All cyclic p-roots of index 3, found by symmetry-preserving calculations

Göran Björck* and Uffe Haagerup†

April 4, 2007

Introduction

When using a Groebner basis to solve the highly symmetric system of algebraic equations defining the cyclic p-roots, one has the feeling that much of the advantage of computerized symbolic algebra over hand calculation is lost through the fact that the symmetry is immediately "thrown out" by the calculations. In this paper, the problem of finding (for all relevant primes p) all cyclic p-roots of index 3 (as defined in Section 1) is treated with the symmetry preserved through the calculations. Once we had found the relevant formulas, using MAPLE and MATHEMATICA, the calculations could even be made by hand (except in Section 6). On the other hand, with respect to a straightforward attack with Groebner basis, it is not even clear how this could be organized for a general p.

In other terminologies, our results (Section 5) involve listings of all bi-unimodular sequences constant on the cosets of the group G_0 of cubic residues, or equivalently all circulant complex Hadamard matrices related to G_0 (cf. [3]).

The corresponding problem for bi-unimodular sequences of index 2 was solved by the first named author in [2] and shortly after independently solved by de la Harpe and Jones [8] in the case $p \equiv 1 \pmod 4$ and by Munemasa and Watatani [11] in the case $p \equiv 3 \pmod 4$, see also [7], sect. 3.

The organization of the paper should be clear from the section headings with the understanding that "the main problem" refers to *simple* sequences of index 3 (cf. Definitions 1.2, 1.3, and 1.4).

*Department of Mathematics, Stockholm University, SE-106 91 STOCKHOLM, Sweden, bjorck@math.su.se

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

1 Notation, definitions, and problem formulation

We begin by quoting from [2] and [3] definitions of and relations between *bi-unimodular p-sequences* and *cyclic p-roots* for any positive integer p. For any p-sequence x, that is any sequence $x = (x_0, \ldots, x_{p-1})$ of p complex numbers, define its normalized Fourier transform by $\hat{x}_\nu = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} x_j \omega^{j\nu}$, where $\omega = \exp(\frac{2\pi i}{p})$. The sequence x is called *unimodular* if $|x_j| = 1$ for $j = 0, 1, \ldots, p-1$, and it is called *bi-unimodular* if both x and $\hat{x}$ are unimodular.

Taking all indices modulo p, we define the *periodic autocorrelation coefficients* γ_k by

$$\gamma_k = \sum_{j \pmod p} \bar{x}_j x_{j+k}. \tag{1.1}$$

Then, by the Parseval relation and an easy calculation,

$$\hat{x} \text{ is unimodular } \Leftrightarrow \Big(\gamma_0 = p \text{ and } \gamma_k = 0 \text{ when } k \not\equiv 0 \pmod p\Big). \tag{1.2}$$

We will now express the property of bi-unimodularity with the help of a certain system of algebraic equations. Let $z = (z_0, \ldots, z_{p-1}) \in \mathbb{C}^p$. We will call z a *"cyclic p-root"*, if z satisfies the following system of p algebraic equations:

$$\begin{aligned} z_0 + z_1 + \cdots + z_{p-1} &= 0, \\ z_0 z_1 + z_1 z_2 + \cdots + z_{p-1} z_0 &= 0, \\ &\vdots \\ z_0 z_1 \cdots z_{p-2} + z_1 z_2 \cdots z_{p-1} + \cdots + z_{p-1} z_0 \cdots z_{p-3} &= 0, \\ z_0 z_1 \cdots z_{p-1} &= 1. \end{aligned} \tag{1.3}$$

(Note that the sums are cyclic and contain just p terms and are in general *not* the elementary symmetric functions.) Let now $x \in (\mathbb{C} \setminus \{0\})^p$ and $z \in (\mathbb{C} \setminus \{0\})^p$ be related by

$$z_j = x_{j+1}/x_j \tag{1.4}$$

(with $x_p := x_0$). Clearly x is unimodular iff $\bar{x}_j = 1/x_j (\forall j)$. In this case, the equation $\gamma_k = 0$ from (1.2) becomes the k'th equation of (1.3) for $k = 1, 2, \ldots, p-1$. Let us call x *normalized* if $x_0 = 1$. Then (1.2) can be expressed as follows:

Proposition 1.1 *A normalized $x = (1, x_1, x_2, \ldots, x_{p-1})$ is bi-unimodular if and only if the corresponding z is a* unimodular *cyclic $p-$root.*

In the rest of the paper, p will be a *prime* $\equiv 1 \pmod 6$, and we will define $s := (p-1)/3$. The multiplicative group $\mathbb{Z}_p^*$ on $\mathbb{Z}_p \setminus \{0\}$ is cyclic (cf. [10]) and has a unique index-3 subgroup G_0 (the group of cubic residues modulo p). Let G_1 and G_2 be the other two cosets of G_0 in $\mathbb{Z}_p^*$. The choice of the subscripts 1 and 2 will be specified later. We will now for p-sequences define a property "being simple of index 3" meaning "taking few values in a way governed by G_0":

Definition 1.2 *We will say that* $x \in (\mathbb{C} \setminus \{0\})^p$ is simple of index 3, *if there are complex numbers,* $c_0, c_1,$ and c_2, *such that*

$$x_j = c_k \text{ when } 0 \neq j \in G_k \quad (k = 0, 1, 2). \tag{1.5}$$

Note that we have slightly changed the notation from [2] where index 3 was called "pre-index 3" and where "index 3" excluded the case of index 1, i.e. $c_0 = c_1 = c_2$.

Allowing shifts and multiplication by exponentials in a way familiar in Fourier transform theory, we make the following definition:

Definition 1.3 *We will say that* $x \in (\mathbb{C} \setminus \{0\})^p$ has index 3, *if for some fixed elements* r *and* l *of* $\mathbb{Z}_p$ *and some* simple y *of index* 3 *we have*

$$x_j = \omega^{rj} y_{j-l}, \tag{1.6}$$

which amounts to

$$x_j = \omega^{rj} c_k \text{ when } 0 \neq j - l \in G_k \quad (k = 0, 1, 2). \tag{1.7}$$

We will now define simple and general *cyclic p-roots* of index 3:

Definition 1.4 *By a cyclic p-root of index* 3 *we will mean a cyclic p-root* z *such that a corresponding* x, *as defined by* (1.4), *has index* 3. *We will also call a cyclic p-root* z *simple of index* 3, *if the corresponding* x *is simple of index* 3.

Note that we do not require x (and thus z) to be unimodular. Also note the terminological flaw that a cyclic p-root of index 3 *does not* have index 3 as an element of $(\mathbb{C} \setminus \{0\})^p$.

The main purpose of the present paper is to find explicitly all cyclic p-roots of index 3 (for every relevant prime p) using a method which utilizes the symmetries of the system (Section 5). We also give asymptotic results for large p (Section 6).

We will now show (following [2]), that if z is a simple cyclic p-root of index 3 and its corresponding x is normalized by $x_0 = 1$, then the system (1.3) reduces to a system of three equations for c_0, c_1 and c_2. (To help the reader, two examples are given at the end of the section.) Let g be a generator for $\mathbb{Z}_p^*$, and let G_0, G_1, G_2 be the cosets of G_0, numbered in such a way that $G_k = \{g^{k+3m};\ m = 0, 1, \ldots, s-1\}$. For every i and $k = 0, 1, 2$, and every $d = 1, \ldots, p-1$, we define the *transition number* $n_{ik}(d)$ as the number of elements b in $\{1, 2, \ldots, (p-1)\}$ for which $b \in G_i$ and $b + d \in G_k$. (Subscripts are taken modulo 3. We do not count $b = p - d$). Suppose now that $d \in G_a$, i.e. that $d \equiv g^{a+3m}$ for some m (congruences are modulo p). For each b which contributes to $n_{ik}(1)$, we have $b \equiv g^{i+3u}$ and $b + 1 \equiv g^{k+3v}$ for some u and v. Thus, from $d(b+1) = db + d$ we get

$$g^{k+a+3(m+v)} \equiv g^{i+a+3(m+u)} + d. \tag{1.8}$$

Writing n_{ik} instead of $n_{ik}(1)$, we thus get

$$n_{i+a,k+a}(d) = n_{ik}. \tag{1.9}$$

Let us now consider a simple cyclic p-root of index 3, and letFwith the nota the corresponding x be normalized by $x_0 = 1$ and have values given by (1.5). Fix d such that $d \in G_a$, and consider the individual products in the degree d equation of (1.3). These products will take the values c_{k+a}/c_{i+a} with the frequency $n_{i+a,k+a}(d)$, the value $c_a/1$ once (since $x_0 = 1$ and $x_d = c_a$), and the value $1/c_a$ once (since $x_{p-d} = c_a$ and $x_0 = 1$). Thus (1.9) implies that all equations whose degrees d belong to the same coset G_a, are identical, and the system (1.3) consists of the following three equations (where $n_{ik} := n_{ik}(1)$ are the transition numbers, and the c subscripts are counted modulo 3):

$$\frac{c_a}{1} \; + \; \frac{1}{c_a} \; + \; \sum_{k=0}^{2}\sum_{i=0}^{2} n_{ik}\frac{c_{k+a}}{c_{i+a}} \; = \; 0, \quad (a = 0, 1, 2). \tag{1.10}$$

We will now return to the choice of the subscripts in G_1 and G_2. Without loss of generality, we can (and do in fact from now on) suppose that

$$n_{02} > n_{01}. \tag{1.11}$$

In fact, we must have $n_{02} \neq n_{01}$ (see Corollary 2.3), and if $n_{02} < n_{01}$, we replace the generator g by $g' := g^{2+3j}$, for some j such that $2 + 3j$ is relatively prime to $p - 1$. Since $g \in G_1$ and $g' \in G_2$, this will interchange G_1 and G_2, and we have arrived at (1.11).

Finally, we will give the promised examples: Let $p = 13$, and take $g = 2$ or 11. Then $G_0 = \{1, 5, 8, 12\}$, $G_1 = \{2, 3, 10, 11\}$, $G_2 = \{4, 6, 7, 9\}$, and we will have $n_{00} = 0$, $n_{01} = n_{10} = n_{12} = n_{21} = n_{22} = 1$, and $n_{02} = n_{20} = n_{11} = 2$. For a further example (with explicit values of c_0, c_1, and c_2), see the beginning of the proof of Propositions 5.2 and 5.3.

2 Number theoretic results used

In this section we give some relations between the transition numbers n_{ik} defined in (1.9) and appearing in (1.10). These relations will lead to explicit formulas for the n_{ik}.

The mapping $b \to p - b$ from Z_p to Z_p will leave each one of the sets G_i invariant and thus we have

$$n_{ij} = n_{ji}, \;\; i, j = 0, 1, 2. \tag{2.1}$$

Moreover $\sum_{j=0}^{2} n_{ij} = \sharp((G_i \setminus \{p-1\})$, and thus (recall that we have defined $s = \frac{p-1}{3}$)

$$\sum_{j=0}^{2} n_{0j} = s - 1, \;\; \sum_{j=0}^{2} n_{1j} = \sum_{j=0}^{2} n_{2j} = s. \tag{2.2}$$

We will get one more linear relation between the n_{ik} in the following way: By (1.9), all $n_{01}(d)$ with d belonging to the same G_a are equal. Thus, since $\sharp(G_0) = \sharp(G_1) = \sharp(G_2) = s$, we get $s \cdot s = \sum_{d=1}^{p-1} n_{01}(d) = \sum_{a=0}^{2} s \cdot n_{-a,1-a}$, which becomes

$$n_{01} + n_{12} + n_{20} = s. \tag{2.3}$$

With the help of (2.1), (2.2) and (2.3) we can express all our nine transition numbers n_{ik} in terms of n_{01} and n_{02}:

$$\begin{cases} n_{00} &= s-1-n_{01}-n_{02}, \\ n_{11} &= n_{20}=n_{02}, \\ n_{22} &= n_{10}=n_{01}, \\ n_{12} &= n_{21}=s-n_{01}-n_{02}. \end{cases} \tag{2.4}$$

These relations are given in [2] and also in [5], Exercise 4.29 (d). There is, however, one further equation satisfied by the transition numbers. We first state this equation in terms of n_{12}, n_{01} and n_{02}:

Proposition 2.1 *Let p be a prime $\equiv 1 \pmod 6$, and let n_{12}, n_{01} and n_{02} be the transition numbers defined in Section 1. Then*

$$n_{01}n_{02}+n_{01}n_{12}+n_{02}n_{12}=n_{01}^2+n_{02}^2+n_{12}^2-n_{12}.$$

We have proved this result by establishing the following explicit formulas for the convolutions $F*G$ (defined by $(F*G)(a)=\sum_{b\in\mathbf{Z_p}}F(a-b)G(b)$) of certain complex-valued functions F and G on $\mathbb{Z}_p$. Let Γ_j be the characteristic functions χ_{G_j} of G_j $(j=0,1,2)$, and let $I=\chi_{\{0\}}$. Then, (with indices taken modulo 3):

$$\Gamma_i*\Gamma_i=n_{i,i}\Gamma_0+n_{i+2,i+2}\Gamma_1+n_{i+1,i+1}\Gamma_2+sI,$$

$$\Gamma_i*\Gamma_{i+1}=n_{i,i+1}\Gamma_0+n_{i+2,i}\Gamma_1+n_{i+1,i+2}\Gamma_2.$$

Our original proof of Proposition 2.1 used these formulas and the commutativity and associativity of the convolution. Also, the reader of [5] is encouraged in Exercise 4.29 (e) to prove this proposition. But it turns out that Proposition 2.1 is just a reformulation of a theorem of Gauss (in *Disquisitiones*, Article 358), which we give in a form a little more precise than in [10] or [13] or [5]:

Proposition 2.2 *Let p be a prime $\equiv 1 \pmod 6$, and let n_{12}, n_{01} and n_{02} be the transition numbers defined in Section 1. Then there are integers A and B such that*

$$4p=A^2+27B^2.$$

If we require that $A\equiv 1 \pmod 3$ and $B>0$ (which is always possible and which we always do), then A and B are unique, and we have

$$A=9n_{12}-p-1 \text{ and } B=|n_{02}-n_{01}|.$$

Since $4p$ is not a square, we must have $B\neq 0$, and hence we get the following corollary, which we needed at the end of Section 1:

Corollary 2.3 *Let p be a prime $\equiv 1 \pmod 6$, and let n_{01} and n_{02} be the transition numbers defined in Section 1. Then $n_{01}\neq n_{02}$.*

Recall that we have in fact chosen G_1 and G_2 in such a way that $n_{02} > n_{01}$. Since $B > 0$, we thus have

$$A = 9n_{12} - p - 1 \text{ and } B = n_{02} - n_{01}. \tag{2.5}$$

Solving for n_{ik} the linear system given by (2.4) and (2.5), we have proved the following corollary of Proposition 2.2:

Corollary 2.4 *Let p be a prime $\equiv 1 \pmod 6$, let n_{ik} be the transition numbers defined in Section 1, and let A and B be the numbers given in Proposition 2.2. Then*

$$\begin{aligned} n_{12} = n_{21} &= \tfrac{1}{9}(p + A + 1), \\ n_{02} = n_{20} = n_{11} &= \tfrac{1}{18}(2p - A + 9B - 4), \\ n_{01} = n_{10} = n_{22} &= \tfrac{1}{18}(2p - A - 9B - 4), \\ n_{00} + n_{11} + n_{22} &= \tfrac{1}{3}(p - 4). \end{aligned} \tag{2.6}$$

Proof of Proposition 2.1: Starting from Proposition 2.2 and replacing A and B by the expressions given there and then replacing p by the expression $p = 3(n_{01}+n_{12}+n_{20})+1$ from (2.3) we get

$$0 = A^2 + 27B^2 - 4p = -36(n_{01}n_{02} + n_{01}n_{12} + n_{02}n_{12} - n_{01}^2 - n_{01}^2 - n_{02}^2 - n_{12}^2 + n_{12})$$

which completes the proof.

Proof of Proposition 2.2: The calculations needed are given very explicitly in [13]. In fact the theorem of Gauss stated there in Section IV.2 is our Proposition 2.2 except that the *statement* of the theorem does not contain the value of B and for A gives the value $M_p - p - 1$, where M_p is the number of solutions (x, y, z) in $\mathbf{Z}_p^3$ of $x^3 + y^3 + z^3 = 0$ in the projective sense. In the *proof* of the theorem, the formula $mB = [STT] - [STS]$ is given where m is our s, where R is our G_0, S and T are our G_1 and G_2 (in some order), and where finally the symbol $[XYZ]$ is defined for subsets X, Y, Z of $\mathbb{Z}_p$ as the number of triples (x, y, z) such that $x \in X$, $y \in Y$, and $z \in Z$ and $x + y + z = 0$. In the course of the proof it is also shown that $mM_p = 9[RTS]$. Thus all that remains for us to have a proof of Proposition 2.2 is to check that $[G_1G_2G_2] - [G_1G_2G_1] = s(n_2 - n_1)$ and $[G_0G_2G_1] = sn$. We write $x + y + z = 0$ as $x + y = -z$, and since $G_2 = -G_2$, we have that

$$[G_{i+2}G_2G_{k+2}] = \sum_{y \in G_2} n_{i+2,k+2}(y) = sn_{ik},$$

where we have used (1.9) with $a = 2$ and $d = y$. Thus $[G_1G_2G_2] - [G_1G_2G_1] = s(n_{20} - n_{22})$ and $[G_0G_2G_1] = sn_{12}$, and the result follows from (2.4), which completes the proof.

