Cyclic p-roots of prime length p and related complex Hadamard matrices

Uffe Haagerup

Abstract

In this paper it is proved, that for every prime number p, the set of cyclic p-roots in $\mathbb{C}^p$ is finite. Moreover the number of cyclic p-roots counted with multiplicity is equal to $\binom{2p-2}{p-1}$. In particular, the number of complex circulant Hadamard matrices of size p, with diagonal entries equal to 1, is less than or equal to $\binom{2p-2}{p-1}$.

1 Introduction

In [Bj], Göran Björck introduced the cyclic n-roots for every $n \in \mathbb{N}$ $(n \geq 2)$ as the solutions $z = (z_0, \ldots, z_{n-1}) \in \mathbb{C}^n$ to the following n polynomial equations:

$$\begin{aligned} z_0 + z_1 + \ldots + z_{n-1} &= 0 \\ z_0 z_1 + z_1 z_2 + \ldots + z_{n-1} z_0 &= 0 \\ &\vdots \\ z_0 z_1 \cdot \ldots \cdot z_{n-2} + \ldots + z_{n-1} z_0 \cdot \ldots \cdot z_{n-3} &= 0 \\ z_0 z_1 \cdot \ldots \cdot z_{n-1} &= 1 \end{aligned} \tag{1.1}$$

This system of equations is invariant under cyclic permutation of the indices $(0, 1, \ldots, n-1)$. The motivation for studying the system of equations (1.1) was to study bi-unimodular sequences of length n, i.e. elements $(x_0, x_1, \ldots, x_{n-1})$ in $\mathbb{C}^n$ for which

$$|x_j| = 1 \quad \text{and} \quad |\hat{x}_j| = 1 \quad \text{for} \quad 0 \leq j \leq n-1$$

where $\hat{x} = (\hat{x}_0, \hat{x}_1, \ldots, \hat{x}_{n-1})$ is the Fourier Transformed of x w.r.t. the group $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, i.e.

$$\hat{x}_j = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \mathrm{e}^{\mathrm{i}2\pi jk/n} x_k, \quad 0 \leq j \leq n-1. \tag{1.2}$$

If $x = (x_0, \ldots, x_{n-1}) \in \mathbb{C}^n$ and $|x_j| = 1$, $1 \leq j \leq n$, then by [Bj], x is a biunimodular sequence if and only if

$$(z_0, \ldots, z_{n-1}) = \Big(\frac{x_1}{x_0}, \frac{x_2}{x_1}, \ldots, \frac{x_{n-1}}{x_{n-2}}, \frac{x_0}{x_{n-1}}\Big)$$

is a cyclic n-root, and this gives a one-to-one correspondence between bimodular sequences $(x_0, x_1, \ldots, x_{n-1})$ with $x_0 = 1$ and cyclic n-roots of modulus 1.

A complex Hadamard matrix of size n is a matrix

$$H = (h_{jk})_{j,k=0,\ldots,n-1}$$

for which all entries are complex numbers with modulus 1, and

$$H^*H = nI.$$

Moreover H is called circulant, if the entries h_{jk} only depend on $j-k$ (calculated modulo n). By [BS] a $n \times n$ matrix H is a complex circulant Hadamard matrix if and only if

$$h_{jk} = x_{j-k}, \quad j,k \in \{0,\dots,n-1\}$$

for a biunimodular sequence $x = (x_0,\dots,x_{n-1})$ (again, indices must be calculated modulo n). Hence there is also a one-to-one correspondence between complex cyclic n roots and circulant Hadamard matrices of size n with diagonal entries equal to 1.

It is elementary to solve the cyclic n-root problem (1.1) for $n = 2, 3$ and 4. In 1991-92 Björck and Fröberg found all cyclic n-roots for $5 \le n \le 8$ by computer algebra methods (cf. [BF1] and [BF2]), for the case $n = 7$ see also [BaF]. Moreover in 2001 Faugère found all cyclic 9-roots by developing more advanced software for computer algebra (cf. [Fa]). For $2 \le n \le 9$, the total number $\gamma(n)$ of cyclic n-roots and the number $\gamma_u(n)$ of cyclic n-roots of modulus 1 are given by the table:

n	2	3	4	5	6	7	8	9
$\gamma(n)$	2	6	∞	70	156	924	∞	∞
$\gamma_u(n)$	2	6	∞	20	48	532	∞	∞

For further results on cyclic n-roots and circulant Hadamard matrices, see also [Ha].

Based on the values of $\gamma(n)$ for $n = 2, 3, 5$ and 7. Ralf Fröberg conjectured that $\gamma(p) = \binom{2p-2}{p-1}$ for all prime numbers p. In this paper we will prove, that for every prime number p, the number of cyclic p-roots counted with multiplicity is equal to $\binom{2p-2}{p-1}$. For $p = 2, 3, 5$ and 7 all the cyclic p-roots have multiplicity 1, but we do not know, whether this holds for all primes. In the non-prime case $n = 9$, Faugère found isolated cyclic 9-roots with multiplicity 4 (cf. [Fa]).

Let us next outline the main steps in our proof. In section 2 we prove that there is a one-to-one correspondence between solutions to (1.1) and solutions to the following system of $2n-2$ equations in $2n-2$ variables $(x_1,\dots,x_{n-1},y_1,\dots,y_{n-1})$,

$$\begin{aligned} x_j y_j &= 1, \quad 1 \le j \le n-1 \\ \hat{x}_j \hat{y}_{-j} &= 1, \quad 1 \le j \le n-1 \end{aligned} \tag{1.3}$$

where $x = (1, x_1,\dots,x_{n-1})$, $y = (1, y_1,\dots,y_{n-1})$ and $\hat{x}, \hat{y}$ are the Fourier transformed vectors of x and y as defined by (1.2).

In section 3, we prove that for every prime number p, the set of solutions to (1.3) with $n = p$ is a finite set. The proof is based on a Theorem of Chebotarëv from 1926, which asserts, that when p is a prime number, then all square sub-matrices of the matrix

$$(\mathrm{e}^{\mathrm{i}2\pi jk/p})_{j,k=0,\dots,p-1}$$

are non-singular. Having only finitely many solutions to (1.3) the same holds for (1.1), but in order to count the number of solutions in (1.3) and (1.1), we have in section 4 collected a number of (mostly) well known results on multiplicity of proper holomorphic functions $\varphi\colon U \to V$, where U, V are regions in $\mathbb{C}^n$, and on multiplicity of the isolated zeros of such a

function. The main result needed is that for all $w \in V$, the number of solutions to $\varphi(z) = w$ (i.e. the number of zeros of $\varphi_w : z \to \varphi(z) - w$) counted with multiplicity is equal to the multiplicity of φ, and it is therefore independent of $w \in V$ (cf. Theorem 4.8). Using this we can count the number of solutions to (1.3) with multiplicity, by counting instead the solutions $(x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1}) \in \mathbb{C}^{2p-2}$ to

$$\begin{array}{ll} x_j y_j = 0, & 1 \le j \le p-1 \\ \hat{x}_j \hat{y}_{-j} = 0, & 1 \le j \le p-1 \end{array} \tag{1.4}$$

where $x = (1, x_1, \ldots, x_{p-1})$ and $y = (1, y_1, \ldots, y_{p-1})$ as in (1.3). The latter problem can be solved by linear algebra (cf. section 5) and it has exactly $\binom{2p-2}{p-1}$ solutions all with multiplicity 1. Hence (1.3) has $\binom{2p-2}{p-1}$ solutions counted with multiplicity.

It is clear from section 2, that (1.1) and (1.3) has the same number of distinct solutions. In section 6, we prove that the same also holds when solutions are counted according to their multiplicities. This is not obvious, because, when passing from (1.3) to (1.1) the number of variables is changed twice in the process, first from $2p-2$ to $p-1$ and next from $p-1$ to p.

In section 7, we use the methods from the previous sections to count the number of cyclic p-roots of simple index k, where $k \in \mathbb{N}$ divides $p-1$. Following [Bj] and [BH] a cyclic p-root has simple index k, if the corresponding cyclic p-root on x-level is constant on the cosets of the unique index k subgroup of $(\mathbb{Z}_p^*, \cdot)$. The cyclic p-roots of simple index k can be determined by solving the following set of equations in k variables $c_0, c_1, \ldots, c_{k-1} \in \mathbb{C}^*$:

$$c_a + \frac{1}{c_{a+m}} + \sum_{i,j=0}^{k-1} n_{ij} \frac{c_{j+a}}{c_{i+a}} = 0 \quad (0 \le a \le k-1) \tag{1.5}$$

where m and n_{ij} are certain integers depending on p and k (cf. [Bj] and section 7 of this paper for more details). For $k = 1, 2, 3$ all cyclic p-roots of simple index k has been explicitly computed in [Bj] and [BH]. The number of distinct cyclic p-roots of simple index k is 2 (resp. 6, 20) for $k = 1$ (resp. 2, 3) for all primes for which k divides $p-1$. We prove in Theorem 7.1 that the number of solutions to (1.5) counted with multiplicity is equal to $\binom{2k}{k}$ for all $k \in \mathbb{N}$ and all primes for which k divides $p-1$.

Acknowledgement

I wish to thank Göran Björck for many fruitful discussions on cyclic n-roots, since we first met in 1992, and for constantly encouraging me to write up a detailed proof of the main result of this paper after a very preliminary version of the proof was communicated to him in the summer of 1996. I also wish to thank Bahman Saffari for his interest in this result and for giving me the opportunity to present it at the workshop on Harmonic Analysis and Number Theory at CIRM/Luminy, October 2005.

2 Reformulations of the cyclic n-root problem

Recall that the cyclic n-roots are the solutions $z = (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{C}^n$ to the system of equations:

$$\begin{aligned} z_0 + z_1 + \ldots + z_{n+1} &= 0 \\ z_0z_1 + z_1z_2 + \ldots + z_{n-1}z_0 &= 0 \\ &\vdots \\ z_0z_1 \cdot \ldots \cdot z_{n-2} + \ldots + z_{n-1}z_0 \cdot \ldots \cdot z_{n-3} &= 0 \\ z_0z_1 \cdot \ldots \cdot z_{n-1} &= 1 \end{aligned} \tag{2.1}$$

Note that by the last equation $z_i \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ for every cyclic n-root $z = (z_0, \ldots, z_{n-1})$. Let $z \in (\mathbb{C}^*)^n$ be a cyclic n-root, and define $x = (x_0, \ldots, x_{n-1}) \in (\mathbb{C}^*)^n$ by

$$x_0 = 1,\ x_1 = z_0,\ x_2 = z_0z_1,\ \ldots,\ x_{n-1} = z_0z_1 \cdot \ldots \cdot z_{n-2} \tag{2.2}$$

Then clearly

$$\frac{x_{j+1}}{x_j} = z_j, \quad j = 0, 1, \ldots, n-2$$

and by the last equation in (2.1) the same formula also holds for $j = n-1$. Moreover, by the first $n-1$ equations in (2.1), $x = (x_0, \ldots, x_{n-1})$ is a solution to

$$\begin{aligned} x_0 &= 1 \\ \frac{x_1}{x_0} + \frac{x_2}{x_1} + \ldots + \frac{x_0}{x_{n-1}} &= 0 \\ \frac{x_2}{x_0} + \frac{x_3}{x_1} + \ldots + \frac{x_1}{x_{n-1}} &= 0 \\ &\vdots \\ \frac{x_{n-1}}{x_0} + \frac{x_0}{x_1} + \ldots + \frac{x_{n-2}}{x_{n-1}} &= 0 \end{aligned} \tag{2.3}$$

Conversely if $x = (x_0, \ldots, x_{n-1}) \in (\mathbb{C}^*)^n$ is a solution to (2.3), then

$$(z_0, z_1, \ldots, z_{n-1}) = \Big(\frac{x_1}{x_0}, \frac{x_2}{x_1}, \ldots, \frac{x_0}{x_{n-1}}\Big)$$

is a solution to (2.1). *We will call the solutions to (2.3) cyclic n-roots on x-level.*

Instead of imposing the condition $x_0 = 1$, it would be equivalent to look for solutions to the last $n-1$ equations of (2.3) in the subset $(\mathbb{C}^*)^n/\sim$ of the complex projective space $P_{n-1} = (\mathbb{C}^n \setminus \{0\})/\sim$, where $x, x' \in \mathbb{C}^n \setminus \{0\}$ are equivalent ($x \sim x'$) iff $x' = cx$ for some $c \in \mathbb{C}^*$.

