https://toc.ui.ac.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 15 No. 4 (2026), pp. 235–250.

https:// www.ui.ac.ir

CIRCULANT MATRICES OF EACH RANK OVER FINITE FIELDS

YANGJIANG WEI AND YI MING ZOU*

Abstract. We consider the enumeration of circulant matrices over a finite field with q elements, and we provide formulas to compute the number of these circulant matrices for each rank. We also consider the computation of the orders of q in multiplicative groups of integers modulo n that are needed in the enumeration, and we give a reduction method to compute these orders. We then use these results to derive explicit formulas for the enumerations of infinite sequences of circulant matrices of some special types.

1. Circulant matrices and their ranks

Circulant matrices have been studied in many publications due to their practical importance (see for examples [3, 4, 5, 6, 7, 9, 11]). In particular, the rank problem of a circulant matrix over a field was considered in [5] (over the field of complex numbers) and in [4] (over an arbitrary field). It was briefly mentioned in [4] how one might be able to enumerate the circulant matrices over a finite field $\mathbb{F}_q$ for each rank by applying the result of [2], but no formula was given. Indeed, such formulas would depend on the computation of the orders of q in multiplicative groups of integers modulo n for certain n (see definition later), but there is no formula to compute these orders in general. For example, in the formula for the number of nonsingular circulant matrices over $\mathbb{F}_q$ given by some later publications (see [11] and the references therein), a minimizing procedure to compute the orders of q in these multiplicative groups

MSC(2010): Primary: 05A15; Secondary: 15B05, 15B33.

Keywords: Circulant matrices, finite fields, orders of group elements.

Article Type: Research Paper.

Communicated by Behruz Tayfeh Rezaie.

*Corresponding author.

Received: 15 August 2023, Accepted: 15 November 2025, Published Online: 20 November 2025.

Cite this article: Y. Wei and Y. M. Zou, Circulant matrices of each rank over finite fields, *Trans. Comb.*, **15** no. 4 (2026) 235–250.
https://dx.doi.org/10.22108/toc.2025.138779.2097 .

of integers modulo n was built into the formula. To use this formula, it is necessary to compute these orders of q first by applying the minimizing procedure to each modulo case. In this paper, we will first discuss how to compute the number of circulant matrices over $\mathbb{F}_q$ for each rank. Then, we provide a procedure to help us to compute the needed orders of q. Our procedure reduces the general computation to the base prime number modulo cases. By using our results, we will be able to derive enumeration formulas (in the forms of integer sequences) for many special sequences of circulant matrices.

Let $\mathbb{F}$ be a field and let $n \geqslant 1$ be an integer. Given a row vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ of size n, where $a_i \in \mathbb{F}$, $0 \leqslant i \leqslant n-1$, the corresponding $n \times n$ *circulant matrix* defined by $\mathbf{a}$ (the generating vector) is the following matrix

$$\operatorname{circ}(\mathbf{a}) = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}. \tag{1.1}$$

The following polynomial

$$f_{\mathbf{a}}(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \tag{1.2}$$

is called the *associated polynomial* of the circulant matrix $\operatorname{circ}(\mathbf{a})$. The name came from the following fact. If C is the permutation matrix corresponding to the cyclic permutation $(n, n-1, \ldots, 1)$ given by

$$C = \begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 1 & & & 0 \end{pmatrix},$$

then

$$\operatorname{circ}(\mathbf{a}) = f_{\mathbf{a}}(C) = a_{n-1}C^{n-1} + a_{n-2}C^{n-2} + \cdots + a_1 C + a_0 I.$$

With the above notation in hand, we can recall the following theorem due to Ingleton [5] and Daykin [4]:

Theorem 1.1. *(Ingleton-Daykin) Let $\mathbb{F}$ be a field. For any given $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$, where $a_i \in \mathbb{F}$, $0 \leqslant i \leqslant n-1$, we have*

$$\operatorname{rank}(\operatorname{circ}(\mathbf{a})) = n - \deg(\gcd(f_{\mathbf{a}}(x), x^n - 1)). \tag{1.3}$$

In particular, $\operatorname{circ}(\mathbf{a})$ *is nonsingular if and only if*

$$\gcd(f_{\mathbf{a}}(x), x^n - 1) = 1.$$

https://dx.doi.org/10.22108/toc.2025.138779.2097

Remark 1.1. *Ingleton* [5] *proved this theorem for the field of the complex numbers, but the proof does not apply to a general field. Daykin* [4] *gave a proof which works for an arbitrary field. We provide a somewhat different proof below.*

Proof. Since the rank of a matrix over $\mathbb{F}$ remains the same in any field extension of $\mathbb{F}$, we can assume that $\mathbb{F}$ contains all the roots of $x^n - 1$, and consider the Jordan form of the circulant matrix C. Let

$$J = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_k \end{pmatrix} \tag{1.4}$$

be the Jordan form of C with the Jordan blocks J_i (upper triangular), $1 \leqslant i \leqslant k$. The rank of the circulant matrix $\mathrm{circ}(\mathbf{a}) = f_{\mathbf{a}}(C)$ is the same as the following matrix

$$f_{\mathbf{a}}(J) = \begin{pmatrix} f_{\mathbf{a}}(J_1) & & & \\ & f_{\mathbf{a}}(J_2) & & \\ & & \ddots & \\ & & & f_{\mathbf{a}}(J_k) \end{pmatrix}. \tag{1.5}$$

Thus the rank of $\mathrm{circ}(\mathbf{a})$ is equal to the sum of the ranks of the matrices $f_{\mathbf{a}}(J_i)$, $1 \leqslant i \leqslant k$. For any $1 \leqslant i \leqslant k$, let the eigenvalue of J_i be λ_i. Then the eigenvalue of $f_{\mathbf{a}}(J_i)$ is $f_{\mathbf{a}}(\lambda_i)$. Thus, if λ_i is not a root of $f_{\mathbf{a}}(x)$, then $f_{\mathbf{a}}(J_i)$ has full rank, since it is an upper triangular matrix with $f_{\mathbf{a}}(\lambda_i)$ on the diagonal. To find the rank of $f_{\mathbf{a}}(J_i)$ when λ_i is a root of $f_{\mathbf{a}}(x)$, consider the structure of $f_{\mathbf{a}}(J_i)$. Suppose that J_i is of size $d \times d$. By induction on $m \geqslant 1$, it is easy to obtain the following formula:

$$J_i^m = \begin{pmatrix} \lambda_i^m & C_1^m\lambda_i^{m-1} & C_2^m\lambda_i^{m-2} & \cdots & C_{d-1}^m\lambda_i^{m-d+1} \\ & \lambda_i^m & C_1^m\lambda_i^{m-1} & \ddots & \vdots \\ & & \lambda_i^m & \ddots & C_2^m\lambda_i^{m-2} \\ & & & \ddots & C_1^m\lambda_i^{m-1} \\ & & & & \lambda_i^m \end{pmatrix}, \tag{1.6}$$

