QUADRATIC POLYNOMIALS WITH THE SAME RESIDUES

K. S. WILLIAMS, Carleton University, Ottawa

It is the purpose of this note to prove the following:

THEOREM. *Two quadratic polynomials* $a_1x_1^2+b_1x_1+c_1$ *and* $a_2x_2^2+b_2x_2+c_2$ *with integral coefficients have the same residues modulo every prime* $p>3$ *not dividing* a_1a_2, *if and only if they are related by a nonsingular rational linear transformation, that is to say, if and only if there exist rationals* r *and* s *with* $r\neq 0$ *such that*

$$a_1(rx+s)^2+b_1(rx+s)+c_1\equiv a_2x^2+b_2x+c_2.$$

For example, this theorem tells us that $12x_1^2+14x_1+1$ and $75x_2^2+55x_2+7$ have the same residues (mod p) for every prime $p\geqq 7$, since

$$12(\tfrac{5}{2}x+\tfrac{1}{3})^2+14(\tfrac{5}{2}x+\tfrac{1}{3})+1\equiv 75x^2+55x+7.$$

We note that there is no *integral* transformation relating $12x_1^2+14x_1+1$ and $75x_2^2+55x_2+7$. In any particular case it is easy to decide whether the two quadratics also have the same residues (mod p) for $p=2$ or 3 or any $p\mid a_1a_2$. In the above example they do for $p=2$, 3 but not for $p=5$.

We begin by calculating the number N_p ($p>2$) of common residues (mod p) of the two quadratic polynomials $a_1x_1^2+b_1x_1+c_1$ and $a_2x_2^2+b_2x_2+c_2$ (a_1, $a_2\not\equiv 0$ (mod p)), that is, the number of integers r satisfying $0\leqq r\leqq p-1$ for which both the congruences

$$a_1x_1^2+b_1x_1+c_1\equiv r,\qquad a_2x_2^2+b_2x_2+c_2\equiv r$$

are soluble. We denote the number of solutions x_i ($i=1, 2$) of $a_ix_i^2+b_ix_i+c_i\equiv r$ by $N_i(r)$ so that

$$N_p=\sum_{r=0}^{p-1}1,\qquad N_i(r)>0\qquad (i=1, 2).$$

Let $d_i=b_i^2-4a_ic_i$ ($i=1, 2$) then we have

$$N_i(r)=1+\left(\frac{d_i+4a_ir}{p}\right)\qquad (i=1, 2)$$

and so $N_p=\sum_{i,j=0}^{1}N_{ij}$, where

$$N_{ij}=\sum_{r=0}^{p-1}1,\qquad \left(\frac{d_1+4a_1r}{p}\right)=i\qquad \left(\frac{d_2+4a_2r}{p}\right)=j.$$

We now evaluate each N_{ij} ($i, j=0, 1$) in turn. For convenience we set $e=a_1d_2-a_2d_1$. Then

$$N_{00} = \sum_{r=0}^{p-1} 1 = \begin{cases} 1, & \text{if } e \equiv 0, \\ 0, & \text{if } e \not\equiv 0, \end{cases}$$
$$r \equiv -4^{-1}a_1^{-1}d_1,$$
$$r \equiv -4^{-1}a_2^{-1}d_2;$$

that is $N_{00} = 1 - (e^2/p)$. Also

$$N_{01} = \sum_{r=0}^{p-1} 1, \qquad r \equiv -4^{-1}a_1^{-1}d_1, \qquad \left(\frac{d_2 + 4a_2r}{p}\right) = 1,$$
$$= \begin{cases} 1, & \text{if } \left(\frac{a_1e}{p}\right) = 1, \\ 0, & \text{if } \left(\frac{a_1e}{p}\right) = 0 \quad \text{or} \quad -1, \end{cases}$$

that is

$$N_{01} = \frac{1}{2}\left\{\left(\frac{a_1e}{p}\right) + \left(\frac{e^2}{p}\right)\right\}.$$