3 Reduction of the main problem

Let p be a prime of the form $p = 3s + 1$, $s \in \mathbb{N}$ and let

$$4p = A^2 + 27B^2$$

be the Gauss decomposition of $4p$, i.e. $A, B \in \mathbb{Z}$, $A \equiv 1 \pmod 3$ and $B > 0$ (cf. Proposition 2.2). Our main problem is to find every triple (c_0, c_1, c_2) that defines a normalized p-sequence x, simple of index 3, which via (1.4) corresponds to a cyclic p-root z, simple of index 3, i.e. to solve the set of equations (cf. (1.10) and Corollary 2.4)

$$\left\{\begin{array}{rcl} c_0 + \frac{1}{c_0} & = & -\frac{p-4}{3} - n_{12}\left(\frac{c_2}{c_1} + \frac{c_1}{c_2}\right) - n_{02}\left(\frac{c_0}{c_2} + \frac{c_2}{c_0}\right) - n_{01}\left(\frac{c_1}{c_0} + \frac{c_0}{c_1}\right) \\ c_1 + \frac{1}{c_1} & = & -\frac{p-4}{3} - n_{12}\left(\frac{c_0}{c_2} + \frac{c_2}{c_0}\right) - n_{02}\left(\frac{c_1}{c_0} + \frac{c_0}{c_1}\right) - n_{01}\left(\frac{c_2}{c_1} + \frac{c_1}{c_2}\right) \\ c_2 + \frac{1}{c_2} & = & -\frac{p-4}{3} - n_{12}\left(\frac{c_1}{c_0} + \frac{c_0}{c_1}\right) - n_{02}\left(\frac{c_2}{c_1} + \frac{c_1}{c_2}\right) - n_{01}\left(\frac{c_0}{c_2} + \frac{c_2}{c_0}\right) \end{array}\right. \tag{3.1}$$

with

$$n_{12} = \frac{p + A + 1}{9}, \quad n_{02} = \frac{2p - A + 9B - 4}{18}, \quad n_{01} = \frac{2p - A - 9B - 4}{18}. \tag{3.2}$$

Proposition 3.1 *Assume (c_0, c_1, c_2) is a solution to (3.1). Then the numbers*

$$h_j = \frac{c_{j+2}}{c_{j+1}} + \frac{c_{j+1}}{c_{j+2}}, \quad j = 0, 1, 2, \tag{3.3}$$

(index counted modulo 3) are up to a cyclic permutation given by

$$h_j = \xi_1 + \eta_1 \cos\left(\theta - \frac{2\pi}{3} j\right), \quad j = 0, 1, 2, \tag{3.4}$$

where $\theta = \frac{1}{3}\mathrm{Arccos}\left(\frac{A}{2\sqrt{p}}\right)$ and the pair (ξ_1, η_1) is one of the following four pairs:

$$\left\{\begin{array}{rcl} \xi_1^{(0)} & = & 2 \\ \eta_1^{(0)} & = & 0\,, \end{array}\right. \tag{3.5}$$

$$\left\{\begin{array}{rcl} \xi_1^{(1)} & = & -\frac{p^2-6p+2A}{p^2-3p-A} \\ \eta_1^{(1)} & = & \frac{6\sqrt{p}(p-4)}{p^2-3p-A}\,, \end{array}\right. \tag{3.6}$$

$$\left\{\begin{array}{rcl} \xi_1^{(2)} & = & \frac{-2pA-9p-4+3\sqrt{p(p+4A+16)}}{2(pA+3p-1)} \\ \eta_1^{(2)} & = & \frac{3\sqrt{p}(p+2)-3p\sqrt{p+4A+16}}{pA+3p-1}\,, \end{array}\right. \tag{3.7}$$

$$\left\{\begin{array}{rcl} \xi_1^{(3)} & = & \frac{-2pA-9p-4-3\sqrt{p(p+4A+16)}}{2(pA+3p-1)} \\ \eta_1^{(3)} & = & \frac{3\sqrt{p}(p+2)+3p\sqrt{p+4A+16}}{pA+3p-1}\,. \end{array}\right. \tag{3.8}$$

Remark 3.2 a) Let us first check that all the above formulas give well-defined real numbers: Since $p > 4$ and $|A| < 2\sqrt{p}$ we have

$$p^2 - 3p - A > p^2 - 3p - 2\sqrt{p} = \sqrt{p}(\sqrt{p} - 2)(\sqrt{p} + 1)^2 > 0.$$

Moreover,

$$p + 4A + 16 > p - 8\sqrt{p} + 16 = (\sqrt{p} - 4)^2 \geq 0$$

and since $A \equiv 1 \pmod 3$, we have $|A + 3| \geq 1$. Hence

$$|pA + 3p - 1| \geq |(A + 3)p| - 1 \geq p - 1 > 0.$$

b) We do not prove in this section that all four cases (3.5)–(3.8) actually occur. However this will follow from the proof of Theorem 4.1 in next section.

Proof of Proposition 3.1: To make our method of proof more transparent, we first consider the case $p = 7$. In this case $A = B = 1$, $n_{12} = n_{02} = 1$, and $n_{01} = 0$. Put

$$f_j = c_j + \frac{1}{c_j} \qquad \text{and} \qquad h_j = \frac{c_{j+2}}{c_{j+1}} + \frac{c_{j+1}}{c_{j+2}}.$$

Then (3.1) becomes

$$\begin{cases} f_0 &= -1 - h_0 - h_1 \\ f_1 &= -1 - h_1 - h_2 \\ f_2 &= -1 - h_2 - h_0. \end{cases} \tag{3.9}$$

Consider now the matrix

$$K = \begin{bmatrix} 2 & f_0 & f_1 & f_2 \\ f_0 & 2 & h_2 & h_1 \\ f_1 & h_2 & 2 & h_0 \\ f_2 & h_1 & h_0 & 2 \end{bmatrix}.$$

Since

$$K = \begin{bmatrix} 1 \\ c_0 \\ c_1 \\ c_2 \end{bmatrix} [1, \frac{1}{c_0}, \frac{1}{c_1}, \frac{1}{c_2}] + \begin{bmatrix} 1 \\ \frac{1}{c_0} \\ \frac{1}{c_1} \\ \frac{1}{c_2} \end{bmatrix} [1, c_0, c_1, c_2],$$

we get (considering K as an operator on column vectors)

$$\text{range}(K) = \text{span} \left\{ \begin{bmatrix} 1 \\ c_0 \\ c_1 \\ c_2 \end{bmatrix}, \begin{bmatrix} 1 \\ \frac{1}{c_0} \\ \frac{1}{c_1} \\ \frac{1}{c_2} \end{bmatrix} \right\}.$$

Hence $\mathrm{rank}(K) \leq 2$, and thus all 3×3 submatrices of K have determinant $= 0$.

Let $L = [\ell_{ij}]_{i,j=1}^{4}$ be the co-factor matrix of K, i.e.

$$\ell_{ij} = (-1)^{i+j} \det(K_{ij}),$$

where K_{ij} is the 3×3 submatrix of K obtained by erasing the i'th row and the j'th column. Put

$$\begin{cases} p_1 &= \ell_{11} \\ p_2 &= \ell_{12} + \ell_{13} + \ell_{14} \\ p_3 &= \ell_{22} + \ell_{33} + \ell_{44} \\ p_4 &= \ell_{23} + \ell_{34} + \ell_{42}. \end{cases} \tag{3.10}$$

Since $\ell_{ij} = 0$ for all i and j, we have in particular

$$p_1 = p_2 = p_3 = p_4 = 0.$$

This gives four equations of degree three in $(f_0, f_1, f_2, h_0, h_1, h_2)$, but taking (3.9) into account, we can consider p_1, p_2, p_3, p_4 as polynomials in (h_0, h_1, h_2) only, namely

$$\begin{aligned} p_1 &= 8 - 2(h_0^2 + h_1^2 + h_2^2) + 2h_0h_1h_2, \\ p_2 &= 12 + 4(h_0 + h_1 + h_2) - 3(h_0^2 + h_1^2 + h_2^2) - 4(h_0h_1 + h_1h_2 + h_2h_0) \\ &\quad -(h_0^3 + h_1^3 + h_2^3) + 2(h_0h_1^2 + h_1h_2^2 + h_2h_0^2) + 3h_0h_1h_2, \\ p_3 &= 12 - 14(h_0 + h_1 + h_2) - 8(h_0^2 + h_1^2 + h_2^2) - 2(h_0h_1 + h_1h_2 + h_2h_0) \\ &\quad +2(h_0h_1^2 + h_1h_2^2 + h_2h_0^2) + 4(h_0^2h_1 + h_1^2h_2 + h_2^2h_0) + 6h_0h_1h_2, \\ p_4 &= 6 + 3(h_0 + h_1 + h_2) + (h_0^2 + h_1^2 + h_2^2) + 5(h_0h_1 + h_1h_2 + h_2h_0) \\ &\quad -2(h_0h_1^2 + h_1h_2^2 + h_2h_0^2) - 6h_0h_1h_2. \end{aligned}$$

Let s_1, s_2, s_3 denote the three elementary symmetric polynomials in h_0, h_1, h_2:

$$\begin{cases} s_1 &= h_0 + h_1 + h_2 \\ s_2 &= h_0h_1 + h_1h_2 + h_2h_0 \\ s_3 &= h_0h_1h_2 \end{cases} \tag{3.11}$$

and let a denote the antisymmetric polynomial:

$$a = (h_0 - h_1)(h_1 - h_2)(h_2 - h_0). \tag{3.12}$$

Then,

$$\begin{aligned} h_0^2 + h_1^2 + h_2^2 &= s_1^2 - 2s_2, \\ h_0^3 + h_1^3 + h_2^3 &= s_1^3 - 3s_1s_2 + 3s_3, \\ h_0h_1^2 + h_1h_2^2 + h_2h_0^2 &= \tfrac{1}{2}(s_1s_2 - 3s_3 + a), \\ h_0^2h_1 + h_1^2h_2 + h_2^2h_0 &= \tfrac{1}{2}(s_1s_2 - 3s_3 - a). \end{aligned}$$

Hence p_1, p_2, p_3, p_4 can be expressed as polynomials in s_1, s_2, s_3 and a. One gets

$$\begin{aligned} p_1 &= (8 - 2s_1^2) + 4s_2 + 2s_3, \\ p_2 &= (12 + 4s_1 - 3s_1^2 - s_1^3) + (2 + 4s_1)s_2 - 3s_3 + a, \\ p_3 &= (12 - 14s_1 - 8s_1^2) + (14 + 3s_1)s_2 - 3s_3 - a, \\ p_4 &= (6 + 3s_1 + s_1^2) + (3 - s_1)s_2 - 3s_3 - a. \end{aligned}$$

Therefore the equations $p_1 = p_2 = p_3 = p_4 = 0$ can be rewritten in the form

$$\begin{bmatrix} 8 - 2s_1^2 & 4 & 2 & 0 \\ 12 + 4s_1 - 3s_1^2 - s_1^3 & 2 + 4s_1 & -3 & 1 \\ 12 - 14s_1 - 8s_1^2 & 14 + 3s_1 & -3 & -1 \\ 6 + 3s_1 + s_1^2 & 3 - s_1 & -3 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ s_2 \\ s_3 \\ a \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{3.13}$$

A necessary condition for the existence of solutions to this system of equations is that the determinant of the coefficient matrix M is 0. One finds

$$\det(M) = 8(s_1 - 6)(s_1 + 1)(s_1^2 + 9s_1 + 15).$$

Thus s_1 must be one of the four numbers

$$s_1^{(0)} = 6, \quad s_1^{(1)} = -1, \quad s_1^{(2)} = \frac{-9 + \sqrt{21}}{2}, \quad \text{and} \quad s_1^{(3)} = \frac{-9 - \sqrt{21}}{2}.$$

Let $M^{(i)}$ be the fourmatrix obtained by substituting $s_1 = s_1^{(i)}$ in M $(i = 0, 1, 2, 3)$. It is easy to compute the kernel for $M^{(i)}$, $i = 0, 1, 2, 3$. One finds $\dim(\ker(M^{(i)}) = 1$ in all cases, and (for convenience writing vectors in row form)

$$\begin{aligned} \ker(M^{(0)}) &= \text{span}\{[1, 12, 8, 0]\}, \\ \ker(M^{(1)}) &= \text{span}\{[1, -2, 1, 7]\}, \\ \ker(M^{(2)}) &= \text{span}\Big\{\Big[1, -9 + 2\sqrt{21}, \frac{79 - 17\sqrt{21}}{2}, -189 + 42\sqrt{21}\Big]\Big\}, \\ \ker(M^{(3)}) &= \text{span}\Big\{\Big[1, -9 - 2\sqrt{21}, \frac{79 + 17\sqrt{21}}{2}, -189 - 42\sqrt{21}\Big]\Big\}. \end{aligned}$$

Hence there are exactly 4 solutions (s_1, s_2, s_3, a) to (3.13):

$$\begin{array}{llll} (s_1^{(0)} = 6, & s_2^{(0)} = 12, & s_3^{(0)} = 8, & a^{(0)} = 0 \quad), \\ (s_1^{(1)} = -1, & s_2^{(1)} = -2, & s_3^{(1)} = 1, & a^{(1)} = -7 \quad), \\ \Big(s_1^{(2)} = \frac{-9+\sqrt{21}}{2}, & s_2^{(2)} = -9 + 2\sqrt{21}, & s_3^{(2)} = \frac{79-17\sqrt{21}}{2}, & a^{(2)} = -189 + 42\sqrt{21} \quad \Big), \\ \Big(s_1^{(3)} = \frac{-9-\sqrt{21}}{2}, & s_2^{(2)} = -9 - 2\sqrt{21}, & s_3^{(2)} = \frac{79+17\sqrt{21}}{2}, & a^{(3)} = -189 - 42\sqrt{21} \quad \Big). \end{array} \tag{3.14}$$

However, there is a hidden relation between s_1, s_2, s_3, and a, namely a^2 is a symmetric polynomial in (h_0, h_1, h_2) and can therefore be expressed in terms of s_1, s_2 and s_3. One finds

$$a^2 = s_1^2 s_2^2 - 4s_1^3 s_3 - 4s_2^3 + 18 s_1 s_2 s_3 - 27 s_3^2. \tag{3.15}$$

It is elementary to check that this equality holds for each of the four sets $(s_1^{(i)}, s_2^{(i)}, s_3^{(i)}, a^{(i)})$ found above.

We must now in each case find h_0, h_1, h_2 by solving the 4 equations:

$$\begin{cases} h_0 + h_1 + h_2 = s_1^{(i)} \\ h_0 h_1 + h_1 h_2 + h_2 h_0 = s_2^{(i)} \\ h_0 h_1 h_2 = s_3^{(i)} \\ (h_0 - h_1)(h_1 - h_2)(h_2 - h_0) = a^{(i)}. \end{cases} \tag{3.16}$$

The solutions (h_0, h_1, h_2) to the first three equations in (3.16) are exactly the three zeros (in arbitrary order) of the polynomial

$$h^3 - s_1^{(i)} h^2 + s_2^{(i)} h - s_3^{(i)}. \tag{3.17}$$

Since (3.15) holds in each of the four cases $i = 0, 1, 2, 3$, we have

$$(h_0 - h_1)(h_1 - h_2)(h_2 - h_0) = \pm a^{(i)}.$$

Hence the fourth coordinate in the solution to the equations (3.13) only determines the cyclic order of the three numbers (h_0, h_1, h_2). For $i = 0$, (3.17) becomes

$$h^3 - 6h^2 + 12h - 8 = 0.$$

Hence $h_0 = h_1 = h_2 = 2$ which corresponds to case (3.5) in Proposition 3.1.

