# ENUMERATING CYCLIC AND PANDIAGONAL LATIN SQUARES AND THEIR PROPERTIES 

## Vatutin E.I.

## What are Latin and diagonal Latin squares?

$\begin{array}{lr}A=\left\|a_{i j}\right\| \\ i, j=\overline{1, N} & \forall i, j, k=\overline{1, N}, j \neq k:\left(a_{i j} \neq a_{i k}\right) \wedge\left(a_{j i} \neq a_{k i}\right) \\ \forall i, j=\overline{1, N}, i \neq j:\left(a_{i i} \neq a_{j i}\right) \wedge\left(a_{N-i+1, N-i+1} \neq a_{N-j+1, N-j+1}\right)\end{array}$
$N=|S|$
$S=\{0,1,2, \ldots, N-1\}$

$$
\left(\begin{array}{llllllllll}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 2 & 9 & 4 & 3 & 6 & 7 & 5 & 0 & 8 \\
2 & 9 & 3 & 1 & 7 & 0 & 5 & 8 & 4 & 6 \\
3 & 4 & 1 & 2 & 8 & 7 & 9 & 6 & 5 & 0 \\
4 & 3 & 5 & 9 & 2 & 1 & 8 & 0 & 6 & 7 \\
5 & 6 & 4 & 8 & 1 & 2 & 0 & 9 & 7 & 3 \\
6 & 5 & 8 & 7 & 0 & 3 & 2 & 1 & 9 & 4 \\
7 & 8 & 6 & 0 & 9 & 4 & 1 & 2 & 3 & 5 \\
8 & 7 & 0 & 5 & 6 & 9 & 3 & 4 & 1 & 2 \\
9 & 0 & 7 & 6 & 5 & 8 & 4 & 3 & 2 & 1
\end{array}\right)
$$

Normalized LS of order 10

$$
N!\times(N-1)!
$$

$$
\left(\begin{array}{llllllllll}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
7 & 2 & 4 & 9 & 0 & 6 & 5 & 1 & 3 & 8 \\
8 & 3 & 6 & 7 & 5 & 9 & 0 & 2 & 4 & 1 \\
2 & 6 & 8 & 5 & 1 & 7 & 4 & 0 & 9 & 3 \\
5 & 8 & 9 & 1 & 7 & 0 & 3 & 4 & 6 & 2 \\
9 & 4 & 1 & 2 & 8 & 3 & 7 & 6 & 0 & 5 \\
4 & 7 & 5 & 6 & 9 & 1 & 8 & 3 & 2 & 0 \\
3 & 0 & 7 & 8 & 2 & 4 & 1 & 9 & 5 & 6 \\
6 & 5 & 0 & 4 & 3 & 2 & 9 & 8 & 1 & 7 \\
1 & 9 & 3 & 0 & 6 & 8 & 2 & 5 & 7 & 4
\end{array}\right)
$$

Normalized DLS of order 10

$$
(N-1)!
$$

## Why is it interesting?

Applied problems:

- experiment planning
- cryptography
- error correcting codes

- scheduling
- algebra, combinatorics, statistics, ...

Mathematical problems:

- existence of a triple of MOLS/MODLS of order 10 (or larger clique)
- increasing world record of orthogonality characteristic for pseudo triple of MOLS (291/300) or MODLS (274/300)
- generating functions
- asymptotic behavior of combinatorial characteristics based on DLSs (OEIS)
- number theory (relations between different fields of knowledge)
- magic squares
- Sudoku (LS of order 9 with additional constraints)


## Special types of LS/DLS

row[i] = cyclic_shift(row[i-1], d)


Cyclic LS (d=1)


Cyclic DLS ( $\mathrm{d}=2$ )

- there are known different special types of LS/DLS (plane symmetric, central symmetric, ...);
- all cyclic squares of small orders are pandiagonal.