Suppose $x = (x_0, \ldots, x_{n-1}) \in (\mathbb{C}^*)^n$ is a solution to (2.3), and put $y_j = \frac{1}{x_j}$, $j = 0, \ldots, n-1$. Then

$$(x, y) = (x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}) \in \mathbb{C}^n \times \mathbb{C}^n$$

is a solution to

$$\begin{aligned} x_0 = y_0 &= 1 \\ x_k y_k &= 1 \text{ for } 1 \le k \le n-1 \\ \sum_{m=0}^{n-1} x_{k+m} y_m &= 0 \text{ for } 1 \le k \le n-1 \end{aligned} \tag{2.4}$$

where again all indices are counted modulo n. Conversely if $(x, y) \in \mathbb{C}^n \times \mathbb{C}^n$ is a solution to (2.4), then $x \in (\mathbb{C}^*)^n$ and x is a solution to (2.3), because $x_n y_n = 1$ for $0 \le k \le n-1$. *We will call the solutions* $(x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1}) \in \mathbb{C}^n \times \mathbb{C}^n$ *to (2.4) cyclic* n*-roots on* (x, y)*-level.*

Instead of imposing the conditions $x_0 = y_0 = 1$, it would be equivalent to look for solutions to

$$\begin{aligned} x_k y_k &= x_0 y_0, \quad 1 \le k \le n-1 \\ \sum_{m=0}^{n-1} x_{k+m} y_m &= 0, \quad 1 \le k \le n-1 \end{aligned} \tag{2.5}$$

in the subset $(\mathbb{C}^*)^n/\!\sim \times (\mathbb{C}^*)^n/\!\sim$ of $P_{n-1} \times P_{n-1}$.

Lemma 2.1. *Let* $n, v \in \mathbb{C}^n$ *and let* $\hat{u}, \hat{v} \in \mathbb{C}^n$ *be the transformed vectors, i.e.*

$$\hat{u} = Fu, \quad \hat{v} = Fv$$

where F *is the unitary matrix*

$$F = \frac{1}{\sqrt{n}} \left(\mathrm{e}^{\mathrm{i}2\pi jk/n} \right)_{j,k=0,\dots,n-1}$$

Still calculating indices cyclic modulo n*, we have*

$$\hat{u}_j \hat{v}_{-j} = \frac{1}{n} \sum_{k=0}^{n-1} \mathrm{e}^{\mathrm{i}2\pi jk/n} \Big(\sum_{m=0}^{n-1} u_{k+m} v_m \Big), \quad 0 \le j \le n-1 \tag{2.6}$$

$$\sum_{j=0}^{n-1} \mathrm{e}^{-\mathrm{i}2\pi kj/n} \hat{u}_j \hat{v}_j = \sum_{m=0}^{n-1} u_{k+m} v_m, \qquad 0 \le k \le n-1 \tag{2.7}$$

In particular

$$\sum_{j=0}^{n-1} \hat{u}_j \hat{v}_{-j} = \sum_{m=0}^{n-1} u_m v_m \tag{2.8}$$

Proof. Let $0 \le j \le n-1$. Then

$$\hat{u}_j \hat{v}_{-j} = \frac{1}{n} \sum_{l,m=0}^{n-1} \mathrm{e}^{\mathrm{i}2\pi j(l-m)/n} u_k v_m.$$

Hence, if we replace (l, m) with $(k + m, m)$ in the double sum, we get

$$\begin{aligned}\hat{u}_j\hat{v}_{-j} &= \frac{1}{n}\sum_{k,m=0}^{n-1} \mathrm{e}^{\mathrm{i}2\pi jk/n}u_{k+m}v_m \\ &= \frac{1}{n}\sum_{k=0} n-1\mathrm{e}^{\mathrm{i}2\pi jk/n}\Big(\sum_{m=0}^{n-1} u_{k+m}v_m\Big),\end{aligned}$$

which proves (2.6). Note that (2.6) can also be written as

$$\Big(\hat{u}_j\hat{v}_{-j}\Big)_{j=0}^{n-1} = \frac{1}{\sqrt{n}}F\bigg(\Big(\sum_{m=0}^{n-1} u_{k+m}v_m\Big)_{k=0}^{n-1}\bigg).$$

Since F is unitary and symmetric, $F^{-1} = \overline{F}$ (complex conjugation). Thus

$$\sqrt{n}\,\overline{F}\bigg(\Big(\hat{u}_j\hat{u}_{-j}\Big)_{j=0}^{n-1}\bigg) = \Big(\sum_{m=0}^{n-1} u_{k+m}v_m\Big)_{k=0}^{n-1}$$

which proves (2.7). (2.8) is the special case $k = 0$ of (2.7). Note that (2.8) can also be proved by applying Parseval's formula

$$\sum_{j=0}^{n-1} \hat{u}_j\overline{\hat{w}}_j = \sum_{m=0}^{n-1} u_m\overline{w}_m$$

to $w = \overline{v}$. □

Proposition 2.2. *The equations (2.4) for cyclic n-roots on (x, y)-level are equivalent to the following set of equations for $(x, y) \in \mathbb{C}^n \times \mathbb{C}^n$.*

$$\begin{aligned} x_0 = y_0 &= 1 \\ x_k y_k &= 1, \quad 1 \le k \le n-1 \\ \hat{x}_k\hat{y}_{-k} &= 1, \quad 1 \le k \le n-1 \end{aligned} \tag{2.9}$$

where $\hat{x} = Fx$ and $\hat{y} = Fy$ as in lemma 2.1.

Proof. Assume (x, y) is a solution to (2.4). By the last $n - 1$ equations of (2.4),

$$\sum_{m=0}^{n-1} x_{k+m}y_m = 0 \qquad 1 \le k \le n-1$$

and by the first $n + 1$ equations of (2.4)

$$\sum_{m=0}^{n-1} x_m y_m = n$$

Hence, by (2.6)

$$\begin{aligned}\hat{x}_j\hat{y}_{-j} &= \frac{1}{n}\sum_{k=0}^{n-1} \mathrm{e}^{\mathrm{i}2\pi jk/n}\Big(\sum_{m=0}^{n-1} u_{k+m}v_m\Big) \\ &= \frac{1}{n}(n + 0 + \ldots + 0) \\ &= 1\end{aligned}$$

for $j = 0, \ldots, n-1$. Hence (2.4) implies (2.9). Conversely if $(x, y) \in \mathbb{C}^n \times \mathbb{C}^n$ satisfies (2.9), then

$$\hat{x}_j \hat{y}_{-j} = 1 \quad \text{for} \quad 1 \le j \le k$$

By (2.8) and the first $n+1$ equations of (2.9),

$$\sum_{j=0}^{n-1} \hat{x}_j \hat{y}_{-j} = \sum_{m=0}^{n-1} x_m y_m = n$$

and therefore

$$\hat{x}_0 \hat{y}_0 = n - \sum_{j=1}^{n-1} \hat{x}_j \hat{y}_{-j} = n - (n-1) = 1$$

Thus by (2.7)

$$\begin{aligned} \sum_{k=0}^{n-1} x_{k+m} y_m &= \sum_{j=0}^{n-1} \mathrm{e}^{-\mathrm{i}2\pi kj/n} \hat{u}_j \hat{v}_{-j} \\ &= \sum_{j=0}^{n-1} \mathrm{e}^{-\mathrm{i}2\pi kj/n} \\ &= 0 \quad \text{for} \quad 1 \le k \le n-1 \end{aligned}$$

Hence (2.9) implies (2.4). □

For later use, (cf. proof of Corollary 5.4.) we prove the following extension of Proposition 2.2.

Proposition 2.3. *Let $a_1, \ldots, a_{n-1}, c_1, \ldots, c_{n-1} \in \mathbb{C}$. Then for $(x, y) \in \mathbb{C}^n \times \mathbb{C}^n$, the set of equations*

$$\begin{aligned} x_0 = y_0 &= 1 \\ x_k y_k &= a_k, \quad 1 \le k \le n-1 \\ \sum_{m=0}^{n-1} x_{k+m} y_m &= c_k, \quad 1 \le k \le n-1 \end{aligned} \tag{2.10}$$

is equivalent to

$$\begin{aligned} x_0 = y_0 &= 1 \\ x_k y_k &= a_k, \quad 1 \le k \le n-1 \\ \hat{x}_k \hat{y}_{-k} &= b_k, \quad 1 \le k \le n-1 \end{aligned} \tag{2.11}$$

where

$$b_j = \frac{1}{n}\left(1 + \sum_{m=1}^{n-1} a_m + \sum_{k=1}^{n-1} \mathrm{e}^{\mathrm{i}2\pi jk/n} c_k\right), \quad 1 \le j \le n-1 \tag{2.12}$$

Moreover for fixed $a_1, \ldots, a_{n-1}, b_1, \ldots, b_{n-1} \in \mathbb{C}$, the $n-1$ equations (2.12) have a unique solution $(c_1, \ldots, c_{n-1}) \in \mathbb{C}^{n-1}$) given by

$$c_k = 1 + \sum_{m=1}^{n-1} a_m + \sum_{j=1}^{n-1} (\mathrm{e}^{-\mathrm{i}2\pi kj/n} - 1) b_j, \quad 1 \le k \le n-1. \tag{2.13}$$

Proof. Assume (2.10). Then

$$\sum_{m=0}^{n-1} x_m y_m = 1 + \sum_{m=1}^{n-1} a_m.$$

Hence by (2.6) and the last $(n-1)$ equations in (2.10)

$$\begin{aligned}\hat{x}_j \hat{y}_{-j} &= \frac{1}{n}\Big(\sum_{m=1}^{n-1} x_m y_m + \sum_{k=1}^{n-1} \mathrm{e}^{\mathrm{i}2\pi jk/n}\Big(\sum_{m=0}^{n-1} x_{k+m} y_m \Big)\Big) \\ &= \frac{1}{n}\Big(1 + \sum_{m=1}^{n-1} a_m + \sum_{k=1}^{n-1} \mathrm{e}^{\mathrm{i}2\pi jk/n} c_k \Big)\end{aligned}$$

for $0 \le j \le n-1$. Hence (2.10) implies (2.11), with $b_1, \dots, b_{n-1}$ as in (2.12).

We next show that (2.12) implies (2.13). Put

$$b_0 = \frac{1}{n}\Big(1 + \sum_{m=1}^{n-1} a_m + \sum_{k=1}^{n-1} c_k \Big).$$

Then (2.12) holds for $0 \le j \le n-1$. Hence, if we furthermore put

$$c_0 = 1 + \sum_{m=1}^{n-1} a_m,$$

then

$$b_j = \frac{1}{n} \sum_{k=0}^{n-1} \mathrm{e}^{\mathrm{i}2\pi jk/n} c_k, \quad j = 0, \dots, n-1.$$

Hence, by Fourier inversion, we have

$$c_k = \sum_{j=0}^{n-1} \mathrm{e}^{-\mathrm{i}2\pi jk/n} b_j, \quad k = 0, \dots, n-1 \tag{2.14}$$

In particular

$$1 + \sum_{m=1}^{n-1} a_m = c_0 = b_0 + \sum_{j=1}^{n-1} b_j.$$

Therefore

$$b_0 = 1 + \sum_{m=1}^{n-1} a_m - \sum_{j=1}^{n-1} b_j$$

which inserted in (2.14) gives

$$\begin{aligned} c_k &= b_0 + \sum_{j=1}^{n-1} \mathrm{e}^{-\mathrm{i}2\pi jk/n} b_j \\ &= 1 + \sum_{m=1}^{n-1} a_m + \sum_{j=1}^{n-1} (\mathrm{e}^{-\mathrm{i}2\pi jk/n} - 1) b_j, \quad 0 \le k \le n-1 \end{aligned}$$

which proves (2.13).