In the cases $i = 1, 2, 3$ we solve (3.17) by the classical trigonometric formula in the form of Lemma 3.5 below, where we use (3.31) when $a < 0$ and (3.33) when $a > 0$. This will give the correct cyclic order of (h_0, h_1, h_2). Note that Lemma 3.5 can be applied because in all three cases ($i = 1, 2, 3$) s_1, s_2, s_3, and a are all real (being solutions to the real linear system (3.13)) and thus $a^2 > 0$, which by (3.15) means that $s_1^2 s_2^2 - 4s_1^3 s_3 - 4s_2^3 + 18 s_1 s_2 s_3 - 27 s_2^3 = a^2 > 0$. Hence, up to cyclic permutation of (h_0, h_1, h_2) we have

$$h_j = \xi_1 + \eta_1 \cos\left(\theta - \frac{2\pi}{3} j\right)$$

where

$$\begin{cases} \xi_1 &= \frac{1}{3} s_1 \\ \eta_1 &= -\mathrm{sign}(a) \cdot \frac{2}{3} (s_1^2 - 3s_2)^{\frac{1}{2}} \\ \theta &= \frac{1}{3} \mathrm{Arccos}\big(- \mathrm{sign}(a) \frac{2s_1^3 - 9 s_1 s_2 + 27 s_3}{2(s_1^2 - 3s_2)^{\frac{3}{2}}} \big). \end{cases}$$

It turns out that $\theta^{(i)} = \frac{1}{3}\mathrm{Arccos}\left(\frac{1}{2\sqrt{7}}\right)$ in all three cases ($i = 1, 2, 3$), while

$$\begin{aligned}
\left(\xi_1^{(1)}, \eta_1^{(1)}\right) &= \left(-\frac{1}{3}, \frac{2}{3}\sqrt{7}\right), \\
\left(\xi_1^{(2)}, \eta_1^{(2)}\right) &= \left(-\frac{3}{2} + \frac{\sqrt{21}}{6}, \sqrt{7} - \frac{7}{3}\sqrt{3}\right), \\
\left(\xi_1^{(3)}, \eta_1^{(3)}\right) &= \left(-\frac{3}{2} - \frac{\sqrt{21}}{6}, \sqrt{7} + \frac{7}{3}\sqrt{3}\right).
\end{aligned}$$

This gives case (3.6), (3.7), and (3.8) respectively in Proposition 3.1 in the case $p = 7$.

Consider now a general prime p, $p \equiv 1 \pmod 3$. This case is mathematically no more difficult than the case $p = 7$, but a computer algebra language as MAPLE or MATHEMATICA is helpful for bookkeeping purpose. Using (3.2) and (3.1) instead of (3.9), the polynomials (3.10) again become polynomials in s_1, s_2, s_3, a, namely

$$\begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} = \begin{bmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{bmatrix} \begin{bmatrix} 1 \\ s_2 \\ s_3 \\ a \end{bmatrix} \tag{3.18}$$

where the m_{ij}:s (after replacing B^2 by $(4p - A^2)/27$) are the following polynomials in s_1:

$$\begin{aligned}
m_{11} &= -2s_1^2 + 8, \\
m_{12} &= 4, \\
m_{13} &= 2, \\
m_{14} &= 0, \\
m_{21} &= -\tfrac{1}{9}(A + p + 1)s_1^3 + \tfrac{1}{9}(2A - 7p + 20)s_1^2 + 4s_1 + (4p - 16), \\
m_{22} &= \tfrac{4}{9}(A + p + 1)s_1 + \tfrac{1}{3}(4p - 2A - 20), \\
m_{23} &= -A - 2, \\
m_{24} &= B, \\
m_{31} &= \tfrac{2}{81}(p^2 - pA - 7p + A^2 + 2A + 4)s_1^3 - \tfrac{2}{27}(pA + 12p + 17)s_1^2 \\
&\quad -\tfrac{2}{3}p(p - 4)s_1 + \tfrac{4}{3}(2 - p^2 + 8p), \\
m_{32} &= \tfrac{1}{27}(-6A + 12p - 3A^2 - 8 + 2pA)s_1 + \tfrac{2}{9}(6p + pA + 14), \\
m_{33} &= \tfrac{1}{3}(2A + A^2 - 2p + 2), \\
m_{34} &= -\tfrac{1}{3}(A + 2)B, \\
m_{41} &= \tfrac{1}{81}(7A - p^2 + 4p + 2A^2 + pA + 5)s_1^3 + \tfrac{1}{27}(-6A + 6p + pA - 16)s_1^2 \\
&\quad +\tfrac{1}{3}(p^2 - 4p - 12)s_1 + \tfrac{2}{3}(p^2 - 8p + 16), \\
m_{42} &= -\tfrac{1}{27}(9A + 3A^2 + pA + 8)s_1 + \tfrac{1}{9}(6A - pA + 28), \\
m_{43} &= \tfrac{1}{3}(2A + A^2 - 2p + 2), \\
m_{44} &= -\tfrac{1}{3}(A + 2)B.
\end{aligned}$$

Since $p_1 = p_2 = p_3 = p_4 = 0$, we must have $\det M = 0$ where $M = [m_{ij}]_{i,j=1}^4$. One finds

$$\det M = \tfrac{8B}{729}(s_1 - 6)q(s_1)r(s_1),$$

where

$$\begin{cases} q(s_1) &= (p^2 - 3p - A)s_1 + (6A + 3p^2 - 18p) \\ r(s_1) &= (pA + 3p - 1)s_1^2 + (6pA + 27p + 12)s_1 + (9pA + 54p - 36). \end{cases} \tag{3.19}$$

It is interesting that if $\det M$ is considered as a polynomial in the independent variables s_1, p, A, B, forgetting the relation $4p = A^2 + 27B^2$, we will get an irreducible cubic polynomial instead of $q(s_1)r(s_1)$. By Remark 3.2, $p^2 - 3p - A \neq 0$ and $pA + 3p - 1 \neq 0$, so the equation $\det(M) = 0$ has exactly 4 solutions (counted with multiplicity), namely

$$\begin{cases} s_1^{(0)} &= 6 \\ s_1^{(1)} &= \frac{18p - 3p^2 - 6A}{p^2 - 3p - A} \\ s_1^{(2)} &= \frac{-6pA - 27p - 12 + 9\sqrt{p(p+4A+16)}}{2(pA+3p-1)} \\ s_1^{(3)} &= \frac{-6pA - 27p - 12 - 9\sqrt{p(p+4A+16)}}{2(pA+3p-1)}. \end{cases} \tag{3.20}$$

Let $M^{(i)}$ be the 4×4-matrix obtained by substituting $s_1 = s_1^{(i)}$ in M. We next compute the kernel of $M^{(i)}$ in each of the four cases. Let $M_{jk}^{(i)}$ be the 3×3 submatrix of $M^{(i)}$ obtained by erasing the j'th row and the k'th column of $M^{(i)}$. Then

$$\det(M_{11}^{(i)}) = -\frac{2B}{27}(A + p + 1)((pA + A + 4p)s_1^{(i)} + 3pA - 6A + 12p).$$

In particular

$$\begin{aligned} \det(M_{11}^{(0)}) &= -\frac{2B}{3}p(p + A + 1)(A + 4), \\ \det(M_{11}^{(1)}) &= -\frac{2B}{3}p(p + A + 1)(4p - A^2), \\ \det(M_{11}^{(2)}) \cdot \det(M_{11}^{(3)}) &= -\frac{4B^2 p(p + A + 1)^2(A + 4)(4p - A^2)}{9(pA + 3p - 1)}. \end{aligned}$$

Since $A \equiv 1 \pmod 3$, we have $A + 4 \neq 0$. Moreover $4p - A^2 = 27B^2 > 0$ and $p + A + 1 > (\sqrt{p} - 1)^2 \geq 0$. Hence $\det(M_{11}^{(i)}) \neq 0$ in all four cases. Together with $\det(M^{(i)}) = 0$, this shows that for all i, $M^{(i)}$ has rank 3 and thus

$$\dim(\ker(M^{(i)}) = 1, \qquad i = 0, 1, 2, 3.$$

Hence in each case ($i = 0, 1, 2, 3$), $s_2^{(i)}, s_3^{(i)}$, and $a^{(i)}$ are uniquely determined by (3.18). Applying Cramer's rule to the last three equations in (3.18) we get

$$s_2^{(i)} = -\frac{\det M_{12}^{(i)}}{\det M_{11}^{(i)}}, \quad s_3^{(i)} = \frac{\det M_{13}^{(i)}}{\det M_{11}^{(i)}}, \quad a^{(i)} = -\frac{\det M_{14}^{(i)}}{\det M_{11}^{(i)}}.$$

For $i=0$, $(s_1^{(0)}, s_2^{(0)}, s_3^{(0)}, a^{(0)}) = (6, 12, 8, 0)$ as in the case $p=7$, and for $i=1$ we have

$$\begin{cases} s_1^{(1)} &= \frac{18p-3p^2-6A}{p^2-3p-A} \\ s_2^{(1)} &= 3\frac{4p^2A-24pA+4A^2+p^4-21p^3+108p^2-144p}{(p^2-3p-A)^2} \\ s_3^{(1)} &= \frac{20p^2A-96pA+8A^2-p^4+42p^3-360p^2+864p}{(p^2-3p-A)^2} \\ a^{(1)} &= -\frac{729p(p-4)^3B}{(p^2-3p-A)^3}. \end{cases} \tag{3.21}$$

For $i=2,3$, it is more convenient to express the solutions in terms of $u=\sqrt{p}$ and $v=\sqrt{p+4A+16}$. We get

$$\begin{cases} s_1^{(2)} &= -3\frac{u^2+uv-4}{u^2+uv+2} \\ s_2^{(2)} &= 3\frac{(u^2+uv+6u-4)(u^2+uv-6u-4)}{(u^2+uv+2)^2} \\ s_3^{(2)} &= -\frac{u^4+2u^3v-176u^2+u^2v^2+40uv-32}{(u^2+uv+2)^2} \\ a^{(2)} &= 5832\frac{Bu^2}{(u^2+uv+2)^3} \end{cases} \tag{3.22}$$

and

$$\begin{cases} s_1^{(3)} &= -3\frac{u^2-uv-4}{u^2-uv+2} \\ s_2^{(3)} &= 3\frac{(u^2-uv+6u-4)(u^2-uv-6u-4)}{(u^2-uv+2)^2} \\ s_3^{(3)} &= -\frac{u^4-2u^3v-176u^2+v^2u^2-40uv-32}{(u^2-uv+2)^2} \\ a^{(3)} &= 5832\frac{Bu^2}{(u^2-uv+2)^3}. \end{cases} \tag{3.23}$$

Note that all the numbers are well-defined because by Remark 3.2, $p^2-3p-A>0$, $p+4A+16>0$ and

$$(u^2+uv+2)(u^2-uv+2) = -4(pA+3p-1) \neq 0. \tag{3.24}$$

For $i=0$, we get as for $p=7$ that $h_0=h_1=h_2=2$ which corresponds to (3.5) in Proposition 3.1. It is easy to check that the identity (3.15) is satisfied for the above sets $(s_1^{(i)}, s_2^{(i)}, s_3^{(i)}, a^{(i)})$, so as in the case $p=7$ we can determine h_0, h_1, h_2 by Lemma 3.5 where we use (3.31) when $a^{(i)}<0$ and (3.33), when $a^{(i)}>0$ to obtain the correct cyclic ordering. Note that $a^{(1)}<0$, $a^{(2)}>0$ and $\mathrm{sign}(a^{(3)}) = \mathrm{sign}(u^2-uv+2) = -\mathrm{sign}(pA+3p-1)$. We obtain

$$h_j = \xi_1^{(i)} + \eta_1^{(i)} \cos\left(\theta^{(i)} - \frac{2\pi}{3}j\right), \quad j=0,1,2,$$

where $\theta^{(i)} = \frac{1}{3}\mathrm{Arccos}\left(\frac{A}{2\sqrt{p}}\right)$ in all three cases $(i=2,3,4)$, while

$$\begin{cases} (\xi_1^{(1)}, \eta_1^{(1)}) &= \left(-\frac{p^2-6p+2A}{p^2-3p-A}, \frac{6\sqrt{p}(p-4)}{p^2-3p-A}\right) \\ (\xi_1^{(2)}, \eta_1^{(2)}) &= \left(-\frac{u^2+uv-4}{u^2+uv+2}, -\frac{12u}{u^2+uv+2}\right) \\ (\xi_1^{(3)}, \eta_1^{(3)}) &= \left(-\frac{u^2-uv-4}{u^2-uv+2}, -\frac{12u}{u^2-uv+2}\right). \end{cases} \tag{3.25}$$

Using $u = \sqrt{p}$, $v = \sqrt{p + 4A + 16}$, and the equality in (3.24), we get (3.6), (3.7) and (3.8) in Proposition 3.1. This completes the proof of the Proposition.

Remark 3.3 It easily follows from the proof that if $c = (c_0, c_1, c_2)$ is a solution to the system (3.1) and two c_i are equal, then they are all equal. In fact, if e.g. $c_1 = c_2$, then with h as in (3.3) we get $h_1 = h_2$, which leads to $a = 0$. But since $B \neq 0$, it follows from (3.21), (3.22), and (3.23) that $a \neq 0$ in all cases except the case where all $h_i = 2$.

Remark 3.4 (a) At a first glance it is surprising that the angle θ in the solution formula above is the same for $i = 1, 2, 3$. However, this fact has a fairly simple explanation: Computing the linear combination

$$(p-1)p_1 - 2p_2 - p_3 - 2p_4$$

of the polynomials $p_i = p_i(s_1, s_2, s_3, a)$ given by (3.18) one gets

$$\frac{4p - A^2}{27}(2s_1^3 - 9s_1s_2 + 27s_3) + ABa.$$

Since $p_1 = p_2 = p_3 = p_4 = 0$ and $B^2 = \frac{4p-A^2}{27}$, we have the following identity

$$B(2s_1^3 - 9s_1s_2 + 27s_3) + Aa = 0. \tag{3.26}$$

But if $h_j = \xi_1 + \eta_1 \cos\left(\theta - \frac{2\pi}{3}j\right)$, $j = 0, 1, 2$, and s_1, s_2, s_3, a are defined as in (3.11) and (3.12) one finds

$$2s_1^3 - 9s_1s_2 + 27s_3 = \frac{27}{4}\eta_1^3 \cos 3\theta$$

and

$$a = -\frac{3\sqrt{3}}{4}\eta_1^3 \sin 3\theta.$$

Hence, when $\eta_1 \neq 0$, (3.26) is equivalent to

$$3\sqrt{3}B\cos 3\theta - A\sin 3\theta = 0.$$

This has a unique solution $\theta \in \left(0, \frac{\pi}{3}\right)$, namely

$$\theta = \frac{1}{3}\mathrm{Arccot}\left(\frac{A}{3\sqrt{3}B}\right) = \frac{1}{3}\mathrm{Arccos}\left(\frac{A}{2\sqrt{p}}\right).$$

(b) It is interesting to compare the solutions in Proposition 3.1 with the Gaussian cubic sum

$$G = \sum_{j=0}^{p-1} \exp(\frac{2\pi i j^3}{p})$$

It is known (cf. [9] or Section IV.2 of [13]) that for p prime, $p \equiv 1 \pmod 3$, G is a solution to the cubic equation

$$x^3 - 3px - pA = 0.$$

This equation has the three solutions

$$x_j = 2\sqrt{p}\cos\left(\theta - \frac{2\pi}{3}j\right), \qquad j = 0, 1, 2$$

where $\theta = \frac{1}{3}\mathrm{Arccos}\left(\frac{A}{2\sqrt{p}}\right)$ as in Proposition 3.1.

It is a famous problem (the Problem of Kummer) to decide for each p which of the three solutions is equal to G (cf.[9] and Section 9.12 of [10] or Section IV.2 of [13]).