where the C_k^m's are the binomial coefficients. Write the first row of the matrix $f_{\mathbf{a}}(J_i)$ as $(b_1, b_2, \ldots, b_d)$, then

$$f_{\mathbf{a}}(J_i) = \begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_d \\ & b_1 & b_2 & \ddots & \vdots \\ & & b_1 & \ddots & b_3 \\ & & & \ddots & b_2 \\ & & & & b_1 \end{pmatrix}, \tag{1.7}$$

where

$$b_j = \sum_{k=j-1}^{n-1} a_k C_{j-1}^k \lambda_i^{k-j+1},\ 1 \leqslant j \leqslant d.$$

https://dx.doi.org/10.22108/toc.2025.138779.2097

It is clear from (1.7) that if b_j is the first nonzero element, then the rank of $f_{\mathbf{a}}(J_i)$ is $d-j+1$; and if all $b_j = 0$, then the rank is 0. Using derivative notation, we can write

$$b_j = \frac{f_{\mathbf{a}}^{(j-1)}(\lambda_i)}{(j-1)!},\ 1 \leqslant j \leqslant d. \tag{1.8}$$

Note that all notation make sense even if $\mathbb{F}$ has positive characteristic. We want to show that if

$$f_{\mathbf{a}}(x) = (x-\lambda_i)^t g(x), \tag{1.9}$$

where $t \geqslant 1$ and $g(\lambda_i) \neq 0$, then $b_j = 0$, $j = 1, \ldots, t$, and $b_{t+1} \neq 0$. This implies that the rank of $f_{\mathbf{a}}(J_i)$ is $d-t$, and thus implies the theorem. Since the size of J_i is d, if $t \geqslant d$, then

$$f_{\mathbf{a}}(J_i) = (J_i - I_d\lambda_i)^t g(J_i) = 0 \cdot g(J_i) = 0.$$

That is, in all cases where $t \geqslant d$, the ranks of $f_{\mathbf{a}}(J_i)$ are always 0. So we can assume $t < d$. To help us see things better, we make a change of variables in (1.9) by letting $x = y + \lambda_i$, and write

$$h(y) = f_{\mathbf{a}}(y+\lambda_i) = c_{n-1}y^{n-1} + \cdots + c_t y^t,\ c_t \neq 0. \tag{1.10}$$

Then for $k \geqslant 1$,

$$\frac{d^k h(y)}{dy^k} = h^{(k)}(y) = f_{\mathbf{a}}^{(k)}(y+\lambda_i),$$

and $f_{\mathbf{a}}^{(j-1)}(\lambda_i) = h^{j-1}(0)$. So by (1.8),

$$b_j = \frac{h^{(j-1)}(0)}{(j-1)!},\ 1 \leqslant j \leqslant d. \tag{1.11}$$

But from (1.10), it is clear that $b_k = h^{(k-1)}(0)/(k-1)! = 0$ for all $1 \leqslant k \leqslant t$, and $b_{t+1} = h^{(t)}(0)/t! = c_t \neq 0$. □

In the next section, we will consider the enumeration of $n \times n$ circulant matrices over a finite field for each rank.

2. Circulant matrices of each rank

From now on we assume that $\mathbb{F}_q$ is a finite field of q elements, where $q = p^c$ for a prime integer p and an integer $c > 0$. Given integers $n \geqslant 1$ and $0 \leqslant r \leqslant n$, let $N(q,n,r)$ be the number of $n \times n$ circulant matrices of rank r over $\mathbb{F}_q$. According to Theorem 1.1, to find $N(q,n,r)$, we can count the number of $\mathbf{a} \in \mathbb{F}_q^n$ such that

$$\deg(\gcd(f_{\mathbf{a}}(x), x^n - 1)) = n - r. \tag{2.1}$$

Define a function $\phi_{q,r} : \mathbb{F}_q[x] \longrightarrow \mathbb{Z}_{\geqslant 0}$ as follows. If f is a nonzero polynomial, then $\phi_{q,r}(f)$ counts the polynomials g of degrees less than r such that $\gcd(f,g) = 1$; and $\phi_{q,r}(0) = 0$. If n is the degree of f, $\phi_{q,n}(f)$ is just the usual Euler function that counts the number of polynomials g of degrees less than the degree of f such that $\gcd(f,g) = 1$, which is usually denoted by $\phi_q(f)$. Assume that $0 \leqslant r \leqslant n$,

https://dx.doi.org/10.22108/toc.2025.138779.2097

and let $g_{r,1}(x), \ldots, g_{r,k_r}(x)$ be distinct monic factors of $x^n - 1$ in $\mathbb{F}_q[x]$ of degree $n - r$. Then we have the following theorem.

Theorem 2.1. *If $x^n - 1$ has no factor of degree $n - r$, then $N(q, n, r) = 0$; otherwise*

$$N(q,n,r) = \begin{cases} 1 & \text{if } r = 0; \\ k_r \phi_{q,r}(x^n - 1) & \text{if } r > 0, \end{cases} \tag{2.2}$$

where k_r is the number of distinct monic factors of $x^n - 1$ of degree $n - r$.

Proof. Notice that since $\phi_{q,0}(x^n - 1) = 0$, we need to separate (2.2) into two cases. We only need to prove the last case, since the other parts are clear. Assume $r > 0$ and $x^n - 1$ has factors of degree $n - r$.

If (2.1) holds, then $f_{\mathbf{a}}(x) = h(x)g_{r,i}(x)$ for a unique $1 \leqslant i \leqslant k_r$ and a unique $h(x)$ of degree less than r such that $\gcd(h(x), x^n - 1) = 1$. Conversely, given an $h(x)$ of degree less than r such that $\gcd(h(x), x^n - 1) = 1$ and a $g_{r,i}(x)$, we obtain a unique $f_{\mathbf{a}}(x) := h(x)g_{r,i}(x)$ that satisfies (2.1). Thus, there is a bijection between the set of pairs of polynomials $(h(x), g_{r,i}(x))$ such that $\deg(h(x)) < r$ and $\gcd(h(x), x^n - 1) = 1$ and the set of polynomials $f(x)$ such that $\deg(f(x)) < n$ and $\deg(\gcd(f(x), x^n - 1)) = n - r$. □

Example 2.1. *Over the field $\mathbb{F}_2$, the irreducible factorization of $x^5 - 1 = x^5 + 1$ is*

$$x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Thus there is no rank 2 nor rank 3 circulant 5×5 matrix over $\mathbb{F}_2$.

Next, we consider the computations of k_r and $\phi_{q,r}(x^n - 1)$ in (2.2). For integers u, v, let $\mu(u, v) = \max\{u - v, 0\}$. Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree $n > 0$ and fix an irreducible factorization $f = g_1^{m_1} g_2^{m_2} \cdots g_k^{m_k}$ in $\mathbb{F}_q[x]$, where the g_i's are distinct and irreducible. Let the degree of g_i be n_i $(1 \leqslant i \leqslant k)$.

