Discrete Mathematics 36 (1981) 33–48
North-Holland Publishing Company

THE MODULAR n-QUEEN PROBLEM II

Torleiv KLØVE

Matematisk institutt, Universitetet i Bergen, 5014 Bergen, Norway

Received 21 September 1978
Revised 24 July 1980

We study classes of solutions to the modular n-queen problem. The main part of the paper is concerned with symmetric solutions (solutions invariant under 90° rotation). In the last section we study maximal partial solutions for those values of n for which no solutions exist.

1. Introduction

The modular n-queen problem is the following. We make an $n \times n$ chessboard into a torus by identifying opposite sides, and we want to place n queens on this board in such a way that none of them attack any other queen.

In [2] we studied this problem. In particular we proved that it has a solution if and only if $\gcd(n, 6) = 1$. Donald Knuth (private communication) has pointed out that this is well known, a proof appears in Pólya's paper [3]. In that paper, Pólya gave several results, and in this paper we will generalize some of these. Our main topic will be "symmetric" solutions. These are solutions which are invariant under 90° rotation.

2. Definitions and basic results

In this section we give a precise definition of a solution, and we state and prove Pólya's results, partly generalized.

Notations. (i) $\mathbb{Z}_n$ will denote the set of residue classes modulo n.

(ii) For any integer a, $[a] = [a]_n$ will denote the residue class containing a. a is called a representative of the residue class $[a]$. Unless otherwise stated we use representatives which satisfy $|a| \leq \frac{1}{2}n$.

Definition 2.1. An *n-solution* is a set

$$S = \{([r_i], [s_i]) \mid i = 1, 2, \ldots, n\} \subset \mathbb{Z}_n \times \mathbb{Z}_n$$

0012-365X/81/0000–0000/$02.50

such that if $i \neq j$, then

$$[r_i] \neq [r_j], \tag{2.1}$$

$$[s_i] \neq [s_j], \tag{2.2}$$

$$[s_i - r_i] \neq [s_j - r_j], \tag{2.3}$$

$$[s_i + r_i] \neq [s_j + r_j]. \tag{2.4}$$

Definition 2.2.

(i) $\{([a], [b]) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid b = 1, 2, \ldots, n\}$ is a *row*,
(ii) $\{([a], [b]) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid a = 1, 2, \ldots, n\}$ is a *column*,
(iii) $\{([a], [a+b]) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid a = 1, 2, \ldots, n\}$ is a *main diagonal*,
(iv) $\{([a], [b-a]) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid a = 1, 2, \ldots, n\}$ is a *bi-diagonal*.

Condition (2.1) says that no row contains two elements from S, (2.2) the same for columns, (2.3) for main diagonals and (2.4) for bi-diagonals.

Lemma 2.3. *If* $\{([r_i], [s_i]) \mid i = 1, 2, \ldots, n\}$ *is an* n*-solution, and* k, l, *and* m *are integers, where* $\gcd(k, n) = 1$, *then* $\{([kr_i + l], [ks_i + m]) \mid i = 1, 2, \ldots, n\}$ *is an* n*-solution.*

Proof. If $[kr_i + l] = [kr_j + l]$, then $[r_i] = [r_j]$ and hence $i = j$. This proves (2.1) and (2.2)–(2.4) are similar.

Definition 2.4. An n-solution $\{([r_i], [s_i]) \mid i = 1, 2, \ldots, n\}$ is *linear* if there exist integers k and l such that $[s_i] = [kr_i + l]$ for $i = 1, 2, \ldots, n$.

Theorem 2.5. *Let* $\{([r_i]_n, [s_i]_n) \mid i = 1, 2, \ldots, n\}$ *be an* n*-solution,* $\{([t_j]_m, [u_j]_m) \mid j = 1, 2, \ldots, m\}$ *be an* m*-solution, and* k_i, l_i, $i = 1, 2, \ldots, n$ *be integers. Then*

$$\{([nt_j + nk_i + r_i]_{mn}, [nu_j + nl_i + s_i]_{mn}) \mid i = 1, 2, \ldots, n; j = 1, 2, \ldots, m\}$$

is an mn*-solution.*

Pólya proved this in the case that the m-solution is linear.

Proof. We have to prove that (2.1)–(2.4) are satisfied. We prove (2.1), the others are similar. Suppose

$$nt_j + nk_i + r_i \equiv nt_{j'} + nk_{i'} + r_{i'} \pmod{mn} \tag{2.5}$$

Then

$$r_i \equiv r_{i'} \pmod{n}.$$

By (2.1), $i = i'$, and so $k_i = k_{i'}$ and $r_i = r_{i'}$. Inserting this in (2.5) and dividing by n

we get

$$t_i \equiv t_{i'} \pmod{m}.$$

By (2.1), $j = j'$, q.e.d.

Definition 2.6. An n-solution $S = \{([r_i], [s_i]) \mid i = 1, 2, \ldots, n\}$ is *symmetric* if $([r], [s]) \in S$ implies $([s], [-r]) \in S$.

Pólya called such solutions "doppelt-symmetrischen." He noted that $n \equiv 1 \pmod 4$ is *necessary* for symmetric n-solutions to exist. Whether $n \equiv 1 \pmod 4$ and $\gcd(n, 6) = 1$ is sufficient for a symmetric n-solution to exist remains an open question. Pólya proved that, if n is a product of primes all congruent 1 modulo 4, then a linear symmetric n-solution exists, namely $\{([r], [kr]) \mid r = 1, 2, \ldots, n\}$ where $k^2 \equiv -1 \pmod n$.