Finally, we show that (2.11) implies (2.10), when (2.12) holds (or equivalently (2.13) holds). Assume $(x, y) \in \mathbb{C}^n \times \mathbb{C}^n$ satisfies (2.11) for given $a_1, \ldots, a_{n-1}, b_1, \ldots, b_{n-1} \in \mathbb{C}$. By (2.11) and (2.8) we get

$$1 + \sum_{m=1}^{n-1} a_m = \sum_{m=0}^{n-1} x_m y_m = \sum_{j=0}^{n-1} \hat{x}_j \hat{y}_{-j} = \hat{x}_0 \hat{y}_0 + \sum_{j=1}^{n-1} bj.$$

Therefore

$$\hat{x}_0 \hat{y}_0 = 1 + \sum_{m=1}^{n-1} a_m - \sum_{j=1}^{n-1} b_j \tag{2.15}$$

Hence by (2.7) we have for $0 \le k \le n-1$,

$$\begin{aligned} \sum_{m=0}^{n-1} x_{k+m} y_m &= \sum_{j=0}^{n-1} \mathrm{e}^{-\mathrm{i}2\pi kj/b} \hat{x}_j \hat{y}_{-j} \\ &= \hat{x}_0 \hat{y}_0 + \sum_{j=0}^{n-1} \mathrm{e}^{-\mathrm{i}2\pi kj/n} bj \\ &= 1 + \sum_{m=1}^{n-1} a_m + \sum_{j=0}^{n-1} (\mathrm{e}^{-\mathrm{i}2\pi kj/n} - 1) b_j. \end{aligned}$$

Thus (2.11) implies (2.10) with $c_1, \ldots, c_{n-1}$ given by (2.13). □

3 Finiteness of the set of cyclic p-roots of prime length p

We shall use the following two classical results:

Theorem 3.1. *A compact algebraic variety in $\mathbb{C}^n$ is a finite set.*

Proof. This is well known, see e.g. [Ru, Thm 14.3.i].

Theorem 3.2. *(Chebotarëv, 1926). Let p be a prime number and let F_p denote the unitary matrix of Fourier transform on $\mathbb{C}^p$:*

$$F_p = \Big(\frac{1}{\sqrt{p}} \mathrm{e}^{\mathrm{i}2\pi kl/p} \Big)_{k,l=0,\ldots,p-1}.$$

Then for every two finite subsets $K, L \subseteq \{0, \ldots, p-1\}$ of the same size $|K| = |L| \ge 1$, the corresponding submatrix

$$(F_p)_{K \times L} = \Big(\frac{1}{\sqrt{p}} \mathrm{e}^{\mathrm{i}2\pi kl/p} \Big)_{k \in K, l \in L}$$

has non-zero determinant.

Proof. See [SL, p. 29-30] and references given there.

The following application of Chebotarëv's Theorem has been known to the author since 1996. After the results of this paper were presented at CIRM in October 2005, we learned, that it has been proved independently by Terence Tao (cf. [Ta, Thm 1.1]). In the same paper, Tao also presents a short and selfcontained proof of Chebotarëv's theorem.

Proposition 3.3. *Let $u = (u_0, \dots, u_{p-1}) \in \mathbb{C}^p$ and let $\hat{u} = F_p u$ be the Fourier transformed vector. If $u \neq 0$, then*

$$|supp(u)| + |supp(\hat{u})| \geq p + 1 \tag{3.1}$$

where for $z \in \mathbb{C}^p$, $|supp(z)|$ denotes the number of $i \in \{0, 1, \dots, p-1\}$ for which $z_i \neq 0$.

Proof. Let p be a prime number, let $u \in \mathbb{C}^p \setminus \{0\}$, assume that

$$|\mathrm{supp}(u)| + |\mathrm{supp}(\hat{u})| \leq p.$$

Put $L = \mathrm{supp}(u)$ and note that $L \neq \emptyset$. Moreover

$$|\mathbb{Z}_p \setminus \mathrm{supp}(\hat{u})| = p - |\mathrm{supp}(\hat{u})| \geq |\mathrm{supp}(u)| = |L|.$$

Hence, we can choose $K \subseteq \mathbb{Z}_p \setminus \mathrm{supp}(\hat{u})$, such that $|K| = |L|$. For every $k \in K$

$$\frac{1}{\sqrt{p}} \sum_{l \in L} \mathrm{e}^{\mathrm{i}2\pi kl/n} u_l = \hat{u}_k = 0. \tag{3.2}$$

By Chebotarëv's Theorem (Theorem 3.2), the matrix

$$\Big(\frac{1}{\sqrt{p}} \mathrm{e}^{\mathrm{i}2\pi kl/n} \Big)_{k \in K, l \in L}$$

has non-zero determinant. Hence by (3.2) $u_l = 0$ for all $l \in L = \mathrm{supp}(\hat{u})$, which implies that $u = 0$ and we have reached a contradictim. Therefore (3.1) holds for every $u \in \mathbb{C}^p \setminus \{0\}$. □

Lemma 3.4. *Let $n \in \mathbb{N}$. If the number of solutions $(x, y) \in \mathbb{C}^n \times \mathbb{C}^n$ to (2.9) is infinite, then there exists $u, v \in \mathbb{C}^n \setminus \{0\}$, such that*

$$u_k v_k = 0 \quad \textit{and} \quad \hat{u}_k \hat{v}_{-k} = 0$$

for $k = 0, 1, \dots, n-1$.

Proof. Let $W \subseteq \mathbb{C}^n \times \mathbb{C}^n$ be the set of solutions to the $2n$ polynomial equations (2.9) and assume that W have infinite many elements. Since W is an algebraic variety, we get by Theorem 3.1 and the Heine-Borel Theorem, that W is an unbounded set. Put

$$\|z\|_2 = \Big(\sum_{j=0}^{n-1} |z_j|^2 \Big)^{\frac{1}{2}}, \quad z \in \mathbb{C}^n.$$

We choose a sequence of elements $(x^{(m)}, y^{(m)})$ in W, $(m \in \mathbb{N})$ such that

$$\lim_{n \to \infty} \big(\|x^{(m)}\|_2^2 + \|y^{(m)}\|_2^2 \big)^{\frac{1}{2}} = +\infty. \tag{3.3}$$

Put next

$$u^{(m)} = \frac{1}{\|x^{(m)}\|_2} x^{(m)}, \quad v^{(m)} = \frac{1}{\|y^{(m)}\|_2} y^{(m)}.$$

Then $\|u^{(m)}\|_2 = \|v^{(m)}\|_2 = 1$, i.e. $(u^{(m)}, v^{(m)}) \in S^{2n-1} \times S^{2n-1}$ where S^{2n-1} denotes the unit sphere in $\mathbb{C}^n$. Since $S^{2n-1} \times S^{2n-1}$ is compact, we can by passing to a subsequence assume that

$$\lim_{m\to\infty} (u^{(m)}, v^{(m)}) = (u, v)$$

for some $u, v \in S^{2n-1}$. Since $x, y \in W$, $x_0^{(m)} = y_0^{(m)} = 1$ for all $m \in \mathbb{N}$. Therefore

$$\|x^{(m)}\|_2^2 = 1 + c_m, \quad \|y^{(m)}\|_2^2 = 1 + d_m$$

for some non-negative real numbers c_m, d_m. Thus

$$\|x^{(m)}\|_2^2 \|y^{(m)}\|_2^2 = (1 + c_m)(1 + d_m) \geq 1 + c_m + d_m = \|x^{(m)}\|_2^2 + \|y^{(m)}\|_2^2 - 1.$$

Hence by (3.3),

$$\lim_{n\to\infty} \|x^{(m)}\|_2 \|y^{(m)}\|_2 = +\infty. \tag{3.4}$$

Since $(x^{(m)}, y^{(m)})$ satisfies (2.9) for all m, we have for $1 \leq k \leq n-1$

$$x_k^{(m)} y_k^{(m)} = 1, \quad \widehat{x_k^{(m)}}\,\widehat{y_{-k}^{(m)}} = 1$$

and the same equalities holds for $k = 0$, by (2.8) combined with $x_0^{(m)} = y_0^{(m)} = 1$. Therefore

$$u_k v_k = \hat{u}_k \hat{v}_{-k} = \lim_{m\to\infty} \left(\|x^{(m)}\|_2 \|y^{(m)}\|_2\right)^{-1} = 0$$

for $0 \leq k \leq n-1$, which proves lemma 3.4. □

Theorem 3.5. *Let p be a prime number, then the set of cyclic p-roots is finite.*

Proof. The transformations of the cyclic n-root problem in section 2 from (2.1) to (2.3) and later from (2.3) to (2.4) and (2.9) do not change the number of distinct solutions. Therefore it is sufficient to show, that the set of solutions W to (2.9) is finite in the case $n = p$.

Assume $|W| = +\infty$. Then by lemma 3.5 there exist $u, v \in \mathbb{C}^p \setminus \{0\}$, such that

$$u_k v_k = 0 \quad \text{and} \quad \hat{u}_k \hat{v}_{-k} = 0$$

for $k = 0, 1, \ldots, p-1$, i.e.

$$\operatorname{supp}(u) \cap \operatorname{supp}(v) = \emptyset \quad \textit{and} \quad \operatorname{supp}(\hat{u}) \cap (-\operatorname{supp}(\hat{v})) = \emptyset$$

Hence

$$|\operatorname{supp}(u)| + |\operatorname{supp}(v)| \leq p \quad \textit{and} \quad |\operatorname{supp}(\hat{u})| + |\operatorname{supp}(\hat{v})| \leq p$$

and therefore

$$|\operatorname{supp}(u)| + |\operatorname{supp}(\hat{u})| + |\operatorname{supp}(v)| + |\operatorname{supp}(\hat{v})| \leq 2p. \tag{3.5}$$

However, by Proposition 3.3 the left hand side of (3.5) is larger or equal to $2(p+1)$. This gives a contradiction, and we have therefore proved, that the set W of solutions to (2.9) is finite. □

4 Multiplicity of a proper holomorphic function

Let U, V be regions in $\mathbb{C}^n$ (i.e. U and V are non-empty connected open subsets of $\mathbb{C}^n$). A holomorphic function $\varphi : U \to V$ is called *proper* if for every compact subset K and V, $\varphi^{-1}(K) = \{z \in U \mid \varphi(z) \in K\}$ is a compact subset of U. When φ is proper its Jacobian $J(z) = \det(\varphi'(z))$ can not vanish for all $z \in U$ (cf. [Ru1, 15.1.3]). Following [Ru1, 15.1.4], we let M denote the set

$$M = \{z \in U \mid J(z) = 0\}.$$

Its range $\varphi(M) \subseteq V$ is called the set of *critical values* for φ and $V \setminus \varphi(M)$ is called the set of *regular values* for φ. By [Ru, Prop. 15.1.5 and Thm. 15.1.9] we have

Theorem 4.1. *Let U, V be regions in $\mathbb{C}^n$ and let $\varphi : U \to V$ be a proper holomorphic function and let $\varphi(M)$ be the set of critical values for φ, then*

(a) $\varphi(U) = V$.

(b) The set $V \setminus \varphi(M)$ of regular values for φ is a connected, open and dense subset of V.

(c) There is a unique natural number $m \in N$ (called the multiplicity of φ) such that the number of elements $|\varphi^{-1}(w)|$ in $\varphi^{-1}(w)$ satisfies

$$|\varphi^{-1}(w)| = m \quad \text{for} \quad w \in V \setminus \varphi(M)$$
$$|\varphi^{-1}(w)| < m \quad \text{for} \quad w \in \varphi(M).$$

(d) The critical set $\varphi(M)$ is a zero-variety in V, i.e. $\varphi(M) = \{w \in V \mid h(w) = 0\}$ for some holomorphic function $h : U \to \mathbb{C}$.

Remark 4.2. The set of critical values $\varphi(M)$ is a zero set with respect to the $2n$-dimensional Lebesgue measure m_{2n} in $\mathbb{C}^n \approx \mathbb{R}^{2n}$, i.e. $m_{2n}(\varphi(M)) = 0$. This follows from Sard's Theorem (cf. [AY, Theorem 0.11]).

Proposition 4.3. [AY, Chap 1, Prop. 2.1]*: Let U, V be regions in $\mathbb{C}^n$ and let $\varphi : U \to V$ be a holomorphic function. Let $a \in U$ be an isolated zero for φ, and choose a neighborhood U_a of a, such that $\varphi(z) \neq 0$ when $z \in U_a \setminus \{a\}$. Then there exists an $\varepsilon > 0$ such that for Lebesgue almost all $w \in B(0, \varepsilon)$, the function*

$$\varphi_w(z) = \varphi(z) - w \tag{4.1}$$

has only simple zeros in U_a (i.e, the Jacobian $\det(\varphi'_w)$ does not vanish at the zeros of φ_w), and their number depends neither on w nor on the choice of the neighborhood U_a.

Definition 4.4. *The number of zeros to (4.1) indicated in Prop. 4.3 is called the multiplicity of the isolated zero a for φ.*

An isolated zero a for φ has multiplicity one if and only if $\det(\varphi'(a)) \neq 0$ (cf. [AY, Chap 1, Prop 2.2 and Prop 2.3]).