Lemma 2.1. *We have*

$$\begin{aligned} \phi_{q,r}(f) &= q^r - \sum_{i=1}^{k} q^{\mu(r,n_i)} + \sum_{1 \leqslant i < j \leqslant k} q^{\mu(r,n_i+n_j)} \\ &\quad - \sum_{1 \leqslant i < j < \ell \leqslant k} q^{\mu(r,n_i+n_j+n_\ell)} + \cdots + (-1)^k q^{\mu(r,\sum_{i=1}^{k} n_i)}. \end{aligned} \tag{2.3}$$

Proof. The number of polynomials of degrees less than r is q^r. If $h(x)$ is one of these polynomials and $\gcd(f, h) \neq 1$, then there is an i such that $g_i | h$. The polynomials of degrees less than r that are divisible by g_i are exactly the multiples of g_i of degrees less than r. Since the degree of g_i is n_i, if $r \leqslant n_i$, then only the zero polynomial 0 satisfies the requirement; and if $r > n_i$, then the multiples of g_i of degrees less than r are kg_i such that $\deg(k) < r - n_i$. There are q^{r-n_i} such polynomials. Thus the number of polynomials of degrees less than r that are divisible by g_i is $q^{\max\{r-n_i,0\}} = q^{\mu(r,n_i)}$. Similarly, the

https://dx.doi.org/10.22108/toc.2025.138779.2097

number of polynomials of degrees less than r that are divisible by g_ig_j, $1 \leqslant i < j \leqslant k$, is $q^{\mu(r,n_i+n_j)}$, etc.. Thus, the lemma follows from the inclusion-exclusion principle. □

To use Lemma 2.1 for $f = x^n - 1$, we recall some known facts about the factorization of $x^n - 1$. If $n = p^a m$, where $p \nmid m$, then $x^n - 1 = (x^m - 1)^{p^a}$. Thus to find the distinct irreducible factors of $x^n - 1$, we only need to work with $x^m - 1$. This polynomial has m distinct roots in its splitting field, and all its irreducible factors in $\mathbb{F}_q[x]$ have multiplicity 1. Let ξ be a primitive mth root of unity (could be in an extension of $\mathbb{F}_q$) and define the mth cyclotomic polynomial over $\mathbb{F}_q$ by

$$g_m(x) = \prod_{\substack{s=1 \\ \gcd(s,m)=1}}^{m} (x - \xi^s). \tag{2.4}$$

It is well-known (see e.g. [8]) that $\deg(g_m(x)) = \phi(m)$, where ϕ is the Euler totient function on integers, the coefficients of $g_m(x)$ belong to the prime subfield of $\mathbb{F}_q$, and $x^m - 1$ factors into the following product of cyclotomic polynomials in $\mathbb{F}_q[x]$:

$$x^m - 1 = \prod_{k|m} g_k(x). \tag{2.5}$$

The following theorem is well-known (see [8, Theorem 2.47]).

Theorem 2.2. *Under the assumption that $p \nmid m$, the mth cyclotomic polynomial $g_m(x)$ factors into $\phi(m)/d$ distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree d, where d is the order of (the residue of) the integer q in the multiplicative modulo group $\mathbb{Z}_m^*$.*

Denote the order of q in the multiplicative group $\mathbb{Z}_k^*$ by $\mathrm{ord}_k(q)$, where $k > 0$ and $p \nmid k$. For a positive integer m, let the set of the divisors of m be $D(m)$, that is

$$D(m) = \{d \mid 1 \leqslant d \leqslant m \text{ and } d|m\},$$

and let (assume $p \nmid m$)

$$D(m)(q) = \{\mathrm{ord}_d(q) \mid d \in D(m)\}.$$

Then we have the following corollary of Theorem 2.2:

Corollary 2.1. *Assume that $p \nmid m$. The set $D(m)(q)$ provides the degrees of the irreducible factors of $x^m - 1$ in $\mathbb{F}_q[x]$. For each $k \in D(m)(q)$, $x^m - 1$ has $n_q(k)$ distinct monic irreducible factors of degree k, where*

$$n_q(k) = \frac{1}{k} \sum_{\substack{d \in D(m) \\ \mathrm{ord}_d(q)=k}} \phi(d). \tag{2.6}$$

Proof. This follows from formula (2.5) and Theorem 2.2. □

https://dx.doi.org/10.22108/toc.2025.138779.2097

Let

$$M = \sum_{k \in D(m)(q)} n_q(k) = \sum_{k|m} \frac{\phi(k)}{\mathrm{ord}_k(q)}.$$

Then M is the number of monic irreducible factors of $x^m - 1$ in $\mathbb{F}_q$. Let $n(m)_i$, $1 \leqslant i \leqslant M$, be the degrees of these irreducible factors arranged in a nondecreasing order: $n(m)_i \leqslant n(m)_j$ if $i < j$. The next corollary gives a formula for $\phi_{q,r}(x^n - 1)$ for an arbitrary positive integer n.

Corollary 2.2. *Notation as above. Let $n > 0$ be an integer and let $n = p^a m$, where $p \nmid m$. Given any integer $r \geqslant 0$, the number of polynomials in $\mathbb{F}_q[x]$ of degrees $< r$ and are relatively prime to $x^n - 1$ is given by the following formula:*

$$\begin{aligned} \phi_{q,r}(x^n - 1) &= q^r - \sum_{k=1}^{M} q^{\mu(r, n(m)_k)} + \sum_{1 \leqslant k_1 < k_2 \leqslant M} q^{\mu(r, n(m)_{k_1} + n(m)_{k_2})} \\ &\quad - \sum_{1 \leqslant k_1 < k_2 < k_3 \leqslant M} q^{\mu(r, n(m)_{k_1} + n(m)_{k_2} + n(m)_{k_3})} \\ &\quad + \cdots + (-1)^M q^{\mu(r, \sum_{k=1}^{M} n(m)_k)}. \end{aligned} \tag{2.7}$$

Proof. This follows from Lemma 2.1 and the fact that under the assumption, $x^n - 1 = (x^m - 1)^{p^a}$ (so the distinct irreducible factors are all from $x^m - 1$). □

The integer coefficient k_r in formula (2.2), i.e. the number of distinct monic factors of $x^n - 1$ in $\mathbb{F}_q[x]$ of degree $n - r$, can be computed by using a partition function as follows. Again, let $n = p^a m$, where $p \nmid m$. Then the multiplicities of the irreducible factors of $x^n - 1 = (x^m - 1)^{p^a}$ are all equal to p^a. Recall that M is the number of monic irreducible factors of $x^m - 1$ in $\mathbb{F}_q$. Let

$$\mathscr{P}_q(n, r) = \{(m_1, \ldots, m_M) \in \mathbb{Z}_{\geqslant 0}^M \mid m_i \leqslant p^a \text{ and } \sum_{i=1}^{M} m_i n(m)_i = n - r\}, \tag{2.8}$$

and let $|\mathscr{P}_q(n, r)| = p_q(n, r)$. Then

$$k_r = p_q(n, r). \tag{2.9}$$

We give an example to explain the notation and the formulas.