3. Classes of symmetric solutions

In this section we show how to construct new symmetric n-solutions from given ones.

If S is a symmetric n-solution, then $([0], [0]) \in S$. Further, if $([r], [s]) \in S$ and $([r], [s]) \neq ([0], [0])$, then $([r], [s])$, $([s], [-r])$, $([-r], [-s])$, $([-s], [r]) \in S$ and these four elements are distinct.

Definitions 3.1. (i) Let $\langle 0 \rangle = ([0], [0])$.

(ii) For $[r], [s] \in \mathbb{Z}_n - [0]$, let

$$\langle r, s \rangle = \{([r], [s]), ([s], [-r]), ([-r], [-s]), ([-s], [r])\}.$$

Definition 3.2. For any integers a and n, n odd, let $\tilde{a}$ denote the integer such that $0 \leqslant \tilde{a} < \frac{1}{2}n$ and $a \equiv \pm\tilde{a} \pmod n$.

In this section $n = 4q + 1$ for some positive integer q.

Lemma 3.1. *Let a_i, b_i, $i = 1, 2, \ldots, q$ be integers. Then*

$$\bigcup_{i=1}^{q} \{\tilde{a}_i, \tilde{b}_i\} = \{1, 2, \ldots, 2q\}$$

if and only if

(i) $[a_i] \neq [0]$ *and* $[b_i] \neq [0]$ *for all* i,

(ii) $[a_i] \neq [\pm a_j]$ *and* $[b_i] \neq [\pm b_j]$ *for all* i, j, $i \neq j$,

(iii) $[a_i] \neq [\pm b_j]$ *for all* i, j.

Proof. We have $\bigcup_{i=1}^{q}\{\tilde{a}_i, \tilde{b}_i\}=\{1, 2, \ldots, 2q\}$ if and only if the integers $\tilde{a}_i$, $\tilde{b}_i$, $i=1, 2, \ldots, q$ are non-zero and distinct, and this is equivalent to (i)–(iii) by the definition of $\tilde{}$.

Theorem 3.2. *$S=\langle 0\rangle \cup \bigcup_{i=1}^{q}\langle r_i, s_i\rangle$ is a symmetric n-solution if and only if*

$$\bigcup_{i=1}^{q}\{\tilde{r}_i, \tilde{s}_i\}=\{1, 2, \ldots, 2q\} \tag{3.1}$$

and

$$\bigcup_{i=1}^{q}\{\widetilde{s_i-r_i}, \widetilde{s_i+r_i}\}=\{1, 2, \ldots, 2q\} \tag{3.2}$$

Proof. Let S be a symmetric n-solution. Then $[0]$, $[r_1]$, $[-s_1]$, $[-r_1]$, $[s_1], \ldots, [r_q]$, $[-s_q]$, $[-r_q]$, $[s_q]$ are all distinct by (2.1), and so (3.1) follows by Lemma 3.1. Similarly (3.2) follows from (2.3) by Lemma 3.1.

Conversely, suppose S satisfies (3.1) and (3.2). Then (2.1) and (2.2) follows from (3.1); (2.3) and (2.4) follows from (3.2); using Lemma 3.1.

Theorem 3.3. *If $S=\langle 0\rangle \cup \bigcup_{i=1}^{q}\langle r_i, s_i\rangle$ is a symmetric n-solution and for some j, $i \leqslant j \leqslant q$,*

$$S'=\langle 0\rangle \cup \langle s_j, r_j\rangle \cup \bigcup_{\substack{1\leqslant i\leqslant q\\ i\neq j}}\langle r_i, s_i\rangle,$$

then S' is a symmetric n-solution.

Proof. Since $\widetilde{r_j-s_j}=\widetilde{s_j-r_j}$, (3.1) and (3.2) are both symmetric in r_i, s_i and Theorem 3.3 follows.

Theorem 3.4. *If $\bigcup_{i=1}^{q}\{\tilde{a}_i, \tilde{b}_i\}=\{1, 2, \ldots, 2q\}$ and $\gcd(k, n)=1$, then $\bigcup_{i=1}^{q}\{\widetilde{ka_i}, \widetilde{kb_i}\}=\{1, 2, \ldots, 2q\}$.*

Proof. Since $[kx]=[ky]$ if and only if $[x]=[y]$, Lemma 3.4 follows from Lemma 3.1.

Theorem 3.5. *If $S=\langle 0\rangle \cup \bigcup_{i=1}^{q}\langle r_i, s_i\rangle$ is a symmetric n-solution and $\gcd(k, n)=1$, then*

$$D(S)=\langle 0\rangle \cup \bigcup_{i=1}^{q}\langle s_i-r_i, s_i+r_i\rangle$$

and

$$C_k(S)=\langle 0\rangle \cup \bigcup_{i=1}^{q}\langle kr_i, ks_i\rangle$$

are symmetric n-solutions.

Proof. The theorem follows directly from Theorem 3.2 and Lemma 3.4.

Starting with one symmetric n-solution and using Theorem 3.3 repeatedly we get 2^q distinct symmetric n-solutions. Using Theorem 3.5 we usually get even more solutions.

Finally in this section we prove the equivalent of Theorem 2.5 for the symmetric case.

