residues mod p, and, mod q, they consist of $p-1$ copies of each of the quadratic residues mod q.

Acknowledgment. Thanks to the referees for suggestions that greatly improved the paper.

REFERENCES

1. Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
2. Richard K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004.
3. E. S. Selmer and Ö. Beyer, On the linear diophantine problem of Frobenius in three variables, *J. reine angew. Math.*, **301** (1978) 161–170.
4. J. J. Sylvester, Question 7382, *Mathematical Questions from the Educational Times*, **37** (1884) 26.

Factoring Quartic Polynomials: A Lost Art

GARY BROOKFIELD
California State University
Los Angeles CA 90032-8204
gbrookf@calstatela.edu

You probably know how to factor the cubic polynomial $x^3 - 4x^2 + 4x - 3$ into $(x-3)(x^2 - x + 1)$. But can you factor the quartic polynomial $x^4 - 8x^3 + 22x^2 - 19x - 8$?

Curiously, techniques for factoring quartic polynomials over the rationals are never discussed in modern algebra textbooks. Indeed, Theorem 1 of this note, giving conditions for the reducibility of quartic polynomials, appears in the literature, so far as I know, in only one other place—on page 553 (the very last page) of *Algebra, Part 1* by G. Chrystal [**3**], first published in 1886. Interest in the theory of equations, the subject of this book and many others of similar vintage, seems to have faded, and the factorization theory for quartic polynomials, presented in this note, seems to have been forgotten. Perhaps it is time for a revival!

All polynomials in this note have rational coefficients, that is, all polynomials are in $\mathbb{Q}[x]$. Moreover, we are interested only in factorizations into polynomials in $\mathbb{Q}[x]$. The factorization $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ is not of this type since $x + \sqrt{2}$ and $x - \sqrt{2}$ are not in $\mathbb{Q}[x]$. In our context, $x^2 - 2$ has no nontrivial factorizations and so is *irreducible*. A polynomial, such as $x^3 - 4x^2 + 4x - 3 = (x-3)(x^2 - x + 1)$, which has a nontrivial factorization is said to be *reducible*. For a nice general discussion about the factorization of polynomials over $\mathbb{Q}$, see [**1**].

Basic tools for factoring polynomials are the following:

- *Factor Theorem:* Let $f \in \mathbb{Q}[x]$ and $c \in \mathbb{Q}$. Then c is a root of f (that is, $f(c) = 0$) if and only if $x - c$ is a factor of $f(x)$.
- *Rational Roots Theorem:* Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with integer coefficients $a_n, a_{n-1}, \ldots, a_0$. If p/q is a rational number in lowest terms such that $f(p/q) = 0$, then p divides a_0 and q divides a_n.

These theorems suffice to factor any quadratic or cubic polynomial since such a polynomial is reducible if and only if it has a root in $\mathbb{Q}$. Finding such a root is made easy by the rational roots theorem, and then long division yields the corresponding factorization.

On the other hand, a quartic polynomial may factor into a product of two quadratic polynomials but have no roots in $\mathbb{Q}$. For example, $f(x) = (x^2 - 2)(x^2 - 2)$ has no roots in $\mathbb{Q}$ but obviously factors. Thus to determine whether or not a quartic polynomial without rational roots is reducible, we need to know whether it factors into a product of two quadratic polynomials. Theorem 1 shows that this question can be answered using an associated cubic polynomial called the resolvent.

To simplify our presentation we will consider only polynomials in reduced form: If $f(x) = ax^4 + bx^3 + cx^2 + dx + e \in \mathbb{Q}[x]$ (with $a \neq 0$) is an arbitrary quartic polynomial, then the *reduced form* of f is the polynomial $f(x - b/4a)/a$. For example, the reduced form of $f(x) = x^4 - 8x^3 + 22x^2 - 19x - 8$ is $f(x + 2) = x^4 - 2x^2 + 5x - 6$. The reduced form has leading coefficient one and no degree three term. It is easy to see how a factorization of the reduced form gives a factorization of the original polynomial (see Example 4). Thus we lose no generality in the following theorem by assuming that f is already in the reduced form $f(x) = x^4 + cx^2 + dx + e$. In this circumstance, the *resolvent* of f is the cubic polynomial

$$R(z) = z^3 + 2c\,z^2 + (c^2 - 4e)\,z - d^2.$$

Since it is easy to calculate the roots of f once it has been factored, it is no surprise that the resolvent also appears in the many published methods for finding the roots of quartic polynomials (see, for example, [**2**]).

In what follows we write $\mathbb{Q}^2 = \{s^2 \mid s \in \mathbb{Q}\}$ for the set of squares in $\mathbb{Q}$.

THEOREM 1. *The quartic polynomial $f(x) = x^4 + cx^2 + dx + e \in \mathbb{Q}[x]$ factors into quadratic polynomials in $\mathbb{Q}[x]$ if and only if (at least) one of the following holds:*

(A) The resolvent R has a nonzero root in $\mathbb{Q}^2$.