Example 2.2. *Let the field be $\mathbb{F}_2$ and let $n = 60 = 4 \times 15$. Then $q = 2$ and $m = 15$. Since the factors of 15 are $1, 3, 5, 15$, by Theorem 1.1, the degrees $(\mathrm{ord}_d(q))$ of the irreducible factors of $x^{15} - 1$ are*

$$\mathrm{ord}_1(2) = 1, \mathrm{ord}_3(2) = 2, \mathrm{ord}_5(2) = 4, \mathrm{ord}_{15}(2) = 4,$$

and the corresponding numbers of these distinct irreducible factors are

$$\frac{\phi(1)}{1} = 1, \ \frac{\phi(3)}{2} = 1, \ \frac{\phi(5)}{4} = 1, \ \frac{\phi(15)}{4} = 2.$$

Thus the numbers of irreducible factors of degrees $1, 2, 4$, respectively, are

$$n_2(1) = 1, \ n_2(2) = 1, \ n_2(4) = 3,$$

https://dx.doi.org/10.22108/toc.2025.138779.2097

and the total number of distinct irreducible factors is $M = 5$. *So the sequence of degrees of the irreducible factors of* $x^{15} - 1$ *is (see the paragraph before Corollary 2.2)*

$$n(15)_1 = 1,\ n(15)_2 = 2,\ n(15)_3 = 4,\ n(15)_4 = 4,\ n(15)_5 = 4.$$

With the above information, we can compute the number of 60×60 *circulant matrices of any given rank. Consider for example, the case* $r = 4$. *To obtain the number of distinct factors of* $x^{60} - 1$ *of degree* $n - r = 56$, *we solve the following integer equation*

$$m_1 + 2m_2 + 4m_3 + 4m_4 + 4m_5 = 56$$

subject to $1 \leqslant m_i \leqslant 4$, $1 \leqslant i \leqslant 5$. *There are* 5 *solutions:*

$$(2,3,4,4,4),\ (4,2,4,4,4),\ (4,4,3,4,4),\ (4,4,4,3,4),\ (4,4,4,4,3).$$

So $p_2(60, 4) = 5$.

For $r = 4$, *the exponents* $\mu(4, s)$ *of* $q = 2$ *in formula (2.7) are all equal to* 0 *except for the following* 3 *cases:*

$$\begin{aligned} & n(15)_1 = 1,\ \mu(4,1) = 3; \\ & n(15)_2 = 2,\ \mu(4,2) = 2; \\ \text{and}\quad & n(15)_1 + n(15)_2 = 3,\ \mu(4,3) = 1. \end{aligned}$$

Therefore by (2.7) we have

$$\phi_{2,4}(x^{60} - 1) = 2^4 - (2^3 + 2^2 + 3) + (2 + 9) - 10 + 5 - 1 = 6.$$

Thus, by Theorem 2.1, the number of 60×60 *rank* 4 *circulant matrices over* $\mathbb{F}_2$ *is*

$$N(2, 60, 4) = p_2(60, 4) \times \phi_{2,4}(x^{60} - 1) = 5 \times 6 = 30.$$

Consider the nonsingular $n \times n$ circulant matrices. In this case, $r = n$, $p_q(n, n) = 1$, and all exponents of q in formula (2.7) satisfy $\mu(n, s) = n - s$. Thus by Theorem 2.1 and Corollary 2.2, we have

https://dx.doi.org/10.22108/toc.2025.138779.2097

$$
\begin{aligned}
(2.10) \qquad N(q,n,n) &= p_q(n,n)\phi_{q,n}(x^n-1) \\
&= \phi_{q,n}(x^n-1) \\
&= q^n - \sum_{k=1}^{M} q^{n-n(m)_k} + \sum_{1\leqslant k_1<k_2\leqslant M} q^{n-(n(m)_{k_1}+n(m)_{k_2})} \\
&\quad - \sum_{1\leqslant k_1<k_2<k_3\leqslant M} q^{n-(n(m)_{k_1}+n(m)_{k_2}+n(m)_{k_3})} \\
&\quad + \cdots + (-1)^M q^{n-\sum_{k=1}^{M} n(m)_k} \\
&= q^n\Big(1 - \sum_{k=1}^{M} q^{-n(m)_k} + \sum_{1\leqslant k_1<k_2\leqslant M} q^{-(n(m)_{k_1}+n(m)_{k_2})} \\
&\quad - \sum_{1\leqslant k_1<k_2<k_3\leqslant M} q^{-(n(m)_{k_1}+n(m)_{k_2}+n(m)_{k_3})} \\
&\quad + \cdots + (-1)^M q^{-\sum_{k=1}^{M} n(m)_k}\Big) \\
&= q^n \prod_{i=1}^{M}(1-q^{-n(m)_i}).
\end{aligned}
$$

The above formula can also be derived by using known results directly, for example, by [8, Lemma 3.69]. By changing the notation, we obtain the following known formula (see [11] and the references therein):

Corollary 2.3. *Let p be a prime integer, and let $n = p^a m$, where $m > 0$ and $p \nmid m$. The number of $n \times n$ nonsingular circulant matrices over $\mathbb{F}_q$, where $q = p^c$, can be computed by the following formula:*

$$
\begin{aligned}
(2.11) \qquad N(q,n,n) &= q^n \prod_{k\mid m}(1-q^{-\operatorname{ord}_k(q)})^{\frac{\phi(k)}{\operatorname{ord}_k(q)}} \\
&= q^{n-m} \prod_{k\mid m}(q^{\operatorname{ord}_k(q)}-1)^{\frac{\phi(k)}{\operatorname{ord}_k(q)}}.
\end{aligned}
$$

Proof. The first equality follows from Theorem 2.2 and formula (2.10). The second equality follows from the fact that $\sum_{k\mid m}\phi(k) = m$. □

Example 2.3. *By using the information in Example 2.2 and formula (2.11), we get the number of nonsingular 60×60 circulant matrices over $\mathbb{F}_2$:*

$$N(2,60,60) = 2^{45}\cdot(2^1-1)\cdot(2^2-1)\cdot(2^4-1)^3 = 2^{45}\cdot 3^4\cdot 5^3.$$

Example 2.4. *Consider the field $\mathbb{F}_{5^2}$ and $n = 60 = 5\times 12$. Then $q = 25$ and $m = 12$. The factors of 12 are $1,2,3,4,6,12$, and $\operatorname{ord}_k(25) = 1$ for all $k = 1,2,3,4,6,12$. Since*

$$\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12) = 12,$$

by formula (2.11), the number of nonsingular 60×60 circulant matrices over $\mathbb{F}_{5^2}$ is

$$N(5^2,60,60) = 25^{48}\cdot(25-1)^{12} = 25^{48}\cdot 24^{12}.$$

https://dx.doi.org/10.22108/toc.2025.138779.2097

We consider another special case: $r = n-1$. Keep the notation of Cor. 2.3 and suppose that $x^m - 1$ has t roots (distinct since $p \nmid m$) in $\mathbb{F}_q$. Then $p_q(n, n-1) = t$, the number of distinct monic linear factors of $x^m - 1$ (see (2.8)). There are two cases to be considered for $\phi_{q,n-1}(x^n - 1)$.