Theorem 3.6. *Let* $S=\{([r_i]_n, [s_i]_n) \mid i=1,2,\ldots,n\}$ *be a symmetric* n*-solution where* $r_i, s_i \in \{-2q, -2q+1, \ldots, 2q\}$ *for* $i=1,2,\ldots,n$, $T=\{([t_j]_m, [u_j]_m) \mid j=1,2,\ldots,m\}$ *be a symmetric* m*-solution, and* k_i, l_i, $i=1,2,\ldots,n$ *be integers such that* $k_{i'}=l_i$ *and* $l_{i'}=-k_i$ *when* $r_{i'}=s_i$. *Then*

$$V=\{([nt_j+nk_i+r_i]_{mn}, [nu_j+nl_i+s_i]_{mn}) \mid i=1,2,\ldots,n; j=1,2,\ldots,m\}$$

is a symmetric mn*-solution.*

Proof. By Theorem 2.5, V is a solution and so we have to show that it is symmetric. Let

$$([nt_j+nk_i+r_i]_{mn}, [nu_j+nl_i+s_i]_{mn}) \in V$$

where $([r_i]_n, [s_i]_n) \in S$ and $([t_j]_m, [u_j]_m) \in T$. Since S and T are symmetric there exist $([r_{i'}]_n, [s_{i'}]_n) \in S$ and $([t_{j'}]_m, [u_{j'}]_m) \in T$ such that $[r_{i'}]_n = [s_i]_n$, $[s_{i'}]_n = [-r_i]_n$, $[t_{j'}]_m = [u_j]_m$ and $[u_{j'}]_m = [-t_j]_m$. By our restriction on r_i and s_i, $r_{i'}=s_i$ and $s_{i'}=-r_i$. Hence $k_{i'}=l_i$ and $l_{i'}=-k_i$. Therefore $([nu_j+nl_i+s_i]_{mn}, [-nt_j-nk_i-r_i]_{mn}) \in V$ and hence V is symmetric.

4. Symmetric p^α-solutions

In this section p is a prime, $p \equiv 1 \pmod 4$, and α is a positive integer.

Definition 4.1. For any non-zero integer N, $v_p(N)$ and $v(N)$ are the greatest integers such that $p^{v_p(N)}$ divides N and $2^{v(N)}$ divides N.

Lemma 4.2. *If* $a \equiv b \pmod N$, *then*

(i) $v(a) \geq \min(v(b), v(N))$.

(ii) *If* $v(b) < v(N)$, *then* $v(a) = v(b)$.

The simple proof is omitted.

Let g be a primitive root modulo p such that $p^2 \nmid g^{p-1}-1$. In [3, p. 52] it is proved that such a g exists and that it is a primitive root modulo p^α for any $\alpha \geq 1$.

Definition 4.3. Let

(i) $W_\beta = 0$ if $\beta = 0$,
$= p^{\beta-1}(p-1)/4$ if $\beta > 0$;

(ii) $Z_\beta = \frac{1}{4}(p^\beta - 1)$.

Definition 4.4. A triple (α, κ, V) of integers where $\alpha \geq 1$, is *permissible* if there exist integers μ and ν such that

$$g^\kappa - 1 \equiv g^\mu \pmod{p^\alpha}, \tag{4.1}$$

$$g^\kappa + 1 \equiv g^\nu \pmod{p^\alpha}, \tag{4.2}$$

$$V \mid \kappa, \qquad V \mid \mu - \nu, \qquad V \nmid W_\alpha, \tag{4.3}$$

$$v(V) = v(\kappa) = v(\mu - \nu) \leq v(W_\alpha). \tag{4.4}$$

Theorem 4.5. *Let (α, κ, V) be permissible and let*

$$S_{\alpha-1} = \langle 0 \rangle \cup \bigcup_{i=1}^{Z_{\alpha-1}} \langle r_i, s_i \rangle$$

by a symmetric $p^{\alpha-1}$-solution. Then

$$S_\alpha = \langle 0 \rangle \cup \bigcup_{i=1}^{Z_{\alpha-1}} \langle pr_i, ps_i \rangle \cup \bigcup_{j=1}^{V} \bigcup_{i=1}^{U} \langle g^{2iV+j}, g^{2iV+j+\kappa} \rangle$$

where $U = W_\alpha / V$, is a symmetric p^α-solution.

Proof. The proof will be based on Theorem 3.2. Hence we have to prove that the analogues of (3.1) and (3.2) are satisfied. We start with (3.1). Since $a \equiv \pm b \pmod{p^{\alpha-1}}$ if and only if $pa \equiv \pm pb \pmod{p^\alpha}$ we see that

$$\bigcup_{i=1}^{Z_{\alpha-1}} \{\widetilde{pr_i}, \widetilde{ps_i}\} = \{pl \mid 1 \leq l \leq \tfrac{1}{2}(p^{\alpha-1} - 1)\}$$

since $S_{\alpha-1}$ is a symmetric $p^{\alpha-1}$-solution. If a and ε are any integers, then $pa \not\equiv \pm g^\varepsilon \pmod{p^\alpha}$. Hence it remains to prove that

$$g^{2iV+j+d} \not\equiv \pm g^{2i'V+j'+d} \pmod{p^\alpha} \tag{4.5}$$

if $d = 0$ or $d = \kappa$ and $(i, j) \neq (i', j')$, and

$$g^{2iV+j+\kappa} \not\equiv \pm g^{2i'V+j'} \pmod{p^\alpha} \tag{4.6}$$

for all (i, j), (i', j'). Suppose $g^{2iV+j+d} \equiv \pm g^{2i'V+j'+d} \pmod{p^\alpha}$. Since g is a primitive root this implies that

$$2iV + j + d \equiv 2i'V + j' + d \pmod{p^{\alpha-1}\tfrac{1}{2}(p-1)}. \tag{4.7}$$