(B) $d = 0$ and $c^2 - 4e \in \mathbb{Q}^2$.

Proof. Suppose f factors as

$$f(x) = (x^2 + hx + k)(x^2 + h'x + k'), \tag{1}$$

with $h, h', k, k' \in \mathbb{Q}$. Multiplying (1) out and matching coefficients we get

$$0 = h + h', \qquad e = kk', \tag{2}$$

$$d = hk' + h'k, \qquad c = hh' + k + k'. \tag{3}$$

In particular, $h' = -h$. The equations in (3) are linear in k and k' and can be solved to yield

$$2hk = h^3 + ch - d, \quad 2hk' = h^3 + ch + d. \tag{4}$$

From $e = kk'$ and (4) we get

$$4h^2e = (2hk)(2hk') = (h^3 + ch - d)(h^3 + ch + d). \tag{5}$$

Multiplying this out we get

$$h^6 + 2c\,h^4 + (c^2 - 4e)\,h^2 - d^2 = 0, \tag{6}$$

and so h^2 is a root of the resolvent R. If $h \neq 0$, then (A) of the theorem holds. Otherwise, $h = 0$ and (6) implies that $d = 0$ and, from (2) and (3), we get $c^2 - 4e = (k + k')^2 - 4kk' = (k - k')^2 \in \mathbb{Q}^2$. Thus, in this case, (B) of the theorem holds.

Now suppose that the resolvent R has a nonzero root in $\mathbb{Q}^2$. Then there is some nonzero $h \in \mathbb{Q}$ such that (6) holds. Set

$$h' = -h, \quad k = \frac{1}{2h}(h^3 + ch - d), \quad k' = \frac{1}{2h}(h^3 + ch + d). \tag{7}$$

Then $h', k, k' \in \mathbb{Q}$ and, since (5) follows from (6), the equations (2) and (3) hold. Thus f factors into quadratic polynomials in $\mathbb{Q}[x]$ as in (1).

Suppose that $d = 0$ and $c^2 - 4e \in \mathbb{Q}^2$. Then $c^2 - 4e = s^2$ for some $s \in \mathbb{Q}$. Set

$$h = h' = 0, \quad k = (c + s)/2 \text{ and } k' = (c - s)/2. \tag{8}$$

Then $h, h', k, k' \in \mathbb{Q}$ and $k + k' = c$, $kk' = (c^2 - s^2)/4 = e$, $f(x) = (x^2 + k)(x^2 + k')$, and so once again f factors into quadratic polynomials in $\mathbb{Q}[x]$. ∎

From the proof of this theorem we can extract an algorithm for factoring a quartic polynomial f in reduced form. First, using the rational roots theorem, look for a rational root of f. If $c \in \mathbb{Q}$ is such a root, then, by the factor theorem, we know that $f(x) = (x - c)\, g(x)$ for some cubic polynomial g (which can be determined by long division). If f has no rational roots, we look for rational roots of the resolvent R. If $h^2 \in \mathbb{Q}^2$ is a nonzero root of R, then condition (A) of Theorem 1 holds, and (7) and (1) give a factorization of f. If condition (B) of Theorem 1 holds, then equations (8) and (1) determine a factorization of f. If these steps fail to produce a factorization, then f is irreducible.

EXAMPLE 1. Let $f(x) = x^4 + x^2 + x + 1$. Then neither f nor the resolvent $R(z) = z^3 + 2z^2 - 3z - 1$ has a rational root. Thus f is irreducible.

EXAMPLE 2. Let $f(x) = x^4 + 2x^2 + 5x + 11$. Then f has no rational roots, and the resolvent $R(z) = z^3 + 4z^2 - 40z - 25$ has one rational root, namely 5, which is not in $\mathbb{Q}^2$. Thus f is irreducible.

EXAMPLE 3. Let $f(x) = x^4 - 12x^2 - 3x + 2$. Then f has no rational roots, and the resolvent $R(z) = z^3 - 24z^2 + 136z - 9$ has one rational root, namely $9 \in \mathbb{Q}^2$. Thus f is reducible. Setting $h = \sqrt{9} = 3$ in (7) and (1) we get $f(x) = (x^2 + 3x - 1)(x^2 - 3x - 2)$.

EXAMPLE 4. Let $f(x) = x^4 - 8x^3 + 22x^2 - 19x - 8$, the motivating example from the beginning of this note. Then f has no rational roots. The reduced form of this polynomial is $f(x + 2) = x^4 - 2x^2 + 5x - 6$, and its resolvent is $R(z) = z^3 - 4z^2 + 28z - 25$ with one rational root, namely, $1 \in \mathbb{Q}^2$. Thus f is reducible. Setting $h = \sqrt{1} = 1$ in (7) and (1) we get $f(x + 2) = (x^2 + x - 3)(x^2 - x + 2)$ and so $f(x) = (x^2 - 3x - 1)(x^2 - 5x + 8)$.