## Integer sequences (OEIS): N queens problem example

The OEIS Foundation is supported by donations from users of the OEIS and by a grant from the Simons Foundation.

n queens Search Himts
(Greetings from The On-Line Encyclopedia of Integer Sequences!)
Search: $\mathbf{n}$ queens

M. B. Wells, Elements of Combinatorial Computing. Pergamon, Oxford, 1971, p. 238. Table of $n$, $a(n)$ for $n=0 . .27$.
queens, Discrete Mathematics, Volume 309, Issue 1, Jan 06 2009, Pages 1-31. o. Bill, Durango Bill's The N-Queens Problem
J. R. Bitner and E. M. Reingold, Backtrack programming_techniques, Commun. ACM, 18 J. R. Bitner and E. M. Reingold, Backtrack programming_techniques, Commun. ACM, 18 (1975), 651-656. [Annotated scanned copy]
p. Capstick and K. McCann, The problem of the $n$ queens, apparently unpublished, no P. Capstick and K. MCCann, The problem of date (circa 1990?) [Scanned copy]
V. Chvatal, All solutions to the probl
https://oeis.org/A000170

## Integer sequences connected with transversals in DLS

A287645 - Minimum number of transversals in a diagonal Latin square of order N ( $\mathrm{N}<10$ )
A287644 - Maximum number of transversals in a diagonal Latin square of order N ( $\mathrm{N}<10$ )
A287647 - Minimum number of diagonal transversals in a diagonal Latin square of order $\mathrm{N}(\mathrm{N}<9)$
A287648 - Maximum number of diagonal transversals in a diagonal Latin square of order N ( $\mathrm{N}<9$ )


Transversal 1


Transversal 2


Transversal 3

## Integer sequences connected with transversals in DLS: exactly known values

```
A287645 - 1, 0, 0, 8, 3, 32, 7, 8, \(68(\mathrm{~N}<10)\)
A287644 - 1, 0, 0, 8, 15, 32, 133, 384, \(2241(\mathrm{~N}<10)\)
A287647 - \(1,0,0,4,1,2,0,0,0(\mathrm{~N}<10)\)
A287648-1, 0, 0, 4, 5, 6, 27, 120, 333? ( \(\mathrm{N}<10\) )
```

$\mathrm{a}(1)-\mathrm{a}(8)$ - Brute Force for all DLS
a(9) - CFs generator for main classes of DLS based on X-fillings of diagonals and ESODLS schemas (currently ongoing, ends)

What about $a(10), a(11), \ldots$ ? They are unknown

$$
0 \leq X_{\min }^{L S}(N) \leq X_{\min }^{D L S}(N) \leq X_{\max }^{D L S}(N) \leq X_{\max }^{L S}(N)
$$



## Integer sequences connected with transversals in DLS: unknown values for high orders

```
A287645 - 1, 0, 0, 8, 3, 32, 7, 8, \(68(0 \leq a(n) \leq A 287644(n) \leq \operatorname{A090741}(\mathrm{n}))\)
A287644 - 1, 0, 0, 8, 15, 32, 133, 384, 2241, \(\geq 5504\) ( \(\mathrm{a}(\mathrm{n})<=\) A090741(n))
A287647 - 1, 0, 0, 4, 1, 2, 0, 0, 0 (a(n) <= A287648(n) <=A007016(n))
A287648 - 1, 0, 0, 4, 5, 6, 27, 120, \(\geq 333, \geq 866, \geq 4828, \geq 24901, \geq 131106\),
\(\mathbf{2 3 6 4 5 9 6}\), \(\mathbf{2 3 8 9 3 1 8}\) (a(n) <=A007016(n))
```

Upper and lower bounds can be expanded and strengthened!