Since $V \mid p^{\alpha-1}\frac{1}{2}(p-1)$ we get

$$j \equiv j' \pmod{V}.$$

By the definition of S_α, $1 \leqslant j, j' \leqslant V$. Hence $j = j'$. Inserting this into (4.7) we get

$$2iV \equiv 2i'V \pmod{2 \cdot W_\alpha}$$
$$i \equiv i' \pmod{W_\alpha/V}.$$

Since $W_\alpha/V = U$ and $1 \leqslant i, i' \leqslant U$, we get $i = i'$. Hence $(i, j) = (i\ \ j')$. This proves (4.5). Next suppose that

$$g^{2iV+j+\kappa} \equiv \pm g^{2i'V+j'} \pmod{p^\alpha}.$$

Then

$$2iV + j + \kappa \equiv 2i'V + j' \pmod{p^{\alpha-1}\tfrac{1}{2}(p-1)}. \tag{4.8}$$

Hence

$$j \equiv j' \pmod{V}$$

and so $j = j'$. Inserting this into (4.8) we get

$$\kappa \equiv 2V(i'-i) \pmod{p^{\alpha-1}\tfrac{1}{2}(p-1)}.$$

By Lemma 4.2, $v(\kappa) \geqslant \min(1+v(V), 1+v(W_\alpha))$. This contradicts (4.4) and so the proof of (4.6) is complete.

The analogue of (3.2) is proved similarly. First we get

$$\bigcup_{i=1}^{z_{\alpha-1}} \{\widetilde{ps_i - pr_i}, \widetilde{ps_i + pr_i}\} = \{pl \mid 1 \leqslant l \leqslant \tfrac{1}{2}(p^{\alpha-1}-1)\}.$$

Further

$$g^{2iV+j+\kappa} - g^{2iV+j} \equiv g^{2iV+j+\mu} \pmod{p^\alpha}$$

and

$$g^{2iV+j+\kappa} + g^{2iV-j} \equiv g^{2iV+j+\nu} \pmod{p^\alpha}.$$

Hence we have to prove that

$$g^{2iV+j+d} \not\equiv \pm g^{2i'V+j'+d} \pmod{p^\alpha}.$$

if $d = \mu$ or $d = \nu$ and $(i, j) \neq (i', j')$, and

$$g^{2iV+j+\mu} \not\equiv \pm g^{2i'V+j'+\nu} \pmod{p^\alpha}$$

for all (i, j), (i', j'). The proof of these are similar to the proof of (4.5) and (4.6), we omit the details.

To use Theorem 4.5 we have to know some permissible triples. In the next theorem we give some results on permissible triples.

Theorem 4.6. (i) *If (α, κ, V) is permissible, then $(\alpha, \kappa + 2\lambda W_\alpha, V)$ is permissible for all integers λ.*

(ii) *If (α, κ, V) is permissible, then $(\alpha, -\kappa, V)$ is permissible.*

(iii) *If (α, κ, V) is permissible, $V' \mid V$, and $v(V') = v(V)$, then (α, κ, V') is permissible.*

(iv) *If* $(\alpha-1, \kappa, V)$ *is permissible, then* (α, κ, V) *is permissible.*

(v) *If* (α, κ, V) *is permissible and* $v_p(V) \leq \alpha-2$, *then* $(\alpha-1, \kappa, V)$ *is permissible.*

(vi) *If* (α, κ, V) *is permissible and* $v_p(V) \geq 1$, *then* $(\alpha-1, \kappa, V/p)$ *is permissible.*

(vii) $(\alpha, W_\alpha, W_\alpha)$ *is permissible for all* $\alpha \geq 1$.

Proof. (i) Let $\kappa' = \kappa + 2\lambda W_\alpha$. By Lemma 4.2, $v(\kappa') = v(\kappa)$. Further, $g^{\kappa'} \equiv g^\kappa (-1)^\lambda \pmod{p^\alpha}$. If λ is even, the

$$g^{\kappa'} - 1 \equiv g^\mu \pmod{p^\alpha},$$
$$g^{\kappa'} + 1 \equiv g^\nu \pmod{p^\alpha}.$$

If λ is odd, then

$$g^{\kappa'} - 1 \equiv -(g^\kappa + 1) \equiv g^{\nu + 2W_\alpha} \pmod{p^\alpha},$$
$$g^{\kappa'} + 1 \equiv -(g^\kappa - 1) \equiv g^{\mu + 2W_\alpha} \pmod{p^\alpha}.$$

It is now straightforward to verify that (α, κ', V) is permissible.

(ii) We get

$$g^{-\kappa} - 1 \equiv g^{-\kappa}(1 - g^\kappa) \equiv -g^{-\kappa} \cdot g^\mu \equiv g^{\mu + 2W_\alpha - \kappa} \pmod{p^\alpha},$$
$$g^{-\kappa} + 1 \equiv g^{\nu - \kappa} \pmod{p^\alpha}.$$

If we put $\mu' = \mu + 2W_\alpha - \kappa$ and $\nu' = \nu - \kappa$, then $\mu' - \nu' = \mu - \nu + 2W_\alpha$. Hence $V \mid \mu' - \nu'$ and $v(\mu' - \nu') = v(\mu - \nu) = v(-\kappa) \leq v(W_\alpha)$ and so $(\alpha, -\kappa, V)$ is permissible.

