Proc. Camb. Phil. Soc. (1968), **64**, 655
PCPS 64–81
Printed in Great Britain

Cubic polynomials with the same residues (mod p)

BY K. MCCANN AND K. S. WILLIAMS
University of Manchester

(*Received* 8 *June* 1966)

1. *Introduction.* Some recent work by the authors (1) on the distribution of the residues of a cubic polynomial modulo an odd prime p led to the conjecture that, in general, two cubic polynomials with integer coefficients possessing the same residues modulo p (not necessarily occurring to the same multiplicity) are equivalent, that is are related by a linear transformation modulo p. The purpose of the present paper is to prove this conjecture. We establish the following theorem.

THEOREM. *If $p > 7$ is an odd prime and $f(x)$, $g(y)$ are cubic polynomials in x and y respectively with integer coefficients, possessing the same residues* (mod p) *then either* (i) *there exist integers $a \not\equiv 0$ and b such that $f(ay+b) \equiv g(y)$ for all integers y or* (ii) *we have $p \equiv 2 \pmod 3$ and integers $a \not\equiv 0, b, c$ and $a' \not\equiv 0, b', c'$ exist such that*

$$f(x) \equiv a(x+b)^3+c \quad \text{and} \quad g(y) \equiv a'(y+b')^3+c.\dagger$$

It will be observed that if (i) or (ii) of our theorem is satisfied then $f(x), g(y)$ certainly possess the same residues mod p. For (i) this is obvious; for (ii) it follows from the fact that, if $p \equiv 2 \pmod 3$, every residue of p is a cubic residue and hence the residues of $f(x)$ or $g(y)$ form a complete set (mod p).

The proof of the theorem depends on combining some results of (1) together with a deep theorem of Perel'muter (2). In this way we are able to deal with all primes $p > 41$; for the remainder we have only a finite number of cases to consider and these we have verified by computer (see §4). The computations showed, in particular, that the theorem would not be valid for $p = 3$, 5 or 7; the pairs x^3, y^3+1; x^3+3x, y^3+4y; x^3+3x, $2y^3+2y$ are not equivalent modulo 3, 5, 7 respectively but possess the same residues namely 0, 1, 2; 0, 1, 4 and 0, 1, 3, 4, 6. The theorem would hold also for $p = 5$, 7 if the residues were assumed to occur to the same multiplicity.

2. *Preliminary transformations.* We shall suppose throughout that p, $f(x)$ and $g(y)$ satisfy the hypotheses of the theorem, the leading coefficients of the polynomials being assumed relatively prime to p. Since a linear transformation on x or y does not affect the residues of the polynomials, and, moreover, since $p > 3$, there is no loss of generality in supposing that the coefficients of x^2, y^2 in $f(x)$, $g(y)$ respectively are 0. By subtracting the same integer from each polynomial we may suppose, again without loss of generality, that the constant coefficient in $f(x)$ is 0. Furthermore, we may suppose now that the constant coefficient $g(0)$ in $g(y)$ is also 0. For since $f(x), g(y)$ have the

† Here, as subsequently, all congruences are supposed to be taken modulo p, unless otherwise specified.

same residues, the congruence $f(x) \equiv g(0)$ is soluble for x. Since further $f(-x) = -f(x)$ we see that $-g(0) \equiv g(y)$ is soluble for y, and this implies that also $g(y) \equiv 3g(0)$ is soluble for y by virtue of the identity $g(y) = -g(-y) + 2g(0)$. It is now easily verified by induction that $f(x) \equiv (2n-1)\,g(0), g(y) \equiv (2n+1)\,g(0)$ are soluble for each positive integer n. But if p does not divide $g(0)$, we see that $(2n-1)\,g(0)$ $(n = 1, 2, \ldots, p)$ runs through a complete set of residues (mod p) and, unless $p \equiv 2 \pmod 3$ and the coefficient of x in $f(x)$ is divisible by p, this contradicts a result of (1) to the effect that the number of residues of $f(x)$ is not greater than $\frac{1}{3}(2p+1)$. Similarly, we obtain a contradiction unless the coefficient of y in $g(y) - g(0)$ is divisible by p. Hence, if p does not divide $g(0)$, case (ii) of our theorem must hold.

We can now write

$$f(x) = a_1 x^3 + c_1 x, \quad g(y) = a_2 y^3 + c_2 y,$$

where a_1, c_1, a_2, c_2 denote integers with a_1, a_2 not divisible by p. If $p \equiv 2 \pmod 3$ we may suppose further that $a_1 = 1, a_2 = 1$. For there exists a unique integer r, not divisible by p, such that $r^3 \equiv a_1 \pmod p$, whence $a_1 x^3 + c_1 x \equiv \bar{x}^3 + c_1 r\bar{x}$, where $rx \equiv \bar{x}$, $r\bar{r} \equiv 1$, and a similar transformation can be applied for y. If $p \equiv 1 \pmod 3$, on the other hand, we can assume that $a_1 = 1$ by substituting $\bar{x}$ for $a_1 x$ and considering $a_1^2 f(x)$, $a_1^2 g(y)$ instead of $f(x)$, $g(y)$, but we cannot necessarily assume that $a_2 = 1$.

