A Theorem about Primes Proved on a Chessboard
Author(s): Loren C. Larson
Source: *Mathematics Magazine*, Vol. 50, No. 2 (Mar., 1977), pp. 69-74
Published by: Mathematical Association of America
Stable URL: http://www.jstor.org/stable/2689726
Accessed: 13/11/2013 15:26

ARTICLES

A Theorem about Primes Proved on a Chessboard

An elementary treatment of a class of solutions to the n-queens problem leads to a proof of Fermat's theorem on primes which are sums of two squares.

LOREN C. LARSON
St. Olaf College

Arrange queens on a 13 × 13 chessboard according to the following rule: place a queen on the center square and from it locate others by making successive $(2,3)$ movements — two squares to the right and three squares upward (top and bottom edges are identified, as well as right and left). The resulting queen placement (FIGURE 1) shows exactly one queen in each row and column, and no two on the same diagonal; as such, it is a solution to the n-queens problem (to place n nonattacking queens on the $n \times n$ chessboard) for $n = 13$. The solution is distinguished from other solutions in two respects: (i) it is **regular,** meaning that the queens are located at successive (s, t) movements from each other, for some integers s and t (a more precise definition will be given later), and (ii) it is **doubly symmetric,** meaning that it is invariant under a 90° rotation of the board about the center square.

More generally, suppose that u and v are positive integers and $u^2 + v^2$ is an odd prime p. We will show that queens located at successive (u, v) movements from a queen on the center square of the $p \times p$ chessboard give a regular, doubly symmetric solution to the p-queens problem. Conversely, we will see that regular, doubly symmetric solutions to the p-queens problem, for p a prime, yield positive integers u and v such that $u^2 + v^2 = p$. In the final section we will show by a simple combinatorial argument that there is a regular, doubly symmetric solution to the p-queens problem whenever p is a prime of the form $4k + 1$. Combining this result with the preceding implication gives a proof of Fermat's Two-Square Theorem: *primes of the form* $4k + 1$ *can be expressed as the sum of two squares.*

This proof of Fermat's theorem is both elementary and concrete. It avoids the usual first step of knowing that -1 is a quadratic residue modulo p when p is a prime of the form $4k + 1$. Moreover it uses the chessboard to provide a specific geometrical setting for illustrating and interpreting abstract concepts usually first encountered in an introductory abstract algebra course. The ideas on which this approach is based are scattered throughout references [**1**] and [**2**]. The chief insight — relating Fermat's Two-Square Theorem to the n-queens problem — is due to George Polya.

Preliminaries

The additive group of integers will be denoted by Z, and $\bar{Z}_n = \{1, 2, 3, \ldots, n\}$ will denote the cyclic group of order n, having the operation of addition modulo n. If x is an integer, $[x]$ will denote that integer between 1 and n inclusive which is congruent to x modulo n. (Since we will be working on an $n \times n$ chessboard, there will be no need to write $[x]_n$ to indicate the modulus.) There is little danger of confusion in using $[x]$ to denote an element of Z and also an element of $\bar{Z}_n$, for the context will make the intention clear.

For convenience we will identify the chessboard with the group $\bar{Z}_n \times \bar{Z}_n$. Geometrically, the group element (i, j) represents the square in the ith column (from the left) and the jth row (from the bottom). A **regular solution** to the n-queens problem is a solution in which the queens are located on the squares (represented by the elements) of the coset $(a, b) + \langle(s, t)\rangle$ for some $(a, b), (s, t) \in \bar{Z}_n \times \bar{Z}_n$, where $\langle(s, t)\rangle$ is the cyclic subgroup of $\bar{Z}_n \times \bar{Z}_n$ generated by (s, t). In this case, we will say that $(a, b) + \langle(s, t)\rangle$ is a regular solution.

