A NEW METHOD FOR CONSTRUCTING NONLINEAR MODULAR n-QUEENS SOLUTIONS

JORDAN BELL

ABSTRACT. In this paper we give a new method for constructing modular n-queens solutions which in particular yields nonlinear solutions for all composite n such that $\gcd(n,6) = 1$ and all prime $n \geq 19$.

1. INTRODUCTION

The modular n-queens problem is to place n nonattacking queens on the $n \times n$ modular chessboard, for which opposite sides are identified, like a torus; this was first considered by Pólya in [4]. This is also known as the toroidal n-queens problem. We number the rows of the $n \times n$ modular board from 0 at the top to $n-1$ at the bottom and 0 at the left to $n-1$ at the right, and we refer to the cell on row i and column j by (i,j). We define a *modular sum diagonal* as the set $\{(i,j)|i+j \equiv c \pmod{n}\}$ for a fixed c, and a *modular difference diagonal* as the set $\{(i,j)|i-j \equiv c \pmod{n}\}$ for a fixed c.

A placement of n nonattacking queens on the $n \times n$ modular board is said to be a *modular n-queens solution.* (This is equivalent to an independent set of n vertices in the queens graph of n^2 vertices, with adjacency determined by queen attacks.) We observe that a permutation g of $\{0,\ldots,n-1\} = \mathbf{Z}_n$, of the columns into the rows, is a modular n-queens solution if and only if $g(x)+x \pmod{n}$ and $g(x)-x \pmod{n}$ are both permutations of $\mathbf{Z}_n$, to avoid modular sum and difference diagonal attacks respectively. We say that a modular n-queens solution g is *linear* when it is of the form $g(x) \equiv cx+d \pmod{n}$ for fixed c and d, and *nonlinear* otherwise. Linear n-queens solutions are also known as regular n-queens solutions in the literature.

We recall from Pólya in [4] that a modular n-queens solution exists if and only if $\gcd(n,6) = 1$. For $\gcd(n,6) = 1$, it can be shown without difficulty that a self-mapping g of $\mathbf{Z}_n$ is a linear modular n-queens solution if and

2000 *Mathematics Subject Classification.* Primary: 05B30, Secondary: 05C69.

Key words and phrases. modular n-queens problem, toroidal n-queens problem, n-queens problem, queens graph.

The author was supported by an NSERC USRA while this paper was written.

only if $g(x) \equiv cx+d \pmod{n}$ for some constants c and d where $c-1, c, c+1$ are all relatively prime to n. Burger, Mynhardt and Cockayne determine in [3] the number of isometry classes of linear modular n-queens solutions for all n such that $\gcd(n,6) = 1$, i.e. for all n such that a modular n-queens solution exists.

In this paper we give a new method for constructing modular n-queens solutions, which gives modular n-queens solutions for all n where $\gcd(n,6) = 1$, and in particular yields nonlinear solutions for all composite n such that $\gcd(n,6) = 1$, and all prime $n = p \geq 19$.

2. Results

Let $\mathbf{U}_n = \{m \in \mathbf{Z}_n | \gcd(m,n) = 1\}$ be the multiplicative group of units of $\mathbf{Z}_n$. For G any subgroup of $\mathbf{U}_n$, we define $R(G) = \{u \in G | u-1, u+1 \in G\}$. Recall that for each $x \in \mathbf{Z}_n$, the orbit of x under the action of G is $Gx = \{gx | g \in G\}$. Then, for $\mathcal{O}(G)$ the set of all orbits of the elements of $\mathbf{Z}_n$ under G, recall further that $\mathcal{O}(G)$ is a partition of $\mathbf{Z}_n$, i.e. each $x \in \mathbf{Z}_n$ is in one and only one orbit under the action of G. We also observe that if $u \in G$, then $G(ux) = Gx$ for all $x \in \mathbf{Z}_n$, since G is a group.