Remark 4.5. The multiplicity defined above is also called the *geometric multiplicity* of an isolated zero (cf [Ts, p. 16]). It coincides with the *algebraic multiplicity* of a:

$$\mu_a(\varphi) = \dim(O_a/I_a(\varphi)),$$

where O_a is the ring of holomorphic germs at a, and $I_a(\varphi)$ is the ideal in O_a generated by the n coordinate functions of φ (cf. [Ts, p. 148]).

We will also use the n-dimensional version of Rouchés Theorem (cf. [AY, Thm. 2.5 and remark after Thm. 2.5]).

Theorem 4.6. *Let U, V be regions in $\mathbb{C}^n$ and let D be a bounded open set, such that $\overline{D} \subseteq U$ and ∂D is piecewise smooth. Let $f, g : U \to V$ be holomorphic functions, such that*

$$\forall z \in \partial D \quad \forall t \in [0,1] : \qquad f(z) + tg(z) \neq 0.$$

Then f and $f+g$ have only isolated zeros in D, and the two functions f and $f+g$ have the same number of zeros in D counted with multiplicity.

Definition 4.7. *Let U, V be regions in $\mathbb{C}^n$, $\varphi : U \to V$ be a proper holomorphic function, and let $w \in V$. By the number $m(w)$ of solutions $z \in U$ to $\varphi(z) = w$ counted with multiplicity, we mean the number of zeros of $\varphi_w(z) = \varphi(z) - w$ in U connected with multiplicity.*

The following theorem is probably well known but since we have not found a concrete reference to it in the literature, we include a proof.

Theorem 4.8. *Let U, V be regions in $\mathbb{C}^n$ and let $\varphi : U \to V$ be a proper holomorphic function of multiplicity m (as defined in Theorem 4.1(c)). Then for every $w \in V$, the number $m(w)$ of solutions $z \in U$ to $\varphi(z) = w$ counted with multiplicity is equal to m.*

Proof. Let $\varphi(M)$ denote the set of critical values for φ as in Theorem 4.1. For $w \in V$ we put

$$\varphi_w(z) = \varphi(z) - w, \quad z \in U.$$

Note that the Jacobian $J_w(z) = \det(\varphi_w'(z))$ is equal to the Jacobian of φ. Assume first, that $w \in V \setminus \varphi(M)$. Then the Jacobian of φ_w is non-zero at all the zeros of φ_w and hence all the zeros have multiplicity 1. Hence by Theorem 4.1,

$$m(w) = |\varphi^{-1}(w)| = m, \quad w \in V \setminus \varphi(M).$$

Let now $w \in V$ be arbitrary. Choose an $\varepsilon > 0$ such that $\overline{B(w,\varepsilon)}$ is contained in V. By the properness of φ,

$$K = \varphi^{-1}(\overline{B(w,\varepsilon)})$$

is a compact subset of U. Moreover

$$|\varphi(z) - w| > \varepsilon \quad \text{for} \quad z \in U \setminus K \tag{4.2}$$

and since $\partial K \subseteq \overline{U \setminus K}$, we have

$$|\varphi(z) - w| \geq \varepsilon \quad \text{for} \quad z \in \partial K. \tag{4.3}$$

Let $v \in B(w,\varepsilon)$. Then $\varphi_v = \varphi_w + c$ where $c = w - v \in \mathbb{C}^n$, and by (4.3)

$$|c| < \varepsilon \leq |\varphi_w(z)|, \quad z \in \partial K.$$

Assume first that the boundary ∂K of K is piecewise smooth. Then we can apply Theorem 4.6 to $f = \varphi_w$ and $g = c$, and obtain, that φ_w and φ_v have the same number of zeros (counted with multiplicity) in $\overset{\circ}{K} = K \setminus \partial K$. By (4.2) and (4.3), neither φ_w nor $\varphi_v = \varphi_w + c$, $|c| < \varepsilon$ has zeros in ∂K or $U \setminus K$. Hence

$$m(v) = m(w), \quad v \in B(w, \varepsilon).$$

Since $V \setminus \varphi(M)$ is dense in V by Theorem 4.1, we can choose a $v \in B(w, \varepsilon) \setminus \varphi(M)$ and for this v, $m(w) = m(v) = m$ by the first part of the proof.

If ∂K is not piecewise smooth, one can find a compact set K' with piecewise smooth boundary, such that $K \subseteq K' \subseteq U$, for instance K' can be a polyhedron or a finite union of disjoint polyhedrons. Then the proof of $m(w) = m$ can be completed as above by using K' instead of K. □

5 The number of cyclic p-roots on (x, y)-level

Throughout this section p is a prime number. We will show, that for $n = p$, the numbers of solutions to (2.4) and (2.9) counted with multiplicity are both equal to $\binom{2p-2}{p-1}$. In both cases we will consider x_0, y_0 as the fixed numbers $x_0 = y_0 = 1$, so the problems (2.4) and (2.9) have $2p-2$ variables: $x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1}$.

Lemma 5.1. *Let $x', y' \in \mathbb{C}^{p-1}$, $x' = (x_1, \ldots, x_{p-1})$, $y' = (y_1, \ldots, y_{p-1})$, put*

$$x = (1, x_1, \ldots, x_{p-1}), \qquad y = (1, y_1, \ldots, y_{p-1}),$$

and let $\hat{x} = F_p x$, $\hat{y} = F_p y$ be their Fourier transformed vectors in $\mathbb{C}^p$. Consider the function $\varphi : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ given by the coordinate functions

$$\varphi_j(x', y') = x_j y_j, \quad 1 \le j \le p-1 \tag{5.1}$$

$$\varphi_{p-1+j}(x', y') = \hat{x}_j \hat{y}_{-j}, \quad 1 \le j \le p-1. \tag{5.2}$$

Then φ is a proper holomorphic function.

Proof. Clearly φ is a holomorphic function of $\mathbb{C}^{2p-2}$ into $\mathbb{C}^{2p-2}$. For $R > 0$, we put

$$\overline{B}(0, R) = \{w \in \mathbb{C}^{2p-2} \mid \|w\|_2 \le R\}.$$

Assume that φ is not proper. Then for some $R > 0$, $\varphi^{-1}(\overline{B}(0, R))$ is not a bounded subset of $\mathbb{C}^{2p-2}$. Hence there exists a sequence $(z^{(m)})_{m=1}^{\infty}$ in $\mathbb{C}^{2p-2}$ such that

$$\lim_{m \to \infty} \|z^{(m)}\|_2 = \infty$$

while

$$\|\varphi(z^{(m)})\|_2 \le R, \quad m \in \mathbb{N}. \tag{5.3}$$

Write $z^{(m)} = (x_1^{(m)}, \ldots, x_{p-1}^{(m)}, y_1^{(m)}, \ldots, y_{p-1}^{(m)})$ and put

$$x^{(m)} = (1, x_1^{(m)}, \ldots, x_{p-1}^{(m)}), \quad y^{(m)} = (1, y_1^{(m)}, \ldots, y_{p-1}^{(m)}).$$

Then

$$\|x^{(m)}\|_2^2\|y^{(m)}\|_2^2 = \left(1+\sum_{j=1}^{p-1}|x_j^{(m)}|^2\right)\left(1+\sum_{j=1}^{p-1}|y_j^{(m)}|^2\right) \geq 1+\|z^{(m)}\|_2^2.$$

Hence

$$\lim_{n\to\infty}\|x^{(m)}\|_2\|y^{(m)}\|_2 = \infty. \tag{5.4}$$

The rest of the proof will follow the proof of Lemma 3.4 and Theorem 3.5. By passing to a subsequence, we can obtain, that the sequences

$$u^{(m)} = \frac{1}{\|x^{(m)}\|_2}x^{(m)}, \quad v^{(m)} = \frac{1}{\|y^{(m)}\|_2}y^{(m)}$$

both converge in the unit sphere S^{2p-1} of $\mathbb{C}^p$. Put

$$u = \lim_{m\to\infty}u^{(m)}, \quad v = \lim_{m\to\infty}v^{(m)}.$$

By (5.1), (5.2) and (5.3),

$$|x_j^{(m)}y_j^{(m)}| \leq R \quad \text{and} \quad |\widehat{x_j^{(m)}}\widehat{y_{-j}^{(m)}}| \leq R$$

for $1 \leq j \leq p-1$. Hence by (5.4)

$$u_jv_j = \lim_{m\to\infty}u_j^{(m)}v_j^{(m)} = 0, \quad 1 \leq j \leq p-1$$

and

$$\hat{u}_j\hat{v}_{-j} = \lim_{m\to\infty}\widehat{x_j^{(m)}}\widehat{y_{-j}^{(m)}} = 0, \quad 1 \leq j \leq p-1.$$

Moreover, since $x_0^{(m)} = y_0^{(m)} = 1$, we also have $u_0v_0 = 0$ and hence by (2.8) also $\hat{u}_0\hat{v}_0 = 0$. We have thus proved that

$$\operatorname{supp}(u)\cap\operatorname{supp}(v) = \emptyset \qquad \text{and} \qquad \operatorname{supp}(\hat{u})\cap(-\operatorname{supp}(\hat{v}) = \emptyset.$$

However u, v are non-zero, because $\|u\|_2 = \|v\|_2 = 1$, so as in the proof of Theorem 3.5, this contradicts Proposition 3.3. Therefore $\varphi : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ is a proper holomorphic function. □

Lemma 5.2. *Let $\varphi : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ be the proper holomorphic function defined in lemma 5.1. Put*

$$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}.$$

(i) Assume $z = (x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1})$ is a solution to $\varphi(z) = 0$, and put

$$x = (1, x_1, \ldots, x_{p-1}), \qquad y = (1, y_1, \ldots, y_{p-1}).$$

Then there is a unique pair (K, L) of subsets $K, L \subseteq \mathbb{Z}_p^*$ satisfying $|K| + |L| = p-1$, such that

$$\mathit{supp}(x) = L \cup \{0\}, \quad \mathit{supp}(\hat{x}) = K \cup \{0\} \tag{5.5}$$

$$\mathit{supp}(y) = \mathbb{Z}_p \setminus L, \quad -\mathit{supp}(\hat{y}) = \mathbb{Z}_p \setminus K. \tag{5.6}$$

(ii) Conversely if $K, L \subseteq \mathbb{Z}_p^*$ satisfy $|K| + |L| = p - 1$, then there exists exactly one solution $(x, y) \in \mathbb{C}^p \times \mathbb{C}^p$ to (5.5) and (5.6) of the form $x = (1, x_1, \ldots, x_{p-1})$, $y = (1, y_1, \ldots, y_{p-1})$ and for this solution, $z = (x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1}) \in \mathbb{C}^{2p-2}$ satisfies $\varphi(z) = 0$.

(iii) The number of distinct zeros for φ is equal to $\binom{2p-2}{p-1}$.

Proof. (i): Assume that $\varphi(z) = 0$ for $z = (x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1}) \in \mathbb{C}^{2p-2}$, and define $x, y \in \mathbb{C}^p$ as in (i). Then by the definition of φ,

$$x_j y_j = 0, \quad \hat{x}_j \hat{y}_{-j} = 0, \quad \text{for} \quad 1 \leq j \leq p-1. \tag{5.7}$$

Moreover $x_0 y_0 = 1$, so by (5.7) and (2.8) also $\hat{x}_0 \hat{y}_0 = 1$. Therefore

$$\begin{aligned} \operatorname{supp}(x) \cap \operatorname{supp}(y) &= \{0\} \\ \operatorname{supp}(\hat{x}) \cap (-\operatorname{supp}(\hat{y})) &= \{0\}. \end{aligned}$$

Hence, there are unique subsets K, K', L, L' of $\mathbb{Z}_p^*$ such that

$$\operatorname{supp}(x) = L \cup \{0\}, \quad \operatorname{supp}(\hat{x}) = K \cup \{0\} \tag{5.8}$$

$$\operatorname{supp}(y) = L' \cup \{0\}, \quad -\operatorname{supp}(\hat{y}) = K' \cup \{0\}. \tag{5.9}$$

Moreover $K \cap K' = \emptyset$ and $L \cap L' = \emptyset$. In particular

$$|K| + |K'| \leq p - 1 \quad \text{and} \quad |L| + |L'| \leq p - 1. \tag{5.10}$$

By Proposition 3.3

$$|K| + |L| = |\operatorname{supp}(x)| + |\operatorname{supp}(\hat{x})| - 2 \geq p - 1 \tag{5.11}$$

$$|K'| + |L'| = |\operatorname{supp}(y)| + |\operatorname{supp}(\hat{y})| - 2 \geq p - 1. \tag{5.12}$$

Hence, equality must hold in the 4 inequalities in (5.10), (5.11) and (5.12). In particular $|K| + |L| = p - 1$ and $K' = \mathbb{Z}_p^* \setminus K$, $L' = \mathbb{Z}_p^* \setminus L$. This proves (5.5) and (5.6), and the uniqueness of K and L is clear.