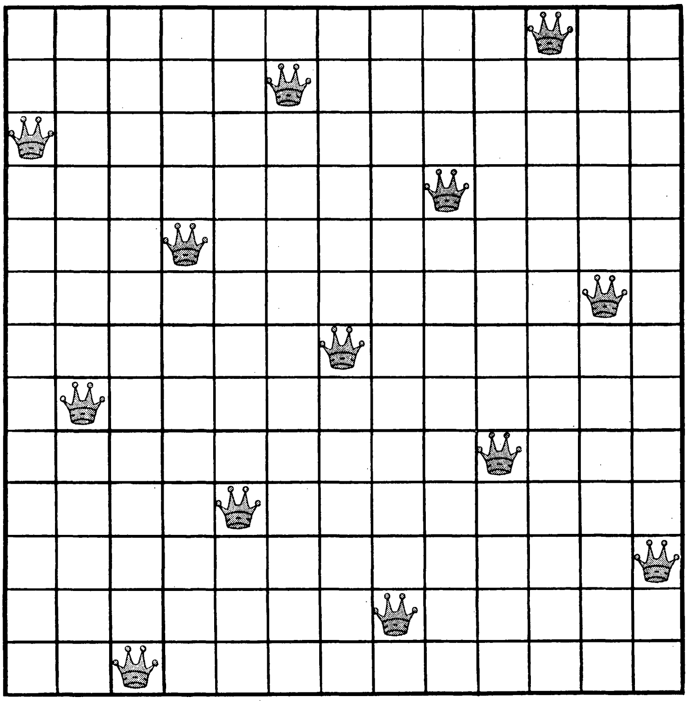


FIGURE 1

It is important to observe that every regular solution can be expressed in the form $(n, c) + \langle(1, d)\rangle$ for some $c, d \in \bar{Z}_n$. For, suppose that $(a, b) + \langle(s, t)\rangle$ is a regular solution. We know that $k(s, t)$ is a generator of $\langle(s, t)\rangle$ whenever k is an integer relatively prime to n. (Geometrically, the solution can be generated by many different regular movements.) Since s must be relatively prime to n in order that each column be occupied (similarly for t and the rows), there exists an integer r, relatively prime to n, such that $rs \equiv 1 \pmod{n}$. For this r, $r(s, t)$ is of the form $(1, d)$ for some $d \in \bar{Z}_n$. Thus $\langle(s, t)\rangle = \langle r(s, t)\rangle = \langle(1, d)\rangle$. Since a queen occurs in column n, we have, for some $c \in \bar{Z}_n$, $(n, c) \in (a, b) + \langle(s, t)\rangle$, or equivalently, $(n, c) \in (a, b) + \langle(1, d)\rangle$. It follows, then, that $(a, b) + \langle(s, t)\rangle = (n, c) + \langle(1, d)\rangle$. (For the example in the introduction, $c = 3$ and $d = 8$.)

We are interested in finding conditions on c and d so that $(n, c) + \langle(1, d)\rangle$ will be a solution to the n-queens problem. It is easy to see that a necessary condition is that d be relatively prime to n (so that each row be occupied); but this is not sufficient, since, for example, $d = 1$ violates the diagonal requirements. Notice that two queens lie on the same rising diagonal (diagonals having slope 1) if the differences (in Z) of their coordinates are the same, and on the same falling diagonal if the sums (in Z) of their coordinates are equal. For the coset above, queens are located on the squares $(i, [c + id])$ for $i = 1, 2, \ldots, n$. Since $i + [c + id] \equiv c + i(d + 1) \pmod n$, the sums of these coordinates will be different provided that $d + 1$ is relatively prime to n. Similarly, since $[c + id] - i \equiv c + i(d - 1) \pmod n$, the differences will be distinct if $d - 1$ is relatively prime to n. Thus, a sufficient condition for $(n, c) + \langle(1, d)\rangle$ to be a solution is that $d - 1$, d and $d + 1$ each be relatively prime to n. We leave it as an exercise to prove that this condition is also necessary. (Warning: this converse is not immediate since two of the coordinate sums (differences) may be equal in $\bar{Z}_n$, but unequal in Z.) We summarize the preceding discussion in the following formal lemma:

FUNDAMENTAL LEMMA. *The placement $(n, c) + \langle(1, d)\rangle$ is a solution to the n-queens problem if and only if $d - 1$, d and $d + 1$ are each relatively prime to n.*

An immediate corollary helps explain why the 8-queeens problem is so much more difficult than the 7-queens problem, which most beginners solve very quickly. We will state and prove it here, even though we will not need it (nor, for that matter, the "only if" part of the Fundamental Lemma) for the main result of the paper.

COROLLARY. *There exists a regular solution to the n-queens problem if and only if $n \equiv \pm 1$* (mod 6).

Proof. We have seen that regular solutions have the form $(n, c) + \langle(1, d)\rangle$ for some c and d. If $n \equiv \pm 1 \pmod 6$ we get a regular solution by taking $d = 2$ (ordinary knight moves). However, for $n \equiv 0, 2, 3, 4 \pmod 6$ we cannot have regular solutions since one of $d - 1$, d, $d + 1$ is divisible by 3 and at least one of them is even.

