) = \frac{1}{4} h_p + O(p^{\frac{1}{2}}\ln p) \quad . \tag{4.13}$$

As $h_p \ge p^{\frac{1}{2}+\varepsilon}$, for some $\varepsilon > 0$, the term $h_p/4$ in (4.13) dominates the error term $O(p^{\frac{1}{2}}\ln p)$ for $p \ge p_0(\varepsilon)$. Hence for $p \ge p_0(\varepsilon)$, $N_4(h_p) > 0$ i.e., $N_4(h_p) \ge 1$, and so

$$a_4(p) \le p^{\frac{1}{2}+\varepsilon} \quad .$$

5. Asymptotic estimates for $N_i(h_p)$ $(i = 2,3,4)$

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

$$\lim_{p\to\infty} \frac{1}{h_p}(2N_2(h_p) + \ell_p) = 1 .$$

As $\ell_p = 0$ or 1 and $h_p > p^{\frac{1}{4}+\varepsilon}$ we have

$$\lim_{p\to\infty} \frac{\ell_p}{h_p} = 0 ,$$

so

$$\lim_{p\to\infty} \frac{2N_2(h_p)}{h_p} = 1 ,$$

establishing (5.1).

THEOREM 5.2. *Let* $\varepsilon > 0$ *and let* h_p *denote an integer satisfying*

$$p^{\frac{1}{2}+\varepsilon} \le h_p \le p ;$$

then

$$N_3(h_p) \sim \frac{h_p}{3} \tag{5.2}$$

and

$$N_4(h_p) \sim \frac{h_p}{4} , \quad \text{as } p\to\infty. \tag{5.3}$$

Proof. (5.2) is established in my paper [6], as I showed there (in different notation) that

$$N_3(h_p) = h_p/3 + O(p^{\frac{1}{2}}\ln p) .$$

(5.3) is contained in the proof of theorem 4.3.

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

REFERENCES

1. E. Bombieri and H. Davenport, On two problems of Mordell. Amer. J. Math. 88 (1966) 61-70.

2. D.A. Burgess, The distribution of quadratic residues and non-residues. Mathematika 4 (1957) 106-112.

3. D.A. Burgess, A note on the distribution of residues and non-residues. Jour. Lond. Math. Soc. 38 (1963) 253-256.

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

5. S. Chowla, A note on the construction of finite Galois fields $GF(p^n)$. Jour. Math. Anal. Appl. 15 (1966) 53-54.

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

7. K. McCann and K.S. Williams, The distribution of the residues of a quartic polynomial. Glasgow Math. J. 8 (1967) 67-88.

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. A. Tietäväinen, On non-residues of a polynomial. Ann. Univ. Turku. Ser A 1 94 (1966) 3-6.

Carleton University
Ottawa

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press

ADDENDUM: After this paper was written, Professor Philip A. Leonard of Arizona State University kindly informed me that he had proved my theorem 2.3 in the form $N_4(p) = \frac{p}{4} + 0\,(p^{\frac{1}{2}})$, in Norske Vid. Selsk. Forh. 40 (1967), 96-97. His paper on factoring quartics (mod p), J. Number Theory 1 (1969), 113-115 contains a simple proof of the results of Skolem [9] which I use in this paper.

https://doi.org/10.4153/CMB-1969-072-5 Published online by Cambridge University Press