Similarly $N_{10} = \frac{1}{2}\left\{(-a_2e/p) + (e^2/p)\right\}$. Finally

$$N_{11} = \sum_{r=0}^{p-1} 1, \qquad \left(\frac{d_1 + 4a_1r}{p}\right) = \left(\frac{d_2 + 4a_2r}{p}\right) = 1$$
$$= \frac{1}{4}\sum_{r=0}^{p-1}\left\{1 + \left(\frac{d_1 + 4a_1r}{p}\right)\right\}\left\{1 + \left(\frac{d_2 + 4a_2r}{p}\right)\right\}$$
$$r \not\equiv -4^{-1}a_1^{-1}d_1 \quad \text{or} \quad -4^{-1}a_2^{-1}d_2$$
$$= \frac{1}{4}\Bigg[\sum_{r=0}^{p-1}\left\{1 + \left(\frac{d_1 + 4a_1r}{p}\right)\right\}\left\{1 + \left(\frac{d_2 + 4a_2r}{p}\right)\right\}$$
$$- \left\{1 + \left(\frac{a_1e}{p}\right)\right\} - \left\{1 + \left(\frac{-a_2e}{p}\right)\right\} + \left\{1 - \left(\frac{e^2}{p}\right)\right\}\Bigg]$$
$$= \frac{1}{4}\Bigg[p + \sum_{r=0}^{p-1}\left(\frac{16a_1a_2r^2 + 4(a_1d_2 + a_2d_1)r + d_1d_2}{p}\right)$$
$$- 1 - \left(\frac{a_1e}{p}\right) - \left(\frac{-a_2e}{p}\right) - \left(\frac{e^2}{p}\right)\Bigg]$$
$$= \frac{1}{4}\left[p + \left\{p - p\left(\frac{e^2}{p}\right) - 1\right\}\left(\frac{a_1a_2}{p}\right) - 1 - \left(\frac{a_1e}{p}\right) - \left(\frac{-a_2e}{p}\right) - \left(\frac{e^2}{p}\right)\right].$$

Hence we have proved

LEMMA 1. *For $p > 2$, $p \nmid a_1a_2$*

$$N_p = \frac{1}{4}\left[\left\{1 + \left(\frac{a_1a_2}{p}\right) - \left(\frac{a_1a_2e^2}{p}\right)\right\}p + \left\{3 - \left(\frac{e^2}{p}\right) + \left(\frac{a_1e}{p}\right) + \left(\frac{-a_2e}{p}\right) - \left(\frac{a_1a_2}{p}\right)\right\}\right].$$

This gives the following table of values of N_p $(p>2)$.

TABLE

						$p\equiv 1$ (mod 4)	$p\equiv 3$ (mod 4)		$p\equiv 1$ (mod 4)	$p\equiv 3$ (mod 4)
$\left(\frac{a_1}{p}\right)$	$\left(\frac{a_2}{p}\right)$	$\left(\frac{e}{p}\right)$	$\left(\frac{a_1a_2}{p}\right)$	$\left(\frac{e^2}{p}\right)$	$\left(\frac{a_1e}{p}\right)$	$\left(\frac{-a_2e}{p}\right)$	$\left(\frac{-a_2e}{p}\right)$	$\left(\frac{a_1a_2e^2}{p}\right)$	N_p	N_p
1	1	1	1	1	1	1	−1	1	$\frac{1}{4}(p+3)$	$\frac{1}{4}(p+1)$
1	1	0	1	0	0	0	0	0	$\frac{1}{2}(p+1)$	$\frac{1}{2}(p+1)$
1	1	−1	1	1	−1	−1	1	1	$\frac{1}{4}(p-1)$	$\frac{1}{4}(p+1)$
1	−1	1	−1	1	1	−1	1	−1	$\frac{1}{4}(p+3)$	$\frac{1}{4}(p+5)$
1	−1	0	−1	0	0	0	0	0	1	1
1	−1	−1	−1	1	−1	1	−1	−1	$\frac{1}{4}(p+3)$	$\frac{1}{4}(p+1)$
−1	1	1	−1	1	−1	1	−1	−1	$\frac{1}{4}(p+3)$	$\frac{1}{4}(p+1)$
−1	1	0	−1	0	0	0	0	0	1	1
−1	1	−1	−1	1	1	−1	1	−1	$\frac{1}{4}(p+3)$	$\frac{1}{4}(p+5)$
−1	−1	1	1	1	−1	−1	1	1	$\frac{1}{4}(p-1)$	$\frac{1}{4}(p+1)$
−1	−1	0	1	0	0	0	0	0	$\frac{1}{2}(p+1)$	$\frac{1}{2}(p+1)$
−1	−1	−1	1	1	1	1	−1	1	$\frac{1}{4}(p+3)$	$\frac{1}{4}(p+1)$