If $a > 0$, then since

$$n - 1 = p^a m - 1 \geqslant m = \sum_{k=1}^{M} n(m)_k,$$

all exponents of q in formula (2.7) satisfy $\mu(n-1, s) = n - 1 - s$. Thus similar to (2.10), we have

$$\phi_{q,n-1}(x^n - 1) = q^{n-1} \prod_{i=1}^{M} (1 - q^{-n(m)_i}).$$

If $a = 0$, then $n = m = \sum_{k=1}^{M} n(m)_k$, so the exponents of q in formula (2.7) satisfy $\mu(n-1, s) = n - 1 - s$ except the last term, which is

$$(-1)^M q^{\mu(n-1, \sum_{k=1}^{M} n(m)_k)} = (-1)^M q^0 = (-1)^M.$$

So by adding and subtracting the following term

$$(-1)^M q^{n-1-\sum_{k=1}^{M} n(m)_k} = (-1)^M q^{-1}$$

to formula (2.7), we have

$$\phi_{q,n-1}(x^n - 1) = q^{n-1} \prod_{i=1}^{M} (1 - q^{-n(m)_i}) + (-1)^M (1 - q^{-1}).$$

Summarizing our discussion, we have the following corollary.

Corollary 2.4. *Let p be a prime integer, and let $n = p^a m$, where $m > 0$ and $p \nmid m$. The number of $n \times n$ circulant matrices of rank $n-1$ over $\mathbb{F}_q$, where $q = p^c$, can be computed by the following formula:*

$$\begin{aligned} & N(q, n, n-1) \\ = \; & t(q^{n-1} \prod_{k|m} (1 - q^{-\operatorname{ord}_k(q)})^{\frac{\phi(k)}{\operatorname{ord}_k(q)}} + \delta_{0,a}(-1)^M (1 - q^{-1})) \\ = \; & t(q^{n-m-1} \prod_{k|m} (q^{\operatorname{ord}_k(q)} - 1)^{\frac{\phi(k)}{\operatorname{ord}_k(q)}} + \delta_{0,a}(-1)^M (1 - q^{-1})). \end{aligned} \tag{2.12}$$

where t is the number of roots of $x^m - 1$ in $\mathbb{F}_q$, $M = \sum_{k|m} \frac{\phi(k)}{\operatorname{ord}_k(q)}$, and $\delta_{0,a} = 1$ or 0 according to $a = 0$ or not.

Proof. The corollary follows from Theorem 2.1, Theorem 2.2, and the discussions just before the corollary. □

Example 2.5. *Consider 60×60 circulant matrices of rank 59 over $\mathbb{F}_2$. Since $x^{15} - 1$ has one linear factor over $\mathbb{F}_2$, $t = 1$. Inputing the information in Example 2.2 into formula (2.12) ($q = 2$, $n = 60$, $m = 15$, $a = 2 \neq 0$), we have*

$$N(2, 60, 59) = 2^{60-15-1}(2-1)(2^2-1)(2^4-1)^3 = 2^{44} \cdot 3^4 \cdot 5^3.$$

Consider 60×60 circulant matrices of rank 59 over $\mathbb{F}_{5^2}$. Since $x^{12} - 1$ factors into linear factors over $\mathbb{F}_{5^2}$ (c.f. Example 2.4), $t = 12$. By formula (2.12) ($q = 25$, $m = 12$, $a = 1 \neq 0$), we have

$$N(5^2, 60, 59) = 12 \cdot 25^{47} \cdot (25-1)^{12} = 12 \cdot 25^{47} \cdot 24^{12}.$$

https://dx.doi.org/10.22108/toc.2025.138779.2097

The formulas on the number of circulant matrices of a given rank all depend on the variable $\mathrm{ord}_k(q)$, so we will consider the computation of $\mathrm{ord}_k(q)$ in the next section. Our result will enable us to give the enumerations of the numbers of certain infinite sequences of circulant matrices of given ranks in the forms of integer sequences.

3. **Computing** $\mathrm{ord}_k(q)$

The computation of $\mathrm{ord}_k(q)$ can be reduced to the prime power cases by using the following lemma.

Lemma 3.1. *Let $b > 0$ be an integer and suppose its prime factorization is $b = p_1^{e_1} \cdots p_s^{e_s}$, where the p_i are prime integers and each $e_i \geqslant 1$. Let $n > 1$ be an integer such that $\gcd(b, n) = 1$. If $\mathrm{ord}_{p_i^{e_i}}(n) = h_i$, $1 \leqslant i \leqslant s$, then*

$$\mathrm{ord}_b(n) = \mathrm{lcm}(h_1, \ldots, h_s). \tag{3.1}$$

Proof. It is a basic fact in group theory that if $g = (g_1, \ldots, g_k) \in G_1 \times \cdots \times G_k$ (a direct product of groups), and each g_i has finite order, then the order of g is the least common multiple of the orders of $g_1, \ldots, g_k$. Therefore, the lemma follows from the fact that $\mathbb{Z}_b^* \cong \mathbb{Z}_{p^{e_1}}^* \times \cdots \times \mathbb{Z}_{p^{e_s}}^*$. □

As for the prime power cases, due to the structure differences of the groups $\mathbb{Z}_{p^e}^*$ according to $p = 2$ or not, we shall treat the cases $p = 2$ and $p > 2$ separately. We first consider the odd prime cases. The following lemma reduces the computation of $\mathrm{ord}_{p_i^{e_i}}(n)$ to the base cases.

Lemma 3.2. *Let p be an odd prime, let $n > 1$ be an integer such that $p \nmid n$, and let h be a positive integer such that $h|(p-1)$. Suppose that the order of n in $\mathbb{Z}_{p^i}^*$ is h for $1 \leqslant i \leqslant t$, and the order of n in $\mathbb{Z}_{p^{t+1}}^*$ is ph. Then for any positive integer $e \geqslant t$, the order of n in $\mathbb{Z}_{p^e}^*$ is $p^{e-t}h$.*

Proof. The case $e = t + 1$ is included in the statement of the lemma, so we can assume that $e > t + 1$ ($\geqslant 2$) in our discussion. It is well-known that $\mathbb{Z}_{p^e}^*$ is a cyclic group of order $p^{e-1}(p-1)$ for any odd prime p (see e.g. [1, Theorem 8.9]). So the order, say k, of n in $\mathbb{Z}_{p^e}^*$ is a factor of $p^{e-1}(p-1)$. Let $k = p^r s$, where $0 \leqslant r \leqslant e-1$ and $s|(p-1)$. Let g be a generator of $\mathbb{Z}_{p^e}^*$. Then by the properties of cyclic groups, there is a positive integer b such that

(1) $n = g^b + vp^e$ for some integer v, and
(2) $\gcd(b, p^{e-1}(p-1)) = p^{e-r-1}a$, where $a = (p-1)/s$.

