TABLE 2 Wild card poker frequencies and probabilities, based on a revised hierarchy

Rank	Type	Frequency	Probability
1	FIVE-OF-A-KIND	78	0.000025
2	ROYAL FLUSH	84	0.000027
3	STRAIGHT FLUSH	480	0.000152
4	FOUR-OF-A-KIND	9360	0.002960
5	FULL HOUSE	9360	0.002960
6	FLUSH	11448	0.003620
7	STRAIGHT	30540	0.009657
8	TWO PAIR	302224	0.095565
9	THREE-OF-A-KIND	54912	0.017363
10	JUNK	1645784	0.520404
11	ONE PAIR	1098240	0.347268

The more one looks, the worse it gets. In the original hierarchy, there were 9360 four-of-a-kind hands and 9360 full house hands. So one could arbitrarily decide to rank a full house above four-of-a-kind. But this would really be disastrous, for then there would turn out to be 18096 full houses and 624 four-of-a-kind! With two added jokers as wild cards, there is *no* hierarchy of hands that is consistent with the frequency of the hands.

REFERENCES

1. Y. L. Cheung, Why poker is played with five cards, *The Mathematical Gazette* 73 (1989), 313–315.
2. Edward W. Packel, *The Mathematics of Games and Gambling*, Mathematical Association of America, 1981.

Counting Squares in $\mathbb{Z}_n$

WALTER D. STANGL
Biola University
LaMirada, CA 90639

An elementary number theory problem is to determine the possible forms of squares among the positive integers. For instance, it is easy to see that any square must be of the form $3k$ or $3k + 1$. (Since every positive integer can be written as either $3q$, $3q + 1$, or $3q + 2$, simply square these numbers and simplify.) Restated, this assertion is that 0 and 1 are the squares in $\mathbb{Z}_3$, the ring of equivalence classes of integers modulo 3. In general, a square has the form $nk + r$ if, and only if, r is a square in the ring $\mathbb{Z}_n$. How many squares are there in $\mathbb{Z}_n$?

Fundamental notions An element a in $\mathbb{Z}_n$ is a *square* in $\mathbb{Z}_n$ if and only if $x^2 = a$ has a solution in $\mathbb{Z}_n$. The *units* of $\mathbb{Z}_n$ are the elements that are relatively prime to n. The units that are squares are commonly called *quadratic residues* (or, more precisely, the quadratic residues mod n in a reduced residue system) [**1**, p. 84]. The quadratic residues have been completely characterized [**2**, p. 201], and the standard results will be utilized in what follows.

We will adopt the following notation: $q(n)$ = the number of quadratic residues in $\mathbb{Z}_n$, and $s(n)$ = the number of squares in $\mathbb{Z}_n$. For example, $q(8) = 1$ since $x^2 = 1$ has a solution in $\mathbb{Z}_8$ (as a matter of fact, all four units, namely 1, 3, 5, and 7, are solutions), and $x^2 = 3$, $x^2 = 5$, and $x^2 = 7$ do not have any solutions in $\mathbb{Z}_8$. Also, $s(8) = 3$ since $x^2 = 0$ and $x^2 = 4$ also have solutions in $\mathbb{Z}_8$, but $x^2 = 2$ and $x^2 = 6$ do not.

A number-theoretic function $f(n)$ is *multiplicative* if $\gcd(m, n) = 1$ implies $f(mn) = f(m) \cdot f(n)$. Typical number-theoretic functions that are multiplicative include the number of positive divisors of n and the sum of these divisors [1, p. 109]. A number-theoretic function that is multiplicative is completely characterized by its values on powers of primes. Both $q(n)$ and $s(n)$ are multiplicative; we derive both recursive and closed-form formulas for these functions on the powers of primes. This will allow us to compute $s(n)$ and $q(n)$ for any n, based on the prime factorization of n.

Suppose $\gcd(m, n) = 1$. Then $\mathbb{Z}_{mn}$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$ under the ring isomorphism h: $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ defined by $h(z) = (z \bmod m, z \bmod n)$ [3, p. 80]. Suppose a is a square in $\mathbb{Z}_{mn}$. Then there is a b in $\mathbb{Z}_{mn}$ such that $b^2 = a$. Since h is a function from $\mathbb{Z}_{mn}$ onto $\mathbb{Z}_m \times \mathbb{Z}_n$, there exists $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$ such that $h(b) = (x, y)$. Then $h(a) = h(b^2) = [h(b)]^2 = (x, y)^2 = (x^2, y^2)$, so $h(a)$ is a square in $\mathbb{Z}_m \times \mathbb{Z}_n$. Hence $s(mn) \leq s(m) \cdot s(n)$.