From Number Theory to the Chessboard

Suppose that p is an odd prime number and that u and v are positive integers such that $u^2 + v^2 = p$. Choose an integer r so that $r(u, v) = (1, d)$ for some $d \in \bar{Z}_p$. Then $r^2u^2 + r^2v^2 = r^2p$, $1^2 + d^2 \equiv 0 \pmod p$ and therefore $d^2 \equiv -1 \pmod p$. Thus $(d + 1)(d - 1) \equiv d^2 - 1 \equiv -2 \pmod p$. It follows that $d - 1$, d and $d + 1$ are each relatively prime to p and therefore $(1, d)$ movements will generate a regular solution. The center square has coordinates $((p + 1)/2, (p + 1)/2)$, so in order that $(p, c) + \langle(1, d)\rangle$ have a queen on the center square, it is necessary and sufficient that

$$c + \left(\frac{p+1}{2}\right) d \equiv \frac{p+1}{2} \pmod p$$

or

$$2c + d \equiv 1 \pmod p. \qquad (1)$$

Suppose that c is so determined. Now under a 90° clockwise rotation, the queen located on the square $(i, [c + id])$ will rotate to the square $([c + id], [1 - i])$. But this square is occupied by a queen in $(p, c) + \langle(1, d)\rangle$, since $[c + [c + id]d] = [c + cd + id^2] = [c(1 + d) - i] = [(1 - d)/2)(1 + d) - i] = [(1 - d^2)/2) - i] = [1 - i]$. Therefore the solution is doubly symmetric.

From the Chessboard to Number Theory

Suppose now that p is a prime and that $(p, c) + \langle(1, d)\rangle$ is a regular, doubly symmetric solution to the p-queens problem. Since the 2×2 board does not admit such a solution, the prime p is odd. Observe that a queen is located on the center square, since queens off the center come in sets of four, these located at quarter turns from each other (rotational symmetry). (Incidentally, this shows that p has the form $4k+1$.)

From among all the queens on the board, pick one that is closest to the queen on the center square; suppose it is located at a (u, v) movement from the center square. Because of rotational symmetry we may suppose that u and v are positive. (Other closest queens will be located at $(v, -u)$, $(-u, -v)$, and $(-v, u)$ movements from the center square.) Because the solution is regular, no two queens can be located closer together than these two queens. (To get from one queen to another requires an $i(1, d) \in \bar{Z}_p \times \bar{Z}_p$ movement for some integer i, and this same movement could be made from the center square.)

The center queen and the two queens located at (u, v) and $(v, -u)$ movements from it, occupy three vertices of a square region; the fourth vertex of this square is occupied by a queen in the solution since it is a $(u, v)+(v, -u) \in \bar{Z}_p \times \bar{Z}_p$ movement from the center (and each summand is a multiple of a $(1, d)$ movement). Furthermore, no queen in the solution will be located in the interior of this square (since that would violate our choice of u and v). In the same way, every queen on the board can be associated with a square region whose vertices are given by its own position and those queens at (u, v), $(v, -u)$ and $(u, v)+(v, -u)$ movements from it. It is understood that left and right, top and bottom edges are identified, so that squares which overlap an edge are continued on the opposite side (see FIGURE 2). In this way the $p \times p$ chessboard is dissected into p regions (one for each queen) each of equal area. Since the total area of the chessboard is p^2, each individual square has an area equal to p. It follows that the side length of each square is $\sqrt{p}$, and therefore, from the Pythagorean theorem, that $p = u^2 + v^2$.