(iii) Follows immediately from the definition.

(iv) Let

$$g^\kappa - 1 \equiv g^{\mu'} \pmod{p^{\alpha-1}},$$
$$g^\kappa + 1 \equiv g^{\nu'} \pmod{p^{\alpha-1}},$$
$$g^\kappa - 1 \equiv g^\mu \pmod{p^\alpha},$$
$$g^\kappa + 1 \equiv g^\nu \pmod{p^\alpha}.$$

By assumption $V \mid \kappa$, $V \mid \mu' - \nu'$, $V \mid W_{\alpha-1}$, and $v(V) = v(\kappa) = v(\mu' - \nu') \leq v(W_{\alpha-1})$. From the equations above we get

$$\mu' \equiv \mu, \qquad \nu' \equiv \nu \pmod{p^{\alpha-2}(p-1)}.$$

Hence

$$\mu - \nu \equiv \mu' - \nu' \pmod{4W_{\alpha-1}}.$$

From this we get $V \mid \mu - \nu$ and $v(\mu - \nu) = v(\mu' - \nu')$. Since $V \mid W_{\alpha-1} \mid W_\alpha$ and $v(W_\alpha) = v(W_{\alpha-1})$, (α, κ, V) is permissible.

The proofs for (v) and (vi) are similar to the proof of (iv) and are omitted.

(vii) Let $W = W_\alpha$ and

$$g^W - 1 \equiv g^\mu, \qquad g^W + 1 \equiv g^\nu \pmod{p^\alpha}.$$

Since $g^{2W} \equiv -1 \pmod{p^\alpha}$ we get

$$g^{\mu-\nu-W} \equiv \frac{g^W - 1}{(g^W+1)g^W} \equiv \frac{g^W-1}{-1+g^W} \equiv 1 \pmod{p^\alpha}.$$

and so

$$\mu - \nu \equiv W_\alpha \pmod{4W_\alpha}.$$

Hence $W_\alpha \mid \mu - \nu$ and $v(\mu-\nu) = v(W_\alpha)$. Therefore $(\alpha, W_\alpha, W_\alpha)$ is permissible.

Finally in this section we use Theorems 4.5 and 4.6 to construct a large class of explicit solutions.

Theorem 4.7. *For $\beta = 1, 2, \ldots, \alpha$ let*

(1) *δ_β be an integer such that $1 \leq \delta_\beta \leq \beta$,*

(2) *λ_β be an odd integer,*

(3) *V_β, U_β be integers such that U_β is odd and $V_\beta U_\beta = W\delta_\beta$.*

Then

$$\langle 0 \rangle \cup \bigcup_{\beta=1}^{\alpha} \bigcup_{j=1}^{V_\beta} \bigcup_{i=1}^{U_\beta} \langle p^{\alpha-\beta} g^{2iV_\beta+j},\ p^{\alpha-\beta} g^{2iV_\beta+j+\lambda_\beta W_{\delta_\beta}} \rangle$$

is a symmetric p^α-solution.

Proof. Let $\beta \leq \alpha$ and $\delta = \delta_\beta$. Referring to Theorem 4.6 we see that $(\delta, W_\delta, W_\delta)$ is permissible by (vii). Since $v(V_\beta) = v(W_\delta) - v(U_\beta) = v(W_\delta)$ by (3), $(\delta, W_\delta, V_\beta)$ is permissible by (iii). Let $\lambda_\beta = 1 + 2\lambda$. By (i), $(\delta, W_\delta + 2\lambda W_\delta, V_\beta) = (\delta, \lambda_\beta W_\delta, V_\beta)$ is permissible. Finally, by (iv), $(\beta, \lambda_\beta W_\delta, V_\beta)$ is permissible. Theorem 4.7 therefore follows from Theorem 4.5 by induction.

5. Computer search for symmetric solutions

If $\gcd(n, 6) = 1$ and $n \equiv 1 \pmod 4$, i.e. if $n \equiv 1$ or $n \equiv 5 \pmod{12}$, but n has prime factors $\equiv 3 \pmod 4$, then nothing is known about possible solutions. Knuth suggested that for small values of n symmetric solutions might be found by a computer search.

The simplest method of attack would be a simple backtrack algorithm trying all possibilities. Even for the first unknown case, $n = 49$, this would be a large job. In this section we describe some modifications of such an algorithm which will speed it up. Throughout the section, $n = 4q+1$.