On the other hand, if u in $\mathbb{Z}_m$ and v in $\mathbb{Z}_n$ are squares, then there exist x in $\mathbb{Z}_m$ and y in $\mathbb{Z}_n$ such that $(x^2, y^2) = (u, v)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$. Thus $h^{-1}(u, v) = h^{-1}[(x, y)^2] = [h^{-1}(x, y)]^2$, so $h^{-1}(u, v)$ is a square in $\mathbb{Z}_{mn}$. Thus $s(mn) \geq s(m) \cdot s(n)$.

Combining these results yields the desired equality, showing that $s(n)$ is a multiplicative function. To extend the proof to $q(n)$ requires merely the observation that for any integer b, $\gcd(b, mn) = 1$ if, and only if, $\gcd(b, m) = 1$ and $\gcd(b, n) = 1$.

Recursion formula Our next goal is to prove a general recursion formula for the number of squares in $\mathbb{Z}_{p^n}$, where p is a prime greater than 2. Once this is achieved, formulas in closed form for the various components will complete our counting procedure. We begin with the observation that the squares in $\mathbb{Z}_{p^n}$ that are not quadratic residues are generated by the squares in $\mathbb{Z}_{p^{n-2}}$, i.e., b is a square in $\mathbb{Z}_{p^{n-2}}$ if and only if bp^2 is a square in $\mathbb{Z}_{p^n}$.

First, suppose there is c in $\mathbb{Z}_{p^{n-2}}$ such that $c^2 = kp^{n-2} + b$ in $\mathbb{Z}$. Then $c^2p^2 = kp^n + bp^2$. Now $cp < p^n$, so $(cp)^2 = bp^2$ is a square in $\mathbb{Z}_{p^n}$. Conversely, suppose there is y in $\mathbb{Z}_{p^n}$ such that $y^2 = mp^n + sp^2$ in $\mathbb{Z}$. Then p^2 divides y^2, so p divides y. Thus there is c such that $y = cp$. Then $c^2 = mp^{n-2} + s$ and s is a square in $\mathbb{Z}_{p^{n-2}}$.

Now we wish to count all the squares in $\mathbb{Z}_{p^n}$. We begin by observing that the squares are of two types. Since $q(p^n)$ counts the squares in $\mathbb{Z}_{p^n}$ that are units, we must merely count the squares that are non-units, i.e., multiples of p. Suppose kp is a square in $\mathbb{Z}_{p^n}$. Then there is a b such that $b^2 = cp^n + kp$. Then p divides b^2, and hence b. Thus p^2 divides b^2, and hence kp, so p divides k. Hence the multiples of p that are squares are multiples of p^2. But by the preceding result, the number of these will be given by $s(p^{n-2})$.

Thus we have proven the following recursion formula.

THEOREM. *For $n \geq 3$, $s(p^n) = q(p^n) + s(p^{n-2})$.*

Powers of odd primes In order to obtain explicit formulas for the functions $q(p^n)$ and $s(p^n)$, it is useful to deal with the case $p = 2$ separately. The argument for powers of an odd prime p depends on the existence of a primitive root for p^n for each n. In algebraic language, this says that the units of $\mathbb{Z}_{p^n}$ form a cyclic group with

respect to multiplication and hence have a generator [**1**, p. 62]. Since this is not true for powers of 2 greater than or equal to 3, our approach and results will need to be altered for that situation.

If p is an odd prime, the Euler phi-function yields the numbers of units of $\mathbb{Z}_{p^n}$, namely $p^n - p^{n-1}$. There is a primitive root of p^n. The even powers of this primitive root are clearly distinct quadratic residues, and the following formula is proven.