(ii): Let $K, L \subseteq Z_p^*$ be such that $|K| + |L| = p - 1$. Put $K' = \mathbb{Z}_p^* \setminus K$, $L' = \mathbb{Z}_p^* \setminus L$. Then (5.6) can be written as

$$\operatorname{supp}(y) = L' \cup \{0\}, \quad -\operatorname{supp}(\hat{y}) = K' \cup \{0\}. \tag{5.13}$$

Moreover

$$|K'| = |L|, |L'| = |K|. \tag{5.14}$$

Assume first that $|K| \geq 1$ and $|L| \geq 1$. Then by Chebotarëv's Theorem (Theorem 2.1), the submatrices $(F_p)_{K' \times L}$ and $(F_p)_{K \times L'}$ of

$$F_p = (\frac{1}{\sqrt{p}} \mathrm{e}^{\mathrm{i}2\pi kl/p})_{j,k=0,\ldots,p-1}$$

have non-zero determinants. We claim that (5.5) and (5.6) have a unique solution (x, y) of the form $x = (1, x_1, \ldots, x_{p-1})$, $y = (1, y_1, \ldots, y_{p-1})$ and that this solution is given by

$$\begin{cases} (x_l)_{l \in L} &= -\dfrac{1}{\sqrt{p}} \big[(F_p)_{K' \times L}\big]^{-1} (1)_{k \in K'} \\ x_l &= 0 \text{ for } l \in L' \end{cases} \tag{5.15}$$

and

$$\begin{cases} (y_l)_{l\in L'} &= -\dfrac{1}{\sqrt{p}}\big[(\overline{F}_p)_{K\times L'}\big]^{-1}(1)_{k\in K} \\ y_l &= 0 \text{ for } l\in L \end{cases} \tag{5.16}$$

where $(1)_{k\in K}$ (resp. $(1)_{k\in K'}$) is the column vector with coordinates indexed by K (resp. K') and all entries equal to 1. Moreover $\overline{F}_p$ is the complex conjugate of F_p.

To prove this claim, observe first that (5.5) is equivalent to

$$\mathrm{supp}(x)\subseteq L\cup\{0\},\quad \mathrm{supp}(\hat{x})\subseteq K\cup\{0\} \tag{5.17}$$

because if one of the inclusions in (5.17) is proper, then

$$|\mathrm{supp}(x)|+|\mathrm{supp}(\hat{x})|<|K|+|L|+2=p+1$$

which contradicts Proposition 3.3. Moreover $x=(1,x_1,\dots,x_{p-1})$ satisfies (5.17) if and only if $x_l=0$ for $l\in L'$ and

$$\frac{1}{\sqrt{p}}+\frac{1}{\sqrt{p}}\sum_{l\in L}\mathrm{e}^{\mathrm{i}2\pi kl/p}x_l=0,\quad k\in K'.$$

The latter formula can be rewritten as

$$(F_p)_{K'\times L}(x_l)_{l\in L}=-\frac{1}{\sqrt{p}}(1)_{k\in K'}$$

which is equivalent to (5.15). Similarly one gets that for $y=(1,y_1,\dots,y_{p-1})$, (5.6) is equivalent to

$$\mathrm{supp}(y)\subseteq L'\cup\{0\},\quad -\mathrm{supp}(\hat{y})\subseteq K'\cup\{0\}$$

which is equivalent to $y_l=0$ for $l\in L$ and

$$\frac{1}{\sqrt{p}}+\frac{1}{\sqrt{p}}\sum_{l\in L'}\mathrm{e}^{-\mathrm{i}2\pi kl}y_l=0,\quad k\in K,$$

and this is equivalent to (5.16). Finally if $|K|=0$, then $K=L'=\emptyset$ and $K'=L=\mathbb{Z}_p^*$. In this case, it is elementary to check that the pair $x=(1,1,\dots 1)$, $y=(1,0,\dots,0)$ is the unique solution to (5.5) and (5.6). Similarly, if $|L|=0$, the pair $x=(1,0,\dots,0)$, $y=(1,1,\dots,1)$ is the unique solution to (5.5) and (5.6).

Note finally, that if (x,y) is a solution to (5.5) and (5.6) of the form $x=(1,x_1,\dots,x_{p-1})$, $y=(1,y_1,\dots,y_{p-1})$, then $z=(x_1,\dots,x_{p-1},y_1,\dots,y_{p-1})$ is a zero for φ, because $\mathrm{supp}(x)\cap\mathrm{supp}(y)=\{0\}$ and $\mathrm{supp}(\hat{x})\cap(-\mathrm{supp}(\hat{y}))=\{0\}$. This proves (ii).

(iii): By (i) and (ii) there is a one-to-one correspondence between the zeros of φ and pairs (K,L) of subsets $\mathbb{Z}_p^*$ satisfying $|K|+|L|=p-1$. The number of such pairs is

$$\sum_{j=0}^{p-1}\binom{p-1}{j}\binom{p-1}{p-1-j}=\binom{2p-2}{p-1},$$

which proves (iii). □

Theorem 5.3. *The map $\varphi:\mathbb{C}^{2p-2}\to\mathbb{C}^{2p-2}$ defined in lemma 5.1 is a proper holomorphic function of multiplicity $\binom{2p-2}{p-1}$. In particular the number of solutions $(x_1,\dots,x_{p-1},y_1,\dots,y_{p-1})$ to (2.9) counted with multiplicity is equal to $\binom{2p-2}{p-1}$.*

Proof. By Theorem 4.8 it is sufficient to prove that for some $w \in \mathbb{C}$, the number of solutions to $\varphi(z) = w$ counted with multiplicity is equal to $\binom{2p-2}{p-1}$. Put now $w = 0$. From lemma 5.2 we know that φ has exactly $\binom{2p-2}{p-1}$ distinct zeros. Hence we just have to show, that all the zeros have multiplicity 1, or equivalently the Jacobian $J(z) = \det(\varphi'(z))$ is non-zero whenever $\varphi(z) = 0$.

Let $z = (x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1})$ be a zero for φ, put $x = (1, x_1, \ldots, x_{p-1})$, $y = (1, y_1, \ldots, y_{p-1})$ and let $K, L \subseteq \mathbb{Z}_p^*$ be the corresponding sets as in lemma 5.2. Then $|K|+|L| = p-1$, and with $K' = \mathbb{Z}_p^* \setminus K$, $L' = \mathbb{Z}_p^* \setminus L$, (5.5) and (5.6) can be written

$$\operatorname{supp}(x) = L \cup \{0\}, \quad \operatorname{supp}(\hat{x}) = K \cup \{0\} \tag{5.18}$$
$$\operatorname{supp}(y) = L' \cup \{0\}, \quad -\operatorname{supp}(\hat{y}) = K' \cup \{0\}. \tag{5.19}$$

In order to determine $\varphi'(z)$ we compute $\varphi(z+h)$ for $h = (f_1, \ldots, f_{p-1}, g_1, \ldots, g_{p-1}) \in \mathbb{C}^{2p-2}$. Put

$$f = (0, f_1, \ldots, f_{p-1}), \quad g = (0, g_1, \ldots, g_{p-1}).$$

Then

$$\varphi(z+h)_j = (x_j + f_j)(y_j + g_j), \quad 1 \le j \le p-1$$
$$\varphi(z+h)_{p-1+j} = (\hat{x}_j + \hat{f}_j)(\hat{y}_{-j} + \hat{g}_{-j}), \quad 1 \le j \le p-1.$$

Using $\|\hat{f}\|_2 \|\hat{g}\|_2 = \|f\|_2 \|g\|_2 \le \|h\|_2^2$, we get

$$\varphi(z+h)_j = \varphi(z)_j + f_j y_j + x_j g_j + O(\|h\|_2^2)$$
$$\varphi(z+h)_{p-1+j} = \varphi(z)_{p-1+j} + \hat{f}_j \hat{y}_{-j} + \hat{x}_j \hat{g}_{-j} + O(\|h\|_2^2)$$

in Landau's O-notation. Hence

$$(\varphi'(z)h)_j \quad = y_j f_j + x_j g_j, \quad 1 \le j \le p-1 \tag{5.20}$$
$$(\varphi'(x)h)_{p-1+j} \quad = \hat{y}_{-j} \hat{f}_j + \hat{x}_j \hat{g}_{-j}, \quad 1 \le j \le p-1. \tag{5.21}$$

To prove that $J(z) = \det(\varphi'(z)) \neq 0$, we just have to show that $\ker(\varphi'(z)) = 0$, i.e.

$$\varphi'(z)h = 0 \;\Rightarrow\; h = 0, \quad h \in \mathbb{C}^{2p-2}.$$

By (5.18) and (5.19), the formulas (5.20) and (5.21) can be written as

$$(\varphi'(z)h)_j = \begin{cases} x_j g_j, & j \in L \\ y_j f_j, & j \in L' \end{cases}$$

and

$$(\varphi'(z)h)_{p-1+j} = \begin{cases} \hat{x}_j \hat{g}_{-j}, & j \in K \\ \hat{y}_{-j} \hat{f}_j, & j \in K' \end{cases}.$$

Hence, if $\varphi'(z)h = 0$, then by (5.18) and (5.19),

$$g_j = 0 \ (j \in L), \quad f_j = 0 \ (j \in L'),$$
$$\hat{g}_{-j} = 0 \ (j \in K), \quad \hat{f}_j = 0 (j \in K'),$$

and since $f_0 = g_0 = 0$ by the definition of f and g, it follows that

$$\begin{aligned} \operatorname{supp}(f) &\subseteq L, \quad \operatorname{supp}(\hat{f}) \subseteq K \cup \{0\} \\ \operatorname{supp}(g) &\subseteq L', \quad -\operatorname{supp}(\hat{g}) \subseteq K' \cup \{0\}. \end{aligned}$$

Hence

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \leq |K| + |L| + 1 = p$$

and

$$|\operatorname{supp}(g)| + |\operatorname{supp}(\hat{g})| \leq |K'| + |L'| + 1 = p$$

By Proposition 3.3, it now follows that $f = g = 0$ and hence $h = 0$. Therefore $\ker(\varphi'(z)) = 0$, and hence $J(z) \neq 0$. □

Corollary 5.4. *Let $x', y' \in \mathbb{C}^{p-1}$, $x' = (x_1, \ldots, x_{p-1})$, $y' = (y_1, \ldots, y_{p-1})$ and put $x = (1, x_1, \ldots, x_{p-1})$, $y = (1, y_1, \ldots, y_{p-1})$. Then the function $\psi : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ given by the coordinate functions*

$$\psi_j(x', y') = x_j y_j, \quad 1 \leq j \leq p-1 \tag{5.22}$$

$$\psi_{p-1+j}(x', y') = \sum_{m=0}^{p-1} x_{j+m} y_m, \quad 1 \leq j \leq p-1 \tag{5.23}$$

is a proper holomorphic function of multiplicity $\binom{2p-2}{p-1}$. In particular the number of solutions $(x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1})$ to (2.4) counted with multiplicity is equal to $\binom{2p-2}{p-1}$.

Proof. Let $\varphi : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ be as in lemma 5.1. By Proposition 2.3

$$\varphi = \Lambda \circ \psi \tag{5.24}$$

where $\Lambda : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ is the affine map given by

$$\Lambda(a_1, \ldots, a_{p-1}, c_1, \ldots, c_{p-1}) = (a_1, \ldots, a_{p-1}, b_1, \ldots, b_{p-1}) \tag{5.25}$$

where

$$b_j = \frac{1}{p}(1 + \sum_{m=1}^{p-1} a_m + \sum_{k=1}^{p-1} e^{i2\pi jk/p} c_k), \quad 1 \leq j \leq p = 1 \tag{5.26}$$

Moreover by Proposition 2.3, Λ is a bijection and its inverse is given by (2.13) with $n = p$. Hence by (5.24)

$$\psi = \Lambda^{-1} \circ \varphi$$

where Λ and Λ^{-1} are affine transformations of $\mathbb{C}^{2p-2}$. Therefore it follows from Theorem 5.3, that ψ is a proper holomorphic function of multiplicity $\binom{2p-2}{p-1}$, so by Theorem 4.8 the number of solutions $(x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1})$ to (2.4) counted with multiplicity is $\binom{2p-2}{p-1}$. □

6 The numbers of cyclic p-roots on x-level and z-level

Throughout this section p is again a prime number. We will show that the numbers of solutions to (2.3) and (2.1) counted with multiplicity are both equal to $\binom{2p-2}{p-1}$. In the case of (2.3), we consider x_0 as the fixed number 1, so the problem has $p-1$ variables $x_1, \ldots, x_{p-1}$.