We conclude this section by stating as a lemma the classical trigonometric solution of a cubic equation with three real roots. For completeness, we recall an elementary proof (cf e.g. §47 of [6])

Lemma 3.5 *Consider the cubic equation*

$$h^3 - s_1h^2 + s_2h - s_3 = 0 \tag{3.27}$$

and assume that $s_1, s_2, s_3 \in \mathbb{R}$ *and*

$$s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2 > 0. \tag{3.28}$$

Then

$$s_1^2 - 3s_2 > 0, \tag{3.29}$$

$$|2s_1^3 - 9s_1s_2 + 27s_3| < 2(s_1^2 - 3s_2)^{\frac{3}{2}}. \tag{3.30}$$

Moreover (3.27) *has three different real solutions. Listed in decreasing order* $h_0 > h_1 > h_2$*, the solutions are*

$$h_j = \frac{s_1}{3} + \frac{2}{3}(s_1^2 - 3s_2)^{\frac{1}{2}}\cos\left(\theta - \frac{2\pi j}{3}\right), \quad j = 0, 1, 2, \tag{3.31}$$

where

$$\theta = \frac{1}{3}\mathrm{Arccos}\left(\frac{2s_1^3 - 9s_1s_2 + 27s_3}{2(s_1^2 - 3s_2)^{\frac{3}{2}}}\right). \tag{3.32}$$

Listed in increasing order $h'_0 < h'_1 < h'_2$*, the solutions are*

$$h'_j = \frac{s_1}{3} - \frac{2}{3}(s_1^2 - 3s_2)^{\frac{1}{2}}\cos\left(\theta' - \frac{2\pi j}{3}\right), \quad j = 0, 1, 2, \tag{3.33}$$

where

$$\theta' = \frac{1}{3}\mathrm{Arccos}\left(-\frac{2s_1^3 - 9s_1s_2 + 27s_3}{2(s_1^2 - 3s_2)^{\frac{3}{2}}}\right). \tag{3.34}$$

Proof: Let h_0, h_1, h_2 be the solutions to (3.27) and define a by (3.12). Then from (3.15) follows that (the discriminant) $a^2 > 0$. Hence h_0, h_1, h_2 are real and different (since if e.g. $h_1 = c+id, h_2 = c-id$ with $d \neq 0$ and $h_0 \in \mathbb{R}$ we would have $a^2 = -4d^2((h_0-c)^2+d^2)^2 < 0$, whereas e.g. $h_0 = h_1$ would imply that $a = 0$). Substituting $h = u + \frac{s_1}{3}$ in equation (3.27) we get (for obvious reasons choosing a fresh letter r where historically p might be expected):

$$u^3 + ru + q = 0 \tag{3.35}$$

where $r = -\frac{1}{3}(s_1^2 - 3s_2)$ and $q = -\frac{1}{27}(2s_1^3 - 9s_1s_2 + 27s_3)$. Applying (3.15) with $s_1 = 0, s_2 = r, s_3 = -q$ we get $a^2 = -4r^3 - 27q^2$. Since the transformation from h to u is a translation, the discriminant does not change and thus (3.28) becomes $-4r^3 - 27q^2 > 0$. Thus $r < 0$, which is (3.29). Next we consider (3.30). Squaring this relation and introducing r and q we give it the form $|-27q|^2 < 4(-3r)^3$, which we have just seen is true.

Taking $u = mz$ in (3.35) we get the equation

$$z^3 + \frac{r}{m^2}z + \frac{q}{m^3} = 0. \tag{3.36}$$

We now start from the trigonometric identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Writing $z = \cos\theta$ we give it the form

$$z^3 - \frac{3}{4}z - \frac{1}{4}\cos 3\theta = 0, \tag{3.37}$$

which clearly has the solutions

$$z_j = \cos\left(\theta - \frac{2\pi j}{3}\right), \quad j = 0, 1, 2. \tag{3.38}$$

We see that equation (3.36) will be identical with (3.37) if $m = \sqrt{-\frac{4r}{3}}$ and $\cos 3\theta = \frac{-27q}{2\sqrt{-27r^3}}$. Returning to the variable h we see that (3.38) will give the solutions (3.31) to the original equation (3.27) and that we can choose θ as in (3.32).

Since $\theta \in (0, \frac{\pi}{3})$, we have

$$-1 < \cos\left(\theta - \frac{4\pi}{3}\right) < -\tfrac{1}{2} < \cos\left(\theta - \frac{2\pi}{3}\right) < \tfrac{1}{2} < \cos\theta < 1.$$

Hence $h_0 > h_1 > h_2$. Finally, note that with the notation from (3.34) we have $\theta' = \frac{\pi}{3} - \theta$. Thus $h_0' = h_2$, $h_1 = h_1'$, $h_2' = h_0$. Hence $h_0' < h_1' < h_2'$ and simple trigonometric formulas will transform the solutions given by (3.31) into those given by (3.33).

4 Solution of the main problem

Theorem 4.1 *The set of equations* (3.1) *has exactly* 20 *solutions in* $\mathbb{C}^3$. *The first two solutions are the "ϵ-solutions":*

$$c_0 = c_1 = c_2 = \frac{2 - p \pm \sqrt{p(p-4)}}{2}. \tag{4.1}$$

The remaining 18 *solutions can be obtained from the three solutions listed below by the six transformations*

$$\begin{aligned}(c_0,c_1,c_2) &\to (c_k,c_{k+1},c_{k+2})\\ (c_0,c_1,c_2) &\to \Big(\frac{1}{c_k},\frac{1}{c_{k+1}},\frac{1}{c_{k+2}}\Big),\end{aligned}$$

where $k=0,1,2$ *with indices computed modulo* 3. *Put* $u=\sqrt{p}$, $v=\sqrt{p+4A+16}$ *and* $\theta=\frac{1}{3}\mathrm{Arccos}(\frac{A}{2\sqrt{p}})$. *The three solutions are* $c^{(i)}=(c_0^{(i)},c_1^{(i)},c_2^{(i)})$, $i=1,2,3$, *where*

$$c_j^{(i)}=\alpha^{(i)}+\beta^{(i)}\cos(\theta-\frac{2\pi}{3}j)+\gamma^{(i)}\sin(\theta-\frac{2\pi}{3}j) \tag{4.2}$$

and

$$\begin{cases}\alpha^{(1)} &= \frac{1}{2}\frac{pA-2p-2A}{p^2-3p-A}+i\frac{3\sqrt{3}B}{2}\frac{\sqrt{p}\sqrt{p-4}}{p^2-3p-A}\\ \beta^{(1)} &= -\frac{1}{2}\frac{\sqrt{p}(p-4)(A+2)}{p^2-3p-A}-i\frac{3\sqrt{3}B}{2}\frac{\sqrt{p-4}(p-2)}{p^2-3p-A}\\ \gamma^{(1)} &= -\frac{3\sqrt{3}B}{2}\frac{\sqrt{p}(p-4)}{p^2-3p-A}+\frac{i}{2}\frac{\sqrt{p-4}(pA-2p-2A)}{p^2-3p-A},\end{cases} \tag{4.3}$$

$$\begin{cases}\alpha^{(2)} &= -\frac{1}{2}\frac{u^2-uv-4}{u^2+uv+2}+\frac{i}{2}\frac{u\sqrt{4+u-v}\sqrt{4-u+v}}{u^2+uv+2}\\ \beta^{(2)} &= \frac{(A+2)u}{u^2+uv+2}+\frac{i}{4}\frac{(u^2+uv+4)\sqrt{4+u-v}\sqrt{4-u+v}}{u^2+uv+2}\\ \gamma^{(2)} &= \frac{3\sqrt{3}Bu}{u^2+uv+2}+\frac{i}{4}\frac{(u^2-uv-4)\sqrt{u+v+4}\sqrt{u+v-4}}{u^2+uv+2},\end{cases} \tag{4.4}$$

$$\begin{cases}\alpha^{(3)} &= -\frac{1}{2}\frac{u^2+uv-4}{u^2-uv+2}-\frac{u}{2}\frac{\sqrt{u+v+4}\sqrt{u+v-4}}{u^2-uv+2}\\ \beta^{(3)} &= \frac{(A+2)u}{u^2-uv+2}-\frac{1}{4}\frac{(u^2-uv+4)\sqrt{u+v+4}\sqrt{u+v-4}}{u^2-uv+2}\\ \gamma^{(3)} &= \frac{3\sqrt{3}Bu}{u^2-uv+2}+\frac{1}{4}\frac{(u^2+uv-4)\sqrt{4+u-v}\sqrt{4-u+v}}{u^2-uv+2}.\end{cases} \tag{4.5}$$

The solutions (4.2) *given by* (4.3) *and* (4.4) *are unimodular while the* ϵ*-solutions and the solution* (4.2) *given by* (4.5) *are real. Hence of the* 20 *solutions* 12 *are unimodular and* 8 *are real.*

Remark 4.2
(a) Of course the choice of a "canonical" solution among six possible ones is arbitrary. Our choice is motivated by a wish to give the asymptotic results in Section 6 a simple form.
(b) It follows from the proof of Theorem 4.1 that the transformation $(c_0,c_1,c_2)\to\left(\frac{1}{c_0},\frac{1}{c_1},\frac{1}{c_2}\right)$ can be obtained by just changing the sign of the second term in the above formulas for $\alpha^{(i)}$, $\beta^{(i)}$, and $\gamma^{(i)}$.

(c) Since $u = \sqrt{p}$ and $v = \sqrt{p + 4A + 16}$ and $|A| < 2\sqrt{p}$, we have

$$|u - 4| < v < u + 4,$$

which means that the numbers u, v, and 4 can be the lengths of the three sides of a non-degenerate triangle. Hence the 4 square roots

$$\sqrt{u + v + 4}, \qquad \sqrt{u + v - 4}, \qquad \sqrt{4 + u - v}, \qquad \sqrt{4 - u + v}$$

are well defined and strictly positive. Note also that

$$A = \frac{v^2 - u^2 - 16}{4} \tag{4.6}$$

and

$$B = \frac{1}{3\sqrt{3}}\sqrt{4p - A^2} = \frac{\sqrt{u + v + 4}\sqrt{u + v - 4}\sqrt{4 + u - v}\sqrt{4 - u + v}}{12\sqrt{3}}. \tag{4.7}$$

The proof of Theorem 4.1 relies on Proposition 3.1 and the following three lemmas:

Lemma 4.3 *Let $a_0, a_1, a_2 \in \mathbb{C}$ and let $\theta \in \mathbb{R}$. Then there are unique numbers $\rho, \sigma, \tau \in \mathbb{C}$ such that*

$$a_j = \rho + \sigma \cos\left(\theta - \frac{2\pi}{3}j\right) + \tau \sin\left(\theta - \frac{2\pi}{3}j\right), \quad j = 0, 1, 2.$$

Proof: By an elementary computation one finds

$$\det \begin{pmatrix} 1 & \cos\theta & \sin\theta \\ 1 & \cos(\theta - \frac{2\pi}{3}) & \sin(\theta - \frac{2\pi}{3}) \\ 1 & \cos(\theta - \frac{4\pi}{3}) & \sin(\theta - \frac{4\pi}{3}) \end{pmatrix} = -\frac{3\sqrt{3}}{2}.$$

In particular the determinant is non-zero, which proves Lemma 4.3.

Lemma 4.4 *Let $\theta \in \mathbb{R}$ and let $\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2 \in \mathbb{C}$, and put*

$$\begin{aligned} c_j &= \frac{\alpha_1 + \alpha_2}{2} + \frac{\beta_1 + \beta_2}{2}\cos\left(\theta - \frac{2\pi}{3}j\right) + \frac{\gamma_1 + \gamma_2}{2}\sin\left(\theta - \frac{2\pi}{3}j\right) \\ \widetilde{c_j} &= \frac{\alpha_1 - \alpha_2}{2} + \frac{\beta_1 - \beta_2}{2}\cos\left(\theta - \frac{2\pi}{3}j\right) + \frac{\gamma_1 - \gamma_2}{2}\sin\left(\theta - \frac{2\pi}{3}j\right) \end{aligned}$$

for $j = 0, 1, 2$. Then the following two conditions are equivalent

(i) $c_0\tilde{c}_0 = c_1\tilde{c}_1 = c_2\tilde{c}_2 = 1$,

(ii) $t_1 = t_2 = t_3 = 0$,

where

$$t_1 = (\alpha_1^2 - \alpha_2^2) + \tfrac{1}{2}(\beta_1^2 - \beta_2^2) + \tfrac{1}{2}(\gamma_1^2 - \gamma_2^2) - 4, \tag{4.8}$$

$$t_2 = 2(\alpha_1\beta_1 - \alpha_2\beta_2) + \tfrac{1}{2}(\beta_1^2 - \beta_2^2 - \gamma_1^2 + \gamma_2^2)\cos 3\theta + (\beta_1\gamma_1 - \beta_2\gamma_2)\sin 3\theta, \tag{4.9}$$

$$t_3 = 2(\alpha_1\gamma_1 - \alpha_2\gamma_2) + \tfrac{1}{2}(\beta_1^2 - \beta_2^2 - \gamma_1^2 + \gamma_2^2)\sin 3\theta - (\beta_1\gamma_1 - \beta_2\gamma_2)\cos 3\theta. \tag{4.10}$$

Proof: Put

$$\begin{aligned} f_j &= c_j + \tilde{c}_j = \alpha_1 + \beta_1 \cos\Big(\theta - \frac{2\pi}{3}j\Big) + \gamma_1 \sin\Big(\theta - \frac{2\pi}{3}j\Big), \\ g_j &= c_j - \tilde{c}_j = \alpha_2 + \beta_2 \cos\Big(\theta - \frac{2\pi}{3}j\Big) + \gamma_2 \sin\Big(\theta - \frac{2\pi}{3}j\Big). \end{aligned}$$

Then (i) is equivalent to

$$f_j^2 - g_j^2 = 4, \qquad j = 0, 1, 2.$$

By expressing $\cos^2\varphi$, $\sin^2\varphi$, and $\cos\varphi\sin\varphi$ in terms of $\cos 2\varphi$ and $\sin 2\varphi$ (with $\varphi = \theta - \frac{2\pi}{3}j$) one finds

$$\begin{aligned} f_j^2 &= \Big(\alpha_1^2 + \frac{\beta_1^2+\gamma_1^2}{2}\Big) + 2\alpha_1\beta_1 \cos\Big(\theta - \frac{2\pi}{3}j\Big) + 2\alpha_1\gamma_1 \sin\Big(\theta - \frac{2\pi}{3}j\Big) \\ &\quad + \frac{\beta_1^2-\gamma_1^2}{2}\cos\Big(2\theta - \frac{4\pi}{3}j\Big) + \beta_1\gamma_1 \sin\Big(2\theta - \frac{4\pi}{3}j\Big). \end{aligned}$$

Using $\frac{4\pi}{3}j \equiv -\frac{2\pi}{3}j \pmod{2\pi}$ one gets

$$\left\{ \begin{array}{rcl} \cos\Big(2\theta - \frac{4\pi}{3}j\Big) &=& \cos 3\theta \cos\Big(\theta - \frac{2\pi}{3}j\Big) + \sin 3\theta \sin\Big(\theta - \frac{2\pi}{3}j\Big) \\ \sin\Big(2\theta - \frac{4\pi}{3}j\Big) &=& \sin 3\theta \cos\Big(\theta - \frac{2\pi}{3}j\Big) - \cos 3\theta \sin\Big(\theta - \frac{2\pi}{3}j\Big). \end{array} \right. \tag{4.11}$$

Hence

$$f_j^2 = \rho_1 + \sigma_1 \cos\Big(\theta - \frac{2\pi}{3}j\Big) + \tau_1 \sin\Big(\theta - \frac{2\pi}{3}j\Big), \tag{4.12}$$

where

$$\left\{ \begin{array}{rcl} \rho_1 &=& \alpha_1^2 + \frac{1}{2}(\beta_1^2 + \gamma_1^2) \\ \sigma_1 &=& 2\alpha_1\beta_1 + \frac{1}{2}(\beta_1^2 - \gamma_1^2)\cos 3\theta + \beta_1\gamma_1 \sin 3\theta \\ \tau_1 &=& 2\alpha_1\gamma_1 + \frac{1}{2}(\beta_1^2 - \gamma_1^2)\sin 3\theta - \beta_1\gamma_1 \cos 3\theta. \end{array} \right.$$

Similarly

$$g_j^2 = \rho_2 + \sigma_2 \cos\Big(\theta - \frac{2\pi}{3}j\Big) + \tau_2 \sin\Big(\theta - \frac{2\pi}{3}j\Big),$$

where

$$\left\{ \begin{array}{rcl} \rho_2 &=& \alpha_2^2 + \frac{1}{2}(\beta_2^2 + \gamma_2^2) \\ \sigma_2 &=& 2\alpha_2\beta_2 + \frac{1}{2}(\beta_2^2 - \gamma_2^2)\cos 3\theta + \beta_2\gamma_2 \sin 3\theta \\ \tau_2 &=& 2\alpha_2\gamma_2 + \frac{1}{2}(\beta_2^2 - \gamma_2^2)\sin 3\theta - \beta_2\gamma_2 \cos 3\theta. \end{array} \right.$$

Since the coefficients in the decomposition

$$f_j^2 - g_j^2 = (\rho_1 - \rho_2) + (\sigma_1 - \sigma_2)\cos\Big(\theta - \frac{2\pi}{3}j\Big) + (\tau_1 - \tau_2)\sin\Big(\theta - \frac{2\pi}{3}j\Big)$$

are unique by Lemma 4.3, we have $f_j^2 - g_j^2 = 4$, $j = 0, 1, 2$, if and only if

$$\rho_1 - \rho_2 = 4, \quad \sigma_1 - \sigma_2 = 0, \quad \text{and} \quad \tau_1 - \tau_2 = 0.$$

This proves Lemma 4.4.