By (2), we can write $b = p^{e-r-1}au$, where u is a positive integer. Then $\gcd(u, p(p-1)) = 1$, thus g^u is also a generator for $\mathbb{Z}_{p^e}^*$. Since $n = (g^u)^{p^{e-r-1}a} + vp^e$, change the generator g if needed, we can assume that $n = g^{p^{e-r-1}a} + vp^e$. We need to show that $r = e - t$ and $s = h$.

Since for each $1 \leqslant i \leqslant e$, $\mathbb{Z}_{p^i}^*$ is cyclic of order $p^{i-1}(p-1)$, $\mathbb{Z}_{p^i}^*$ is a quotient of $\mathbb{Z}_{p^e}^*$. Hence g is also a generator of $\mathbb{Z}_{p^i}^*$ for all $1 \leqslant i \leqslant e$. Notice also that for any $1 \leqslant i \leqslant e$, $n \equiv g^{p^{e-r-1}a} \pmod{p^i}$ and $g^{p^{i-1}(p-1)} \equiv 1 \pmod{p^i}$.

To see that $s = h$, we observe that since $g^{p^k} \equiv g \pmod{p}$ for $k \geqslant 0$, $g^{p^{e-r-1}} \equiv g \pmod{p}$. Hence $n \equiv g^{p^{e-r-1}a} \equiv g^a \pmod{p}$. Thus the order of n in $\mathbb{Z}_p^*$ is $s = (p-1)/a$, which is equal to h by assumption.

If $r > e - t$, then $e - r - 1 < t - 1$. Since the order of $\mathbb{Z}_{p^t}^*$ is $p^{t-1}(p-1)$, the order of $n \equiv g^{p^{e-r-1}a} \pmod{p^t}$ in $\mathbb{Z}_{p^t}^*$ is $p^{t-1}(p-1)/p^{e-r-1}a = p^j h$ for some $j > 0$. This is a contradiction to the assumption.

If $r < e - t$, then $e - r - 1 \geqslant t$. Thus $\gcd(p^{e-r-1}a, p^t(p-1)) = p^t a$. Hence the order of n in $\mathbb{Z}_{p^{t+1}}^*$ is $p^t(p-1)/p^t a = h$, which is also a contradiction to the assumption. So we must have $r = e - t$. □

https://dx.doi.org/10.22108/toc.2025.138779.2097

Next, we consider the case $p = 2$. The structure of $\mathbb{Z}_{2^e}^*$ depends on e, and it is not cyclic for $e \geqslant 3$:

$$\mathbb{Z}_{2^e}^* \cong \begin{cases} \{1\}, & \text{if } e = 1; \\ \mathbb{Z}_2, & \text{if } e = 2; \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}, & \text{if } e \geqslant 3. \end{cases} \tag{3.2}$$

Furthermore, for $e \geqslant 3$, $\mathbb{Z}_{2^e}^*$ is generated by the residues of -1 and 5, and it can be viewed as the direct product of the cyclic subgroups $\langle -1 \rangle$ and $\langle 5 \rangle$ (see e.g. [10, Theorem 2.43]):

$$\mathbb{Z}_{2^e}^* \cong \langle -1 \rangle \times \langle 5 \rangle = \{\pm 1\} \times \{1, 5, 5^2, 5^3, \ldots, 5^{2^{e-2}-1}\}. \tag{3.3}$$

The order of any given odd integer n in $\mathbb{Z}_2^*$ is 1, and its order in $\mathbb{Z}_{2^2}^*$ is either 1 or 2. For other powers of 2, we have a result that is similar to Lemma 3.2. Notice that $\mathbb{Z}_{2^3}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so the order of n in $\mathbb{Z}_{2^3}^*$ must also be either 1 or 2. This is the reason for the assumption that $t \geqslant 3$ in the following lemma. Also, notice that for e large enough, the order of a given odd integer $n > 1$ in $\mathbb{Z}_{2^e}^*$ will be > 2.

Lemma 3.3. *Let $n > 1$ be an odd positive integer. Assume that for some $t \geqslant 3$, the order of n is 2 in $\mathbb{Z}_{2^t}^*$ and is 4 in $\mathbb{Z}_{2^{t+1}}^*$. Then for all $e \geqslant t$, the order of n in $\mathbb{Z}_{2^e}^*$ is 2^{e-t+1}.*

Proof. Though the proof is similar to the proof of Lemma 3.2, some modifications are needed, so we give a detailed proof here. Since the order of the noncyclic group $\mathbb{Z}_{2^e}^*$ is 2^{e-1}, we can assume that the order of n in $\mathbb{Z}_{2^e}^*$ is 2^r for some $0 < r < e-1$. According to (3.3), $n = (-1)^a 5^b + k2^e$, where $a \in \{0, 1\}$, and $0 \leqslant b \leqslant 2^{e-2} - 1$ such that $\gcd(b, 2^{e-2}) = 2^{e-2-r}$. Let $b = 2^{e-2-r}u$, and let $g = 5^u$. Then g also generates the cyclic subgroup $\langle 5 \rangle$ for any $\mathbb{Z}_{2^e}^*$ ($e \geqslant 3$), and $n = (-1)^a g^{2^{e-2-r}} + k2^e$. The factor $(-1)^a$ does not matter since $((-1)^a)^2 = 1$, so we need to show that $r = e - t + 1$. The case that $e = t$ is part of the assumption, so we assume that $e > t$.

If $r > e - t + 1$, then $0 \leqslant e - 2 - r < t - 3$, so $t - 2 - (e - 2 - r) > 1$. Thus from $n \equiv (-1)^a g^{2^{e-2-r}} \pmod{2^t}$, we see that the order of n in $\mathbb{Z}_{2^t}^*$ is $2^{t-2}/2^{e-2-r} > 2$. This is a contradiction to the assumption.

If $r < e - t + 1$, then $t - 1 - e + r < 0$, and so $t - 1 - (e - 2 - r) < 2$. Thus from $n \equiv (-1)^a g^{2^{e-2-r}} \pmod{2^{t+1}}$ (notice that $e > t$), we see that the order of n in $\mathbb{Z}_{2^{t+1}}^*$ is $2^{t-1}/2^{e-2-r} < 2^2 = 4$. This is also a contradiction. Thus we must have $r = e - t + 1$. □

Example 3.1. *Consider the orders of 3 in $\mathbb{Z}_{2^e}^*$, $\mathbb{Z}_{5^e}^*$, and $\mathbb{Z}_{10^e}^*$.*

Some simple computations show that

$$\operatorname{ord}_2(3) = 1, \quad \operatorname{ord}_{2^2}(3) = 2, \quad \operatorname{ord}_{2^3}(3) = 2, \quad \textit{and} \quad \operatorname{ord}_{2^4}(3) = 4.$$

So by Lemma 3.3, $\operatorname{ord}_{2^e}(3) = 2^{e-2}$ for all $e \geqslant 3$.

Since $\operatorname{ord}_5(3) = 4$ and $\operatorname{ord}_{5^2}(3) = 20$, by Lemma 3.2, $\operatorname{ord}_{5^e}(3) = 4 \cdot 5^{e-1}$ for all $e \geqslant 1$.