Lemma 6.1. *Put $a_0 = x_0 = 1$ and define for $a = (a_1, \ldots, a_{p-1}) \in (\mathbb{C}^*)^{p-1}$ a map $\sigma_a : (\mathbb{C}^*)^{p-1} \to \mathbb{C}^{p-1}$ by*

$$\sigma_a(x_1, \ldots, x_{p-1})_j = \sum_{m=0}^{p-1} a_m \frac{x_{m+j}}{x_m}, \quad 1 \le j \le p-1$$

Then σ_a is a proper holomorphic function, and the multiplicity of σ_a is independent of $a \in (\mathbb{C}^*)^{p-1}$.

Proof. Let $a \in (\mathbb{C}^*)^{p-1}$. Then σ_a is clearly holomorphic. To prove that σ_a is proper, we let $K \subseteq \mathbb{C}^{p-1}$ be compact. Put $a_0 = x_0 = y_0 = 1$ and let ψ be the holomorphic map defined in Corollary 5.4. Since ψ is proper, the set

$$L_a = \psi^{-1}(\{a\} \times K)$$

is compact. Moreover L_a is the set of $(x', y') = (x_1, \ldots, x_{p-1}, y_1, \ldots, y_{p-1}) \in \mathbb{C}^{2p-2}$ for which

$$x_j y_j = a_j, \quad 1 \le j \le p-1$$

and

$$\left(\sum_{m=0}^{p-1} x_{j+m} y_m \right)_{j=1}^{p-1} \in K$$

Since $a_j \neq 0$ $(1 \le j \le p-1)$, L_a can be expressed as the set of

$$\left(x_1, \ldots, x_{p-1}, \frac{a_1}{x_1}, \ldots, \frac{a_{p-1}}{x_{p-1}}\right) \in \mathbb{C}^{2p-2}$$

for which $(x_1, \ldots, x_{p-1}) \in (\mathbb{C}^*)^{p-1}$ and

$$\left(\sum_{m=0}^{p-1} a_m \frac{x_{j+m}}{x_m} \right)_{j=1}^{p-1} \in K$$

Hence $\sigma_a^{-1}(K) = \pi(L_a)$, where $\pi : \mathbb{C}^{2p-2} \to \mathbb{C}^{p-1}$ is the map that takes out the first $p-1$ coordinates of an element in $\mathbb{C}^{2p-2}$. Therefore $\sigma_a^{-1}(K)$ is compact, and we have proved that σ_a is proper.

Note that $(\mathbb{C}^*)^{p-1}$ is a connected open set in $\mathbb{C}^{p-1}$. In order to prove that $a \to m(\sigma_a)$ is a constant function on $(\mathbb{C}^*)^{p-1}$, it is therefore sufficient to prove that for every $a_0 \in (\mathbb{C}^*)^{p-1}$, $m(\sigma_a)$ is constant in a ball $U = B(a_0, \varepsilon)$, where $\varepsilon > 0$ is chosen such that $\overline{U} \subseteq (\mathbb{C}^*)^{p-1}$. Put now

$$M = \max\{\|a\|_2 \mid a \in \overline{U}\}.$$

Since the map $\psi : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ is proper, we can choose $R > 0$, such that

$$\|\psi(z)\|_2 \ge (M^2+1)^{1/2}, \quad \text{when} \quad \|z\|_2 \ge R \tag{6.1}$$

Applying (6.1) to

$$z = \Big(x_1, \dots, x_{p-1}, \frac{a_1}{x_1}, \dots, \frac{a_{p-1}}{x_{p-1}}\Big)$$

for $x' = (x_1, \dots, x_{p-1}) \in (\mathbb{C}^*)^{p-1}$, we get that

$$\|a\|_2^2 + \|\sigma_a(x')\|_2^2 = \|\psi(z)\|_2^2 \geq M^2 + 1$$

when

$$\|(x_1, \dots, x_{p-1})\|_2^2 + \|\Big(\frac{a_1}{x_1}, \dots, \frac{a_{p-1}}{x_{p-1}}\Big)\|_2^2 \geq R^2$$

and since $\|a\|_2 \leq M$ for $a \in \overline{U}$ it follows that

$$\begin{gathered} \|\sigma_a(x')\|_2 \geq 1, \quad \text{when} \quad a \in \overline{U} \quad \text{and} \\ \|(x_1, \dots, x_{p-1})\|_2 \geq R \quad \text{or} \quad \|\Big(\frac{a_1}{x_1}, \dots, \frac{a_{p-1}}{x_{p-1}}\Big)\|_2 \geq R \end{gathered} \tag{6.2}$$

Put

$$D = \{(x_1, \dots, x_{p-1}) \in \{(\mathbb{C}^*)^n \mid \frac{c}{R} < x_j < R\}$$

where $c = \min\{|a_j| \mid a \in \overline{U},\ j = 1, \dots, p-1\} > 0$. By replacing R with a larger number, we can assume that $\frac{c}{R} < R$. Then $\overline{D}$ is a non-empty compact subset of $(\mathbb{C}^*)^{p-1}$ and its boundary ∂D has 2^{p-1} smooth components. By (6.2) all the zeros of σ_a are in D, when $a \in \overline{U}$. Let $a \in \overline{U}$. Since $\overline{U}$ is convex, all the functions

$$(1-t)\sigma_{a_0} + t\sigma_a, \quad 0 \leq t \leq 1$$

are of the form $\sigma_{a'}$ for an $a' \in \overline{U}$, namely $a' = (1-t)a_0 + t_a$. Hence by applying Rouchés Theorem (Theorem 4.6) to $f = \sigma_{a_0}$ and $g = \sigma_a - \sigma_{a_0}$, we get that σ_{a_0} and σ_a have the same number of zeros in D counted with multiplicity, and since neither σ_{a_0} nor σ_a has zeros in $(\mathbb{C}^*)^{p-1} \setminus D$, it follows that σ_{a_0} and σ_a have the same number of zeros in $(\mathbb{C}^*)^{p-1}$ counted with multiplicity. Therefore by Theorem 4.8, $m(\varphi_a) = m(\varphi_{a_0})$ for all $a \in \overline{U}$. Hence we have proved that $m(\varphi_a)$ is a constant function on $(\mathbb{C}^*)^{p-1}$. □

Theorem 6.2. *Put $x_0 = 1$, and let $\sigma : (\mathbb{C}^*)^{p-1} \to \mathbb{C}^{p-1}$ be the function defined by*

$$\sigma(x_1, \dots, x_{p-1})_j = \sum_{m=0}^{p-1} \frac{x_{m+j}}{x_m} \quad 1 \leq j \leq p-1$$

Then σ is a proper holomorphic function of multiplicity $\binom{2p-2}{p-1}$. In particular there are $\binom{2p-2}{p-1}$ cyclic p-roots on x-level counted with multiplicity.

Proof. Let $\psi : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ be the holomorphic function defined in Theorem 5.4. Then ψ is proper and has multiplicity $m(\psi) = \binom{2p-2}{p-1}$. Let $N = \psi(M)$ denote the set of critical values for ψ. Then by Theorem 4.1, and Remark 4.2, N is a closed set, and

$$m_{4p-4}(N) = 0$$

where m_{4p-4} is the Lebesgue measure in $\mathbb{C}^{2p-2} \simeq \mathbb{R}^{4p-4}$. By Theorem 4.1 the number of district solutions $z \in \mathbb{C}^{2p-2}$ to

$$\varphi(z) = w$$

is $m(\varphi)$ for every $w = (a, c) \in (\mathbb{C}^{p-1} \times \mathbb{C}^{p-1}) \setminus N$. Since $m_{4p-4}(N) = (m_{2p-2} \times m_{2p-2})(N)$, where m_{2p-2} is the Lebesgue measure in $\mathbb{C}^{p-1}$, it follows that

$$0 = m_{4p-4}(N) = \int_{\mathbb{R}^{2p-2}} m_{2p-2}(N_a) dm_{2p-2}(a)$$

where $N_a = \{c \in \mathbb{C}^{p-1} \mid (a, c) \in N\}$ (see e.g. [Ru 2, Sect. 8].) Hence the set

$$N' = \{a \in \mathbb{C}^{p-1} \mid m_{2p-2}(N_a) \neq 0\}$$

is a m_{2p-2}–null set in $\mathbb{C}^{p-1}$. Moreover for all $a \in \mathbb{C}^{p-1} \setminus N'$, the number of district solutions to

$$\psi(z) = (a, c) \tag{6.3}$$

is exactly $m(\psi)$ for all $c \in \mathbb{C}^{p-1}$ outside the Lebesgue null set N_a. If $a \in (\mathbb{C}^*)^{p-1}$ we have from the proof of lemma 6.1. that the solution (6.3) are precisely the elements in $(\mathbb{C}^*)^{2p-2}$ of the form

$$\Big(x_1, x_2, \ldots, x_{p-1}, \frac{a_1}{x_1}, \ldots, \frac{a_{p-1}}{x_{p-1}}\Big)$$

for which $\sigma_a(x_1, \ldots, x_{p-1}) = c$. Hence for $a \in (\mathbb{C}^*)^{p-1} \setminus N'$, the number of distinct solutions to $\sigma_a(x') = c$ is equal to $m(\psi)$ for Lebseque almost all $c \in \mathbb{C}^{p-1}$. Therefore by Theorem 4.1 and Remark 4.2, the multiplicity $m(\sigma_a)$ of σ_a is equal to $m(\psi)$ for all $a \in (\mathbb{C}^*)^{p-1} \setminus N'$. But since $a \to m(\sigma_a)$ is a constant function on $(\mathbb{C}^*)^{p-1}$ by lemma 6.1, it follows that $m(\sigma_a) = m(\psi)$ for all $a \in (\mathbb{C}^*)^{p-1}$. Putting $a = (1, \ldots, 1)$, we get in particular, that $m(\sigma) = m(\psi) = \binom{2p-2}{p-1}$. Thus by Theorem 4.8, the number of solution $(x_1, \ldots, x_{p-1})$ to (2.3) counted with multiplicity is equal to $\binom{2p-2}{p-1}$ where $n = p$. □

Lemma 6.3. *Put $x_0 = 1$ and let $h : (\mathbb{C}^*)^p \to (\mathbb{C}^*)^p$ be the function given by*

$$h(x_1, \ldots, x_{p-1}, \alpha) = \Big(\frac{\alpha x_1}{x_0}, \frac{\alpha x_2}{x_1}, \ldots, \frac{\alpha x_0}{x_{p-1}}\Big) \tag{6.4}$$

Then h is proper, and for every $(z_0, \ldots, z_{p-1}) \in (\mathbb{C}^*)^p$ there are exactly p distinct solutions in $(\mathbb{C}^*)^p$ to the equation

$$h(x_1, \ldots, x_{p-1}, \alpha) = (z_0, \ldots, z_{p-1}) \tag{6.5}$$

Proof. We start by solving (6.5) w.r.t. $(x_1, \ldots, x_{p-1}, \alpha)$. By (6.4)

$$z_0 z_1 \cdot \ldots \cdot z_{p-1} = \alpha^p \tag{6.6}$$

Hence α is one of the p distinct p'th roots of $z_0 z_1 \cdot \ldots \cdot z_{p-1}$. For each such α, there is a unique solution to (6.5) given by

$$x_1 = \frac{z_0}{\alpha},\ x_2 = \frac{z_0 z_1}{\alpha^2}, \ldots, x_{p-1} = \frac{z_0 z_1 \cdot \ldots \cdot z_{p-2}}{\alpha^{p-1}} \tag{6.7}$$

Hence (6.5) has exactly p distinct solutions. Let $K \subseteq (\mathbb{C}^*)^p$ be compact. Then there exists $R > 0$, such that

$$K \subseteq \{z \in (\mathbb{C}^*)^p \mid \frac{1}{R} \leq \mid z_j \mid \leq R,\ 0 \leq j \leq p-1\}.$$

¿From (6.6) and (6.7) it now follows that $h^{-1}(K)$ is relatively compact in $(\mathbb{C}^*)^p$, which by the continuity of h implies that $h^{-1}(K)$ is compact. Hence h is proper. □

Theorem 6.4. *Let $\rho : (\mathbb{C}^*)^p \to \mathbb{C}^{p-1} \times \mathbb{C}^*$ be the function given by*

$$\begin{aligned}
\rho_1(z) &= z_0 + z_1 + \ldots + z_{p-1} \\
\rho_2(z) &= z_0z_1 + z_1z_2 + \ldots + z_{p-1}z_0 \\
&\vdots \\
\rho_{p-1}(z) &= z_0z_1 \cdot \ldots \cdot z_{p-2} + \ldots + z_{p-1}z_0 \cdot \ldots \cdot z_{p-3} \\
\rho_p(z) &= z_0z_1 \cdot \ldots \cdot z_{p-1}
\end{aligned}$$

Then ρ is a proper holomorphic function of multiplicity $\binom{2p-2}{p-1}$. In particular, the numbers of cyclic p-roots on z-level (i.e. the number of solutions to (2.1) counted with multiplicity is equal to $\binom{2p-2}{p-1}$.

