ACTA ARITHMETICA
129.4 (2007)

Polynomial modular n-queens solutions

by

Jordan Bell (Ottawa)

1. Introduction. The *modular n-queens problem* is to place n nonattacking queens on the $n \times n$ modular chessboard, in which opposite sides are identified like a torus. We number the rows from the top to bottom as $0, 1, \ldots, n-1$ respectively, and the columns from the left to right as $0, 1, \ldots, n-1$ respectively, and refer to a queen on row i and column j by (i, j). A queen on the square (i, j) attacks its row and column, and the (modular) diagonals $\{(k, l) : k - l \equiv i - j \pmod{n}\}$ and $\{(k, l) : k + l \equiv i + j \pmod{n}\}$.

Let $\mathbb{Z}/n = \{0, 1, \ldots, n-1\}$ be the ring of integers modulo n. A polynomial $f(x)$ over $\mathbb{Z}/n$ is called a *permutation polynomial* if the evaluation mapping $t \mapsto f(t)$ is a permutation of $\mathbb{Z}/n$. We say that a permutation f of $\mathbb{Z}/n$ is a *modular n-queens solution* if the mappings $t \mapsto f(t) - t$ and $t \mapsto f(t) + t$ are also permutations of $\mathbb{Z}/n$; f being a permutation means no two queens are on the same row or column, and $t \mapsto f(t) - t$ and $t \mapsto f(t) + t$ being permutations means no two queens are on the same diagonal. For a prime power q, let $\mathbb{F}_q$ be the finite field with q elements. In particular, for a prime p we write $\mathbb{F}_p = \mathbb{Z}/p = \{0, 1, \ldots, p-1\}$.

The modular n-queens problem is a variant of the original n-queens problem of putting n nonattacking queens on the $n \times n$ (standard) chessboard. An n-queens solution is a placement of n nonattacking queens on the $n \times n$ chessboard; it is clear that a modular n-queens solution is necessarily an n-queens solution. Pólya [8] proves that there exists a modular n-queens solution if and only if $\gcd(n, 6) = 1$, that is, if and only if n is not divisible by 2 or 3. To prove that $\gcd(n, 6) = 1$ is sufficient for a modular n-queens solution to exist, Pólya notes that if $a-1, a, a+1$ are relatively prime to n, then the linear polynomials $f(x) = ax + b$ are modular n-queens solutions. Kløve [3] constructs a class of nonlinear polynomials that are modular n-queens

2000 *Mathematics Subject Classification*: 11T06, 11E16, 05B30.

Key words and phrases: permutation polynomials, binary quadratic forms, n-queens problem.

solutions. Modular n-queens solutions are related to certain combinatorial structures, in particular Latin squares (cf. [1]).

This paper gives three constructions of modular n-queens solutions using permutation polynomials of $\mathbb{Z}/n$. In particular, using results from the theory of binary quadratic forms, conditions are given when certain trinomials represent modular n-queens solutions. This is useful because the only presently known class of polynomial modular n-queens solutions are Kløve's [3]. Polynomial modular n-queens solutions are particularly desirable because they can be efficiently computed.

2. Results

THEOREM 1. *Let p be prime. If $p = L^2 + 675M^2$ then $x(x^{2(p-1)/3} + x^{(p-1)/3} + 3)$ represents a modular p-queens solution. If $p = L^2 + 81675M^2$ then $x(2x^{2(p-1)/3} + 2x^{(p-1)/3} + 7)$ represents a modular p-queens solution.*

Proof. For q a prime power $\equiv 1 \pmod 3$, $s = (q-1)/3$, and ω an element of $\mathbb{F}_q$ of order 3, Lee and Park [5] prove that for $\gcd(r, s) = 1$, $x^r(ax^{2s} + a\omega^i x^s + b)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $r \not\equiv 0 \pmod 3$ and $(b\omega^i + 2a)/(b\omega^i - a)$ is a nonzero cube in $\mathbb{F}_q$. Thus if $q = p$, $r = 1$, $i = 0$, then $x(ax^{2s} + ax^s + b)$ is a permutation polynomial of $\mathbb{F}_p$ if and only if $(b + 2a)/(b - a)$ is a nonzero cube in $\mathbb{F}_p$. Therefore we see that $x(ax^{2s} + ax^s + b)$ is a modular p-queens solution if and only if

$$\frac{b-1+2a}{b-1-a}, \quad \frac{b+2a}{b-a}, \quad \frac{b+1+2a}{b+1-a} \tag{1}$$

are nonzero cubes in $\mathbb{F}_p$.

If $b = 3$, $a = 1$, the elements (1) are $4/1 = 4$, $5/2$, $6/3 = 2$, which are nonzero cubes if and only if $2, 5$ are nonzero cubes.

If $b = 7$, $a = 2$, the elements (1) are $10/4 = 5/2$, $11/5$, $12/6 = 2$, which are nonzero cubes if and only if $2, 5, 11$ are nonzero cubes.