Lemma 4.5 *Let $\theta \in \mathbb{R}$ and let $c_0, c_1, c_2 \in \mathbb{C}\backslash\{0\}$. Put*

$$f_j = c_j + \frac{1}{c_j}, \quad g_j = c_j - \frac{1}{c_j}, \quad h_j = \frac{c_{j+2}}{c_{j+1}} + \frac{c_{j+1}}{c_{j+2}}, \quad k_j = \frac{c_{j+2}}{c_{j+1}} - \frac{c_{j+1}}{c_{j+2}},$$

where $j = 0, 1, 2$ (counted modulo 3).

Let moreover $\alpha_\nu, \beta_\nu, \gamma_\nu, \xi_\nu, \eta_\nu, \zeta_\nu$ ($\nu = 1, 2$) be the coefficients in the decompositions

$$\begin{cases} f_j &= \alpha_1 + \beta_1 \cos(\theta - \frac{2\pi}{3} j) + \gamma_1 \sin(\theta - \frac{2\pi}{3} j) \\ g_j &= \alpha_2 + \beta_2 \cos(\theta - \frac{2\pi}{3} j) + \gamma_2 \sin(\theta - \frac{2\pi}{3} j) \end{cases} \tag{4.13}$$

$$\begin{cases} h_j &= \xi_1 + \eta_1 \cos(\theta - \frac{2\pi}{3} j) + \zeta_1 \sin(\theta - \frac{2\pi}{3} j) \\ k_j &= \xi_2 + \eta_2 \cos(\theta - \frac{2\pi}{3} j) + \zeta_2 \sin(\theta - \frac{2\pi}{3} j) \end{cases} \tag{4.14}$$

Then

$$\begin{cases} \xi_1 &= \frac{3}{4}(\alpha_1^2 - \alpha_2^2) - 1 \\ \eta_1 &= -\frac{3}{2}(\alpha_1\beta_1 - \alpha_2\beta_2) \\ \zeta_1 &= -\frac{3}{2}(\alpha_1\gamma_1 - \alpha_2\gamma_2) \end{cases} \tag{4.15}$$

and

$$\begin{cases} \xi_2 &= \frac{\sqrt{3}}{4}(\beta_2\gamma_1 - \beta_1\gamma_2) \\ \eta_2 &= \frac{\sqrt{3}}{2}(\gamma_2\alpha_1 - \gamma_1\alpha_2) \\ \zeta_2 &= \frac{\sqrt{3}}{2}(\alpha_2\beta_1 - \alpha_1\beta_2). \end{cases} \tag{4.16}$$

Proof: Clearly

$$c_j = \tfrac{1}{2}(f_j + g_j), \qquad \tfrac{1}{c_j} = \tfrac{1}{2}(f_j - g_j).$$

Hence

$$\begin{aligned} h_j &= \tfrac{1}{2}(f_{j+1}f_{j+2} - g_{j+1}g_{j+2}) \\ k_j &= \tfrac{1}{2}(f_{j+1}g_{j+2} - g_{j+1}f_{j+2}). \end{aligned}$$

By expressing $\cos(\theta - \frac{2\pi}{3})$, $\sin(\theta - \frac{2\pi}{3})$, $\cos(\theta - \frac{2\pi}{3})$, and $\sin(\theta - \frac{4\pi}{3})$ as linear combinations of $\cos\theta$ and $\sin\theta$ one gets

$$f_1 f_2 = (\alpha_1^2 - \frac{\beta_1^2 + \gamma_1^2}{4}) - \alpha_1\beta_1 \cos\theta - \alpha_1\gamma_1 \sin\theta + \frac{\beta_1^2 - \gamma_1^2}{2} \cos 2\theta + \beta_1\gamma_1 \sin 2\theta. \tag{4.17}$$

Using now (4.12) from the proof of Lemma 4.4, we have

$$f_1 f_2 - f_0^2 = -\tfrac{3}{4}(\beta_1^2 + \gamma_1^2) - 3\alpha_1\beta_1 \cos\theta - 3\alpha_1\gamma_1 \sin\theta.$$

Repeating the same argument with $\theta - \frac{2\pi}{3} j$ instead of θ, we have

$$f_{j+1}f_{j+2} - f_j^2 = -\tfrac{3}{4}(\beta_1^2 + \gamma_1^2) - 3\alpha_1\beta_1 \cos\left(\theta - \frac{2\pi}{3} j\right) - 3\alpha_1\gamma_1 \sin\left(\theta - \frac{2\pi}{3} j\right) \tag{4.18}$$

and in the same way we have

$$g_{j+1}g_{j+2} - g_j^2 = -\tfrac{3}{4}(\beta_2^2 + \gamma_2^2) - 3\alpha_2\beta_2 \cos\Big(\theta - \frac{2\pi}{3}j\Big) - 3\alpha_2\gamma_2 \sin\Big(\theta - \frac{2\pi}{3}j\Big). \qquad (4.19)$$

By the definition of f_j and g_j we have

$$f_j^2 - g_j^2 = \Big(c_j + \frac{1}{c_j}\Big)^2 - \Big(c_j - \frac{1}{c_j}\Big)^2 = 4. \qquad (4.20)$$

Hence, by (4.18), (4.19), and (4.20)

$$\begin{aligned} 2h_j &= f_{j+1}f_{j+2} - g_{j+1}g_{j+2} \\ &= 4 - \tfrac{3}{4}(\beta_1^2 + \gamma_1^2 - \beta_2^2 - \gamma_2^2) - 3(\alpha_1\beta_1 - \alpha_2\beta_2)\cos(\theta - \tfrac{2\pi}{3}j) \\ &\quad -3(\alpha_1\gamma_1 - \alpha_2\gamma_2)\sin(\theta - \tfrac{2\pi}{3}j). \end{aligned}$$

By uniqueness of this decomposition (Lemma 4.3) we can read off the coefficients ξ_1, η_1, ζ_1 in (4.14) namely

$$\begin{aligned} \xi_1 &= 2 - \tfrac{3}{8}(\beta_1^2 + \gamma_1^2 - \beta_2^2 - \gamma_2^2), \\ \eta_1 &= -\tfrac{3}{2}(\alpha_1\beta_1 - \alpha_2\beta_2), \\ \zeta_1 &= -\tfrac{3}{2}(\alpha_1\gamma_1 - \alpha_2\gamma_2). \end{aligned}$$

However by (4.8) in Lemma 4.4, we have

$$(\alpha_1^2 - \alpha_2^2) + \tfrac{1}{2}(\beta_1^2 - \beta_2^2) + \tfrac{1}{2}(\gamma_1^2 - \gamma_2^2) = 4.$$

Hence the above formula for ξ_1 can be changed to

$$\xi_1 = \tfrac{3}{4}(\alpha_1^2 - \alpha_2^2) - 1.$$

This proves (4.15). A similar but much simpler computation gives

$$\begin{aligned} k_j &= \tfrac{1}{2}(f_{j+1}g_{j+2} - f_{j+2}g_{j+1}) \\ &= \frac{\sqrt{3}}{4}(\beta_2\gamma_1 - \beta_1\gamma_2) + \frac{\sqrt{3}}{2}(\gamma_2\alpha_1 - \gamma_1\alpha_2)\cos\Big(\theta - \frac{2\pi}{3}j\Big) \\ &\qquad + \frac{\sqrt{3}}{2}(\alpha_2\beta_1 - \alpha_1\beta_2)\sin\Big(\theta - \frac{2\pi}{3}j\Big), \end{aligned}$$

which proves (4.16).

Proof of Theorem 4.1: Assume that (c_0, c_1, c_2) is a solution to the set of equations (3.1). By Proposition 3.1, the numbers

$$h_j = \frac{c_{j+2}}{c_{j+1}} + \frac{c_{j+1}}{c_{j+2}}, \qquad j = 0, 1, 2,$$

must be of the form

$$h_j = \xi_1 + \eta_1 \cos\Big(\theta - \frac{2\pi}{3} j\Big), \qquad j = 0, 1, 2, \tag{4.21}$$

where (ξ_1, η_1) is one of the four pairs $(\xi_1^{(i)}, \eta_1^{(i)})$, $i = 0, 1, 2, 3$, listed in (3.5)–(3.8). For $i = 0$, we have $\xi_1 = 2$ and $\eta_1 = 0$. Hence $h_0 = h_1 = h_2 = 2$ which implies that $c_0 = c_1 = c_2$, and in this case the only solutions to (3.1) are the 2 "ϵ-solutions" from [2], namely

$$c_0 = c_1 = c_2 = \frac{2 - p \pm \sqrt{p(p-4)}}{2}.$$

For $i = 1, 2, 3$ we can compute the numbers c_j from (ξ_1, η_1) by Lemma 4.5. Define

$$f_j = c_j + \frac{1}{c_j}, \quad g_j = c_j - \frac{1}{c_j}, \quad h_j = \frac{c_{j+2}}{c_{j+1}} + \frac{c_{j+1}}{c_{j+2}}, \quad k_j = \frac{c_{j+2}}{c_{j+1}} - \frac{c_{j+1}}{c_{j+2}}$$

as in Lemma 4.5, and let $\alpha_\nu, \beta_\nu, \gamma_\nu, \xi_\nu, \eta_\nu, \zeta_\nu$, $\nu = 1, 2$ be the coefficients in the decompositions (4.13) and (4.14). Note that by Lemma 4.3 this new definition of ξ_1 and η_1 is consistent with (4.21). Moreover $\zeta_1 = 0$ by (4.21).

By (3.1)

$$f_j = -\frac{p-4}{3} - \frac{p + A + 1}{9} h_j - \frac{2p - A - 9B - 4}{18} h_{j+1} - \frac{2p - A - 9B - 4}{18} h_{j+2}.$$

Since

$$\begin{aligned} h_0 &= \xi_1 + \eta_1 \cos\theta, \\ h_1 &= \xi_1 + \eta_1 \Big(-\tfrac{1}{2} \cos\theta + i \frac{\sqrt{3}}{2} \sin\theta \Big), \\ h_2 &= \xi_1 + \eta_1 \Big(-\tfrac{1}{2} \cos\theta - i \frac{\sqrt{3}}{2} \sin\theta \Big), \end{aligned}$$

we have

$$f_0 = \left(-\frac{p-4}{3} - \frac{p-1}{3} \xi_1 \right) - \frac{A+2}{6} \eta_1 \cos\theta - \frac{\sqrt{3}}{2} B \eta_1.$$

Repeating the same computation with θ replaced by $\theta - \frac{2\pi}{3} j$, we get that the coefficients $\alpha_1, \beta_1, \gamma_1$ in the decomposition

$$f_j = \alpha_1 + \beta_1 \cos\Big(\theta - \frac{2\pi}{3} j\Big) + \gamma_1 \sin\Big(\theta - \frac{2\pi}{3} j\Big)$$

are given by

$$\begin{cases} \alpha_1 &= -\frac{p-4}{3} - \frac{p-1}{3} \xi_1 \\ \beta_1 &= -\frac{A+2}{6} \eta_1 \\ \gamma_1 &= -\frac{\sqrt{3}}{2} B. \end{cases} \tag{4.22}$$

Provided $\alpha_1^2 - \frac{4}{3}(\xi_1+1) \neq 0$ we then get from (4.15) with $\zeta_1 = 0$

$$\left\{\begin{array}{lcl} \alpha_2 &=& \pm\sqrt{\alpha_1^2 - \frac{4}{3}(\xi_1+1)} \\ \beta_2 &=& \frac{1}{\alpha_2}(\alpha_1\beta_1 + \frac{2}{3}\eta_1) \\ \gamma_2 &=& \frac{\alpha_1\gamma_1}{\alpha_2}. \end{array}\right. \tag{4.23}$$

Inserting the values $(\xi_1^{(i)}, \eta_1^{(i)})$, $i = 1, 2, 3$ from (3.25) in (4.22) we find that $\alpha_1^2 - \frac{4}{3}(\xi_1+1) \neq 0$ in all the cases $i = 1, 2, 3$. Hence the numbers α_1, β_1, γ_1, α_2, β_2, γ_2 given by (4.22) and (4.23) are unique up to simultaneous sign change of $(\alpha_2, \beta_2, \gamma_2)$. For $i = 1, 2$,

$$\alpha_2 = \pm\sqrt{\alpha_1^2 - \frac{4}{3}(\xi_1+1)}$$

is purely imaginary, and we choose the solution with $\Im(\alpha_2^{(i)}) > 0$ $(i = 1, 2)$. For $i = 3$, α_2 is real and we choose the solution with $\mathrm{sign}(\alpha_2^{(3)}) = -\mathrm{sign}(u^2 - uv + 2)$. It is now easy to compute α_1, β_1, γ_1, α_2, β_2, γ_2 explicitly from (3.25) in the three cases $i = 1, 2, 3$. One finds

$$\left\{\begin{array}{lcllcl} \alpha_1^{(1)} &=& \frac{pA-2p-2A}{p^2-3p-A}, & \alpha_2^{(1)} &=& i\frac{3\sqrt{3}\sqrt{p}\sqrt{p-4}B}{p^2-3p-A} \\ \beta_1^{(1)} &=& -\frac{\sqrt{p}(p-4)(A+2)}{p^2-3p-A}, & \beta_2^{(1)} &=& -i\frac{3\sqrt{3}\sqrt{p-4}(p-2)B}{p^2-3p-A} \\ \gamma_1^{(1)} &=& -\frac{3\sqrt{3}\sqrt{p}(p-4)B}{p^2-3p-A}, & \beta_3^{(1)} &=& i\frac{\sqrt{p-4}(pA-2p-2A)}{p^2-3p-A}. \end{array}\right. \tag{4.24}$$

$$\left\{\begin{array}{lcllcl} \alpha_1^{(2)} &=& -\frac{u^2-uv-4}{u^2+uv+2}, & \alpha_2^{(2)} &=& i\frac{u\sqrt{4+u-v}\sqrt{4-u+v}}{u^2+uv+2} \\ \beta_1^{(2)} &=& \frac{2(A+2)u}{u^2+uv+2}, & \beta_2^{(2)} &=& \frac{i}{2}\frac{(u^2+uv+4)\sqrt{4+u-v}\sqrt{4-u+v}}{u^2+uv+2} \\ \gamma_1^{(2)} &=& \frac{6\sqrt{3}Bu}{u^2+uv+2}, & \gamma_2^{(2)} &=& \frac{i}{2}\frac{(u^2-uv-4)\sqrt{u+v+4}\sqrt{u+v-4}}{u^2+uv+2}. \end{array}\right. \tag{4.25}$$

$$\left\{\begin{array}{lcllcl} \alpha_1^{(3)} &=& -\frac{u^2+uv-4}{u^2-uv+2}, & \alpha_2^{(3)} &=& -\frac{u\sqrt{u+v+4}\sqrt{u+v-4}}{u^2-uv+2} \\ \beta_1^{(3)} &=& \frac{2(A+2)u}{u^2-uv+2}, & \beta_2^{(3)} &=& -\frac{1}{2}\frac{(u^2-uv+4)\sqrt{u+v+4}\sqrt{u+v-4}}{u^2-uv+2} \\ \gamma_1^{(3)} &=& \frac{6\sqrt{3}Bu}{u^2-uv+2}, & \gamma_2^{(3)} &=& \frac{1}{2}\frac{(u^2+uv-4)\sqrt{4+u-v}\sqrt{4-u+v}}{u^2-uv+2}. \end{array}\right. \tag{4.26}$$

Since

$$c_j = \tfrac{1}{2}(f_j + g_j) = \frac{\alpha_1+\alpha_2}{2} + \frac{\beta_1+\beta_2}{2}\cos\Big(\theta - \frac{2\pi}{3}j\Big) + \frac{\gamma_1+\gamma_2}{2}\sin\Big(\theta - \frac{2\pi}{3}j\Big), \tag{4.27}$$

we obtain (4.2) with $\alpha^{(i)}, \beta^{(i)}, \gamma^{(i)}$ given by (4.3), (4.4) and (4.5).

We still have to check that the $(c_0^{(i)}, c_1^{(i)}, c_2^{(i)})$ given by (4.2)–(4.5) actually are solutions to (3.1). From Lemma 4.4 and Lemma 4.5 it follows that the only thing left to check is that $c_j \neq 0$, $j = 0, 1, 2$ and that

$$\frac{1}{c_j} = \frac{\alpha_1 - \alpha_2}{2} + \frac{\beta_1 - \beta_2}{2} \cos\Big(\theta - \frac{2\pi}{3} j\Big) + \frac{\gamma_1 - \gamma_2}{2} \sin\Big(\theta - \frac{2\pi}{3} j\Big), \tag{4.28}$$

which is equivalent to checking that the numbers t_1, t_2, and t_3 listed in (4.8)–(4.10) are zero.