We conclude by investigating the interesting special case when $f(x) = x^4 + cx^2 + e$. If $r \in \mathbb{Q}$ is a root of $f(x) = x^4 + cx^2 + e$ then so is $-r$, and $x^2 - r^2 \in \mathbb{Q}[x]$ divides f. Thus f is reducible if and only if it factors into two quadratic polynomials. Since $d = 0$, the resolvent of f is

$$R(z) = z\left(z^2 + 2c\,z + (c^2 - 4e)\right),$$

with roots $0, -c \pm 2\sqrt{e}$. Theorem 1 now provides a test for the irreducibility of f:

THEOREM 2. [**4**, Theorem 2] *A quartic polynomial $f(x) = x^4 + cx^2 + e \in \mathbb{Q}[x]$ is reducible if and only if $c^2 - 4e \in \mathbb{Q}^2$ or $-c + 2\sqrt{e} \in \mathbb{Q}^2$ or $-c - 2\sqrt{e} \in \mathbb{Q}^2$. For the conditions involving $\sqrt{e}$ to hold it is, of course, necessary that $e \in \mathbb{Q}^2$.*

EXAMPLE 5. If $f(x) = x^4 - 3x^2 + 1$, then $c = -3$ and $e = 1$. We have $c^2 - 4e = 5 \notin \mathbb{Q}^2$, $-c + 2\sqrt{e} = 5 \notin \mathbb{Q}^2$ and $-c - 2\sqrt{e} = 1 \in \mathbb{Q}^2$. Thus f is reducible. To cal-

culate the factorization we set $h = 1$ in (7) and (1) to get $f(x) = (x^2 + x - 1)(x^2 - x - 1)$.

EXAMPLE 6. If $f(x) = x^4 - 16x^2 + 4$, then $c = -16$ and $e = 4$. We have $c^2 - 4e = 240 \notin \mathbb{Q}^2$, $-c + 2\sqrt{e} = 20 \notin \mathbb{Q}^2$ and $-c - 2\sqrt{e} = 12 \notin \mathbb{Q}^2$, and so f is irreducible.

REFERENCES

1. H.L. Dorwarts, Can This Polynomial Be Factored? *Two-Year College Math. J.*, **8**(2) (1977) 67–72.
2. William F. Carpenter, On the Solution of the Real Quartic, this MAGAZINE, **39** (1966) 28–30.
3. G. Chrystal, *Algebra, An Elementary Textbook, Part I, Seventh ed.*, AMS Chelsea Pub., 1964.
4. L. Kappe and B. Warren, An Elementary Test for the Galois Group of a Quartic Polynomial, *Amer. Math. Monthly*, **96** (1989) 133–137.

Butterflies in Quadrilaterals: A Comment on a Note by Sidney Kung

EISSO J. ATZEMA
University of Maine
Orono, ME 04469-5752
atzema@math.umaine.edu

In the October 2005 issue of *Mathematics Magazine*, Sidney Kung published a note on a theorem on butterflies inscribed in a quadrilateral which bears remarkable similarity to the usual Butterfly Theorem (see [**5**]). In this note, we will show that this similarity is not a coincidence. In fact, Kung's Theorem really is the usual Butterfly Theorem in disguise. To see this, it is easiest to try to prove Kung's Theorem using projective geometry. Indeed, if we insist on using the standard toolbox of projective geometry, it might not even be possible to prove the theorem without reducing it to some version of the usual Butterfly Theorem no matter what the kind of tools we allow—at least we have not been able to find such a proof. For the purposes of this note we will only use a few basic tools of the field, specifically the notion of an involution on a (projective) straight line and Desargues' Involution Theorem.[1]

We start with a reformulation of the Butterfly Theorem in terms of projective geometry. Consider a self-intersecting quadrilateral $AB'A'B$ (the "butterfly" in FIGURE 1) inscribed in a conic section $\mathcal{C}$. Let I be the point of intersection of the sides $A'B$ and AB'. Now draw an arbitrary line through I and let C, C' be the points of intersection of the line with the conic section. By Desargues' Involution Theorem, the family of conic sections circumscribing $AB'A'B$ defines an involution on the line CC', with I a fixed point of this involution and C, C' a conjugate pair (i.e. they are each other's images under the involution).[2] This completely determines the involution: Since the fixed points of an involution are in harmonic position with respect to any conjugate

[1] Most of the theory needed can be found in any textbook on projective geometry. A classic is [**2**]. For a discussion of Desargues' Theorem, see also Problem 63 of [**3**, pp. 265–273] . Within the canon of projective geometry, Desargues' Theorem is usually derived from Steiner's Theorems and some other fundamental tools. With a little bit of analytic geometry, however, the theorem is almost immediately proved. See also the next footnote.

[2] Intuitively, this follows from the fact that five points determine a conic section. Therefore, for any point on CC', there is a unique conic passing through the point and circumscribing $AB'A'B$. This conic intersects CC' in only one other point (possibly the same point). Thus all the points on CC' come in pairs.