REFERENCES

1. G. D. Birkhoff, A set of postulates for plane geometry based on scale and protractor, *Ann. Math.*, **33** (1932) 329–345.
2. B. Bold, *Famous Problems of Geometry and How To Solve Them*, Dover, 1969.
3. H. Busemann, Angle measure and integral curvature, *Canad. J. Math.*, **1** (1949) 279–296.
4. H. Busemann, Planes with analogues to Euclidean angular bisectors, *Math. Scand.*, **36** (1975) 5–11.
5. D. R. Byrkit, Taxicab geometry—a non-Euclidean geometry of lattice points, *The Mathematics Teacher*, **64** (1971), 418–422.
6. B. V. Dekster, An angle in Minkowski space, *Jour. of Geometry*, **80** (2004) 31–47.
7. V. V. Glogovśkiĭ, Bisectors on the Minkowski plane with norm $(x^p + y^p)^{1/p}$, (Ukrainian. Russian summary) *Vīsnik Lvīv. Polītehn. Īnst. No.*, **44** (1970) 192–198.
8. T. L. Heath, *The Thirteen Books of Euclid's Elements*, Dover Publications, 1956.
9. E. F. Krause, *Taxicab Geometry: An Adventure in Non-Euclidean Geometry*, Dover Publications, 1986.
10. G. E. Martin, *The Foundations of Geometry and the Non-Euclidean Plane*, Intext Educational Publications, 1975.
11. A. C. Thompson, Minkowski Geometry, *Encyclopedia of Mathematics and its Applications*, **63**, Cambridge University Press, 1996.
12. K. Thompson and T. Dray, Taxicab angles and trigonometry, *Pi Mu Epsilon Journal*, **11** (2000) 87–96.
13. S. Stahl, *Geometry: from Euclid to Knots*, Pearson Education Inc., 2003.
14. M. L. Wantzel, Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas, *J. Math. pures appliq.*, **1** (1836) 366–372.

Quadratic Residues and the Frobenius Coin Problem

MICHAEL Z. SPIVEY
University of Puget Sound
Tacoma, Washington 98416-1043
mspivey@ups.edu

Recently I was struck by the fact that an odd prime p has $(p-1)/2$ quadratic residues mod p and that for relatively prime p and q, there are $(p-1)(q-1)/2$ non-representable Frobenius numbers. I found the presence of $(p-1)/2$ in both expressions curious. Is there some relationship between quadratic residues and the Frobenius numbers that accounts for the presence of $(p-1)/2$ in the two expressions?

As it so happens, there is. Square the non-representable Frobenius numbers for p and q. Mod p, these numbers consist of $q-1$ copies of each of the $(p-1)/2$ quadratic residues mod p, and, mod q, they consist of $p-1$ copies of each of the $(q-1)/2$ quadratic residues mod q. The situation for 5 and 7 is illustrated in the following table. The first row consists of the non-representable Frobenius numbers for 5 and 7, and the second the squares of these numbers. The third and fourth rows are the second row mod 5 and mod 7, respectively.

x	1	2	3	4	6	8	9	11	13	16	18	23
x^2	1	4	9	16	36	64	81	121	169	256	324	529
x^2 mod 5	1	4	4	1	1	4	1	1	4	1	4	4
x^2 mod 7	1	4	2	2	1	1	4	2	1	4	2	4

As we can see, the squares of the non-representable numbers mod 5 consist of six copies each of the two quadratic residues mod 5 (1 and 4) and, mod 7, they consist of four copies each of the three quadratic residues mod 7 (1, 2, and 4). It is not obvious from the table why this might be the case, as there appears to be no pattern to the distribution of the residues.

Before we prove our observation, we should define our terms more carefully. A *quadratic residue* of p is a value of n for which $n \not\equiv 0 \bmod p$ and the equation $x^2 \equiv n \bmod p$ has a solution in x. The quadratic residues mod 5 are 1 and 4 because, mod 5, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 4$, and $4^2 \equiv 1$, and any number larger than 5 that is not a multiple of 5 is congruent to one of 1, 2, 3, and 4. One of the most well-known theorems concerning quadratic residues is that an odd prime p has $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues mod p [**1**, p. 179].

Given relatively prime integers p and q, an integer n is *representable* by p and q if there exist nonnonegative integers a and b such that $ap + bq = n$. The *coin problem of Frobenius* is to determine the largest non-representable integer n for a given p and q. The problem is so named because it can be posed like this: A shopkeeper has coins of denominations p and q only. What is the largest amount of money for which the shopkeeper cannot make change? The example given in the table describes the case for five- and seven-cent coins. Using only coins of these two denominations, the shopkeeper can make change for any amount of cents other than those listed in row 1 of the table. The two-coin Frobenius problem—in which coins of two denominations are allowed—was solved by Sylvester [**4**]. His results are that the largest non-representable integer for relatively prime p and q is $(p-1)(q-1)-1$, and there are $(p-1)(q-1)/2$ such non-representable integers. The three-coin Frobenius problem was solved by Selmer and Beyer [**3**]. The Frobenius problem for four or more coin denominations, however, remains unsolved. Guy [**2**, pp. 171–174] contains a discussion of partial results related to the Frobenius coin problem and a long list of references.