It is well known that 2 is a cubic residue modulo a prime $p \equiv 1 \pmod 3$ if and only if p is represented by the quadratic form $L^2 + 27M^2$ [2, Theorem 4.15]. Lemmermeyer [6, §7.1] shows that 5 is a cubic residue modulo p if and only if $LM \equiv 0 \pmod 5$. Thus if $p = L^2 + 25 \cdot 27M^2 = L^2 + 675M^2$, then $2, 5$ are cubic residues modulo p.

As well, Lemmermeyer [6, §7.1] shows that 11 is a cubic residue modulo p if and only if $LM(L - 3M)(L + 3M) \equiv 0 \pmod{11}$. Thus if $p = L^2 + 25 \cdot 121 \cdot 27M^2 = L^2 + 81675M^2$, then $2, 5, 11$ are cubic residues modulo p. ∎

For example, let $L = 4$ and $M = 1$. We find that $p = L^2 + 675M^2 = 16 + 675 = 691$ is prime. Thus by the above theorem, the polynomial $x(x^{460} + x^{230} + 3)$ represents a modular 691-queens solution.

We now recall some definitions about binary quadratic forms [4, Part Four], which we use in the following remark. A form $f(x,y)$ is *properly equivalent* to a form $g(x,y)$ if there is an element $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$. The *opposite* of a form $ax^2 + bxy + cy^2$ is the form $ax^2 - bxy + cy^2$.

Remark 2. By the Dirichlet density theorem for binary quadratic forms [2, Theorem 9.12], the set of primes represented by a primitive positive definite binary quadratic form of discriminant D has Dirichlet density $1/2h(D)$ if the form is properly equivalent to its opposite and $1/h(D)$ otherwise, where $h(D)$ is the class number. Clearly, $L^2 + 675M^2$ and $L^2 + 81675M^2$ are properly equivalent to their opposites, by the identity transformation $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Their discriminants are $-4 \cdot 675 = -2700$ and $-4 \cdot 81675 = -326700$ respectively, and using [4, Theorem 214] we find that $h(-2700) = h((2\cdot 3\cdot 5)^2 \cdot (-3)) = 18$ and $h(-326700) = h((2\cdot 3\cdot 5\cdot 11)^2 \cdot (-3)) = 216$. In particular, there are infinitely many primes represented by the quadratic forms $L^2 + 675M^2$ and $L^2 + 81675M^2$.

Theorem 3. *Let $p \geq 7$ be prime and e be a positive integer. Then $f(x) = x^{(p+1)/2} + \frac{5}{4}x$ is a modular p^e-queens solution if*

$$
\begin{aligned}
(2)\quad p \equiv{}& 1, 601, 121, 61, 361, 181, 469, 289, 589, 529, 49, 649,\\
& 197, 317, 617, 137, 437, 557, 353, 473, 773, 293, 593, 713,\\
& 587, 707, 227, 527, 47, 167, 743, 83, 383, 683, 203, 323,\\
& 391, 211, 511, 451, 751, 571, 79, 679, 199, 139, 439, 259 \pmod{780}.
\end{aligned}
$$

Proof. Nöbauer [7] proves that for all primes $p \geq 7$ and integers $e \geq 1$, if $a = (c^2+1)/(c^2-1)$ with c such that $c^2 \not\equiv \pm 1, \pm 3 \pmod{p}$, then $f(x) = x^{(p+1)/2} + ax$ is a permutation polynomial of $\mathbb{Z}/p^e$.

Let $c = 3$. Then $a = 5/4$. If there exist b, d such that

$$a - 1 = \frac{b^2+1}{b^2-1} \quad \text{and} \quad a + 1 = \frac{d^2+1}{d^2-1},$$

then $f(x) - x$ and $f(x) + x$ are permutation polynomials of $\mathbb{Z}/p^e$, hence $f(x)$ will be a modular p^e-queens solution. Now, $5/4 - 1 = (b^2+1)/(b^2-1)$ if and only if $b^2 - 1 = 4(b^2+1)$ if and only if $b^2 = -5/3$. Similarly, $5/4 + 1 = (d^2+1)/(d^2-1)$ if and only if $9(d^2-1) = 4(d^2+1)$ if and only if $d^2 = 13/5$. We consider the two cases of when $p \equiv 1 \pmod{4}$ and when $p \equiv 3 \pmod{4}$.

We note first that the squares modulo 3 are $\equiv 1 \pmod{3}$, the squares modulo 5 are $\equiv 1, 4 \pmod{5}$, and the squares modulo 13 are $\equiv 1, 3, 4, 9, 10, 12 \pmod{13}$. We recall the law of quadratic reciprocity [10, Chapter I, Theorem 6], that if p, q are distinct odd primes, then p is a square modulo q if and only if q is a square modulo p, unless both p, q are $\equiv 3 \pmod{4}$, in which case p is a square modulo q if and only if q is a nonsquare modulo p.