Our main tools are Theorems 3.2 and 3.3. By Theorem 3.3 it is enough to search for solutions for which $1 \leq r_i < s_i \leq 2q$. By Theorem 3.2 our problem is to

find integers r_i, s_i, $i = 1, 2, \ldots, q$ such that

$$1 \leq r_i < s_i \leq 2q \quad \text{for } i = 1, 2, \ldots, q, \tag{5.1}$$

$$\bigcup_{i=1}^{q} \{r_i, s_i\} = \{1, 2, \ldots, 2q\}, \tag{5.2}$$

$$\bigcup_{i=1}^{q} \{\widetilde{s_i - r_i}, \widetilde{s_i + r_i}\} = \{1, 2, \ldots, 2q\}. \tag{5.3}$$

Definition 5.1. A solution $\langle 0\rangle \cup \bigcup_{i=1}^{q} \langle r_i, s_i\rangle$ which satisfies (5.1) is *normal*. Since $0 < s_i + r_i < n$, we have

$$\widetilde{s_i + r_i} = \min(s_i + r_i, n - s_i - r_i). \tag{5.4}$$

Further $0 < s_i - r_i < 2q$ and so

$$\widetilde{s_i - r_i} = s_i - r_i. \tag{5.5}$$

Hence we may rewrite (5.3) as follows:

$$\bigcup_{i=1}^{q} \{s_i - r_i, \min(s_i + r_i, n - s_i - r_i)\} = \{1, 2, \ldots, 2q\}. \tag{5.6}$$

Finally it is no restriction to assume that

$$r_1 < r_2 < \cdots < r_q. \tag{5.7}$$

Theorem 5.2. *If $S = \langle 0\rangle \cup \bigcup_{i=1}^{q} \langle r_i, s_i\rangle$ is a normal symmetric n-solution, then*

$$\sum_{i=1}^{q} r_i = \tfrac{1}{3}q(2q+1).$$

Proof. Let $N = \frac{1}{3}q(2q+1)$ and let $\sigma(S) = \sum_{i=1}^{q} r_i$, $\rho(S) = \sum_{i=1}^{q} s_i$. Since S is a solution, (5.2) is satisfied. Hence

$$\sigma(S) + \rho(S) = \sum_{i=1}^{2q} i = 2q(2q+1)/2 = 3N. \tag{5.8}$$

Let

$$E(S) = \langle 0\rangle \cup \bigcup_{i=1}^{q} \langle \widetilde{s_i - r_i}, \widetilde{s_i + r_i}\rangle.$$

By Theorems 3.3 and 3.5, $E(S)$ is a symmetric n-solution since it may be obtained from $D(S)$ using Theorem 3.3 repeatedly zero or more times. We will show that $E(S)$ is normal. Since $r_i > 0$ we have $s_i - r_i < s_i + r_i$, and since $s_i \leq 2q = \frac{1}{2}(n-1)$ we have $s_i - r_i < n - s_i - r_i$. By (5.4) and (5.5)

$$\widetilde{s_i - r_i} = s_i - r_i < \min(s_i + r_i, n - s_i - r_i) = \widetilde{s_i + r_i}.$$

Further, by (5.5) and (5.8)

$$\sigma(E(S)) = \sum_{i=1}^{q} (s_i - r_i) = \rho(S) - \sigma(S)$$
$$= 3N - \sigma(S) - \sigma(S) = N - 2(\sigma(S) - N).$$

Using E repeatedly, we get, by induction, normal solutions $E^k(S)$, $k = 1, 2, \ldots$, and

$$\sigma(E^k(S)) = N + (-2)^k(\sigma(S) - N). \tag{5.9}$$

Since $\sigma(E^k(S)) > 0$ for all k, (5.9) implies that $\sigma(S) = N$.

From Theorem 5.2 we can derive some relations which will further restrict the number of cases we have to search through.

Theorem 5.3. *Let $S = \langle 0 \rangle \cup \bigcup_{i=1}^{q} \langle r_i, s_i \rangle$ be a normal symmetric n-solution which satisfies* (5.7)

Further, let $1 \leq j \leq q$ and $t = \sum_{i=1}^{j} r_i$. Then

(i) $r_j \leq 2j - 1$,

(ii) $t \geq j^2 + \frac{1}{3}(q - q^2)$,

(iii) *if $j < q$, then*

$$r_{j+1} \leq -1 + (\tfrac{1}{3}q(2q+1) - \tfrac{1}{2}(q-j)(q-j+1) - t)/(q-j).$$

Proof. (i) Since $r_i < s_i$ for all i, the set $\{1, 2, \ldots, 2j-1\}$ must contain at least j r_i's. Hence $r_j \leq 2j - 1$.

(ii) We first note that by (i),

$$\sum_{i=j+1}^{q} r_i \leq \sum_{i=j+1}^{q} (2i - 1) = q^2 - j^2.$$

Hence

$$t = \tfrac{1}{3}q(2q+1) - \sum_{i=j+1}^{q} r_i \geq \tfrac{2}{3}q^2 + \tfrac{1}{3}q - q^2 + j^2.$$

(iii) Let $r_{j+1} = k + 1$. Then $r_{j+i} \geq k + i$ for $i = 1, 2, \ldots, q - j$ and so

$$\tfrac{1}{3}q(2q+1) = t + \sum_{i=j+1}^{q} r_i \geq t + \sum_{i=1}^{q-j} (k+i)$$
$$= t + k(q-j) + \tfrac{1}{2}(q-j)(q-j+1).$$

Hence

$$k \leq (\tfrac{1}{3}q(2q+1) - \tfrac{1}{2}(q-j)(q-j+1) - t)/(q-j).$$

This completes the proof of Theorem 5.3.

Using the results of this section we get an algorithm which we describe informally.