Using

$$\cos 3\theta = \frac{A}{2\sqrt{p}}, \quad \sin 3\theta = \frac{\sqrt{4p - A^2}}{2\sqrt{p}} = \frac{3\sqrt{3}B}{2\sqrt{p}}$$

it is elementary to check by MAPLE or MATHEMATICA that $t_1 = t_2 = t_3 = 0$ in each of the three cases (4.24), (4.25), and (4.26) above. It is also possible to avoid a case by case check by relating t_1, t_2, and t_3 to the polynomials p_1, p_2, p_3, and p_4 used in the proof of Proposition 3.1 (see Remark 4.6 below).

Finally we have to show that we have found 20 distinct solutions: Since $\eta_1^{(i)} \neq 0$, $i = 1, 2, 3$, the 18 solutions given by (4.2)–(4.5) are distinct from the two ϵ-solutions. This also implies that in each of the three cases, the six solutions given by

$$\begin{cases} (c_k, c_{k+1}, c_{k+2}) & k = 0, 1, 2 \\ (\frac{1}{c_k}, \frac{1}{c_{k+1}}, \frac{1}{c_{k+2}}) & k = 0, 1, 2 \end{cases} \tag{4.29}$$

are all distinct. To check that there is no overlap between these three groups of six solutions it is sufficient to check that the three numbers $s_1^{(i)} = 3\xi_1^{(i)}$ are distinct because

$$s_1 = h_0 + h_1 + h_2 = \frac{c_2}{c_1} + \frac{c_1}{c_2} + \frac{c_0}{c_2} + \frac{c_2}{c_0} + \frac{c_1}{c_0} + \frac{c_0}{c_1}$$

is invariant under the six transformations listed in (4.29). From (3.20)

$$\begin{aligned} s_1^{(1)} &= \frac{18p - 3p^2 - 6A}{p^2 - 3p - A}, \\ \left.\begin{matrix} s_1^{(2)} \\ s_1^{(3)} \end{matrix}\right\} &= \frac{-6pA - 27 - 12 \pm 9\sqrt{p(p + 4A + 16)}}{2(pA + 2p - 1)}. \end{aligned}$$

Clearly $s_1^{(2)} \neq s_1^{(3)}$, since $p + 4A + 16 > 0$ by Remark 3.2. Moreover $s_1^{(2)}$ and $s_1^{(3)}$ are the two zeros of the polynomial r from (3.19):

$$r(s_1) = (pA + 3p - 1)s_1^2 + (6pA + 27p + 12)s_1 + (9pA + 54p - 36).$$

We get

$$r(s_1^{(1)}) = 81 \frac{(2p - A - 4)(4p - A^2)}{(p^2 - 3p - A)^2},$$

but $2p-A-4>2p-2\sqrt{p}-4=2(\sqrt{p}+1)(\sqrt{p}-2)>0$, and $4p-A^2=27B^2>0$. Hence $s_1^{(1)}\neq s_1^{(2)}$ and $s_1^{(1)}\neq s_1^{(3)}$. Therefore we have found altogether $2+3\cdot 6=20$ solutions. By (4.28), passing from $c_j^{(i)}$ to $\frac{1}{c_j^{(i)}}$ in (4.2) corresponds to a change of sign of α_2,β_2, and γ_2. Hence the 12 solutions generated by (4.3), (4.4), and the transformations (4.29) are all unimodular while the remaining 8 solutions clearly are real. This completes the proof of Theorem 4.1.

Remark 4.6 We sketch here a different proof of $t_1=t_2=t_3=0$ for the values of $\alpha_1,\beta_1,\gamma_1,\alpha_2,\beta_2,\gamma_2$ listed in (4.24)–(4.26):

By (4.22) and (4.23), $\alpha_1,\beta_1,\gamma_1,\alpha_2,\beta_2,\gamma_2$ can be expressed in terms of (ξ_1,η_1), and hence t_1,t_2,t_3 given by (4.8)–(4.10) can be expressed in terms of ξ_1,η_1, and θ. Next we observe that if

$$h_j=\xi_1+\eta_1\cos\Big(\theta-\frac{2\pi}{3}j\Big),\quad j=0,1,2,$$

then

$$\begin{aligned}
s_1 &= h_0+h_1+h_2=3\xi_1,\\
s_2 &= h_0h_1+h_1h_2+h_2h_0=3\xi_1^2-\frac{3}{4}\eta_1^2,\\
s_3 &= h_0h_1h_2=\xi_1^3-\tfrac{3}{4}\xi_1\eta_1^2+\tfrac{1}{4}\eta_1^3\cos 3\theta,\\
a &= (h_0-h_1)(h_1-h_2)(h_2-h_0)=-\frac{3\sqrt{3}}{4}\eta_1\sin 3\theta.
\end{aligned}$$

Inserting this into the 4 polynomials $p_i=p_i(s_1,s_2,s_3,a)$ from the proof of Proposition 3.1 and comparing these new formulas for p_1,p_2,p_3, and p_4 with the formulas found above for t_1,t_2, and t_3, one discovers after some work that (as functions of ξ_1,η_1 and θ)

$$\begin{aligned}
t_1 &= \frac{4(p_3-p_4)}{27\alpha_2^2},\\
t_2 &= -\frac{4(3p_1+(\xi_1-p\xi_1-p+4)p_2+(2\xi_1-1)p_3+(\xi_1+4)p_4}{27\eta_1\alpha_2^2},
\end{aligned}$$

and since $(\xi_1^{(i)},\eta_1^{(i)})$, $i=1,2,3$, were found by solving the equations $p_1=p_2=p_3=p_4=0$, it follows that $t_1=t_2=0$ in all three cases. For t_3 the situation is simpler: Introducing $\cos 3\theta=A/(2\sqrt{p})$ and $\sin 3\theta=3\sqrt{3}B/(2\sqrt{p})$ in the formula just found for t_3, we find that the resulting function of ξ_1 and η_1 is *identically* 0.

5 Corollaries of the main result (Leaving the simple case)

In this section we will formulate and prove various consequences of the main result; in particular we will identify all bi-unimodular p-sequences and cyclic p-roots of index 3. We will give the $c^{(i)}$ names:

Definition 5.1 *We denote as the* first, second and third canonical solution *the solutions* $c^{(1)}$, $c^{(2)}$, *and* $c^{(3)}$ *defined in Theorem* 4.1.

We will start by presenting all bi-unimodular p-sequences of index 3 (cf. Definition 1.3). Recall that $\omega = \exp(\frac{2\pi i}{p})$.

Proposition 5.2 *Let* p *be a prime* $\equiv 1 \pmod 6$, *and let* x *be a bi-unimodular* p*-sequence of index* 3. *Then there are a complex number* b *of modulus one and integers* r *and* l *such that* x *is given by* $x_l = b$ *and* $x_j = b \cdot \omega^{rj} \cdot c_k$ when $0 \neq j - l \in G_k \quad (k = 0, 1, 2)$, *where* $c = (c_0, c_1, c_2)$ *is one of the* 12 *solutions to* (3.1) *coming from the the first or second canonical solution* $c^{(1)}, c^{(2)}$, *as described in Theorem* 4.1. *If* $p \neq 7$, *there are* $12p^2$ *different* normalized *bi-unimodular* p*-sequences of index* 3 *(i.e. with* $x_0 = 1$*). There are* 336 *different normalized bi-unimodular* 7*-sequences. Of these,* $6 \cdot 7^2$ *come from the second canonical solution, whereas only* $6 \cdot 7$ *come from the first canonical solution. The last-mentioned sequences can be uniquely written in the form* $x_j = \omega^{m \cdot j^2 + nj}$, *where* m *and* $n \in \mathbb{Z}_7$ *and* $m \neq 0$.

Next we formulate our result as a theorem bearing on cyclic p-roots rather than on bi-unimodular p-sequences:

Proposition 5.3 *Let* p *be a prime* $\equiv 1 \pmod 6$, *and let* $z = (z_0, \ldots, z_{p-1})$ *be a cyclic* p*-root of index* 3. *Then there are integers* r *and* l *such that* z *is given by* $z_j = \omega^r \cdot c_k / c_\kappa$ *when* $j + 1 - l \in G_k$ *and* $j - l \in G_\kappa$, *where* $c = (c_0, c_1, c_2)$ *is one of the* 20 *solutions to* (3.1) *as described in Theorem* 4.1. *If* $p \neq 7$, *there are* $20p^2$ *different cyclic* p*-roots of index* 3, *(*$2p^2$ *of which being in fact of index* 1*). There are only* 434 *different cyclic* 7*-roots of index* 3. *Of these,* 42 *come from the first canonical solution. These "Gaussian" cyclic* 7*-roots can be uniquely written in the form* $z_j = \omega^{mj+n}$ *where* m *and* $n \in \mathbb{Z}_7$ *and* $m \neq 0$.

Proof of Proposition 5.2 and Proposition 5.3 The first statements in these theorems are obvious reformulations of Theorem 4.1 in terms of the concepts introduced in Section 1, and we leave it to the reader to check this. We will only prove the statements about the number of different normalized bi-unimodular sequences of index 3 (NBUS3), the number of different cyclic p-roots of index 3, and the explicit forms given in the first canonical case for $p = 7$.

We start with the last topic. Since the 42 possible ω-exponents in the z_j-formula in Proposition 5.3 form the set of all differences (as functions of j) of those in the x_j-formula in Proposition 5.2, it suffices to consider the latter (cf. (1.4) and Proposition 1.1). We start by taking $m = 1$ and $n = 0$, which gives $x = (1, \omega, \omega^4, \omega^2, \omega^2, \omega^4, \omega)$. Since for $p = 7$ we have $G_0 = \{1, 6\}$, $G_1 = \{3, 4\}$, and $G_2 = \{2, 5\}$, this means that this particular x is in fact simple of index 3 with $c_0 = \omega$, $c_1 = \omega^2$, and $c_2 = \omega^4$ (cf. Definition 1.2). We claim that this $c = (c_0, c_1, c_2)$ is one of the six solutions coming from $c^{(1)}$ in Theorem 4.1. To prove this, we calculate $h_0 = \frac{c_1}{c_2} + \frac{c_2}{c_1} = \omega^2 + \omega^{-2}$, $h_1 = \frac{c_2}{c_0} + \frac{c_0}{c_2} = \omega^3 + \omega^{-3}$, and $h_2 = c_0/c_1 + c_1/c_0 = \omega + \omega^{-1}$. Thus, using the relation $1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = 0$, we get $s_1 = h_0 + h_1 + h_2 = -1$, $s_2 = h_0h_1 + h_1h_2 + h_2h_0 = -2$, $s_3 = h_0h_1h_2 = 1$, and

$a = (h_1 - h_0)(h_2 - h_1)(h_0 - h_{02}) = -7$. Since these values agree with those of $s_1^{(1)}, s_2^{(1)}, s_3^{(1)}$, and $a^{(1)}$ in (3.14), our last claim is proved.

Next we keep $n = 0$ but consider a general m. But all we have used about ω in our calculations is that ω is a primitive seventh root of unity. So is ω^m. Thus, $x_j = \omega^{m \cdot j^2} = (\omega^m)^{j^2}$ will also give a simple bi-unimodular 7-sequence of index 3. Of course the six possibilities for m correspond to the six transformations mentioned in Theorem 4.1. Finally, taking a general n, we see by (1.6) in Definition 1.3 (with $l = 0$ and $h = n$) that all our x are bi-unimodular 7-sequences of index 3. Clearly they are normalized.

It is clear that the 42 normalized bi-unimodular 7-sequences of index 3 we have found are different. Next we show that no other normalized bi-unimodular 7-sequence comes from the first canonical case. All we have to prove is that taking $l \neq 0$ in (1.6) does not give anything new when y is a simple bi-uninormal sequence of index 3 given by $y_j = \omega^{mj^2}$. But this is trivial, since (1.6) gives the unnormalized bi-uninormal sequence x of index 3 defined by $x_j = \omega^{rj}\omega^{m(j-l)^2} = \omega^{ml^2 + j(r-2ml) + mj^2}$ which is normalized through division by $x_0 = \omega^{ml^2}$ and becomes $\omega^{j(r-2ml)+mj^2} = \omega^{j(r-2ml)}y_j$, which is (1.6) with l replaced by 0 and r replaced by $(r - 2ml)$.

It remains to prove that the numbers of different NBUS3:s and different cyclic p-roots of index 3 given in our two propositions are correct, that is that no such "collapse" occurs except in the first canonical case for $p = 7$. Recall that in the end of the proof of Theorem 4.1 we showed that all the 20 solutions to the main problem are different. We now have to extend this from the simple to the general case, and we start by considering the ϵ-solutions. Every corresponding NBUS3 x has the form $x_j = d_j\omega^{rj}$ with $r \in \mathbb{Z}$ and $d = (1, \epsilon, \epsilon, \ldots, \epsilon, \epsilon)$ or $d = (\ldots, 1, 1, \epsilon, 1, 1, \ldots)$ with $\epsilon = (2 - p \pm \sqrt{p(p-4)}\ )/2$. These $2p^2$ NBUS3:s are clearly distinct. Note that changing the sign of the square root means replacing ϵ by $1/\epsilon$.

Let us when r and l are in $\mathbb{Z}_p$ and $c = (c_0, c_1, c_2) \in \mathbb{C}^3$ is one of the 20 solutions mentioned in Theorem 4.1, define $x(r, l, c)$ as the NBUS3 $x = (x_0, x', \ldots, x_{p-1})$ given by (cf.(1.7)):

$$x_j = b\omega^{rj}c_k \text{ when } 0 \neq j - l \in G_k, \tag{5.1}$$

$$x_l = b\omega^{rl}, \tag{5.2}$$

where b is determined by the normalization

$$x_0 = 1. \tag{5.3}$$

Suppose now that we have a collapse, i.e. that $x(r', l', c') = x(r'', l'', c'')$ for two NBUS3:s which do not satisfy all the three equalities $r' = r'', l' = l'', c' = c''$. We denote the two b:s defined by (5.3) by b' and b'', respectively. We start by considering the possibility that $l'' = l'$. Denote the common value by l and fix a k. From (5.1) follows that $b'\omega^{r'j}c'_k = b''\omega^{r''j}c''_k$ if $j - l \in G_k$ and thus for at least two different j, which leads to $r' = r''$. Then (5.2) gives $b' = b''$. Now (5.1) implies that we have also $c' = c''$, which is against our hypothesis that at least one of r, l, and c differs between the two NBUS3:s.

Thus we have $l' \neq l''$. Let us now suppose that $r' = r''$ (and $l' \neq l''$). Denote the common r-value by r. Choose j_1 such that $j_1 \neq l'$ and $j_1 \neq l''$ and define k_1 and k_2 by

$$(j_1 - l') \in G_{k_1}, \quad (j_1 - l'') \in G_{k_2}. \tag{5.4}$$

Consider the set $F := \{j \in \mathbb{Z}_p \setminus \{l', l''\};\ (j - l') \in G_{k_1} \text{ and } j - l'' \in G_{k_2}\}$. Taking $d = l'' - l'$ in (1.9), we see that if $d \in G_a$, then the cardinality of F is a transition number: $\sharp(F) = n_{k_1,k_2}(d) = n_{k_1-a,k_2-a}$. By (2.4) and Corollary 2.3, all transition numbers are $\leq s - 1$, and since $\sharp(G_{k_1}) = s$, there is at least one j_2 and one $k_3 \neq k_2$ such that

$$(j_2 - l') \in G_{k_1} \quad \text{and} \quad (j_2 - l'') \in G_{k_3}. \tag{5.5}$$

Now from (5.4) and (5.5) follows that (5.1) with $j = j_1$ and with $j = j_2$ gives

$$b'\omega^{rj_1}c'_{k_1} = b''\omega^{rj_1}c''_{k_2},$$
$$b'\omega^{rj_2}c'_{k_1} = b''\omega^{rj_2}c''_{k_3}.$$

This leads to $c''_{k_2} = c''_{k_3}$. Then it follows from Remark 3.3 that c'' is an ϵ-solution. Since c' and c'' play the same part in our situation, c' must also be an ϵ-solution. But we know already that there is no internal collapse among the NBUS3:s coming from ϵ-solutions, so the case $r' = r''$ also leads to a contradiction. Now we know that $r' \neq r''$ and $l' \neq l''$. From (5.2) and (5.1) with $j = l'$ we get

$$x_{l'} = b'\omega^{r'l'} = b''\omega^{r''l'}c''_k, \tag{5.6}$$

where k is determined by $0 \neq (l' - l'') \in G_k$. Since G_k has at least two elements we can choose $j \in \mathbb{Z}_p \setminus \{l', l''\}$ with $(j - l') \in G_k$. For this j we get from (5.1)

$$x_j = b'\omega^{r'j}c'_k = b''\omega^{r''j}c''_k. \tag{5.7}$$

From (5.6) and (5.7) we get by division

$$c'_k = \omega^{(r''-r')(j-l')}.$$

Since the exponent of ω is not zero (modulo p) , we have found a c'_k which is a primitive p'th root of unity. But we have also proved that we must have $p = 7$. For if $p \geq 13$, there are *more than* two elements in G_k, and we can make two different choices of j, giving conflicting values to c'_k (since $r'' - r' \neq 0$). Thus, to have collapse we must have $p = 7$, and some c'_k, and by our "same part" argument also some c''_k, must be a primitive seventh root of unity and hence non-real. Thus neither c' nor c'' can be an ϵ-solution or come from the third canonical case. We can also easily exclude the second canonical case e.g. with the following numerical argument: The imaginary part of the seventh power of the six values of the components of $c^{(2)}$ are approximately $\pm 0.92, \pm 0.94$, and ± 0.41 rather than 0. So the collapse is an internal affair within the first canonical case for $p = 7$. This was all that remained to complete the proof of the two propositions.