LEMMA 2. *If $p>3$, the quadratics $a_1x_1^2+b_1x_1+c_1$ and $a_2x_2^2+b_2x_2+c_2$ have exactly the same residues* (mod p), *if and only if* $(a_1a_2/p)=+1$ *and* $e\equiv 0$ (mod p).

Proof. This is immediate from the table as the quadratics $a_1x_1^2+b_1x_1+c_1$ and $a_2x_2^2+b_2x_2+c_2$ have exactly the same residues if and only if $N_p=\frac{1}{2}(p+1)$. (Recall that the number of residues (mod p) of a quadratic polynomial ax^2+bx+c (a, b, c, integers, $a\not\equiv 0$ (mod p) $(p>2)$ is $\frac{1}{2}(p+1)$.)

Our last lemma is based upon an idea contained in a paper of H. Salié [1].

LEMMA 3. *For any prime q, there exists an integer $l\equiv 1$* (mod 4) *and $\not\equiv 0$* (mod q) *such that if p is a prime $\equiv l$* (mod $4q$) *then* $(q/p)=-1$.

Proof. If $q=2$ take $l=5$ as $(2/p)=-1$ for primes $p\equiv 5$ (mod 8). We may therefore suppose that $q>2$. Let

$$L = \{l \mid l = 1, 5, 9, 13, \cdots, 4q-3\}.$$

The number of integers in L is just q. They are distinct (mod q) for if l_1, $l_2\in L$

with $l_1 \equiv l_2 \pmod{q}$ then as $q>2$ and $l_1 \equiv l_2 \equiv 1 \pmod 4$ we have $l_1 \equiv l_2 \pmod{4q}$ i.e. $l_1 = l_2$. Hence the residues of the integers in $L \pmod q$ form a complete residue set (mod q). Let n denote the least positive quadratic nonresidue (mod q) and choose $l \in L$ such that $l \equiv n \pmod q$. Then $l \equiv 1 \pmod 4$, $l \not\equiv 0 \pmod q$ and if p is a prime $\equiv l \pmod{4q}$ (so that in particular $p \equiv 1 \pmod 4$) we have by the law of quadratic reciprocity

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{[(p-1)(q-1)]/4} = -1,$$

as required.

We are now in a position to prove the theorem.

Proof of Theorem. From Lemma 2, the quadratics $a_1x_1^2+b_1x_1+c_1$ and $a_2x_2^2+b_2x_2+c_2$ have the same residues modulo every prime p strictly greater than 3 and not dividing a_1 or a_2 if and only if

$$\left(\frac{a_1a_2}{p}\right) = +1 \quad \text{and} \quad e \equiv 0 \pmod p$$

for these primes. Now $e \equiv 0 \pmod p$ for any infinity of primes p if and only if $e=0$ i.e. if and only if

$$a_1d_2 = a_2d_1. \tag{1}$$

Clearly if a_1a_2 is a square then $(a_1a_2/p) = +1$ for all $p \nmid a_1a_2$. We now show conversely that if $(a_1a_2/p) = +1$ for all $p>3$ not dividing a_1a_2 then a_1a_2 is a square. Suppose that it is not. Then it can be expressed as