Proof. Consider the composed map $\rho \circ h : (\mathbb{C}^*)^p \to \mathbb{C}^{p-1} \times \mathbb{C}^*$, where h is given by (6.4) with $x_0 = 1$. Then

$$(\rho \circ h)_j(x_1, \ldots, x_{p-1}, \alpha) = \alpha^j \sum_{m=0}^{p-1} \frac{x_{m+j}}{x_m}, \quad 1 \leq j \leq p-1$$

and

$$(\rho \circ h)_p(x_1, \ldots, x_{p-1}, \alpha) = \alpha^p$$

Let $\sigma : (\mathbb{C}^*)^{p-1} \to \mathbb{C}^{p-1}$ be the proper holomorphic map from Theorem 6.2. Then for $x' = (x_1, \ldots, x_{p-1}) \in (\mathbb{C}^*)^{p-1}$ and $\alpha \in \mathbb{C}^*$

$$(\rho \circ h)(x', \alpha) = (\alpha\sigma_1(x'), \ldots, \alpha^{p-1}\sigma_{p-1}(x'), \alpha^p) \tag{6.8}$$

Since $\sigma : (\mathbb{C}^*)^{p-1} \to \mathbb{C}^{p-1}$ is proper, it is elementary to deduce from (6.8), that $\rho \circ h$ is a proper map from $(\mathbb{C}^*)^p$ to $\mathbb{C}^{p-1} \times \mathbb{C}^*$. Moreover since h maps $(\mathbb{C}^*)^p$ into $(\mathbb{C}^*)^p$, we have for every compact subset K of $\mathbb{C}^{p-1} \times \mathbb{C}^*$, that

$$\rho^{-1}(K) = h(h^{-1}(\rho^{-1}(K)) = h((\rho \circ h)^{-1}(K)),$$

which is compact by the properness of $\rho \circ h$. Hence ρ is proper.

We will prove that $m(\rho) = m(\sigma)$ by computing the multiplicity of $g \circ h$ in two ways: By Theorem 4.1 and Remark 4.2, there exists a Lebesgue nullset $N_0 \subseteq \mathbb{C}^{p-1}$ such that for all $w \in \mathbb{C}^{p-1} \setminus N_0$ the equation $\sigma_p(x') = w$ has $m(\sigma)$ district solutions in $(\mathbb{C}^*)^{p-1}$. For $(x', \alpha) \in (\mathbb{C}^{p-1} \setminus N_0) \times \mathbb{C}^*$, $(\rho \circ h)(x', \alpha) = w$ if and only if

$$\alpha^p = w_p \tag{6.9}$$

and

$$\sigma(x') = \Big(\frac{1}{\alpha}w_1, \ldots, \frac{1}{\alpha^{p-1}}w_{p-1}\Big) \tag{6.10}$$

Since (6.9) has exactly p distinct solutions, it follows that $(\rho\circ h)(x',\alpha)=w$ has exactly $pm(\sigma)$ distinct solution for all such w. The complement of $(\mathbb{C}^{p-1}\setminus N_0)\times\mathbb{C}^*$ in $\mathbb{C}^{p-1}\times\mathbb{C}^*$ is $N_0\times\mathbb{C}^*$ which is a null set w.r.t. the Lebesgue measure in $\mathbb{C}^p$. Hence by Theorem 4.1 and Remark 4.2, $m(\rho\circ h)=pm(\sigma)$.

By the definition of $m(\rho)$, there exists a Lebesgue null set N in $\mathbb{C}^{p-1}\times\mathbb{C}^*$, such that for all $w\in\mathbb{C}^{p-1}\times\mathbb{C}^*\setminus N$, the number of distinct solutions $z\in(\mathbb{C}^*)^p$ to $\rho(z)=w$ is equal to $m(\rho)$. By lemma 6.3 we then get that the number of distinct solutions $u\in(\mathbb{C}^*)^p$ to $\rho(h(u))=w$ is equal to $pm(\rho)$. Since N is a Lebesgue nullset it follows that $m(\rho\circ h)=p\cdot m(\rho)$. Hence

$$m(\rho)=\frac{1}{p}m(\rho\circ h)=m(\sigma)=\binom{2p-2}{p-1}.$$

By Theorem 4.8 the number of solutions to (2.1) with $n=p$ counted with multiplicity is equal to $\binom{2p-2}{p-1}$. □

7 Cyclic p-roots of simple index k

Let p be a prime number and let $k\in\mathbb{N}$ be a number that divides $p-1$. Since the group $(\mathbb{Z}_p^*,\cdot)$ is cyclic, it has a unique subgroup G_0 of index k, namely

$$G_0=\{h^k|h\in\mathbb{Z}_p^*\}.$$

Moreover, if $g\in\mathbb{Z}_p^*$ is a generator for $\mathbb{Z}_p^*$, then

$$G_l=g^lG_0,\qquad 1\le l\le k-1$$

are the $k-1$ non-trivial cosets of G_0 in $\mathbb{Z}_p^*$. Following the notation of [BH], a cyclic p-root $z=(z_0,z,\dots,z_{p-1})$ has simple index k if the corresponding cyclic p-roots on x-level

$$x=(1,z_0,z_0z_1,\dots,z_0z_i\cdot\ldots\cdot z_{p-2})$$

is of the form

$$\begin{cases} x_0=1 \\ x_i=c_l, \quad \text{if} \quad i\in G_l, \quad 1\le i\le p-1, \end{cases} \tag{7.1}$$

where $(c_0,c_1,\dots,c_{k-1})\in(\mathbb{C}^*)^k$. These special cyclic p-roots where introduced by Björck in [Bj] under a slightly different name (cyclic p-roots of simple preindex k). It was shown in [Bj], that if $x=(1,x_1,x_2,\dots,x_{p-1})$ has the form (7.1), then the equations (2.3) can be reduced to the following set of k rational equations in $c_0,\dots,c_{k-1}$:

$$c_a+\frac{1}{c_{a+m}}+\sum_{i,j=0}^{k-1}n_{ij}\frac{c_{a+j}}{c_{a+i}}=0\qquad(0\le a\le k-1) \tag{7.2}$$

where indices are calculated modulo k. In (7.2) the number m is determined by $p-1\in G_m$ and n_{ij} denote the number of $b\in G_i$ for which $b+1\in G_{i+1}$ $(0\le i,j\le k-1)$. The set of equations (7.2) is independent of the choice of the generator g for $\mathbb{Z}_p^*$ up to permutation of the variables and of the equations. The main result of this section is:

Theorem 7.1. *For every $k \in \mathbb{N}$ and for every prime number p for which k divides $p-1$, the function $\chi : (\mathbb{C}^*)^k \to \mathbb{C}^k$ given by*

$$\chi(c_0, \ldots, c_{k-1})_a = c_a + \frac{1}{c_{a+m}} + \sum_{i,j=0}^{k-1} n_{ij} \frac{c_{a+j}}{c_{a+i}} = 0, \qquad (0 \le a \le k-1)$$

is a proper holomorphic function of multiplicity $\binom{2k}{k}$. In particular the number of solutions $(c_0, \ldots, c_{k-1}) \in (\mathbb{C}^*)^k$ to (7.2) counted with multiplicity is equal to $\binom{2k}{k}$.

The proof of Theorem 7.1 relies on Proposition 7.3 and Proposition 7.4 below. We first introduce some notation: Let $n \in \mathbb{N}$ and let F be a subspace of $\mathbb{C}^n$ of dimension $d \ge 1$. A subset $U \subseteq F$ is called a region in F if it is non-empty, open and connected in the relative topology on F. By choosing a fixed basis for F, we can identify F with $\mathbb{C}^d$, and thereby extend the defintion of holomorphic functions, proper holomorphic functions and their multiplicities to maps $\varphi : U \to V$, where U and V are two regions in F. Clearly these definitions are independent of the choice of a basis for F.

Definition 7.2. *Let E denote the set of $(x_i)_{i=1}^{p-1} \in \mathbb{C}^{p-1}$ for which the function $i \to x_i, i \in \mathbb{Z}_p^* = \{1, \ldots, p-1\}$ is constant on each of the cosets $G_0, \ldots, G_{k-1}$ of G_0.*

Note that E is the k-dimensional subspace of $\mathbb{C}^{p-1}$, and the indicator functions $1_{G_0}, \ldots, 1_{G_{k-1}}$ given by

$$(1_{G_l})_i = \begin{cases} 1 & i \in G_l \\ 0 & i \notin G_l \end{cases} \tag{7.3}$$

form a basis for E. Note also, that $E \times E$ is a subspace of $\mathbb{C}^{p-1} \times \mathbb{C}^{p-1} \simeq \mathbb{C}^{2p-2}$ of dimension $2k$.

Proposition 7.3. *Let $\varphi, \psi : \mathbb{C}^{2p-2} \to \mathbb{C}^{2p-2}$ be the proper holomorphic functions defined in Lemma 5.1 and corollary 5.4. Then*

(a) $\varphi(E \times E) \subseteq E \times E$ and $\psi(E \times E) \subseteq E \times E$.

(b) The restrictions φ_E and ψ_E of φ and ψ to $E \times E$ are proper holomorphic functions.

(c) The multiplicities of φ_E and ψ_E are given by

$$m(\varphi_E) = m(\psi_E) = \binom{2k}{k}.$$

Proof. (a) Let $x' = (x_1, \ldots, x_{p-1}) \in E$, $y' = (y_1, \ldots, y_{p-1}) \in E$ and put

$$x = (1, x_1, \ldots, x_{p-1}) \qquad \text{and} \qquad y = (1, y_1, \ldots, y_{p-1}).$$

To prove that $\varphi(E \times E) \subseteq E \times E$ and $\psi(E \times E) \subseteq E \times E$, it is by (5.1), (5.2), (5.22) and (5.23) sufficient to show that

$$(x_j y_j)_{1 \le j \le p-1} \in E \tag{7.4}$$

$$(\hat{x}_j \hat{y}_{-j})_{1 \le j \le p-1} \in E \tag{7.5}$$

$$\Big(\sum_{m=0}^{p-1} x_{j+m} y_m \Big)_{1 \le j \le p-1} \in E \tag{7.6}$$

Note that (7.4) follows immediately from the conditions $x' \in E$ and $y' \in E$. To prove (7.5), note first that G_0 acts transitively on each of its cosets, i.e.

$$G_l = \{hj | h \in G_0\} \quad \text{for all} \quad j \in G_l.$$

Hence

$$E = \{(x_j)_{j=1}^{p-1} | x_{hj} = x_j \quad \text{for all} \quad h \in G_0\} \tag{7.7}$$

where as usual indices are calculated modulo p. Let $h \in G_0$ and $0 \leq j \leq p-1$. Then

$$\hat{x}_{hj} = \frac{1}{\sqrt{p}} \Big(\sum_{m=0}^{p-1} \mathrm{e}^{\mathrm{i}2\pi jhm/p} x_m \Big)$$

Since $m \to hm$ is a bijetion of $\mathbb{Z}_p$ onto itself, we can replace m by $h^{-1}m$ in the above summation (h^{-1} is the inverse of h in the group $G_0 \subseteq \mathbb{Z}_p^*$). Hence

$$\hat{x}_{hj} = \frac{1}{\sqrt{p}} \Big(\sum_{m=0}^{p-1} \mathrm{e}^{\mathrm{i}2\pi jm/p} x_{h^{-1}m} \Big). \tag{7.8}$$

Since $(x_1, \ldots, x_{p-1}) \in E$ and $h^{-1}0 = 0$ we have $x_{h^{-1}m} = x_m$ for $0 \leq m \leq p-1$ and therefore $\hat{x}_{hj} = \hat{x}_j$, $j \in \mathbb{Z}_p$. In the same way we get $\hat{y}_{-hj} = \hat{y}_{-j}$, $j \in \mathbb{Z}_p$. Hence (7.5) follows from (7.7).