## Transversals in random Latin squares

A287645 (minimum number of transversals)

```
a(11) \leq 3266->3255->3185->3175
a(12) \leq 15462
a(13) \leq 78253
a(14) \leq 422312
a(15) \leq2415635
a(16) \leq 14689972
```

A287644 (maximum number of transversals)
$\mathrm{a}(11) \geq 3867$
$a(12) \geq 16600$
$a(13) \geq 80999(a(13) \geq 1030367$ for cyclic squares)
$a(14) \geq 428296$
$a(15) \geq 2429398$
$a(16) \geq 14720910$

- 16 days on Core i7 4770 CPU, special program implementation of DLX (enumeration only without covers collecting)
- https://vk.com/wall162891802 1449


## Diagonal transversals in random Latin squares

A287647 (minimum number of diagonal transversals)

$$
a(11) \leq 324
$$

$$
a(12) \leq 1816
$$

A287648 (maximum number of diagonal transversals) $\mathrm{a}(11) \geq 550$
$a(12) \geq 2200$

- 16 days on Core i7 4770 CPU, special program implementation of DLX (enumeration only without covers collecting)
- https://vk.com/wall162891802 1449


## Cyclic Latin squares: one of special types of LS


. 4 cyclic DLS, 6 cyclic LS for $\mathrm{N}=7$

## Number of transversals in cyclic Latin squares

$1,0,3,0,15,0,133,0,2025,0,37851,0,1030367,0,36362925$
or without zeroes:
$1,3,15,133,2025,37851,1030367,36362925$
A006717 - Number of ways of arranging $2 \mathrm{n}+1$ nonattacking semi-queens on a $(2 n+1) X(2 n+1)$ toroidal board

Also the number of transversals of a cyclic Latin square of order $2 n+1$ and the number of orthomorphisms of the cyclic group of order $2 n+1$ (Ian Wanless, 2001).

- Number of transversals are same for all cyclic LS of given order N


## Number of transversals in cyclic Latin squares: consequence

A090741 (maximum number of transversals in LS):
$\mathrm{a}(11) \geq 37851$
$a(13) \geq 1030367$
$a(15) \geq 36362925$
$a(17) \geq 1606008513$
$a(19) \geq 87656896891$
$a(21) \geq 5778121715415$
$a(23) \geq 452794797220965$
$a(25) \geq 41609568918940625$

Lower bounds can be added to sequence A090741 in OEIS...

- Number of transversals are same for all cyclic LS of given order N


## Number of transversals in cyclic diagonal Latin squares: consequence

$a(11) \geq 37851$
$a(13) \geq 1030367$
cyclic DLS are not exists for $\mathrm{N}=15$
$a(17) \geq 1606008513$
$a(19) \geq 87656896891$
cyclic DLS are not exists for $\mathrm{N}=21$
$a(23) \geq 452794797220965$
$a(25) \geq 41609568918940625$
Lower bounds can be added to sequence A287644 in OEIS...

- exists not for all orders N


## Number of diagonal transversals in cyclic diagonal Latin squares

Minimal number of diagonal transversals in cyclic DLS of order $N=2 n+1: \underline{\mathbf{1}, \mathbf{0}, \mathbf{5}, 27,}$ $\mathbf{0}, 4523,128818, \mathbf{0}, 204330233,11232045257$ (not presented in OEIS)

Maximal number of diagonal transversals in cyclic DLS of order $N=2 n+1: \mathbf{1}, \mathbf{0}, \mathbf{5}$, 27, 0, 4665, 131106, 0, 204995269, 11254190082 (not presented in OEIS)

Corresponding upper and lower bounds can be added to A287647 (weak) and A287648...

## Enumerating the cyclic (diagonal) Latin squares

## DLS:

$1,0,0,0,2,0,4,0,0,0,8,0,10,0,0,0,14,0,16,0,0,0,20,0,10,0,0$, $0,26,0,28, \ldots$

Squares of this special type exists not for all orders N .
The number of positive integers $k$ which are $\leq n$ and where $k, k-1$ and $k+1$ are each coprime to $n$ (well known numerical series that directly not connected with Latin squares!).

LS:
$1,1,2,2,4,2,6,4,6,4,10,4,12,6,8,8,16,6,18,8, \ldots$
Euler totient function phi(N)!!!
Not connected directly with Latin squares! Can be calculated through Latin squares...