THEOREM. *If p is an odd prime, then $q(p^n) = (p^n - p^{n-1})/2$, for all $n \geq 1$.*

In order to count all of the squares in $\mathbb{Z}_{p^n}$, it is useful to look at the first two cases separately. Since 0 is the only non-unit in $\mathbb{Z}_p$, clearly $s(p) = q(p) + 1 = (p+1)/2$. In $\mathbb{Z}_{p^2}$, the non-units are multiples of p, and have squares equal to 0. So $s(p^2) = q(p^2) + 1 = (p^2 - p + 2)/2$.

Now suppose $n \geq 3$ and n is even. By repeated applications of the recursion formula, we obtain

$$\begin{aligned} s(p^n) &= \frac{p^n - p^{n-1}}{2} + \frac{p^{n-2} - p^{n-1}}{2} + \cdots \frac{p^4 - p^3}{2} + \frac{p^2 - p + 2}{2} \\ &= \frac{p^{n+1} - p^n + p^n - p^{n-1} + p^{n-1} - \cdots + p^3 - p^2 + 2p + p^2 - p + 2}{2(p+1)} \\ &= \frac{p^{n+1} + p + 2}{2(p+1)}. \end{aligned}$$

If n is odd, we obtain

$$\begin{aligned} s(p^n) &= \frac{p^n - p^{n-1}}{2} + \frac{p^{n-2} - p^{n-1}}{2} + \cdots \frac{p^3 - p^2}{2} + \frac{p+1}{2} \\ &= \frac{p^{n+1} - p^n + p^n - p^{n-1} - \cdots + p^2 + 2p + 1}{2(p+1)} \\ &= \frac{p^{n+1} + 2p + 1}{2(p+1)}. \end{aligned}$$

Our results are summarized in the following theorem.

THEOREM. *Suppose p is an odd prime. Then*

$$s(p) = \frac{p+1}{2} \quad \text{and} \quad s(p^2) = \frac{p^2 - p + 2}{2}.$$

If $n \geq 3$, then

$$s(p^n) = \begin{cases} \dfrac{p^{n+1} + p + 2}{2(p+1)} & n \text{ even} \\ \dfrac{p^{n+1} + 2p + 1}{2(p+1)} & n \text{ odd}. \end{cases}$$

Powers of two Now we proceed to the remaining case: powers of 2. We need a preliminary result before moving to our main goal.

Suppose $n \geq 3$, and $\gcd(a, 2^n) = 1$. Consider the equation $x^2 = a$ in $\mathbb{Z}_{2^n}$. Suppose b is a solution. Then, clearly, $-b$ is also a solution. Also $b \neq -b$, since otherwise $2b = 0$ which implies $\gcd(b, 2^n) \neq 1$ while we know $\gcd(b^2, 2^n) = 1$. Another pair of solutions is easily verified to be given by $2^{n-1} \pm b$. These values are also seen to be distinct by the above argument.

To show these four solutions are the only solutions, suppose $\gcd(c, 2^n) = 1$ and c is a solution in addition to b. Then $b^2 = a = c^2$ in $\mathbb{Z}_{2^n}$ implies $b^2 - c^2 = 0$ or $(b-c)(b+c) = 0$ in $\mathbb{Z}_{2^n}$. Since b and c are both odd, either $(b-c)$ or $(b+c)$ must be of the form $4m + 2 = 2(2m+1)$. So the other factor is a multiple of 2^{n-1} or 0. Hence $c = 2^{n-1} \pm b$ or $c = \pm b$.

Thus we conclude that if $x^2 = a$ has a solution in $\mathbb{Z}_{2^n}$, then the equation has exactly 4 distinct solutions in $\mathbb{Z}_{2^n}$.

We observe that the only quadratic residue in either $\mathbb{Z}_2$ or $\mathbb{Z}_4$ is 1. It follows that $q(2) = q(4) = 1$.

For $n \geq 3$, there are 2^{n-1} units in $\mathbb{Z}_{2^n}$, namely the odd numbers. Consider two units equivalent if their squares are equal. Then the units can be divided into equivalence classes of 4 units each; hence there will be $2^{-2}2^{n-1} = 2^{n-3}$ quadratic residues in $\mathbb{Z}_{2^n}$. Thus for $n \geq 3$, $q(2^n) = 2^{n-3}$.

We are now ready to prove our final formulas. Here's the result.