1. Let $q \leftarrow \frac{1}{4}(n-1)$.
2. Let $N \leftarrow \frac{1}{3}q(2q+1)$, $M \leftarrow \frac{1}{3}(q-q^2)$.
3. Let $r_1 \leftarrow 1$, $s_1 \leftarrow 3$, $t \leftarrow 1$, $j \leftarrow 1$.
4. *Let* $u \leftarrow$ least element of $\{1, 2, \ldots, 2q\} - \{r_1, s_1, \ldots, r_j, s_j\}$.
5. If $u < (j+1)^2 + M - t$ goto 15.
6. If $u+1 > (N - \frac{1}{2}(q-j)(q-j+1) - t)/(q-j)$ goto 15.
7. Let $w \leftarrow$ least element of $\{1, 2, \ldots, 2q\} - \{r_1, s_1, \ldots, r_j, s_j, u\}$.
8. If $w - u \in \bigcup_{i=1}^{j} \{s_i - r_i, \min(s_i + r_i, n - s_i - r_i)\}$ goto 12.
9. If $\min(w+u, n-w-u) \in \bigcup_{i=1}^{j} \{s_i - r_i, \min(s_i + r_i, n - s_i - r_i)\}$ goto 12.
10. $j \leftarrow j+1$, $r_j \leftarrow u$, $s_j \leftarrow w$, $t \leftarrow t+u$.
11. If $j < q$ goto 4, else stop.
12. $w \leftarrow w+1$.
13. If $w \in \{r_1, s_1, \ldots, r_j, s_j\}$ goto 12.
14. If $w \leq 2q$ goto 8.
15. $j \leftarrow j-1$, $t \leftarrow t - r_{j+1}$.
16. If $j = 0$ stop.
17. $w \leftarrow s_j$.
18. Goto 12.

If a solution is found, the algorithm stops at 11, if no solution exists, it stops at 16. We only search for solutions where $s_1 \geq 3$. This is no restriction, because if $S = \langle 0 \rangle \cup \langle 1, 2 \rangle \cup \cdots$ is a solution, then $E(S) = \langle 0 \rangle \cup \langle 1, 3 \rangle \cup \cdots$ is another solution. At 5 and 6 we test for properties (ii) and (iii) of Theorem 5.3. At 4, 7 and 13 we test for (5.2) and at 8 and 9 for (5.3), cf. (5.4) and (5.5).

A FORTRAN program based on this algorithm was run on a NORD-10 at the University of Bergen. The program was run for $n = 49$ and $n = 77$. For each value it came up with a solution, for $n = 77$ after 10 hours computing. The solutions are given in Table 1.

Table 1

Solution for $n = 49$

r	1	2	4	6	7	8	9	10	11	13	14	15
s	3	5	16	21	23	17	22	18	12	19	24	20

Solution for $n = 77$

r	1	2	4	6	7	8	10	11	13	14	15	16	17	18	19	20	21	22	23
s	5	5	9	12	30	35	38	27	32	28	36	25	29	26	34	37	31	33	24

6. Partial solutions

In this section we represent any residue class $[a]_n$ by the representative a which satisfies $0 \leq a < n$.

A set $S = \{(r_i, s_i) \mid i = 1, 2, \ldots, n'\}$ where $n' \leq n$ and which satisfies (2.1)–(2.4) we call a *partial* n-solution. Partial n-solutions exist for all n, e.g. the set $\{(0, 0)\}$.

Let $M(n)$ be the maximal m such that there exists a partial n-solution with m elements.

Theorem 6.1. (i) $M(n) = n$ *if* $\gcd(n, 6) = 1$,
(ii) $M(n) = n - 2$ *if* $\gcd(n, 6) = 3$,
(iii) $n - 3 \leq M(n) \leq n - 1$ *if* $\gcd(n, 6) = 2$,
(iv) $n - 5 \leq M(n) \leq n - 1$ *if* $\gcd(n, 6) = 6$.

Proof. A solution exists if and only if $\gcd(n, 6) = 1$. Hence $M(n) = n$ if $\gcd(n, 6) = 1$ and $M(n) \leq n - 1$ otherwise. Next we show that $M(n) \leq n - 2$ if $\gcd(n, 6) = 3$.

Let $\gcd(n, 6) = 3$ and suppose that there exists a partial n-solution S with $n - 1$ elements. Let r be the empty row, s the empty column, d the empty main diagonal and b the empty bi-diagonal. Then

$$r + \sum_{i=1}^{n-1} r_i \equiv \sum_{i=1}^{n} i \equiv \tfrac{1}{2}n(n+1) \equiv 0 \pmod{n}$$

since n is odd. Similarly

$$s + \sum_{i=1}^{n-1} s_i \equiv 0 \pmod{n},$$

$$d + \sum_{i=1}^{n-1} (s_i - r_i) \equiv 0 \pmod{n},$$

$$b + \sum_{i=1}^{n-1} (s_i + r_i) \equiv 0 \pmod{n}.$$

Combining these congruences we get

$$d \equiv s - r \pmod{n},$$

$$b \equiv s + r \pmod{n}.$$

Hence $S \cup \{(r, s)\}$ is an n-solution. This is a contradiction, since $M(n) \leq n - 1$ in this case. Hence $M(n) \leq n - 2$ when $\gcd(n, 6) = 3$.

To prove the lower bounds we give explicit partial n-solutions.