Now by Lemma 3.1, we have

$$\begin{aligned} \operatorname{ord}_{10}(3) &= \operatorname{lcm}(2, 4) = 4, \\ \operatorname{ord}_{10^2}(3) &= \operatorname{lcm}(2, 20) = 20, \\ \operatorname{ord}_{10^3}(3) &= \operatorname{lcm}(2, 100) = 100, \end{aligned}$$

https://dx.doi.org/10.22108/toc.2025.138779.2097

and for $e \geqslant 4$,

$$\mathrm{ord}_{10^e}(3) = \mathrm{lcm}(2^{e-2}, 4 \times 5^{e-1}) = 2^{e-2}5^{e-1} = 5 \cdot 10^{e-2}.$$

We finish this section by giving an example on using the lemmas in this section in the computation of the numbers of $n \times n$ nonsingular and rank $n-1$ circulant matrices over the field of 9 elements.

Example 3.2. *Let the field be* $\mathbb{F}_{3^2}$ *and let* $n = 3^2 \cdot 5^2 \cdot 7^2$. *According to the notation of Corollary 2.3,* $q = 3^2$ *and* $m = 5^2 \cdot 7^2$. *We have*

$$\mathrm{ord}_5(3^2) = 2,\ \mathrm{ord}_{5^2}(3^2) = 2 \cdot 5,\ \textit{and}$$
$$\mathrm{ord}_7(3^2) = 3,\ \mathrm{ord}_{7^2}(3^2) = 3 \cdot 7.$$

So, $\mathrm{ord}_{5\cdot 7}(3^2) = 2 \cdot 3 = 6$, *etc.. We summarize the information in the table below, where* k *stands for the factors of* m *arranged in ascending order:*

k	1	5	7	5^2	$5 \cdot 7$	7^2	$5^2 \cdot 7$	$5 \cdot 7^2$	$5^2 \cdot 7^2$
$\mathrm{ord}_k(q)$	1	2	3	10	6	21	30	42	210
$\phi(k)/\mathrm{ord}_k(q)$	1	2	2	2	4	2	4	4	4

Thus by formula (2.11), the number of nonsingular circulant matrices of size $3^2 \cdot 5^2 \cdot 7^2$ *over* $\mathbb{F}_9$ *is*

$$\begin{aligned} & N(3^2, 3^2 \cdot 5^2 \cdot 7^2, 3^2 \cdot 5^2 \cdot 7^2) \\ = \ & 9^{8\cdot 25\cdot 49} \cdot (9^1-1) \cdot (9^2-1)^2 \cdot (9^3-1)^2 \cdot (9^{10}-1)^2 \\ & \cdot (9^6-1)^4 \cdot (9^{21}-1)^2 \cdot (9^{30}-1)^4 \cdot (9^{42}-1)^4 \cdot (9^{210}-1)^4, \end{aligned}$$

and by formula (2.12), the number of rank $3^2 \cdot 5^2 \cdot 7^2 - 1$ *circulant matrices over* $\mathbb{F}_9$ *is (only one linear factor,* $t = 1$*)*

$$\begin{aligned} & N(3^2, 3^2 \cdot 5^2 \cdot 7^2, 3^2 \cdot 5^2 \cdot 7^2 - 1) \\ = \ & 9^{8\cdot 25\cdot 49-1} \cdot (9^1-1) \cdot (9^2-1)^2 \cdot (9^3-1)^2 \cdot (9^{10}-1)^2 \\ & \cdot (9^6-1)^4 \cdot (9^{21}-1)^2 \cdot (9^{30}-1)^4 \cdot (9^{42}-1)^4 \cdot (9^{210}-1)^4. \end{aligned}$$

4. Over the field $\mathbb{F}_2$

In this section, we restrict our attention to the field $\mathbb{F}_2$ and consider nonsingular and rank $n-1$ circulant matrices of prime power sizes. We start with some general comments. Let $n = 2^a m$, where $m \geqslant 1$ and $2 \nmid m$. Assume that the prime factorization of m is known. According to formulas (2.11) and (2.12), to obtain the numbers of nonsingular and rank $n-1$ circulant $n \times n$ matrices over $\mathbb{F}_2$, we need to compute the orders of 2 in $\mathbb{Z}_k^*$ for the factors k of m. By using the two lemmas in section 3, we need to find the t such that $\mathrm{ord}_{p^i}(2)$ changes its values after $\mathrm{ord}_{p^t}(2)$. However, even $\mathrm{ord}_p(2)$ is unknown in general. For example, if $p = 2^u - 1$ is a Mersenne prime, then $\mathrm{ord}_p(2) = u$, which is much smaller than $p-1$ (the order of the group $\mathbb{Z}_p^*$). On the other hand, 2 can also be a generator of $\mathbb{Z}_p^*$. For example, in the case $a = 19$, 2 generates $\mathbb{Z}_{19}^*$. Nevertheless, for any given prime p,

https://dx.doi.org/10.22108/toc.2025.138779.2097

the desired t can be computed easily, and then we can enumerate these matrices of sizes $p^k \times p^k$ for all integers $k > 0$. We list the formulas for primes < 20 in the theorem below.

Theorem 4.1. *The formulas below give the numbers of nonsingular and rank $n-1$ circulant $n \times n$ matrices over $\mathbb{F}_2$, where $n = p^b$ ($b \geqslant 1$) for primes $p < 20$:*

$$(p=2) \qquad N(2,2^b,2^b) = 2^{2^b-1}, \quad N(2,2^b,2^b-1) = 2^{2^b-2}.$$

$$(p=3) \qquad N(2,3^b,3^b) = \prod_{i=1}^{b}(2^{2\cdot 3^{i-1}}-1),$$

$$N(2,3^b,3^b-1) = \frac{1}{2}(\prod_{i=1}^{b}(2^{2\cdot 3^{i-1}}-1)+(-1)^{1+b}).$$

$$(p=5) \qquad N(2,5^b,5^b) = \prod_{i=1}^{b}(2^{4\cdot 5^{i-1}}-1),$$

$$N(2,5^b,5^b-1) = \frac{1}{2}(\prod_{i=1}^{b}(2^{4\cdot 5^{i-1}}-1)+(-1)^{1+b}).$$

$$(p=7) \qquad N(2,7^b,7^b) = \prod_{i=1}^{b}(2^{3\cdot 7^{i-1}}-1)^2,$$

$$N(2,7^b,7^b-1) = \frac{1}{2}(\prod_{i=1}^{b}(2^{3\cdot 7^{i-1}}-1)^2-1).$$

$$(p=11) \qquad N(2,11^b,11^b) = \prod_{i=1}^{b}(2^{10\cdot 11^{i-1}}-1),$$

$$N(2,11^b,11^b-1) = \frac{1}{2}(\prod_{i=1}^{b}(2^{10\cdot 11^{i-1}}-1)+(-1)^{1+b}).$$

$$(p=13) \qquad N(2,13^b,13^b) = \prod_{i=1}^{b}(2^{12\cdot 13^{i-1}}-1),$$

$$N(2,13^b,13^b-1) = \frac{1}{2}(\prod_{i=1}^{b}(2^{12\cdot 13^{i-1}}-1)+(-1)^{1+b}).$$

$$(p=17) \qquad N(2,17^b,17^b) = \prod_{i=1}^{b}(2^{8\cdot 17^{i-1}}-1)^2,$$

$$N(2,17^b,17^b-1) = \frac{1}{2}(\prod_{i=1}^{b}(2^{8\cdot 17^{i-1}}-1)^2-1).$$

$$(p=19) \qquad N(2,19^b,19^b) = \prod_{i=1}^{b}(2^{18\cdot 19^{i-1}}-1),$$

$$N(2,19^b,19^b-1) = \frac{1}{2}(\prod_{i=1}^{b}(2^{18\cdot 19^{i-1}}-1)+(-1)^{1+b}).$$