6 Numerical and asymptotic results

In this section we will study the behavior for large p of the solutions $c^{(i)}, i = 1, 2, 3$, defined in Theorem 4.1. We will give numerical data leading to educated guesses about this behavior (see Remark 6.3), and we will prove quantitative forms of these guesses.

In Table 6.1 below we list the first few primes $\equiv 1 \pmod 6$ and corresponding numerical values of $A, B, \theta, c_0^{(1)}, c_1^{(1)}$, and $c_2^{(1)}$. In Table 6.2, we give the corresponding information for $c^{(2)}$. We will also include an indication of the shape of the triangle formed by the three complex numbers $c_0^{(i)}, c_1^{(i)}, c_2^{(i)}$, $(i = 1, 2)$, reasoning as follows:

In the corresponding situation for simple bi-unimodular sequences of index *two* (cf. [2]) we have *two* complex numbers c_0 and c_1 on the unit circle, and with increasing p their sum tends to zero. A natural guess in our situation might therefore be that he sum of the three numbers tends to zero or, equivalently, that the triangle becomes more and more equilateral when p grows. We prefer the latter description. To be able to give quantitative results we will revive the old noun *scalenity*, (cf. [1]) and give it a precise meaning:

Definition 6.1 *In the complex plane, let $b = (b_0, b_1, b_2)$ be a triple of points on a circle C with center w. Let $\phi_i = \arg(b_i - w)$. Let the* scalenity *of b be*

$$\operatorname{scal}(b) = \max_j \left| \frac{1}{2} + \cos(\phi_{j+2} - \phi_{j+1}) \right|,$$

(indices counted modulo 3).

Remark 6.2 Since $\frac{1}{2} = -\cos 2\pi/3$, the triangle with vertices b will be equilateral iff its scalenity is zero. Let us now consider the definition of h_j (in Proposition 3.1). If we take $b = c^{(i)}$ with $i = 1$ or 2, we have all $|b_j| = 1$ and thus $w = 0$. Hence $\operatorname{scal}(c^{(1)}) = \frac{1}{2} \max_j |1 + h_j|$, where h_j is given by (3.3) with c replaced by b.

Table 6.1 (First canonical case)

p	A	B	θ	$c_0^{(1)}$	$c_1^{(1)}$	$c_2^{(1)}$	$\operatorname{scal}(c^{(1)})$
7	1	1	0.4602	−0.9010 − 0.4339 i	0.6235 + 0.7818 i	−0.2225 + 0.9749 i	1.1235
13	−5	1	0.7790	−0.4822 − 0.8761 i	0.3953 + 0.9185 i	−0.8132 + 0.5820 i	0.7132
19	7	1	0.2129	−0.9528 − 0.3037 i	0.9838 − 0.1791 i	0.3780 + 0.9258 i	0.7061
31	4	2	0.4011	−0.8023 − 0.5969 i	0.9923 + 0.1235 i	−0.0963 + 0.9954 i	0.5274
37	−11	1	0.9001	−0.0604 − 0.9982 i	0.4630 + 0.8863 i	−0.9452 + 0.3265 i	0.4127
43	−8	2	0.7423	−0.3124 − 0.9499 i	0.7272 + 0.6864 i	−0.7742 + 0.6330 i	0.3792
61	1	3	0.5022	−0.6466 − 0.7628 i	0.9759 + 0.2181 i	−0.3560 + 0.9345 i	0.3564
67	−5	3	0.6271	−0.4569 − 0.8895 i	0.8964 + 0.4433 i	−0.5999 + 0.8001 i	0.3170
73	7	3	0.3829	−0.7843 − 0.6204 i	0.9988 − 0.0481 i	−0.1114 + 0.9938 i	0.3409
79	−17	1	0.9483	0.1286 − 0.9917 i	0.4824 + 0.8759 i	−0.9765 + 0.2154 i	0.3066
97	19	1	0.0890	−0.9875 − 0.1576 i	0.7708 − 0.6371 i	0.4823 + 0.8760 i	0.3137
103	13	3	0.2919	−0.8668 − 0.4986 i	0.9629 − 0.2697 i	0.0653 + 0.9979 i	0.2937
109	−2	4	0.5556	−0.5387 − 0.8425 i	0.9666 + 0.2561 i	−0.4841 + 0.8750 i	0.2562
127	−20	2	0.8875	0.0580 − 0.9983 i	0.6211 + 0.7837 i	−0.9411 + 0.3382 i	0.2464
139	−23	1	0.9731	0.2257 − 0.9742 i	0.4899 + 0.8718 i	−0.9873 + 0.1588 i	0.2387
151	19	3	0.2290	−0.9138 − 0.4062 i	0.9066 − 0.4219 i	0.1770 + 0.9842 i	0.2452
157	−14	4	0.7212	−0.2380 − 0.9713 i	0.8495 + 0.5276 i	−0.7655 + 0.6434 i	0.2146
163	25	1	0.0683	−0.9922 − 0.1248 i	0.7153 − 0.6988 i	0.4898 + 0.8718 i	0.2411
181	7	5	0.4359	−0.6932 − 0.7207 i	0.9996 − 0.0270 i	−0.2649 + 0.9643 i	0.2092

Table 6.2 (Second canonical case)							
p	A	B	θ	$c_0^{(2)}$	$c_1^{(2)}$	$c_2^{(2)}$	scal$(c^{(2)})$
7	1	1	0.4602	0.8173 + 0.5762 i	−0.3890 + 0.9212 i	0.2804 − 0.9599 i	0.7129
13	−5	1	0.7790	0.2469 + 0.9690 i	−0.7728 + 0.6346 i	0.6315 − 0.7754 i	0.9242
19	7	1	0.2129	0.9520 + 0.3061 i	−0.4274 + 0.9041 i	0.0041 − 1.0000 i	0.4058
31	4	2	0.4011	0.8025 + 0.5967 i	−0.6855 + 0.7281 i	0.2171 − 0.9761 i	0.3844
37	−11	1	0.9001	−0.2907 + 0.9568 i	−0.9939 − 0.1106 i	0.8980 − 0.4399 i	0.6830
43	−8	2	0.7423	0.1847 + 0.9828 i	−0.9804 + 0.1971 i	0.7022 − 0.7120 i	0.5126
61	1	3	0.5022	0.6436 + 0.7653 i	−0.8671 + 0.4982 i	0.3730 − 0.9278 i	0.3232
67	−5	3	0.6271	0.4178 + 0.9085 i	−0.9589 + 0.2837 i	0.5632 − 0.8263 i	0.3571
73	7	3	0.3829	0.7932 + 0.6089 i	−0.7822 + 0.6231 i	0.1987 − 0.9801 i	0.2661
79	−17	1	0.9483	−0.4295 + 0.9031 i	−0.8761 − 0.4821 i	0.9657 − 0.2596 i	0.4408
97	19	1	0.0890	0.9887 + 0.1498 i	−0.4791 + 0.8778 i	−0.2383 − 0.9712 i	0.2383
103	13	3	0.2919	0.8757 + 0.4828 i	−0.7239 + 0.6899 i	0.0609 − 0.9981 i	0.2327
109	−2	4	0.5556	0.5288 + 0.8487 i	−0.9508 + 0.3097 i	0.4751 − 0.8799 i	0.2600
127	−20	2	0.8875	−0.2473 + 0.9689 i	−0.9083 − 0.4183 i	0.9253 − 0.3794 i	0.3193
139	−23	1	0.9731	−0.4663 + 0.8846 i	−0.7821 − 0.6231 i	0.9836 − 0.1804 i	0.3135
151	19	3	0.2290	0.9203 + 0.3913 i	−0.6848 + 0.7287 i	−0.0415 − 0.9991 i	0.1997
157	−14	4	0.7212	0.1708 + 0.9853 i	−0.9969 − 0.0789 i	0.7371 − 0.6757 i	0.2520
163	25	1	0.0683	0.9929 + 0.1190 i	−0.4865 + 0.8737 i	−0.2912 − 0.9567 i	0.1941
181	7	5	0.4359	0.7010 + 0.7132 i	−0.9002 + 0.4355 i	0.2959 − 0.9552 i	0.1824

We present the corresponding values for $c^{(3)}$ in Table 6.3. Since these values are real, we will save some space and we use this for giving the information also in another form, namely $\frac{c_j^{(3)}}{\sqrt{p}}$, which should shed some light on the surprising behavior of the components.

Table 6.3 (Third canonical case)									
p	A	B	θ	$c_0^{(3)}$	$c_1^{(3)}$	$c_2^{(3)}$	$c_0^{(3)}/\sqrt{p}$	$c_1^{(3)}/\sqrt{p}$	$c_2^{(3)}/\sqrt{p}$
7	1	1	0.4602	−1.2221	9.4127	2.7389	−0.4619	3.5577	1.0352
13	−5	1	0.7790	−1.4201	−14.6415	2.1601	−0.3939	−4.0608	0.5991
19	7	1	0.2129	−2.2521	8.4655	4.8488	−0.5167	1.9421	1.1124
31	4	2	0.4011	−2.8168	17.2938	4.6888	−0.5059	3.1061	0.8421
37	−11	1	0.9001	−3.0328	−7.1015	2.8445	−0.4986	−1.1675	0.4676
43	−8	2	0.7423	−3.2558	−20.3776	3.6527	−0.4965	−3.1075	0.5570
61	1	3	0.5022	−4.0014	50.9574	5.4586	−0.5123	6.5244	0.6989
67	−5	3	0.6271	−4.2289	−95.9688	5.0005	−0.5166	−11.7245	0.6109
73	7	3	0.3829	-4.4100	25.6091	6.6407	-0.5162	2.9973	0.7772
79	-17	1	0.9483	-5.6126	-8.9422	4.1623	-0.6315	-1.0061	0.4683
97	19	1	0.0890	-5.0982	13.5365	10.4124	-0.5176	1.3744	1.0572
103	13	3	0.2919	-5.2556	21.9500	8.4142	-0.5179	2.1628	0.8291
109	-2	4	0.5556	-5.5068	337.8101	6.6180	-0.5275	32.3563	0.6339
127	-20	2	0.8875	-7.1148	-14.4873	5.5161	-0.6313	-1.2855	0.4895
139	-23	1	0.9731	-8.4417	-11.5986	5.6060	-0.7160	-0.9838	0.4755
151	19	3	0.2209	-6.3543	22.1314	10.5843	-0.5171	1.8010	0.8613
157	-14	4	0.7212	-7.1235	-36.5459	6.8056	-0.5685	-2.9167	0.5431
163	25	1	0.0683	-6.5753	16.4057	13.3294	-0.5150	1.2850	1.0440
181	7	5	0.4359	-7.0841	58.2887	9.2448	-0.5266	4.3326	0.6872

Our observations are summarized in the following remark:

Remark 6.3 Our numerical observations and our results are of five kinds:
(1) For each large p, the first and second canonical solutions are approximately symmetric to each other w.r.t. the origin.
(2) Even though two large primes may be close to each other without their canonical solutions being close, large primes with approximately the same θ will have approximately the same first canonical solutions and approximately the same second canonical solutions (even if the primes are not close to each other).
(3) The first and second canonical solution each forms a positively oriented triangle. For large p, each triangle is approximately equilateral.
(4) For large p, the approximate *positions* of the nearly equilateral triangles are simple functions of θ.
(5) If p is large, then all components of $|c^{(3)}|$ are large. If in addition $|A|$ is small, that is if θ is close to $\pi/6$, then $|c_1^{(3)}|$ is very large.

To make it easier to guess *quantitative* results (making "approximately" more precise in Remark 6.3) we present a few more numerical results in Table 6.4.

Table 6.4 (Large primes, close in size vs. close in θ-value)

p	A	B	θ	$\arg(c_0^{(1)})$	$2\theta-\pi$	$\arg(c_0^{(2)})$	2θ	$\mathrm{scal}(c^{(1)})$
1 003 273	973	337	0.354542	−2.433203	−2.432509	0.708033	0.709084	0.002810
1 003 279	1993	39	0.033775	−3.074105	−3.074038	0.067421	0.067555	0.002995
100 205 473	9733	3367	0.354372	−2.432917	−2.432848	0.708639	0.708744	0.000281

From Table 6.4 it seems that "approximately"means agreement in approximately $\frac{n}{2}$ decimals. Thus quantitative results in terms of $O(1/\sqrt{p})$ might seem plausible. In our quantitative results we will use the maximum norm to measure distances in $\mathbb{C}^3$. We will also need a notation for the equilateral "limit" triangle hinted at in item (4) of Remark 6.3, hopefully visible in Tables 6.2 and 6.3, and certainly present in columns 6 and 8 of Table 6.4. Thus we make the following two definitions:

Definition 6.4 *Let $a=(a_0,a_1,a_2)\in\mathbb{C}^3$. We define $\|a\|=\max(|a_0|,|a_1|,|a_2|)$.*

Definition 6.5 *Let p be a prime $\equiv 1 \pmod 6$ and let $\theta=\frac{1}{3}\mathrm{Arccos}\left(\frac{A}{2\sqrt{p}}\right)$, where $4p=A^2+27B^2$ and $A\equiv 1 \pmod 3$. We denote by $d=d(p)=(d_0,d_1,d_2)$ the (equilateral) triangle for which*

$$d_j=\exp\Big(2i(\theta-\frac{2j\pi}{3})\Big)=\exp\Big(i\,(2\theta+\frac{2j\pi}{3})\Big),\ \ j=0,1,2.$$

We will now state four quantitative results for the first and second canonical cases, where Proposition 6.j for $j=6,\dots,9$ is of kind $(j-5)$ as listed in Remark 6.3. (Kind (5) is discussed after Corollary 6.11 below.)

Proposition 6.6 *Let p be a prime $\equiv 1 \pmod 6$, and let $c^{(1)}$ and $c^{(2)}$ be the corresponding first and second canonical solution. Then*

$$\|c^{(1)}+c^{(2)}\|\le\frac{36}{5\sqrt{p}}.$$

Proposition 6.7 *Let $p'$and p'' be primes $\equiv 1 \pmod 6$, let θ' and θ'' be their respective θ-values and let c' and c'' be their respective first canonical solutions. Then*

$$\|c' - c''\| \le 2|\theta' - \theta''| + \frac{3}{\sqrt{p'}} + \frac{3}{\sqrt{p''}}.$$

The same result, with the constants 3 *replaced by* $\frac{21}{5}$*, holds if c' and c'' are their respective* second *canonical solutions.*

Proposition 6.8 *Let p be a prime $\equiv 1 \pmod 6$, and let $c^{(1)}$ and $c^{(2)}$ be the corresponding first and second canonical solution. Then*

$$\mathrm{scal}(c^{(1)}) \le \frac{7}{2\sqrt{p}} \quad \textit{and} \quad \mathrm{scal}(c^{(2)}) \le \frac{21}{5\sqrt{p}}.$$

Proposition 6.9 *Let p be a prime $\equiv 1 \pmod 6$, let $c^{(1)}$ and $c^{(2)}$ be the corresponding first and second canonical solution, and let d be as in Definition* 6.5*. Then*

$$\|c^{(1)} + d\| \le \frac{3}{\sqrt{p}} \text{ and } \|c^{(2)} - d\| \le \frac{21}{5\sqrt{p}}.$$

Remark 6.10 The constants in these propositions are not best possible but are chosen as compromises to make the proofs less cumbersome. Even if we restrict our claims to hold only for $p > M$ for some large M, the constants cannot always be significantly improved. For instance, for $p = 10^{10} + 279$ we have $\|c^{(2)} - d\| \approx 4/\sqrt{p}$. For a kind of "best possible", result, see Remark 6.13.