Finally, we note that there is no loss of generality in assuming that neither c_1 nor c_2 is divisible by p. For suppose $c_2 \equiv 0$. Then also $c_1 \equiv 0$, for otherwise, by (1), $f(x)$ would have $\frac{1}{3}(2p + (-3/p))$ distinct residues but $g(y)$ would have $\frac{1}{3}(p+2)$ or p residues according as $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. Similarly $c_1 \equiv 0$ implies $c_2 \equiv 0$. Now if $p \equiv 2 \pmod 3$ we again have case (ii) of our theorem. If $p \equiv 1 \pmod 3$ the theorem follows from the fact that x^3 is equivalent to $a_2 y^3$, and assumes the same residues, if and only if a_2 is a cubic residue modulo p.

3. *Proof of Theorem* ($p > 41$). For each integer $r = 0, 1, \ldots, p-1$ let $D_f(r)$ and $D_g(r)$ denote the discriminants of $f(x) - r$ and $g(y) - r$ respectively. Then $(D_f(r)/p)$ is given by -1 if $f(x) - r$ has exactly one linear factor (mod p), by 0 if it has a squared factor (mod p) and by 1 otherwise, that is if it is irreducible or has three linear factors. We may suppose, without loss of generality, that $D_f(r)\,D_g(r)$ is not congruent to a square (mod p). For otherwise, noting that c_1, a_2 and c_2 are relatively prime to p, neither $D_f(r) = -27r^2 - 4c_1^3$ nor $D_g(r) = -27a_2^2 r^2 - 4c_2^3 a_2$ has a repeated factor (mod p) and hence we would have $D_g(r) \equiv \lambda^2 D_f(r)$ for all r, that is $a_2^2 \equiv \lambda^2$ and $\lambda^2 c_1^3 \equiv c_2^3 a_2$. Thus $f(x)$ would be transformed into $g(y)$ by the equation $x = c_2 \bar{c}_1 y$, where $c_1 \bar{c}_1 \equiv 1$.

Since $D_f(r)\,D_g(r)$ is a quartic in r which has been assumed not congruent to a square, we have, by a deep result of Perel'muter (2),

$$S = \sum_{r=0}^{p-1} \left(\frac{D_f(r)}{p}\right)\left(\frac{D_g(r)}{p}\right) \leqslant 2p^{\frac{1}{2}} + 1.$$

We proceed to evaluate a lower bound for S, which, by comparison, will yield the required contradiction. We clearly have

$$S = k_{00} - (k_{01} + k_{10}) + (k_{03} + k_{30}) - (k_{13} + k_{31}) + k_{11} + k_{33},$$

where $k_{ij}\,(i,j = 0,1,2,3)$ is defined as the number of integers r for which $f(x) \equiv r$ and $g(y) \equiv r$ have exactly i and j solutions (mod p) respectively. Here $k_{01}, k_{10}, k_{03}, k_{30}$ are all 0, since $f(x)$, $g(y)$ are supposed to have the same residues (and hence also the same non-residues). Further, k_{00} is just the number of non-residues of $f(x)$ (or $g(y)$) and thus, by (1), we have

$$k_{00} = \tfrac{1}{3}(p-(-3/p)).$$

To estimate $k_{11}+k_{33}-(k_{13}+k_{31})$ we note that

$$k_{i1}+k_{i2}+k_{i3} = n_i(f), \quad k_{1i}+k_{2i}+k_{3i} = n_i(g) \quad (i = 1,2,3),$$

where $n_i(f)$ denotes the number of integers r for which $f(x) \equiv r$ has exactly i solutions and $n_i(g)$ denotes the corresponding number for the congruences $g(y) \equiv r$. Hence we have $k_{ij} \leqslant n_i(f)$, $k_{ji} \leqslant n_i(g)\,(i = 1,2,3)$, and this gives

$$\begin{aligned} k_{11}+k_{33}-(k_{13}+k_{31}) &\geqslant k_{11}-k_{13}-k_{31} \\ &= n_1(f)-k_{12}-2k_{13}-k_{31} \\ &\geqslant n_1(f)-n_2(g)-2n_3(g)-n_3(f). \end{aligned}$$