$n = 6l + 2$:

$$\{(i, 2i) \mid i = 0, 1, \ldots, 3l - 1\} \cup \{(3l + i, 2i + 1) \mid i = 0, 1, \ldots, 3l - 2\}.$$

$n = 6l + 4$:

$$\{(i, 2i) \mid i = 0, 1, \ldots, 3l + 1\} \cup \{(3l + 2 + i, 2i + 3) \mid i = 0, 1, \ldots, 3l - 2\}.$$

Table 2

Set	Occupies			
	Rows	Columns	Main-diagonals	Bi-diagonals
$\{(i, 2i) \mid i = 0, 1, \ldots, 2l\}$	$0, 1, \ldots, 2l$	$0, 2, \ldots, 4l$	$0, 1, \ldots, 2l$	$0, 3, \ldots, 6l$
$\{(i, 2i+1) \mid i = 2l+1, \ldots, 3l\}$	$2l+1, 2l+2, \ldots, 3l$	$4l+3, 4l+5, \ldots, 6l+1$	$2l+2, 2l+3, \ldots, 3l+1$	$1, 4, \ldots, 3l-2$
$\{(3l+1+i, 2i+1) \mid i = 0, 1, \ldots, 2l\}$	$3l+1, 3l+2, \ldots, 5l+1$	$1, 3, \ldots, 4l+1$	$3l+3, 3l+4, \ldots, 5l+3$	$3l+2, 3l+5, \ldots, 6l+2,$ $2, 5, \ldots, 3l-1$
$\{(3l+1+i, 2i) \mid i = 2l+2, \ldots, 3l\}$	$5l+3, 5l+4, \ldots, 6l+1$	$4l+4, 4l+6, \ldots, 6l$	$5l+4, 5l+5, \ldots, 6l+2$	$3l+4, 3l+7, \ldots, 6l-2$

Table 4

n	$M(n) \geq$	r:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
20	18		1	3	5	2	8	10	12	16	18	20	4	9	19	6	14	7	∧	13	15	∧						
22	20		1	3	5	2	4	10	15	17	14	7	21	6	8	20	22	19	9	11	∧	16	12	∧				
24	21		1	3	5	2	4	9	11	13	15	17	23	7	22	8	∧	24	6	10	12	16	∧	19	14	∧		
26	24		1	3	5	2	4	9	11	13	16	20	22	∧	25	23	7	24	6	8	10	26	15	17	19	21	18	∧

$n = 6l+3$:

$$\{(i, 2i) \mid i = 0, 1, \ldots, 2l\} \cup \{(i, 2i+1) \mid i = 2l+1, \ldots, 3l\}$$
$$\cup \{(3l+1+i, 2i+1) \mid i = 0, 1, \ldots, 2l\} \cup \{(3l+1+i, 2i) \mid i = 2l+2, \ldots, 3\},$$

$n = 6l$:

$$\{(i, 2i) \mid i = 0, 1, \ldots, 2l-1\} \cup \{(2l+i, 4l+2+2i) \mid i = 0, 1, \ldots, l-2\}$$
$$\cup \{(3m-1+i, 2i+3) \mid i = 0, 1, \ldots, l-1\}$$
$$\cup \{(4l+3+i, 2l+4+2i) \mid i = 0, 1, \ldots, 2l-5\}.$$

We have to show that these are partial solutions. We do this for $n = 6l+3$, the other cases are similar. We arrange the proof in Table 2.

From Table 2 we see that no two elements occupy the same row, same column, same main diagonal, or same bi-diagonal. Hence we have a partial solution.

We wrote a FORTRAN program which searched for partial n-solutions for even n. For $n \leq 18$ it searched all possibilities. Table 3 gives $M(n)$ and the s-coordinate of one partial n-solution with $M(n)$ elements for these values of n. An $\wedge$ in the s-coordinate means that the row is empty.

The amount of computing time required to find $M(n)$ by testing all cases is increasing rapidly with n. For $n = 16$ the computing time was 54 minutes, for $n = 18$ it was 24 hours and 9 minutes.

For $n \leq 18$ the partial solutions which give $M(n)$ came up early during the computation. Therefore the program was run for some time also for $20 \leq n \leq 30$ to search for partial solutions which increase the lower bound of $M(n)$ given by Theorem 6.1. For $n \leq 26$ such partial solutions were found.

The lower bounds and the partial solutions that prove these lower bounds are given in Table 4. For $n = 28$ the program was run for 10 minutes, and for $n = 30$ for 60 minutes before it was cut without having found better lowers bounds for $M(n)$.

Table 3

n	$M(n)$	r: 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	1	1	$\wedge$																
4	2	1	3	$\wedge$	$\wedge$														
6	4	1	3	6	2	$\wedge$	$\wedge$												
8	6	1	3	6	2	7	5	$\wedge$	$\wedge$										
10	9	1	3	8	6	4	2	10	5	7	$\wedge$								
12	10	1	3	5	7	4	10	12	2	6	8	$\wedge$	$\wedge$						
14	13		3	6	9	12	14	4	7	5	2	13	10	8	$\wedge$				
16	14	1	3	5	2	8	10	13	15	6	4	16	7	12	$\wedge$	11	$\wedge$		
18	16	1	3	5	2	8	10	15	13	6	17	7	18	4	$\wedge$	14	9	11	$\wedge$

References

[1] A. Bruen and R. Dixon, The n-queen problem, Discrete Math. 12 (1975) 393–395.
[2] T. Kløve, The modular n-queen problem, Discrete Math. 19 (1977) 289–291.
[3] W.J. LeVeque, Topics in Number Theory, Vol. I, (Addison-Wesley, Reading, MA, 1956).
[4] G. Pólya, Über die "doppelt-periodischen" Lösungen des n-Damen-Problems, in: W. Ahrens, Mathematische Unterhaltungen und Spiele, Vol. 2, 2nd. ed. (Leipzig, 1921).