Theorem 1. *Let n be a positive integer such that $\gcd(n,6) = 1$, and let G be a fixed subgroup of $\mathbf{U}_n$. Then for any function $f : \mathcal{O}(G) \to R(G)$, the self-mapping g of $\mathbf{Z}_n$ defined by $g(x) \equiv f(Gx)x \pmod{n}$ is a modular n-queens solution.*

Proof. Suppose that for some $x \not\equiv y \pmod{n}$, $g(x) \equiv g(y) \pmod{n}$. Thus:

$$f(Gx)x \equiv f(Gy)y \pmod{n}. \tag{1}$$

Since $f(Gx) \in G$, then $f(Gx)x \in Gx$, and similarly $f(Gy)y \in Gy$. Because $\mathcal{O}(G)$ is a partition of $\mathbf{Z}_n$, it must then be that $Gx = Gy$, and so $f(Gx) = f(Gy)$. Since $f(Gx) \in \mathbf{U}_n$, we can divide (1) by $f(Gx) = f(Gy)$, yielding $x \equiv y \pmod{n}$, a contradiction.

Suppose that for some $x \not\equiv y \pmod{n}$, $g(x) + x \equiv g(y) + y \pmod{n}$. Thus:

$$f(Gx)x + x \equiv f(Gy)y + y \pmod{n}. \tag{2}$$

Since $f(Gx) \in R(G)$, then $f(Gx)+1 \in G$. As $f(Gx)x + x = (f(Gx)+1)x$, then $f(Gx)x + x \in Gx$, and likewise $f(Gy)y + y \in Gy$. Since $\mathcal{O}(G)$ is a partition of $\mathbf{Z}_n$ it must be that $Gx = Gy$, and thus $f(Gx) = f(Gy)$. But since $f(Gx) \in R(G)$, then $f(Gx) + 1 \in G$, so we can divide (2) by $f(Gx) + 1 = f(Gy) + 1$, obtaining $x \equiv y \pmod{n}$, a contradiction.

Showing that $g(x) - x \pmod{n}$ is a permutation can be done in the same way as for $g(x) + x \pmod{n}$ above. Hence g is a modular n-queens solution. □

The following theorem is then clear:

Theorem 2. *Let n be a positive integer such that* $\gcd(n,6) = 1$. *For G a subgroup of $\mathbf{U}_n$ and $f : \mathcal{O}(G) \to R(G)$, the modular n-queens solution g given by Theorem 1 is nonlinear if and only if there exists an $x \in \mathbf{Z}_n$ such that* $f(Gx)x \not\equiv f(G1)x \pmod{n}$.

In particular we note that $\gcd(n,6) = 1$ implies that $2, 3 \in R(G)$. Hence for all composite n such that $\gcd(n,6) = 1$, it is clear that for $G = \mathbf{U}_n$, the function $f : \mathcal{O}(G) \to R(G)$ defined by $f(G1) = 2$ and $f(Gx) = 3$ for all $x \notin G$ satisfies the above theorem. Thus for all composite n such that $\gcd(n,6) = 1$ there exists a nonlinear modular n-queens solution g.

For example, for $n = 35$, let $G = \mathbf{U}_{35}$. Then $R(G) = \{0, 2, 3, 12, 17, 18, 23, 32, 33\}$, and $\mathcal{O}(G) = \{G0, G1, G5, G7\}$. Define the function $f : \mathcal{O}(G) \to R(G)$ by $f(G1) = 3, f(G5) = 32, f(G7) = 3$, and $f(G0)$ an arbitrary element in $R(G)$. Then for the self-mapping g of $\mathbf{Z}_{35}$ defined by $g(x) \equiv f(Gx)x \pmod{35}$, Theorems 1 and 2 imply that g is a nonlinear modular n-queens solution. Expressing g by $g = (g(0), g(1), \ldots, g(34))$, we have:

$$g = (0,3,6,9,12,20,18,21,24,27,5,33,1,4,7,25,13,16,19,22,10,28,31,34,\\ 2,30,8,11,14,17,15,23,26,29,32),$$

which we show in Figure 1.

Theorem 3. *For p prime, G a subgroup of $\mathbf{U}_p$, and $f : \mathcal{O}(G) \to R(G)$, the modular n-queens solution g given by Theorem 1 is nonlinear if and only if* $|f(\mathcal{O}(G) \setminus \{0\})| > 1$.