Since to each number θ (in the interval $[0, \pi/3]$) there corresponds at most one p, it does not make sense to consider a sequence of p:s with a common θ. However, Proposition 6.9 obviously has the following corollary, where we have used the notation $\theta(p)$, $c^{(2)}(p)$ and $c^{(1)}(p)$ for the values of θ and the first and second canonical solutions corresponding to p:

Corollary 6.11 *Let θ_0 be a real number in the interval $[0, \pi/3]$. Denote by $d = (d_0, d_1, d_2)$ the (equilateral) triangle for which $d_j = \exp\Big(2i(\theta_0 - \frac{2j\pi}{3})\Big)$, $j = 0, 1, 2$. Let $\{p_n\}_1^\infty$ be a sequence of primes $\equiv 1 \pmod 6$ going to infinity in such a way that $\lim_{n\to\infty} \theta(p_n) = \theta_0$. Then $\lim_{n\to\infty} c^{(1)}(p_n) = -d$ and $\lim_{n\to\infty} c^{(2)}(p_n) = d$.*

Before proving our four Propositions we will discuss item (5) of Remark 6.3. In Table 6.5 we present some more numerical values with focus on θ-values close to $0, \pi/6$ and $\pi/3$.

Table 6.5 (Third canonical case for some large primes)

p	A	B	θ	$c_0^{(3)}/\sqrt{p}$	$c_1^{(3)}/\sqrt{p}$	$c_2^{(3)}/\sqrt{p}$
67 521 601 729	−2	100 016	0.523600	−0.577348	779 547.6	0.577352
67 544 557 351	1	100 033	0.523598	−0.577347	194 920.0	0.577353
250 004 500 027	1 000 009	1	0.000002	−0.500000	1.000007	1.000001
250 018 500 349	−1 000 037	1	1.047196	−0.999993	−0.999999	0.500000

These and other numerical results make it plausible that "large" in item (5) of Remark 6.3, may be specified to mean "not much smaller than $\frac{1}{2}\sqrt{p}$ ", but it seems difficult to find θ-independent estimates of "convergence rate" for the third canonical case. Thus we prefer to give our quantitative result for the third canonical case the following form:

Proposition 6.12 *If $\{p_n\}_1^\infty$ is any sequence of primes $\equiv 1 \pmod 6$ going to infinity, then (with obvious notation) for $i = 0, 1,$ and 2,*

$$\liminf_{n\to\infty} \frac{|c_i^{(3)}(p_n)|}{\sqrt{p_n}} \geq 0.5. \tag{6.1}$$

We remark that this proposition implies that for every normalized $x = (1, x_1 \ldots, x_{p-1}) \in \mathbb{R}^p$ of index 3 coming from the third canonical case for a large p, either all $|x_j|,\ j \neq 0$, are large or they are all small (leaving the canonical case via the transformations mentioned in Theorem 4.1 and leaving the simple case via Definition 1.3).

We will now prove our five propositions.

Proof of Propositions 6.6 and 6.7 Proposition 6.6 follows from Proposition 6.9 via a straightforward application of the triangle inequality. Similarly, Proposition 6.7 follows from Proposition 6.9 via the triangle inequality and the inequality $|\exp(2i\phi') - \exp(2i\phi'')| \leq 2|\phi' - \phi''|$.

Proof of Proposition 6.8. From (3.4) and (3.6) and Remark 6.2 we get

$$\sqrt{p}\,\mathrm{scal}\ (c^{(1)}) = \tfrac{1}{2}\sqrt{p}\max_j |h_j + 1| \leq \tfrac{1}{2}\sqrt{p}\left(|1 + \xi_1^{(1)}| + |\eta_1^{(1)}|\right) = \frac{3\sqrt{p}(p - A) + p(6p - 24)}{2(p^2 - 3p - A)}. \tag{6.2}$$

Since the right-hand side of of (6.2) is a decreasing function of A and $A > -2\sqrt{p}$, we get

$$\sqrt{p}\,\mathrm{scal}\ (c^{(1)}) < \frac{3\sqrt{p}(p + 2\sqrt{p}) + p(6p - 24)}{2(p^2 - 3p + 2\sqrt{p})} = 3 + \frac{3(\sqrt{p} - 2)}{2(\sqrt{p} - 1)^2}. \tag{6.3}$$

The right-hand side of (6.3) as a function of p is decreasing for $p > 9$ and takes values < 3.4 for $p = 7$ and 13. This completes the proof of the first part of the proposition.

For the second part, we will use (3.7), the fact that $\eta_1^{(2)} = -2\sqrt{p}(1 + \xi_1^{(2)})$ and the identity

$$\left(\sqrt{p}\sqrt{p + 4A + 16} + p + 2\right)\left(\sqrt{p}\sqrt{p + 4A + 16} - p - 2\right) = 4(Ap + 3p - 1)$$

to give the counterpart of (6.2) the form

$$\sqrt{p}\,\mathrm{scal}\ (c^{(2)}) \leq \tfrac{1}{2}\sqrt{p}\left(|1+\xi_1^{(2)}| + |\eta_1^{(2)}|\right) = \tfrac{1}{2}(2p+\sqrt{p})\,|1+\xi_1^{(2)}| = \frac{3(2p + \sqrt{p})}{p + 2 + \sqrt{p}\sqrt{p + 4A + 16}}.$$

We can again take $A = -2\sqrt{p}$. The resulting expression is easily seen to be < 4 for $p > 100$ and for the remaining p we take from Table 6.2 the true value of A (or of scal $(c^{(2)})$) to get a maximum ≈ 4.1966 (or ≈ 4.155, respectively) for $p = 37$. This completes the proof.

Remark 6.13 From (6.3) we easily get the following result: For each ϵ with $0 < \epsilon < 1$ we have

$$\mathrm{scal}(c^{(1)}) \leq \frac{3+\epsilon}{\sqrt{p}} \quad if \quad p > \Big(\frac{3}{2\epsilon}\Big)^2.$$

This is close to"best possible" in the following sense: If we take e.g. $\epsilon = \sqrt{p}\,\mathrm{scal}(c^{(1)}) - 3$ for $p = 10\ 002\ 900\ 217$, then $(3/2\epsilon)^2 \approx 1.000095\,p$.

In the proof of Proposition 6.9 we will work with α, β and γ as given in Theorem 4.1 and ρ, σ, and τ as given in Lemma 4.3. We will use the following lemma:

Lemma 6.14 *Let $b' = (b'_0, b'_1, b'_2) \in \mathbb{C}^3$ and $b'' = (b''_0, b''_1, b''_2) \in \mathbb{C}^3$ be given by*

$$b'_j = \rho' + \sigma' \cos\left(\theta - \frac{2\pi}{3}j\right) + \tau' \sin\left(\theta - \frac{2\pi}{3}j\right), \quad j = 0, 1, 2,$$

$$b''_j = \rho'' + \sigma'' \cos\left(\theta - \frac{2\pi}{3}j\right) + \tau'' \sin\left(\theta - \frac{2\pi}{3}j\right), \quad j = 0, 1, 2,$$

where $\theta \in \mathbb{R}$ and $\rho', \sigma', \tau', \rho'', \sigma'', \tau'' \in \mathbb{C}$, Then

$$\|b' - b''\| \leq |\rho' - \rho''| + \sqrt{|\sigma' - \sigma''|^2 + |\tau' - \tau''|^2}.$$

The proof of Lemma 6.14 is a straightforward application of the triangle inequality, the Cauchy inequality, and the identity $\cos^2 + \sin^2 = 1$.

Proof of Proposition 6.9 In Lemma 6.14 we take $b' = c^{(1)}$ and $b'' = -d$ (cf. Definitions 5.1 and 6.5). Then $\rho' = \alpha^{(1)}, \sigma' = \beta^{(1)}, \tau' = \gamma^{(1)}$ as given in (4.3), whereas $\rho'' = 0, \sigma'' = -\cos 3\theta - i \sin 3\theta$, and $\tau'' = -\sin 3\theta + i \cos 3\theta$, as is easily seen from (4.11). Since $\cos 3\theta = \dfrac{A}{2\sqrt{p}}$ and $\sin 3\theta = \dfrac{3B\sqrt{3}}{2\sqrt{p}}$, Lemma 6.14 shows that for the proof of the first half of Proposition 6.9 it only remains to check that with $\alpha^{(1)}, \beta^{(1)}$, and $\gamma^{(1]}$ as in (4.3) we have

$$\sqrt{p}\,|\alpha^{(1)}| + \sqrt{p\Big|\beta^{(1)} + \frac{A + i3\sqrt{3}B}{2\sqrt{p}}\Big|^2 + p\Big|\gamma^{(1)} + \frac{3\sqrt{3}B - iA}{2\sqrt{p}}\Big|^2} \leq 3. \tag{6.4}$$

Introducing the values of $\alpha^{(1)}, \beta^{(1)}$, and $\gamma^{(1]}$ and replacing $3B\sqrt{3}$ by $\sqrt{4p - A^2}$ we can after some calculation treat the first term of the left-hand side of (6.4) as follows

$$\sqrt{p}\,|\alpha^{(1)}| = \sqrt{\frac{p^2 - Ap}{p^2 - 3p - A}} < \sqrt{\frac{p^2 + 2p\sqrt{p}}{p^2 - 3p + 2\sqrt{p}}} = \sqrt{\frac{p(2+\sqrt{p})}{(p-3)\sqrt{p} + 2}}, \tag{6.5}$$

where the estimate comes from the facts that the second term of (6.5) is a decreasing function of A and that $A > -2\sqrt{p}$. Let us denote by Q the expression under the big root

sign in (6.4). Since the right-hand side of (6.5) is a decreasing function of p with a value < 1.5 for $p = 31$, we can prove (6.4) for $p \geq 31$ by checking that

$$Q \leq (3 - 1.5)^2 = 2.25 \text{ for } p \geq 31 \tag{6.6}$$

Treating Q in the same way as we did with first term of the left-hand side of (6.4) we find

$$Q = \frac{2p^3 - (A+6)p^2 + 2Ap - (2p - A - 4)\sqrt{p^4 - 4p^3}}{p^2 - 3p - A}. \tag{6.7}$$

Using a Taylor formula with rest term we have

$$\sqrt{p^4 - 4p^3} = p^2\Big(1 - \frac{4}{p}\Big)^{\frac{1}{2}} = p^2 - 2p - 2 + R_3,$$

where $-\frac{6}{p} < R_3 < 0$ (since $p > 31$). Introducing this in (6.7) we get

$$Q = \frac{2p^2 - 4p - 2A - 8 - (2p - A - 4)R_3}{p^2 - 3p - A} < \frac{2(p^3 - 2p^2 - Ap + 2p - 3A - 12)}{p(p^2 - 3p - A)}. \tag{6.8}$$

Since the right-hand side of (6.8) is a decreasing function of A we can estimate it with its value for $A = -2\sqrt{p}$, which is a decreasing function of p and thus not larger than its value for $p = 31$, which turns out to be ≈ 2.08 in agreement with (6.6). Finally, we check numerically the value of $\sqrt{p}\|c^{(1)} + d\|$ for $p = 7, 13$, and 19. We find 2.59, 2.31, and 1.91, which are all < 3. This completes the proof of the first half of the proposition.

For the second part of the proof we proceed in the same way but let MATHEMATICA help us to get a good start, namely by telling us that defining $m(p) = \sqrt{p}\,\|c^{(2)} - d\|$ we have $m(p) \leq m(43) < 4.1$ if $p < 10\ 000$. We get after some calculation

$$\sqrt{p}\,|\alpha^{(2)}| = \sqrt{\frac{2p}{2 + p + \sqrt{p}\sqrt{p + 4A + 16}}} \leq \sqrt{\frac{2p}{2 + p + \sqrt{p}\sqrt{p - 8\sqrt{p} + 16}}} < \frac{100}{99}$$

if $p > 10\ 000$, (the absurd "prime" 10 000 with the absurd $A = -2\sqrt{10\ 000}$ giving equality). Thus to complete the proof is enough to prove that

$$p\Big|\beta^{(2)} - \frac{A + i3\sqrt{3}B}{2\sqrt{p}}\Big|^2 + p\Big|\gamma^{(2)} - \frac{3\sqrt{3}B - iA}{2\sqrt{p}}\Big|^2 \leq 10.17 \tag{6.9}$$

if $p >$10 000, e.g. by proving that the first term of (6.9) is < 1.07 and the second term is < 9.1. This can be done as in the proof of the first part, using (4.4). Just as we have studied functions of A restricted to the interval $|A| < 2\sqrt{p}$, we will now with the help of (4.6) and (4.7) write the left-hand side of (6.9) as a function of u and v, where $|u - 4| < v < u + 4$. Again a certain square root can be estimated with a Taylor formula. We leave the details to the reader.

Proof of Proposition 6.12 Inspired by the first two rows of Table 6.5 we expect infinities near $\theta = \pi/6$, and thus, to avoid zeros in the denominator, we "turn everything upside down". Thus we want to prove that

$$\limsup_{n\to\infty} \frac{\sqrt{p_n}}{|c_i^{(3)}(p_n)|} \leq 2.$$

Suppose this is not true. Then (by taking subsequences if needed) we can find a sequence $\{p_n\}_1^\infty$ of primes $\equiv 1 \pmod 6$ going to infinity, such that

$$\lim_{n\to\infty} \frac{\sqrt{p_n}}{c_j^{(3)}(p_n)} = l_j, \tag{6.10}$$

where these three limits exist (finite or $+\infty$ or $-\infty$) and $|l_j| > 2$ for at least one j (0, 1, or 2). Since the interval $[0, \pi/3]$ is compact, we can by again taking a subsequence (keeping the notation $\{p_n\}_1^\infty$) arrange that $\theta_0 = \lim_{n\to\infty} \theta(p_n)$ exists.

But the left hand side of (6.10) can be computed for $j = 1, 2, 3$ by using (4.26) and (4.28) as follows. By estimating various square roots with a Taylor formula, we get after a considerable amount of calculation:

$$\begin{aligned}
\lim_{n\to\infty} \left(\sqrt{p_n}\,(\alpha_1^{(3)} - \alpha_2^{(3)})\right) &= 0, \\
\lim_{n\to\infty} \left(\sqrt{p_n}\,(\beta_1^{(3)} - \beta_2^{(3)})\right) &= -4, \\
\lim_{n\to\infty} \left(\sqrt{p_n}\,(\gamma_1^{(3)} - \gamma_2^{(3)})\right) &= 0,
\end{aligned}$$

where $\alpha_k^{(3)}, \beta_k^{(3)}$, and $\gamma_k^{(3)}$ $(k = 1, 2)$ are obtained by taking $p = p_n$ [in the expressions for A, B, u, and v] in (4.26). Hence by (4.28), the left hand side of (6.10) is given by

$$-2\cos\theta_0, \quad -2\cos(\theta_0 - 2\pi/3), \quad -2\cos(\theta_0 - 4\pi/3)$$

for $j = 0, 1, 2$, respectively. Therefore,

$$l_0 = -2\cos\theta_0,\ l_1 = -2\cos(\theta_0 - 2\pi/3),\ l_2 = -2\cos(\theta_0 - 4\pi/3). \tag{6.11}$$

This is a contradiction, since we have supposed that $|l_j| > 2$ for at least one j. We have thus completed the proof and also substantiated the "very large" part of item (5) of Remark 6.3 (take l_1 from (6.11) and consider $|1/l_1|$ for θ_0 close to $\pi/6$).

7 Software

It is the ambition of the authors to make relevant MATHEMATICA software available on the following webpage:

`http://www.math.su.se/index3/`

References

[1] *A New English Dictionary on Historic Priciples*, Volume VIII, Part II, p. 167, Clarendon, Oxford, 1914.

[2] G. Björck. Functions of modulus one on $\mathbf{Z}_p$, whose Fourier transform have constant modulus, and 'cyclic n-roots'. *Recent Advances in Fourier Analysis and its Applications (J .S. Byrnes and J.F. Byrnes, eds), NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci. , Kluwer*, 315:131–140, 1989.

[3] 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*, 320:319–324, 1995.

[4] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer Graduate Texts in Mathematics, 138, New York, 1992.

[5] D. A. Cox. *Primes of the Form $x^2 + ny^2$*. Wiley, New York, 1989.

[6] L. E. Dickson. *First Course in the Theory of Equations*. Wiley, New York, 1947.

[7] 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)*, International Press, Cambridge, 296-322, 1997.

[8] P. de la Harpe and V. R. F. Jones. Paires de sous-algebres semi-simples et graphes fortement reguliers. *C. R. Acad. Sci. Paris*, 311:147-150, 1990.

[9] D.R. Heath-Brown and S.J. Patterson. The distribution of Kummer sums at prime arguments. *J. Reine Angew, Math.*, 310:111-130, 1979.

[10] Ireland and Rosen. *A Classical Introduction to Modern Number Theory*. Springer Graduate Texts in Mathematics, 84, New York, 1992.

[11] A. Munemasa and Y. Watatani Orthogonal pairs of *-subalgebras and Association Schemes. *C. R. Acad. Sci. Paris*, 314:329-331, 1992.

[12] S. Popa. Orthogonal pairs of *-subalgebras in finite von Neumann algebras. *J. Operator Theory*, 9:253–268, 1983.

[13] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.