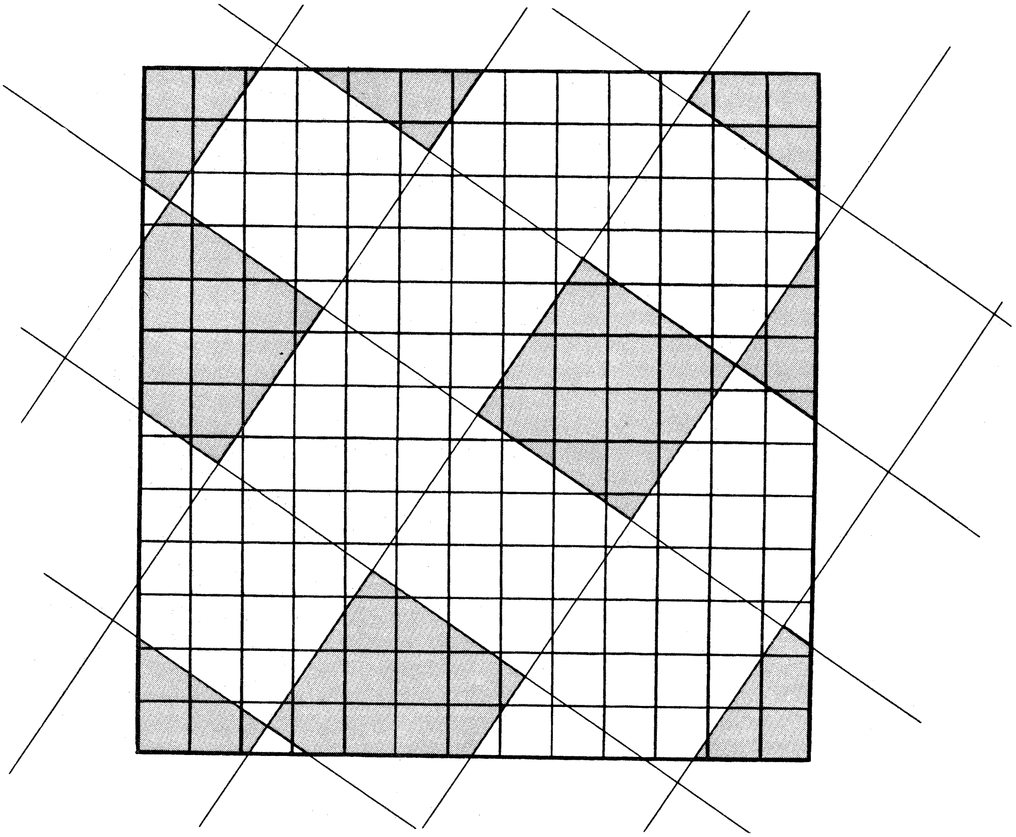


FIGURE 2

It may be instructive to point out that the queen positions in a regular solution are part of a lattice that extends to the entire plane. This can be seen algebraically by first observing that the mapping ϕ: $Z \times Z \rightarrow \bar{Z}_n \times \bar{Z}_n$ defined by $((x, y))\phi = ([x], [y])$ is a group homomorphism. Let H be the cyclic subgroup of $Z \times Z$ generated by (u, v). Then the elements of $(H\phi)\phi^{-1}$ may be interpreted geometrically as the positions of the queens obtained by tiling the entire plane with copies of the chessboard having queens located on the squares $H\phi$. However, $(H\phi)\phi^{-1}$ is a subgroup of $Z \times Z$, and therefore it is a lattice of dimension two, having a fundamental region of area equal to the absolute value of the determinant of the matrix gotten by expressing the lattice basis in terms of the canonical basis of $Z \times Z$. Now an arbitrary regular solution to the n-queens problem is a translation of $H\phi$ for some cyclic group H of $Z \times Z$, and this corresponds to the same translation in $Z \times Z$ of the subgroup $(H\phi)\phi^{-1}$.

Fermat's Two Square Theorem

In order to prove Fermat's result, we need to show that there is a regular, doubly symmetric solution to the p-queens problem whenever p is a prime of the form $4k + 1$. To do this, we will count the total number of regular solutions for the $p \times p$ board in two different ways.

LEMMA. *The number of regular solutions to the p-queens problem, where p is a prime, is $p(p-3)$.*

Proof. We know that regular solutions have the form $(p, c) + \langle(1, d)\rangle$. Clearly we do not get a solution when d is $p, p-1$, or 1. But any of the other $p-3$ possibilities for d, in $\bar{Z}_p$, will produce regular solutions, since in these cases $d-1$, d, and $d+1$ will each be relatively prime to p. Since c can take on any of p values, the total number of regular solutions is $p(p-3)$.

A second way of counting the regular solutions is to partition them into three classes, depending upon their symmetry — doubly symmetric, symmetric (invariant under a 180° rotation but not a 90° rotation), or nonsymmetric (no symmetry). The symmetries of the square consist of four reflections and four rotations, and these form a group G, under composition. If x denotes a regular solution and $U \in G$, the regular solution which results from x by applying the transformation U will be denoted by xU. Two regular solutions x and y are **essentially the same** if and only if there exists a $U \in G$ such that $xU = y$. This is an equivalence relation on the set of all regular solutions. The equivalence class of a solution x consists of all those solutions that can be obtained from x by rotation and reflection. For each regular solution x, let H_x denote the set of all symmetries of x; that is, $H_x = \{U \in G \mid xU = x\}$. H_x is a subgroup of G. Furthermore, if $U, V \in G$, $xU = xV$ if and only if $xUV^{-1} = x$, and this happens if and only if $UV^{-1} \in H_x$. It follows that the number of elements in the equivalence class of x is equal to the index of H_x in G, and this is 2, 4, or 8 depending upon whether x is doubly symmetric, symmetric, or nonsymmetric respectively. Thus we have the following lemma:

LEMMA. *The number of regular solutions to the n-queens problem is $2x + 4y + 8z$, where x, y, z are, respectively, the number of essentially different doubly symmetric, symmetric, and nonsymmetric regular solutions to the n-queens problem.*

Now suppose that p is a prime of the form $4k + 1$. Combining the results of the preceding two lemmas, we know that $p(p-3) = 2x + 4y + 8z$. Since, in this equation, $p \equiv 1 \pmod 4$, it becomes $2 \equiv 2x \pmod 4$. But this completes the proof, since this last equation implies that x, the number of essentially different regular, doubly symmetric solutions, is not zero.

Finally, we can show that the positive integers u and v in Fermat's result are unique. To do this, it is sufficient to prove that there are only two regular, doubly symmetric solutions to the p-queens problem — a single solution, and its horizontal reflection, both of which induce the same positive integers u and v for which $u^2 + v^2 = p$. So, suppose that $(p, c) + \langle(1, d)\rangle$ is a regular, doubly symmetric solution to the p-queens problem. Since a queen is located on the square $(1, [c + d])$, there must also be (by rotational symmetry) a queen on the square $([c + d], p)$. This means that

$$c+[c+d]d \equiv p \pmod{p}. \tag{2}$$

The fact that the center square is occupied means that (1) holds, so that we may substitute $c \equiv (1-d)/2$ from (1) into (2) to get

$$\left(\frac{1-d}{2}\right)+\left(\frac{1+d}{2}\right) d \equiv p \pmod{p}$$

which simplifies to

$$d^2+1 \equiv 0 \pmod{p}. \tag{3}$$

Thus d satisfies $x^2+1=0$ over the field $\bar{Z}_p$. Alternatively, if we substitute $d \equiv 1-2c$ from (1) into (2) we see that c must satisfy $x^2+(x-1)^2=0$ over $\bar{Z}_p$. Thus the existence of a regular, doubly symmetric solution to the p queens problem, for p a prime of the form $4k+1$, also implies the existence of two solutions to each of the equations $x^2+1=0$ and $x^2+(x-1)^2=0$ in $\bar{Z}_p$. Since $\bar{Z}_p$ is a field, these second order polynomial equations can have only two solutions in $\bar{Z}_p$, which implies that there can be only two possible values for d and c. But once one of these values is known, so is the other by equation (1), proving that there are at most two regular, doubly symmetric solutions to the p-queens problem when p is a prime.

In conclusion, we note that these latter equations offer an alternative, albeit less elegant, procedure for proving the existence of a regular, doubly symmetric solution to the p-queens problem for p a prime of the form $4k+1$; simply choose d by (3) and c by (1) and apply the argument following equation (1).

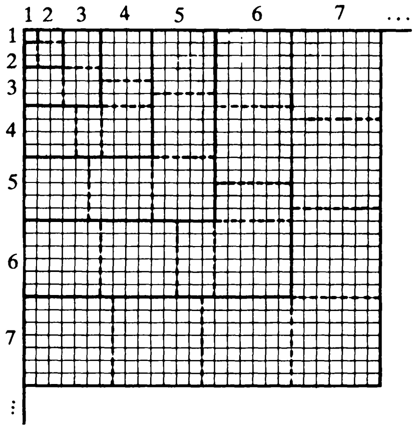
References

[1] Maurice Kraitchik, La Mathématique des Jeux ou Récréations Mathématiques, Chapter XIII, Le Problème des Reines, Bruxelles, 1930, pp. 300–356.

[2] G. Polya, Über die "doppelt-periodischen" Lösungen des n-Damen Problems, Mathematische Unterhaltungen und Spiele, Dr. W. Ahrens. Zweiter Band, B. G. Teubner, Leipzig, 1918, pp. 363–374.

Proof without words: Cubes and squares

$$1^3+2^3+3^3+\cdots+n^3$$
$$=(1+2+3+\cdots+n)^2$$



— J. Barry Love
National Liberty Corp.
Valley Forge, Penn.