It turns out that the set of non-representable Frobenius numbers is a member of a collection of subsets of $\{1, 2, \ldots, pq\}$, all of which produce the quadratic residue phenomena we have observed. We begin our proof of these claims with the following lemma.

LEMMA 1. *If p and q are relatively prime, then any arithmetic sequence of length q with common difference p contains exactly one multiple of q.*

Proof. Let $\{a, a+p, a+2p, \ldots, a+(q-1)p\}$ be an arithmetic sequence of length q with common difference p. Clearly, $\{0, 1, 2, \ldots, q-1\}$ contains exactly one multiple of q. Since p and q are relatively prime, multiplying by p simply permutes this set, mod q. Adding a just permutes the set again, mod q. Thus $\{a, a+p, a+2p, \ldots, a+(q-1)p\}$ contains exactly one multiple of q. ∎

With the result of Lemma 1, we can now define a certain class of subsets of $\{1, 2, \ldots, pq\}$ and prove that all of its members produce the observed quadratic residue behavior.

LEMMA 2. *Let p and q be odd primes. Let S be a subset of $\{1, 2, \ldots, pq\}$ with the following properties:*

- *S contains no multiples of p or q.*
- *If x is not a multiple of p or q, then exactly one of x and $pq - x$ is in S.*

Then the squares of the integers in S, mod p, consist of $q-1$ copies of each quadratic residue mod p, and, mod q, they consist of $p-1$ copies of each quadratic residue mod q.

Proof. Let $T = S \cup \{x : x \in \{1, 2, \ldots, pq\}$ and $pq - x \in S\}$. By definition of S, T is $\{1, 2, \ldots, pq\}$ less the multiples of p and q. Also, $\{1, 2, \ldots, pq\}$ can be expressed as $\{a + kp : 1 \leq a \leq p, 0 \leq k \leq q - 1\}$. By Lemma 1, then, the set T consists of $q - 1$ representatives from each of the $p - 1$ nonzero congruence classes of p. Since the squares of a complete residue system mod p produce two copies of each of the quadratic residues mod p [**1**, p. 179], the squares, mod p, of the integers in T consist of $2(q - 1)$ copies of the quadratic residues mod p. As $x^2 \equiv (pq - x)^2$ mod p, the squares of the integers in S, mod p, comprise $q - 1$ copies of each quadratic residue mod p. Swapping the roles of p and q in this argument shows that the squares of S also form $p - 1$ copies of each quadratic residue mod q. ∎

All that remains now is to prove that the non-representable Frobenius numbers have the properties of the set S described in Lemma 2. Since every multiple of p or q is clearly representable, and Sylvester's results [**4**] imply that every integer larger than pq is representable, this reduces to proving the following result. (The result is actually true for relatively prime p and q, not just for p and q prime.)

LEMMA 3. *If p and q are relatively prime, x is an integer such that $0 < x < pq$, and x is not a multiple of p or q, then exactly one of x and $pq - x$ can be represented as a nonnegative combination of p and q.*

Proof. Suppose that $x = ap + bq$ for some nonnegative a and b. Since x is not a multiple of q, we have $0 < a$, and $x < pq$ implies $a < q$. Similarly, $0 < b < p$. Now,

$$pq - x = pq - ap - bq = (q - a)p - bq = -ap + (p - b)q.$$

Both representations of $pq - x$ given here have a negative term. Moreover, any other solution, formed by adding and subtracting kpq from the two terms to obtain

$$pq - x = (q - a - kq)p + (kp - b)q,$$

or

$$pq - x = (kq - a)p + (p - b - kp)q,$$

will necessarily have a negative term for every choice of k. Therefore, $pq - x$ has no nonnegative representation.

Conversely, if x has no nonnegative representation, then, as x is not a multiple of p or q, we must have one negative term and one positive term in any representation. Choose the representation with smallest positive a. Therefore, b must be negative. We have

$$x = ap + bq.$$

If $q \leq a$, we can replace a by $a - q$ and b by $b + p$ to obtain another representation of x. This, however, contradicts the definition of a. Thus $0 < a < q$. Next, if $b \leq -p$, then we have $x < 0$, also a contradiction. Therefore $-p < b < 0$. Consequently,

$$pq - x = pq - ap - bq = (q - a)p - bq,$$

yielding a nonnegative representation of $pq - x$. ∎

Since Lemma 3 shows that the non-representable Frobenius numbers have the properties of the set S described in Lemma 2, we have proved our initial observation:

THEOREM. *Let p and q be odd primes. Then the squares of the non-representable Frobenius numbers for p and q consist, mod p, of $q - 1$ copies of each of the quadratic*

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.