## Euler totient function calculating

$$
\begin{gathered}
n=p_{1}^{\alpha_{1}} \cdot p_{2}^{\alpha_{2}} \cdot \ldots \cdot p_{m}^{\alpha_{m}} \\
\varphi(n)=n\left(1-\frac{1}{p_{1}}\right)\left(1-\frac{1}{p_{2}}\right) \ldots\left(1-\frac{1}{p_{m}}\right) \\
6=2^{1} \cdot 3^{1}, \varphi(6)=6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=2
\end{gathered}
$$

- calculating by definition (enumerating coprimes (k,n), $k<n$, Euclid algorithm)
- calculating using factoring and formula
- new method: calculating by enumerating cyclic Latin squares of order n



## Euler totient function calculating by enumerating cyclic Latin squares

| 0 | 1 | 2 | 3 | 4 | 5 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 1 | 2 | 3 | 4 | 5 |
| 0 | 1 | 2 | 3 | 4 | 5 |
| 0 | 1 | 2 | 3 | 4 | 5 |
| 0 | 1 | 2 | 3 | 4 | 5 |
| 0 | 1 | 2 | 3 | 4 | 5 |



$$
\varphi(6)=2
$$



- polynomial algorithm ( $\mathrm{t} \sim \mathrm{O}\left(\mathrm{N}^{2}\right)$, $\mathrm{m} \sim \mathrm{O}(\mathrm{N})$ ) without multiplications and divisions



## Euler totient function OEIS description slightly expanded

Phi $\left(p^{*} n\right)=$ phi $(n)^{*}(f 100 r((x)$ Gary Detiefs, Apr 212012


theorem of Pedersen et al. Cf. A135303. - Gary $W$ W. Adamson, Aug 152012
G.f.: Sum $\{n>=1\} \operatorname{mu}(n) * x^{\wedge} n /\left(1-x^{\wedge} n\right)^{\wedge}$, where mu(n) $=A 008683(n)$. Mamuka
G.f.: Sum_\{n>=1\} mu(n)*x^n/(1-x^n)^2, where mu(n) $=\underline{A 008683(n) \text {. - Mamuka }}$

Jibladze, Apr 052015
$a(n)=\lim _{1}\{s->1\} n^{*} z e t a(s)^{*}\left(S u m \_\{d \text { divides } n\}\right.$ A008683 (d) $\left./\left(e^{\wedge}(1 / d)\right)^{\wedge}(s-1)\right)$, for $n>$

1.     - Mats Granvik, Jan 262017

Conjecture: $a(n)=$ sum_ $\{0=1 \ldots n\}$ Sum_ $\{b=1 \ldots n\}$ Sum_\{c=1..n\} 1 for $n>1$. The sum is
over $a, b, c$ such that $n^{*} c-a * b=1$. - Benedict $W$. J. Irwin, Apr 03201
$\left.a(n)=\operatorname{Sum}_{\exp \left(2^{*} \mathrm{P}^{*} \mathrm{i}^{*} j / n\right)} \mathrm{j}\right)$ where i is the imagivary unit. Notice that the Famanujan's sun $\operatorname{cop}_{-n}(k):=\operatorname{sum}\{j=1 \ldots n, \operatorname{gcd}(j, n)=1\} \exp \left(2^{*} \mathrm{P}^{*} \mathrm{i}^{*} j^{*} k / n\right)$ gives $a(n)=\operatorname{sum} \_\{k \mid n\}$ $k^{{ }^{*}} c_{C}(n / k)(1)=$ sum_\{ $\{k \mid n\} k^{*}$ mu $(n / k)$. - Michael Somos, May 132018
G.f.: $x^{*} d / c x\left(x^{*} d / d x\left(\log (\right.\right.$ Product_( $\left.\left.k>-1)\left(1 \quad x^{\wedge} k\right) \wedge\left(m u(k) / k^{\wedge} 2\right)\right)\right)$, wherc $m u(n)$ -

