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 $f(x) \pmod{p}$ satisfies

$$\ell \leq d\, p^{1/2} \log p ,$$

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 $f(x) \pmod{p}$ is* $O(p^{1/2} \log p)$. It is the purpose of this note to discuss the distribution of the residues of the cubic $f(x) \pmod{p}$ 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 $a \not\equiv 0 \pmod{p}$. Let

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

---

* Unless otherwise stated all constants implied by O-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) $$n_1 = \frac{1}{2} \{p + (\frac{-3}{p}) - (\frac{-3a}{p}) - 1\} ,$$

(4) $$n_2 = (\frac{-3a}{p}) + 1$$

and

(5) $$n_3 = \frac{1}{6} \{p - (\frac{-3}{p}) - 3(\frac{-3a}{p}) - 3\} .$$

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

(6) $$\frac{1}{3} \{ 2p + (\frac{-3}{p}) \} = \frac{2}{3} p + 0(1) , \qquad \text{as } p \to \infty .$$

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) $$\frac{2}{3} h + 0(p^{1/2} \log p) .$$

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

https://doi.org/10.4153/CMB-1967-004-0 Published online by Cambridge University Press

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,

$$(10) \qquad \sum_{y=1}^{p-1} \left| \sum_{x=1}^{h} e(yx) \right| \leq p \log p ,$$

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

$$(11) \qquad \left| \sum_{x=1}^{p} e(f(x)) \right| \leq (d-1)p^{1/2} ,$$

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

$$(12) \qquad \left| \sum_{x=1}^{p-1} e(ax + bx^{-1}) \right| \leq 2p^{1/2} ,$$

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

$$(13) \qquad m_i = \sum_{\substack{r=1 \\ N_r = i}}^{h} 1 \qquad (i = 0, 1, 2, 3) \quad ,$$

so that we require $m_1 + m_2 + m_3$. From [4] we have

$$(14) \qquad m_2 = O(1)$$

and from Mordell's paper [4]

https://doi.org/10.4153/CMB-1967-004-0 Published online by Cambridge University Press

(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

$$m_1 = \frac{1}{2} \sum_{r=1}^{h} \left\{ 1 - \left(\frac{-4a^3 - 27r^2}{p}\right)\right\} + 0(1) .$$

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

$$\sum_{r=1}^{h} \left(\frac{-4a^3 - 27r^2}{p}\right) = 0(p^{1/2} \log p)$$

so that

(16) $$m_1 = \frac{1}{2}h + 0(p^{1/2} \log p) .$$

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

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

so that the number of such pairs is just

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

From (4) n_{i2}, $n_{2j} = 0(1)$ for $0 \leq i, j \leq 3$. Also it is easy to

https://doi.org/10.4153/CMB-1967-004-0 Published online by Cambridge University Press

show that $n_{13} = n_{31}$ so it suffices to evaluate n_{11}, n_{13} and n_{33}. We begin by showing that

$$n_{11} = \frac{p}{4} + 0(p^{1/2}) . \tag{19}$$

We have

$$n_{11} = \sum_{\substack{r=1 \\ \left(\frac{-4a^3 - 27r^2}{p}\right) = -1 ,\ \left(\frac{-4a^3 - 27(r+1)^2}{p}\right) = -1}}^{p} 1$$

$$= \frac{1}{4} \sum_{r=1}^{p} \left\{ 1 - \left(\frac{-4a^3 - 27r^2}{p}\right)\right\}\left\{1 - \left(\frac{-4a^3 - 27(r+1)^2}{p}\right)\right\} + 0(1)$$

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

$$+ \frac{1}{4} \sum_{r=1}^{p} \left(\frac{(-4a^3 - 27r^2)(-4a^3 - 27(r+1)^2)}{p}\right) + 0(1) .$$

The first two character sums are $0(1)$ 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 (mod p) a square in r .

We next prove that

$$n_{13} = \frac{p}{12} + 0(p^{1/2}) . \tag{20}$$

We do this by showing that

$$n_{11} + 2n_{12} + 3n_{13} = \frac{p}{2} + 0(p^{1/2}) . \tag{21}$$

(20) follows since we know n_{11} and n_{12}. We have

https://doi.org/10.4153/CMB-1967-004-0 Published online by Cambridge University Press

$$\sum_{j=0}^{3} jn_{1j} = \sum_{j=0}^{3} j \sum_{\substack{r=1 \\ N_r=1 \\ N_{r+1}=j}}^{p} 1 = \sum_{\substack{r=1 \\ N_r=1}}^{p} N_{r+1}$$

$$= \sum_{\substack{r=1 \\ \left(\frac{-4a^3-27r^2}{p}\right)=-1}}^{p} \sum_{\substack{x=1 \\ x^3+ax \equiv r+1}}^{p} 1$$

$$= \frac{1}{2} \sum_{x=1}^{p} \{1 - \left(\frac{-4a^3 - 27(x^3+ax-1)^2}{p}\right)\} + 0(1)$$

$$= \frac{p}{2} - \frac{1}{2} \sum_{x=1}^{p} \left(\frac{-4a^3 - 27(x^3+ax-1)^2}{p}\right) + 0(1) .$$

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

Finally consider

$$n_{11} + 2(n_{12} + n_{21}) + 3(n_{13} + n_{31}) + 4n_{22} + 6(n_{23} + n_{32}) + 9n_{33} .$$