Case $p \equiv 1 \pmod 4$: -1 is a square modulo p. Either $3, 5, 13$ are squares modulo p or $3, 5, 13$ are nonsquares modulo p. By quadratic reciprocity, $q = 3, 5, 13$ is a square or nonsquare modulo p according as p is a square or nonsquare modulo q. Hence either $p \equiv 1 \pmod 3$, $p \equiv 1, 4 \pmod 5$, $p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$ or $p \equiv 2 \pmod 3$, $p \equiv 2, 3 \pmod 5$, $p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$.

Case $p \equiv 3 \pmod 4$: -1 is a nonsquare modulo p. Either 3 is a square and $5, 13$ are nonsquares modulo p, or 3 is a nonsquare and $5, 13$ are squares modulo p. By quadratic reciprocity, 3 is a square or nonsquare modulo p according as p is a nonsquare or square modulo 3. By quadratic reciprocity, $q = 5, 13$ is a square or nonsquare modulo p according as p is a square or nonsquare modulo q. Hence either $p \equiv 2 \pmod 3$, $p \equiv 2, 3 \pmod 5$, $p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$ or $p \equiv 1 \pmod 3$, $p \equiv 1, 4 \pmod 5$, $p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$.

Using the Chinese remainder theorem we compute the common solutions of these congruences modulo $4 \cdot 3 \cdot 5 \cdot 13 = 780$, listed in (2). ∎

For example, for the prime $p = 61$ and $e = 2$, the above theorem shows that $x^{(61+1)/2} + \frac{5}{4}x = x^{31} + 47x$ represents a modular p^e-queens solution, which is a modular 3721-queens solution.

Remark 4. By Dirichlet's theorem for primes in an arithmetic progression [10, Chapter VI, Theorem 2], the set of primes p that satisfy (2) has Dirichlet density $48/\phi(780) = 48/192 = 1/4$, where ϕ is Euler's totient function. In particular, there are infinitely many primes p that satisfy (2).

Theorem 5. *Let N be a positive integer not divisible by 2 or 3. If $h_1 - 1$, $h_1, h_1 + 1$ are relatively prime to N and every prime factor of N divides h_2, then $H(x) = h_1 x + h_2 x^2$ is a modular N-queens solution.*

Proof. Let $n_{m,p}$ denote the multiplicity of the prime p in m. Ryu and Takeshita [9] prove that for $2 \nmid N$, $H(x) = h_1 x + h_2 x^2$ is a permutation polynomial of $\mathbb{Z}/N$ if and only if $\gcd(h_1, N) = 1$ and $n_{h_2,p} \geq 1$ for all primes p such that $n_{N,p} \geq 1$ (i.e. if p divides N then p divides h_2). This implies that $H(x) - x, H(x), H(x) + x$ are permutation polynomials of $\mathbb{Z}/N$. Hence $H(x)$ is a modular N-queens solution. ∎

For example, let $N = 175 = 25 \cdot 7$, $h_1 = 3$, $h_2 = 35$. Then $H(x) = 3x + 35x^2$. Since $h_1 - 1 = 2, h_1 = 3, h_1 + 1 = 4$ are relatively prime to $N = 175$ and the prime divisors $5, 7$ of N divide h_2, the above theorem shows that $H(x) = 3x + 35x^2$ represents a modular 175-queens solution.

Acknowledgements. The author would like to thank the referee for some helpful suggestions.

References

[1] J. Bell and B. Stevens, *Constructing orthogonal pandiagonal Latin squares and panmagic squares from modular n-queens solutions*, J. Combin. Des. 15 (2007), 221–234.

[2] D. A. Cox, *Primes of the Form x^2+ny^2, Fermat, Class Field Theory, and Complex Multiplication*, Wiley, New York, 1997.

[3] T. Kløve, *The modular n-queen problem*, Discrete Math. 19 (1977), 289–291 (1978).

[4] E. Landau, *Elementary Number Theory*, Chelsea, New York, 1958.

[5] J. B. Lee and Y. H. Park, *Some permuting trinomials over finite fields*, Acta Math. Sci. (Engl. Ed.) 17 (1997), 250–254.

[6] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer Monogr. Math., Springer, Berlin, 2000.

[7] W. Nöbauer, *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math. 69 (1965), 230–238.

[8] G. Pólya, *Über die "doppelt-periodischen" Lösungen des n-Damen-Problems*, in: Mathematische Unterhaltungen und Spiele, 2nd ed., W. Ahrens (ed.), Vol. 2, B. G. Teubner, 1918, 364–374.

[9] J. Ryu and O. Y. Takeshita, *On quadratic inverses for quadratic permutation polynomials over integer rings*, IEEE Trans. Inform. Theory 52 (2006), 1254–1260.

[10] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, New York, 1973.

School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada
E-mail: jbell3@connect.carleton.ca

Received on 30.1.2007
and in revised form on 6.5.2007 (5382)