A008683(n). - Mamuka Jibladze, Sep 292018
 062019
$a(n)>=\operatorname{sqrt}(n / 2)$ (Nicolas). - Hugo Pfoertner, Jun 012020
(n) $>n /\left(\exp (\right.$ gamma $\left.) * \log (\log (n))+5 /\left(2^{*} \log (\log (n))\right)\right)$, except for $n=223092870$
(Rosser, Schoenfeld). - Hugo Pfoertner, Jun 022020
$a(8)=4$ with $\{1,3,5,7\}$ units modulo $8, a(10)=4$ with $\{1,3,7,9\}$ units modulo
10. - Michael Somos, Aug 272013

From Eduard I. Vatutin, Nov 01 2020: (Start)
The $a(5)=4$ cyclic Latin squares with the first row 10 ascending order are:
$\begin{array}{lllllllllllllllllll}0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3\end{array}$
$\begin{array}{lllllllllllllllllll}1 & 2 & 3 & 4 & 6 & 2 & 3 & 4 & 0 & 1 & 3 & 4 & 0 & 1 & 2 & 4 & 0 & 1 & 2\end{array}$

40
(End)
with(numtheory): A000010 := phi; [ seq(phi(n), n=1..100) ]; \# version 1 with(numtheory): phi $:=\operatorname{proc}(n)$ local $i$, $\mathrm{t} 1, \mathrm{t} 2$; $\mathrm{t} 1:=\mathrm{ifactors}(\mathrm{n})[2]$; $\mathrm{t} 2:=$
mathematica
Array[EulerPhi, 70]
(Axiom) [eulerPhi( $n$ ) for $n$ in 1..100]
(Axiom) [eulerPhi(n) for $n$ in 1..100]
(MGMM) [ EulerPhi(n) : $n$ in [1..100] ]; // Sergei Haller (sergei(AT)sergei(Maller.de), Dec 212006
(PARI) $\{a(r)=i f(n=0,0$, eulerphi( $n \mathfrak{l})\}$; /* Michael Somos, Feb 052011 */
(Sage)
\# euler_phi is a standard function in sage.
def $\frac{\text { A00001 }}{}(\mathrm{n})$ : return euler_phi ( n )
def $\frac{\text { A000016 }}{}$ list ( $n$ ): return [ euler_phi(i) for $i$ in range ( $1, n+1$ )]
(PARI) \{ for ( $n=1,100000$, write("bøo0010.txt", $n$, " ", eulerphi(n))); \} <br> Harry J. Smith, Apr 262009
(Sage) [euler_phi(n) for $n$ in range (1, 70)] \# Zerinvary Lajos, Jun 062009 (Maxima) makelist(totient(n), n, 0, 1000); /* Emanuele Munarini, Mar 262011 */ Haskell) $\varepsilon_{n}=$ length (filter ( $==1$ ) (nap (gcd $n$ ) [1..n])) -- Allan C. Wechsler, (Python)
rom sympy.
([

Jordan function J $k(n)$ is a generalization - 5 ee A059379 and A059380 (triangle of

## Euler totient function calculating by enumerating cyclic Latin squares: practice implementation



- slower than factorization based calculating
- slower than long arithmetic implementation (extimation)


## Brief conclusion

- new numerical series was calculated
- new upper and lower bounds for some series was established
- interconnections between Latin squares and different type combinatorial objects was established
- new method of Euler totient function calculating based on Latin squares was proposed


## Related work

Collecting CFs and new combinatorial structures search:

- triple of MODLS (is it exist?)
- different structures?

GPU implementation of transversal, cover and ESODLS algorithms?
Enumeration problems (OEIS):

- expanding current sequences
- enumerating DLS and ODLS of special kind (string-inverse, symmetric, ...) and its CFs

Pseudo triples:

- 3 kinds of pseudo triples, only 1 was investigated in details


## Thank you for your attention!

## Thanks to all the volunteers who took part in the Gerasim@home project!

WWW: http://evatutin.narod.ru, http://gerasim.boinc.ru
E-mail: evatutin@rambler.ru
LJ: http://evatutin.livejournal.com
Skype: evatutin