THEOREM.

$$s(2^n) = \begin{cases} \dfrac{2^{n-1}+4}{3} & n \text{ even} \\ \dfrac{2^{n-1}+5}{3} & n \text{ odd } n \geq 3. \end{cases}$$

Proof. The argument is by induction. Starting with $n = 2$, it is clear that $s(2^2) = 2$. Now assume that the formula holds for $n \leq k$. There are two cases.

Case I. $k+1$ is even. Then

$$s(2^{k+1}) = q(2^{k+1}) + s(2^{k-1}) = 2^{(k+1)-3} + \frac{2^{(k-1)-1}+4}{3}$$
$$= 2^{k-2} + \frac{2^{k-2}+4}{3} = \frac{4\cdot 2^{k-2}+4}{3} = \frac{2^{(k+1)-1}+4}{3}.$$

Case II. $k+1$ is odd. Then

$$s(2^{k+1}) = q(2^{k+1}) + s(2^{k-1}) = 2^{(k+1)-3} + \frac{2^{(k-1)-1}+5}{3}$$
$$= 2^{k-2} + \frac{2^{k-2}+5}{3} = \frac{4\cdot 2^{k-2}+5}{3} = \frac{2^{(k+1)-1}+5}{3}.$$

The preceding formulas are derivable directly from the recursion formula. For instance, if n is odd, repeated applications yield

$$s(2^n) = q(2^n) + q(2^{n-2}) + \cdots + q(2^3) + s(2^1)$$
$$= 2^{n-3} + 2^{n-5} + \cdots + 1 + 2.$$

So we need a formula for the sum of the even powers of 2. Letting $x_n = 1 + 2^2 + \cdots + 2^{2n}$, we have

$$x_n = (2^2)^0 + (2^2)^1 + \cdots + (2^2)^n$$
$$= \frac{(2^2)^{n+1} - 1}{2^n - 1}.$$

So $x_n = \dfrac{2^{2n+2}-1}{3}$, and

$$s(2^n) = x_{(n-3)/2} + 2$$
$$= \frac{2^{n-1}-1}{3} + 2 = \frac{2^{n-1}+5}{3}.$$

A formula for the sum of the odd powers of 2 is obtained from x_n by factoring, and then $s(2^n)$ is easily computed.

REFERENCES

1. Ivan Niven and Herbert Zuckerman, *An Introduction to the Theory of Numbers*, 4th edition, John Wiley & Sons, Inc., New York, 1980.
2. David M. Burton, *Elementary Number Theory*, 3rd edition, Wm. C. Brown, Dubuque, IA, 1994.
3. John Fraleigh, *A First Course in Abstract Algebra*, 3rd edition, Addison-Wesley, Reading, MA, 1982.

Magic Squares of Squares

JOHN P. ROBERTSON
560 Bair Road
Berwyn, PA 19312

A problem in the second edition of Guy's *Unsolved Problems in Number Theory* [1] is to prove or disprove that a three-by-three magic square can be constructed from nine distinct integer squares (Problem D15). There are relationships between magic squares, arithmetic progressions, Pythagorean right triangles, congruent numbers, and elliptic curves. This note will follow this chain and show that the following three problems are equivalent to the original problem:

P1. Prove or disprove that there are three arithmetic progressions such that each has three terms, each has the same difference between terms as the other two, the terms are all perfect squares, and the middle terms of the three arithmetic progressions themselves form an arithmetic progression.

P2. Prove or disprove that there are three rational right triangles with the same area, such that the squares of the hypotenuses are in arithmetic progression.

P3. Prove or disprove that there is an elliptic curve, $y^2 = x^3 - n^2x$, where n is a congruent number, with three rational points on the curve, (x_1, y_1), (x_2, y_2), and (x_3, y_3), such that each point is "double" another rational point on the elliptic curve ("double" in the sense of the group structure for points on an elliptic curve), and x_1, x_2, and x_3 are in arithmetic progression.

The original problem is due to LaBar [2]. Guy [1] notes that the problem requires finding x, y, and z so that the nine quantities x^2, y^2, z^2, $y^2+z^2-x^2$, $z^2+x^2-y^2$, $x^2+y^2-z^2$, $2x^2-y^2$, $2x^2-z^2$, and $3x^2-y^2-z^2$, are distinct perfect squares.

Magic squares and arithmetic progressions For any three-by-three magic square made up of distinct positive integers, there are three positive integers a, u, and v,