$$\pm\, p_1p_2 \cdots p_sk^2 \quad \text{or} \quad -k^2,$$

where $p_1, \cdots, p_s$ are $s \geqq 1$ distinct primes. We deal with the case when a_1a_2 is positive first. To obtain the necessary contradiction it suffices to show the existence of a prime $p > 3a_1a_2$ such that $(a_1a_2/p) = -1$. We do this by showing the existence of such a prime p with $(p_1/p) = \cdots = (p_{s-1}/p) = +1$ and $(p_s/p) = -1$. Let l_1 denote the integer l given by Lemma 3 with $q = p_s$. We now define an integer l_2 as follows: if $s=1$ take $l_2 = l_1$ and if $s>1$ choose l_2 such that

$$l_2 \equiv 1 \pmod{4p_1 \cdots p_{s-1}}$$
$$l_2 \equiv a_1 \pmod{4p_s}.$$

This is possible as $4 = (4p_1 \cdots p_{s-1},\ 4p_s) \mid l_1 - 1$. Obviously $(l_2,\ 4p_1 \cdots p_s) = 1$. By Dirichlet's theorem there exists an infinity of primes $\equiv l_2 \pmod{4p_1 \cdots p_s}$. Let p denote the least such $> 3a_1a_2$. Then by Lemma 3 $(p_s/p) = -1$. Also

$$\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right)(-1)^{[(p-1)(p_i-1)]/4} = \left(\frac{l_2}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1,$$

for $i = 1, 2, \cdots, s-1$ as required.

We now deal with the case when a_1a_2 is negative. Suppose firstly that $a_1a_2 = -k^2$. We show this is impossible. By Dirichlet's theorem there are an

infinity of primes $\equiv 3 \pmod 4$. Take p to be the least such one $> -3a_1a_2$. Then $p > 3$ and $p \nmid a_1a_2$ and moreover

$$\left(\frac{a_1a_2}{p}\right) = \left(\frac{-k^2}{p}\right) = \left(\frac{-1}{p}\right) = -1,$$

which is a contradiction. Thus if a_1a_2 is negative it must be of the form $-p_1p_2 \cdots p_sk^2$, where $p_1, \cdots, p_s$ are $s \geqq 1$ distinct primes. As in the case when a_1a_2 was assumed to be positive we can find a prime $p > -3a_1a_2$ for which $(-a_1a_2/p) = -1$. This prime is $\equiv 1 \pmod 4$ so $(-a_1a_2/p) = (a_1a_2/p)$, completing the proof that a_1a_2 must be a square.

Now let $a_1a_2 = a^2$ and set $r = a/a_1$, $s = (b_2 - b_1r)/(2a_1r)$, so that both r and s are rational. Then $a_1r^2 = a^2/a_1 = a_2$,

$$2a_1rs + b_1r = (b_2 - b_1r) + b_1r = b_2$$

and

$$\begin{aligned} a_1s^2 + b_1s + c_1 &= \frac{1}{4a_1r^2}\left\{(b_2 - b_1r)^2 + 2b_1r(b_2 - b_1r) + 4a_1c_1r^2\right\} \\ &= \frac{1}{4a_1r^2}\left\{b_2^2 - d_1r^2\right\} = \frac{1}{4a_2}\left\{b_2^2 - \frac{a_2d_1}{a_1}\right\} \\ &\quad \frac{1}{4a_2}\left\{b_2^2 - d_2\right\} = c_2 \qquad \text{(from (1))} \end{aligned}$$

giving

$$a_1(rx + s)^2 + b_1(rx + s) + c_1 \equiv a_2x^2 + b_2x + c_2$$

as required.

Reference

1. H. Salié, Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl, Math. Nachr., 3 (1949/50) 7–8.

MATHEMATICAL NOTES

Material for this department should be sent to David Drasin, Division of Mathematical Sciences, Purdue University, Lafayette, IN 47907.

THE CONCEPT OF A TORSION MODULE

V. Dlab, Institute of Advanced Studies, Australian National University, Canberra

The concept of a torsion group (or of a torsion element) in the theory of abelian groups (in what follows, we shall use the word group to mean always additive abelian group) is very simple: G is torsion if all elements of G have