Now (by (1), for example) we have

$$n_1(g) = \frac{p-1}{2}+\frac{1}{2}\left(\frac{-3}{p}\right)-\frac{1}{2}\left(\frac{-3a_2}{p}\right),$$

$$n_2(g) = 1+\left(\frac{-3a_2}{p}\right),$$

$$n_3(g) = \frac{p}{6}-\frac{1}{2}-\frac{1}{6}\left(\frac{-3}{p}\right)-\frac{1}{2}\left(\frac{-3a_2}{p}\right),$$

and the $n_i(f)$ are given by the same expressions with a_2 replaced by 1. A simple calculation therefore shows that

$$n_1(f)-n_2(g)-2n_3(g)-n_3(f) = (-3/p),$$

and we obtain

$$S \geqslant \frac{p}{3}+\frac{2}{3}\left(\frac{-3}{p}\right).$$

Comparing this with the upper bound $2p^{\frac{1}{2}}+1$ for S stated earlier we see that $6p^{\frac{1}{2}} \geqslant p-5$ when $p \equiv 2 \pmod 3$ and $6p^{\frac{1}{2}} \geqslant p-1$ when $p \equiv 1 \pmod 3$. The first inequality gives $p \leqslant 41$, the second gives $p \leqslant 37$ and our theorem is therefore proved for all primes $p > 41$.

4. *Proof of theorem* ($7 < p \leqslant 41$). It remains only to prove that the theorem is valid for all primes p with $7 < p \leqslant 41$. This involves considering only a finite number of cases, that is we have only to test the cubic polynomials for each fixed prime p in the above range and determine whether they have the same residues and yet are unrelated by a linear transformation. We consider the two cases $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 3$ separately.

Case (i): $p \equiv 2 \pmod 3$. We have already shown in § 2 that the cubics may be assumed to have the forms $x^3 + c_1 x$ and $y^3 + c_2 y$ and we need therefore only evaluate the residues of the $p-1$ polynomials $x^3 + ax$ with $a = 1, 2, \ldots, p-1$. To do this we used the Manchester Atlas computer. It was programmed to calculate the residues for each fixed a by letting x take the p value $0, 1, 2, \ldots, p-1$ and then reducing the numbers so formed modulo p. Some residues do of course occur several times, but we are not concerned with their multiplicity, only with their values. The computer recorded each different residue and arranged them in ascending order of magnitude so it was then straightforward to check that the set of residues for each different polynomial is in fact different for $p > 7$.

Case (ii): $p \equiv 1 \pmod 3$. We have shown in § 2 that the cubics $f(x)$, $g(y)$ may be assumed to have the forms $x^3 + c_1 x$ and $a_2 y^3 + c_2 y$. Now $x^3 + ax$ and $y^3 + by$ are equivalent if and only if $a^3 \equiv b^3 \pmod p$ and, in this case, the congruence has three solutions b for a fixed a. Thus we can choose a set S of $\frac{1}{3}(p-1)$ values of a from the set $1, 2, \ldots, p-1$ such that no two of the corresponding polynomials $x^3 + ax$ are equivalent. If a_2 is a cubic residue $(\mathrm{mod}\, p)$ then $a_2 y^3 + c_2 y$ is equivalent to $x^3 + ax$ for some $a \in S$. Suppose now that a_2 is a cubic non-residue $(\mathrm{mod}\, p)$ and let β denote the least cubic non-residue $(\mathrm{mod}\, p)$ in the range $0 < \beta < p$. The set T of integers $\beta\alpha$, $\beta^2\alpha$, where α runs through all the cubic residues $(\mathrm{mod}\, p)$ forms a complete system of cubic non-residues. Hence we see that $a_2 \equiv \beta\gamma^3$ or $\beta^2\gamma^3$ for some integer γ and $g(y)$ is equivalent to a polynomial of the form $\beta(z^3 + \bar{c}_2 \bar{a}_2 \gamma^2 z)$, or the same with β replaced by β^2. Finally it follows from the fact that if $f(x)$, $g(y)$ have the same residues then so also have $\beta f(x)$, $\beta g(y)$, that we need only evaluate the residues of the $\frac{2}{3}(p-1)$ polynomials $x^3 + ax$ and $\beta(x^3 + ax)$. This was done on the computer and, as before, with the residues for each polynomial ordered, it was an easy task to verify that for any fixed prime p satisfying $7 < p \leqslant 41$, no pair had the same set of residues.

REFERENCES

(1) McCANN, K. and WILLIAMS, K. S. On the residues of a cubic polynomial (mod p) *Canad. Math. Bull.*, **10** (1967), 29–38.

(2) PEREL'MUTER, G. I. On certain sums of characters, *Uspehi Mat. Nauk.*, (2), **18** (1963), 145–9.