Proof. If g is nonlinear then by Theorem 2 there is some x such that $f(Gx)x \not\equiv f(G1)x \pmod{p}$. Clearly $x \not\equiv 0 \pmod{p}$, and so $x \in \mathbf{U}_p$, which implies that $f(Gx) \not\equiv f(G1) \pmod{p}$, so the image of $\mathcal{O}(G) \setminus \{0\}$ under f has more than one element in it.

If the image of $\mathcal{O}(G) \setminus \{0\}$ under f has more than one element in it, then there is some $x \not\equiv 0 \pmod{p}$ such that $f(Gx) \not\equiv f(G1) \pmod{p}$. But $x \in \mathbf{U}_p$, implying that $f(Gx)x \not\equiv f(G1)x \pmod{p}$, so by Theorem 2, g is nonlinear. □

The following lemma shows that for all $p \geq 19$, such an $f : \mathcal{O}(G) \to R(G)$ exists:

Lemma 4. *For all prime $p \geq 19$, there exists a proper subgroup G of $\mathbf{U}_p$ such that* $|R(G)| > 1$.

Proof. Let $\nu(p)$ be the number of quadratic residues x modulo p in the set $\{1, 2, \ldots, p-1\}$ such that $x-1$ and $x+1$ are also quadratic residues modulo p. Andrews in [1, Theorem 10.4] proves that $|\nu(p) - \frac{1}{8}p| < \frac{1}{4}\sqrt{p} + 2$. Note that for all $p \geq 37$, $\frac{1}{8}p - \frac{1}{4}\sqrt{p} - 2 > 1$, hence for all $p \geq 37$, $\nu(p) > 1$. Hence for all $p \geq 37$, for G the (proper) subgroup of $\mathbf{U}_p$ of the quadratic residues

modulo p, $|R(G)| > 1$. For $19 \leq p < 37$, in the following we give quadratic residues x and y modulo p such that $x-1, x+1$ and $y-1, y+1$ are also quadratic residues modulo p:

$$\begin{aligned} p = 19: &\quad x = 5, y = 6 \\ p = 23: &\quad x = 2, y = 3 \\ p = 29: &\quad x = 5, y = 6 \\ p = 31: &\quad x = 8, y = 9 \end{aligned}$$

Hence for all prime $p \geq 19$, for G the (proper) subgroup of $\mathbf{U}_p$ of quadratic residues modulo p, $|R(G)| > 1$. □

More generally, for $1 < k < p-1$ a divisor of $p-1$ for p prime, let G be the (proper) subgroup of $\mathbf{U}_p$ of kth power residues modulo p. For $|R(G)| > 1$, Theorem 3 then yields a nonlinear modular n-queens solution. In particular, a quadruple of kth power residues gives two triples of kth power residues. Brauer in [2] proves that for any positive integers k and l, for all sufficiently large prime p there exists a positive integer r such that $r, r+1, \ldots, r+l-1$ are all kth power residues modulo p. Taking $l = 4$ in Brauer's result gives us the following:

Remark 5. *For each integer $k > 1$, for all sufficiently large prime p such that k properly divides $p-1$, for G the (proper) subgroup of $\mathbf{U}_p$ of kth power residues modulo p, Theorem 3 yields a nonlinear modular n-queens solution.*

3. Acknowledgements

The author is grateful to the anonymous referee for excellent ideas to generalize the original construction.

References

[1] George E. Andrews, *Number theory*, Dover Publications, New York, 1994.

[2] Alfred Brauer, *Über sequenzen von potenzresten*, Sitzungsberichte Akad. Berlin (1928), 9–16.

[3] A. P. Burger, C. M. Mynhardt, and E. J. Cockayne, *Regular solutions of the n-queens problem on the torus*, Util. Math. **65** (2004), 219–230.

[4] George Pólya, *Über die "doppelt-periodischen" losüngen des n-damenproblem*, Mathematische Unterhaltungen und Spiele (W. Ahrens, ed.), vol. 2, B. G. Teubner, second ed., 1918, pp. 364–374.

E-mail address: jbell3@connect.carleton.ca

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada.

FIGURE 1. Nonlinear solution for 35×35 modular board