Proof. For the case $n = 2^b$, notice that according to the notation in Corollary 2.3, $p = 2$ and $m = 1$. So for the orders $\mathrm{ord}_k(2)$, the only k we need to consider is 1 (there is only one term in the product part of formulas (2.11) and (2.12)). Since $\mathrm{ord}_1(2) = 1$ and $\phi(1)/\mathrm{ord}_1(2) = 1$, by the first formula of (2.11), we have

$$N(2,2^b,2^b) = 2^{2^b}(1-\frac{1}{2}) = 2^{2^b-1}.$$

https://dx.doi.org/10.22108/toc.2025.138779.2097

Since $x^m - 1 = x - 1$, $t = 1$. Thus

$$N(2, 2^b, 2^b - 1) = 2^{2^b-1}(1 - \frac{1}{2}) = 2^{2^b-2}.$$

The other cases can be derived from (2.11), (2.12), and Lemma 3.2. As an example, we consider the case $n = 7^b$. In this case, $m = n = 7^b$ and $a = 0$ in Cor. 2.3 and Cor. 2.4.

The divisors of m to be considered are $7^i, 0 \leqslant i \leqslant b$. We have $\mathrm{ord}_1(2) = 1$, $\mathrm{ord}_7(2) = 3$, and $\mathrm{ord}_{7^2}(2) = 21$. Thus by Lemma 3.2, for $i > 0$, $\mathrm{ord}_{7^i}(2) = 3 \cdot 7^{i-1}$. For $i = 0$, $\phi(1)/\mathrm{ord}_1(2) = 1$; and for $1 \leqslant i \leqslant b$,

$$\frac{\phi(7^i)}{3 \cdot 7^{i-1}} = \frac{7^{i-1} \cdot 6}{3 \cdot 7^{i-1}} = 2. \tag{4.1}$$

So by the second formula of (2.11), the number of nonsingular $7^b \times 7^b$ matrices over $\mathbb{F}_2$ is

$$\begin{aligned} N(2, 7^b, 7^b) &= 2^{7^b-7^b}(2-1)\prod_{i=1}^{b}(2^{3\cdot 7^{i-1}} - 1)^2 \\ &= \prod_{i=1}^{b}(2^{3\cdot 7^{i-1}} - 1)^2. \end{aligned}$$

As for the rank $n - 1$ ones, since $x^m - 1$ has only one root in $\mathbb{F}_2$, in formula (2.12), $t = 1$; and since $a = 0$, the added term exists. From what we have computed and (4.1), we have

$$M = \sum_{k|7^b} \frac{\phi(k)}{\mathrm{ord}_k(2)} = 1 + 2b.$$

Therefore, by the second formula of (2.11), the number of $n \times n$ ($n = 7^b$) rank $n - 1$ matrices over $\mathbb{F}_2$ is

$$\begin{aligned} N(2, 7^b, 7^b - 1) &= 2^{7^b-7^b-1}(2-1)\prod_{i=1}^{b}(2^{3\cdot 7^{i-1}} - 1)^2 + (-1)^{1+2b}(1 - 2^{-1}) \\ &= \frac{1}{2}(\prod_{i=1}^{b}(2^{3\cdot 7^{i-1}} - 1)^2 - 1). \end{aligned}$$

The proofs are similar for other cases. □

Given a general n, if the factorization of n is known, then we can compute the number of $n \times n$ circulant matrices of any given rank by using the formulas derived in this paper. We finish this paper by listing the numbers (N) of nonsingular circulant matrices over $\mathbb{F}_2$ of sizes $1 \leqslant n \leqslant 31$ in the table below.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
N	1	2	3	8	15	24	49	128	189	480	1023	1536	4095	6272	10125

n	16	17	18	19	20	21	22	23	24
N	32768	65025	96768	262143	491520	583443	2095104	4190209	6291456

Acknowledgments

https://dx.doi.org/10.22108/toc.2025.138779.2097

n	25	26	27	28	29	30	31
N	15728625	67092480	49545027	102760448	268435455	331776000	887503681

Wei acknowledges the supports of Innovation Project of Guangxi Graduate Education (JGY2025281), and Guangxi Science and Technology Base and Talent Special Program (AD23023003). Zou acknowledges the support of a Simons Foundation Collaboration Grant for Mathematicians (416937).

References

[1] D. Burton, *Elementary number theory*, McGraw Hill Companies, 7th ed., 2010.

[2] M. C. R. Butler, The irreducible factors of $f(x^m)$ over a finite field, *J. London Math. Soc.*, **30** (1955) 480–482.

[3] P. J. Davis, *Circulant matrices*, AMS Chelsea Publishing, 1994.

[4] D. E. Daykin, On the rank of the matrix $f(A)$ and the enumeration of certain matrices over a finite field, *J. London Math. Soc.*, **35** (1960) 36–42.

[5] A. W. Ingleton, The rank of circulant matrices, *J. London Math. Soc.*, **31** (1956), 632–635.

[6] D. Kalman and J. E. White, Polynomial equations and circulant matrices, *Amer. Math. Monthly*, **108** no. 9 (2001) 821–840.

[7] I. Kra and S. R. Simanca, On circulant matrices, *Notices Amer. Math. Soc.*, *59* no. 3 (2012) 368–377.

[8] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 2000.

[9] M. Liu and S. M. Sim, Lightweight MDS generalized circulant matrices, *International Conference on Fast Software Encryption 2016*, 101–120.

[10] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers*, Fifth edition, John Wiley & Sons, Inc., New York, 1991.

[11] Y. Zhao and D. D. Lin, Nonsingular circulant matrices over finite fields, *J. of Graduate University of Chinese Academy of Sciences*, **29** no. 6 (2012) 805–814.

Yangjiang Wei

School of Mathematics and Statistics, Nanning Normal University, and Center for Applied Mathematics of Guangxi at Nanning Normal University, Nanning, P. R. China

Email: gus02@163.com

Yi Ming Zou

Department of Mathematical Sciences, University of Wisconsin, Milwaukee, USA

Email: ymzou@uwm.edu

https://dx.doi.org/10.22108/toc.2025.138779.2097