To prove (7.6), put $w = (w_1, \ldots, w_{p-1})$, where

$$w_j = \sum_{m=0}^{p-1} x_{j+m} y_m, \qquad 1 \leq j \leq p-1.$$

Let $h \in G_0$. Then

$$w_{hj} = \sum_{m=0}^{p-1} x_{h_j+m} y_m, \qquad 1 \leq j \leq p-1.$$

By replacing m by hm in the above summation, we get

$$w_{hj} = \sum_{m=0}^{p-1} x_{h(j+m)} y_{hm}.$$

Since $x', y', \in E$ and $h0 = 0$, it follows that

$$w_{hj} = \sum_{m=0}^{p-1} x_{j+m} y_m = w_j.$$

Hence by (7.7), $w \in E$ which proves (7.6).

(b) It is clear that φ_E and ψ_E are holomorphic functions on $E \times E$. Let $K \subseteq E \times E$ be a compact set. Then

$$(\varphi_E)^{-1}(K) = \varphi^{-1}(K) \cap (E \times E).$$

Since φ is proper, it follows that φ_E is a proper holomorphic function of $E \times E$ into itself. The same argument shows that ψ_E is proper.

(c) Assume that $z = (x_1, \dots, x_{p-1}, y_1, \dots, y_{p-1}) \in E \times E$ is a solution to $\varphi(z) = 0$, and put

$$x = (1, x_1, \dots, x_{p-1}) \qquad \text{and} \qquad y = (1, y_1, \dots, y_{p-1}).$$

By Lemma 5.2 there exists a unique pair of subsets $K, L \subseteq \mathbb{Z}_p^*$ satisfying $|K| + |L| = p - 1$ such that

$$\operatorname{supp}(x) = L \cup \{0\}, \qquad \operatorname{supp}(\hat{x}) = K \cup \{0\} \tag{7.9}$$

$$\operatorname{supp}(y) = \mathbb{Z}_p \setminus L, \qquad -\operatorname{supp}(\hat{y}) = \mathbb{Z}_p \setminus K \tag{7.10}$$

Let $h \in G_0$. Since $z \in E \times E$ we get from the proof of (a), that $x_{hj} = x_j$ and $\hat{x}_{hj} = \hat{x}_j$ for $1 \le j \le p-1$. Hence the sets $K, L \in \mathbb{Z}_p^*$ are invariant under multiplication by all $h \in G_0$, which implies that K and L are disjoint unions of G_0-cosets, i.e

$$K = \bigcup_{l \in I} G_l, \qquad L = \bigcup_{l \in I'} G_l \tag{7.11}$$

where I and I' are finite subsets of $\{0, \dots, k-1\}$. Moreover $|I| + |I'| = k$, because $|K| + |L| = p - 1$ and each coset G_l has $\frac{p-1}{k}$ elements.

Conversely, if K, L are of the form (7.11) for $I, I' \subseteq \{0, \dots, k-1\}$ and $|I| + |I'| = K$, then by Lemma 5.2 (ii), there is precisely one element $(x, y) \in \mathbb{C}^p \times \mathbb{C}^p$ with $x_0 = y_0 = 1$ for which (7.9) and (7.10) holds and for this pair (x, y),

$$z = (x_1, \dots, x_{p-1}, y_1, \dots, y_{p-1})$$

is a solution to $\varphi(z) = 0$. We claim that $z \in E \times E$. To prove this, let $h \in G_0$ and define $(\tilde{x}, \tilde{y}) \in \mathbb{C}^p \times \mathbb{C}^p$ by

$$\tilde{x}_j = x_{hj} \quad \text{and} \quad \tilde{y}_j = y_{hj}, \qquad 0 \le j \le p-1.$$

Then $\tilde{x}_0 = \tilde{y}_0 = 1$ and by the proof of (7.8)

$$(\hat{\tilde{x}})_j = \hat{x}_{h^{-1}j} \quad \text{and} \quad (\hat{\tilde{y}})_{-j} = \hat{y}_{-h^{-1}j}, \qquad 0 \le j \le p-1.$$

Since $h, h^{-1} \in G_0$ and since K and L are invariant under multiplication by elements from G_0, it follows that (7.9) and (7.10) are satisfied for the pair $(\tilde{x}, \tilde{y})$ as well. Thus by the uniqueness of (x, y) in Lemma 5.2 (ii), we have $\tilde{x} = x$ and $\tilde{y} = y$. Hence by (7.7), $z \in E \times E$ as claimed.

Altogether, we have established a one-to-one correspondence between the zeros of φ_E and the pairs of subsets (I, I') of $\{0, \dots, k-1\}$ for which $|I| + |I'| = k$. Hence φ_E has exactly

$$\sum_{l=0}^{k} \binom{k}{l} \binom{k}{k-l} = \binom{2k}{j}$$

zeros. Let z be a zero for φ_E. Then $z \in E \times E$ and $\varphi(z) = 0$. By the proof of Theorem 5.3, $\ker \varphi'(z) = \{0\}$ and since φ'_E is the restriction of $\varphi'(z)$ to $E \times E$ also $\ker \varphi'_E(z) = \{0\}$. Therefore all the zeros of φ_E have multiplicity 1. It now follows from Theorem 4.8, that $m(\varphi_E) = \binom{2k}{k}$.

From the proof of corollary 5.4 we know that $\psi = \Lambda^{-1} \circ \varphi$, where Λ is the affine transformation of $\mathbb{C}^{2p-2}$ given by (5.25) and (5.26). It is elementary to check, that $\Lambda_E = \Lambda_{|E \times E}$ is an affine transformation of $E \times E$ onto itself. Hence $\psi_E = \Lambda_E^{-1} \circ \varphi_E$, and therefore $m(\psi_E) = m(\varphi_E) = \binom{2k}{k}$. □

Proposition 7.4. *Let $\sigma : (\mathbb{C}^*)^{p-1} \to \mathbb{C}^{p-1}$ be the proper holomorphic map defined in Theorem 6.2, i.e.*

$$\sigma(x_1, \ldots, x_{p-1})_j = \sum_{m=0}^{p-1} \frac{x_{m+j}}{x_m}, \qquad 1 \le j \le p-1$$

where $x_0 = 1$. Then the restriction σ_E of σ to $E_0 = E \cap (C^*)^{p-1}$ is a proper holomorphic function of E_0 into E with multiplicity $\binom{2k}{k}$.

Proof. Note first that $E_0 = E \cap (C^*)^{p-1}$ is an open, connected and dense subset of E. Put $a_0 = 1$ and define for $a \in E_0$

$$\sigma_a(x_1, \ldots, x_{p-1})_j = \sum_{m=0}^{p-1} a_m \frac{x_{m+j}}{x_m}, \quad 1 \le j \le p-1$$

as in lemma 6.1. It is clear from the proof of (7.6) that $\sigma_a(E_0) \subseteq E$ for all $a \in E_0$. Let $\sigma_{a,E}$ denote the restriction of σ_a to E_0. By lemma 6.1, σ_a is a proper holomorphic map from $(\mathbb{C}^*)^{p-1}$ to $\mathbb{C}^{p-1}$. As in the proof of Proposition 7.4(b), it follows that σ_a is a proper holomorphic map from E_0 to E. By simple modifications of the proofs of lemma 6.1 and Theorem 6.2 one gets first that the multiplicity of $\sigma_{a,E}$ is independent of $a \in E_0$ and next that $m(\sigma_{a,E}) = m(\psi_E)$ for all $a \in E_0$. In particular

$$m(\sigma_E) = m(\psi_E) = \binom{2k}{k}.$$

Proof of Theorem 7.1. The function $\chi : (\mathbb{C}^*)^{k-1} \to \mathbb{C}^{k-1}$ defined in Theorem 7.1 is just the function $\sigma_E : E_0 \to E$ written out in coordinates $(c_0, \ldots, c_{k-1})$ with respect to the basis $(1_{G_0}, \ldots, 1_{G_{k-1}})$ for E defined by (7.3) (cf. the derivation of the equations (7.2) in [Bj]). Therefore Theorem 7.1 is an immediate consequence of Proposition 7.4 and Theorem 4.8. □

Remark 7.5. (a) If $k = p-1$ all cyclic p-roots are of simple index k, and this special case of Theorem 7.1 is the same as Theorem 6.2.

(b) It follows from Theorem 7.1 that there are at most $\binom{2k}{k}$ distinct cyclic p-roots of simple index k on x-level (or z-level). Moreover the number of cyclic p-roots of simple index k on x-level (or z-level) counted with multiplicity is at least $\binom{2k}{k}$. However, for $k < p-1$, we have not been able to rule out the possibility that a cyclic p-root of simple index k could have higher multiplicity with respect to the set of equations (2.3) than with respect to the set of equations (7.2).

References

[AY] I.A. Aizenberg and A.P. Yuzhakov, Integral representations and Residues in Multidimensional Complex Analysis. Translations of Mathematical Monographs, Vol. 58, Amer. Math. Soc (1983).

[BaF] J. Backelin and R. Fröberg, How we proved that there are exactly 924 7-roots, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation (ISSAC'91), ACM-press (1991).

[Bj] G. Björck, Functions of modulus 1 on $\mathbb{Z}_n$, whose Fourier transforms have constant modulus, and "cyclic n-roots". Recent Advances in Fourier Analysis and its applications, NATO, Adv. Sci. Inst. Ser. C, Math. Phys. Sci., Vol 315, pp. 131-140, Klüwer Acad. Publ. (1990).

[BF1] G. Björck and R. Fröberg, A faster way to count the solutions of inhomogenious systems of algebraic equations with application to cyclic n-roots, Journ. Symbolic Computation 12, pp. 329-336 (1991).

[BF2] G. Björck and R. Fröberg, Methods to "divide out" certain solutions from systems of algebraic equations, applied to find all cyclic 8 roots. Analysis, algebra, and computers in mathematical research (Lulea 1992), Lecture Notes in Pure and Appl. Math. 156, pp. 57–70, Dekker, New York 1994.

[BH] G. Björck and U. Haagerup, All cyclic p-roots of index 3 found by symmetry-preserving calculations. Preprint (2008). `http://front.math.ucdavis.edu/0803.2506`

[BS] G. Björck and B. Saffari, New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries. C.R. Acad. Sci. Paris 320, pp. 319-324 (1995).

[Fa] J.-C. Faugère, Finding all the solutions of cyclic 9 using Gröbner basis techniques, Computer Mathematics (Matsuyama, 2001), 1-12, Lecture Notes Ser. Comput. 9, World Sci. Publ. (2001).

[Ha] U. Haagerup, Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots, Operator Algebras and Quantum Field Theory (S. Doplicher, R. Longo, J.E. Roberts, L. Zsido, eds.) pp. 296-322, International Press, Cambridge (1997).

[Ru1] W. Rudin, Function Theory in the unit ball of $\mathbb{C}^n$. Grundlehren der mathematischen Wissenschaften, Vol. 241, Springer-Verlag (1980).

[Ru2] W. Rudin, Real and Complex Analysis, 3rd edition, McGraw-Hill (1987).

[SL] P. Stevenhagen and H.W. Lenstra, Jr., Chebotarëv and his density theorem, The Mathematical Intelligencer, 18, no. 2, 26-37 (1996).

[Ta] T. Tao, An uncertainty principle for cyclic groups of prime order. Math. Research Letters 12, 121-127 (2005).

[Ts] A.K. Tsikh, Multidimensional Residues and Their Applications, Translations of mathematical Monographs Vol. 103, Amer. Math. Soc. (1991).

Uffe Haagerup
Department of Mathematics and Computer Science
University of Southern Denmark
Campusvej 55, DK-5230 Odense M
Denmark
`haagerup@imada.sdu.dk`