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

$$p + 0(p^{1/2}) .$$

Hence

(22) $$n_{33} = \frac{p}{36} + 0(p^{1/2}) .$$

https://doi.org/10.4153/CMB-1967-004-0 Published online by Cambridge University Press

Thus the number of pairs of consecutive residues is

(23) $$\frac{4}{9} p + 0(p^{1/2}) .$$

We conclude by calculating the number of pairs of residues of $x^3 + ax \pmod p$ in (8). We define m_{ij} $(0 \leq i, j \leq 3)$ by

(24) $$m_{ij} = \sum_{\substack{r=1 \\ N_r = i,\ N_{r+1} = j}}^{p} 1 .$$

From (4) we have m_{i2}, $m_{2j} = 0(1)$ $(0 \leq i, j \leq 3)$ and, much as before, we can show that

(25) $$m_{11} = \frac{h}{4} + 0(p^{1/2} \log p)$$

and

(26) $$m_{13} = m_{31} = \frac{h}{12} + 0(p^{1/2} \log p) .$$

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

$$\sum_{\substack{x, y=1 \\ \emptyset(x, y) \equiv 0 \pmod p}}^{p} e(f(x))$$

where $\emptyset(x, y)$ is absolutely irreducible $\pmod p$. We have

$$m_{11} + 2(m_{12} + m_{21}) + 3(m_{13} + m_{31}) + 4m_{22} + 6(m_{23} + m_{32}) + 9m_{33}$$

$$= \sum_{r=1}^{h} N_r N_{r+1}$$

https://doi.org/10.4153/CMB-1967-004-0 Published online by Cambridge University Press

$$= \frac{1}{p} \sum_{r=1}^{p} \sum_{s=1}^{h} \sum_{t=1}^{p} N_r \, N_{r+1} \quad e(t(r-s))$$

$$= \frac{h}{p} \sum_{r=1}^{p} N_r \, N_{r+1} + \frac{1}{p} \sum_{t=1}^{p-1} \left\{ \sum_{r=1}^{p} N_r \, N_{r+1} \, e(tr) \right\} \left\{ \sum_{s=1}^{h} e(-st) \right\} .$$

Hence

$$\left| m_{11} + 2(m_{12} + m_{21}) + \ldots + 9m_{33} - \frac{h}{p} (p + 0(p^{1/2})) \right|$$

$$\leq \max_{1 \leq t \leq p-1} \left| \sum_{r=1}^{p} N_r \, N_{r+1} \quad e(tr) \right| \log p .$$

Now

$$\sum_{r=1}^{p} N_r \, N_{r+1} \quad e(tr)$$

$$= \frac{1}{p^2} \sum_{r=1}^{p} \sum_{x=1}^{p} \sum_{u=1}^{p} e\,\{u(f(x) - r)\} \sum_{y=1}^{p} \sum_{v=1}^{p} e\,\{v(f(y) - r - 1)\} \quad e(tr)$$

$$= \frac{1}{p^2} \sum_{x,y,u,v=1}^{p} e\,\{uf(x) + vf(y) - v\} \sum_{r=1}^{p} e\,\{(t-u-v)r\}$$

$$= \frac{1}{p} \sum_{x,y,v=1}^{p} e\,\{(t-v)f(x) + vf(y) - v\}$$

$$= \frac{1}{p} \sum_{x,y=1}^{p} e\,\{tf(x)\} \sum_{y=1}^{p} e\,\{v(f(y) - f(x) - 1)\}$$

$$= \sum_{\substack{x,y=1 \\ f(y)-f(x)-1 \equiv 0}}^{p} e(tf(x)) \quad .$$

https://doi.org/10.4153/CMB-1967-004-0 Published online by Cambridge University Press

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

$$m_{33} = \frac{h}{36} + 0(p^{1/2} \log p) \tag{27}$$

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

$$\frac{4h}{9} + 0(p^{1/2} \log p) . \tag{28}$$

This implies that the least triple of consecutive positive residues of $x^3 + ax \pmod p$ is also $0(p^{1/2} \log p)$.

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 $a \not\equiv 0 \pmod p$.

This has been verified for $k = 1$ and 2.

REFERENCES

1. E. Bombieri and H. Davenport, On Two Problems of Mordell. Amer. Jour. Math., 88 (1966), pages 61-70.

2. L. Carlitz and S. Uchiyama, Bounds for Exponential Sums. Duke Math. Jour., 24 (1957), pages 37-41.

3. S. Lang and A. Weil, Number of Points of Varieties in Finite Fields. Amer. Jour. Math., 76 (1954), pages 819-827.

https://doi.org/10.4153/CMB-1967-004-0 Published online by Cambridge University Press

4. L. J. Mordell, On the Least Residue and Non-residue of a Polynomial. Jour. Lond. Math. Soc., 38 (1963), pages 451-453.

5. G.I. Perel'muter, On Certain Sums of Characters. Uspektii Matematicheskikh Nauk., 18 (1963), pages 145-149.

6. A. Weil, On Some Exponential Sums. Proc. Nat. Acad. Sci. (U.S.A.), 34 (1948), pages 204-207.

Manchester University
Manchester, England

Carleton University
Ottawa, Canada