CONSTRUCTIBLE POLYGONS

JOAN M TAYLOR

1. Preliminaries

Definition 1.0.1. The *νth irreducible negative cyclotomic polynomial,* Ψ_ν, has zeros that are the νth primitive roots of negative unity. That is, Ψ_ν is what remains of the νth negative cyclotomic polynomial, $x^\nu+1$, after the removal of any polynomial factors with rational coefficients. Ψ_ν has zeros with the form $e^{iu\pi/\nu}$ with $\gcd(u,2\nu)=1, 1\le u<2\nu$.

Remark 1.0.2. The group of units $\mathcal{U}_\nu$, also called the modulo multiplicative group $\mathfrak{M}_\nu$, is the group of positive integers less than and relatively prime to ν under the operation of multiplication modulo ν. There exists a natural correspondence between the zeros of Ψ_ν and the elements, u, of $\mathcal{U}_{2\nu}$, $e^{iu\pi/\nu} \leftrightarrow u$.

In section 2 we describe the algebraic method of discovery of a constructible expression for $e^{ik\pi/n}$, where k is any integer and n is restricted as follows in remark 1.0.4, and in section 3 the algorithm for the numeric method for the same construction. It will be seen that it is sufficient for each of the methods that the order of $\mathcal{U}_{2n}$ is equal to a power of 2, $|\mathcal{U}_{2n}|=2^m$ for some non-negative integer m.

Theorem 1.0.3. *$|\mathcal{U}_\nu|=2^m$ has solutions only when $\nu=p_1p_2\cdots p_j2^k$, for any number (possibly none) of distinct odd primes, p_i, of the form $2^{2^t}+1$, k a non-negative integer and $\nu>1$.*

Proof. Euler's phi function gives $\phi(\nu)=|\mathcal{U}_\nu|$. For prime p, $\phi(p^k)=p^{k-1}(p-1)$ which provides $\phi(2^k)=2^{k-1}$ and $\phi(p)=p-1$. $\phi(n_1n_2)=\phi(n_1)\phi(n_2)$ when $\gcd(n_1,\ n_2)=1$ for positive integers $n_1,\ n_2$, and hence is multiplicative on prime powers. [ref] It follows that $|\mathcal{U}_\nu|=2^m$ when (i) ν is an odd prime with form 2^k+1 (whence $k=2^t$ because 2^r+1 divides $2^{rs}+1$ whenever s is odd) or a product of such distinct primes and when (ii) $\nu=2^k$ for a positive integer k. These two cases combine to form the general case where ν is equal to a product of any number of distinct odd primes of form $2^{2^t}+1$ and any power of 2 but $\nu>1$ and for no other values of ν. $\square$

Remark 1.0.4. For $|\mathcal{U}_{2n}|=2^m$ we therefore have $n=p_1p_2\cdots p_j2^k$ with any number of odd primes, p_i, having form $2^{2^t}+1$, k a non-negative integer but now $n=1$ is possible. (The element of $\mathcal{U}_2$, defined on $\{1\}$, corresponds to the zero of $\Psi_1=x+1$, the 1-gon's polynomial) and we may by the following methods construct the zeros of Ψ_n. These values for n correspond to the numbers of sides of the constructible regular polygons. [ref] All subsequent mention of $\mathcal{U}_{2n}$ and Ψ_n have n restricted to these values.

It follows from $|\mathcal{U}_{2n}|=2^m$ that for each element, u, of $\mathcal{U}_{2n}$, $u^{2^j}\equiv 1 \pmod{2n}$, $0\le j\le m$, where 2^j is the least such power, by the Theorem of Lagrange. The square root pictures in figure 1.0.5 show the interrelationships among the elements of $\mathcal{U}_{10}$, $\mathcal{U}_{16}$, $\mathcal{U}_{20}$ and $\mathcal{U}_{30}$. $\beta\to\alpha$ indicates that β is a square root of α, $\beta^2\equiv\alpha \pmod{2n}$. Of course unity is its own square root in every case.

Date: 15th July, 2003.

$$\begin{tikzcd} & \mathcal{U}_{10} & \\ & 1 & \\ & 9 \arrow[u] & \\ 3 \arrow[ur] & & 7 \arrow[ul] \end{tikzcd}
\qquad
\begin{tikzcd} & \mathcal{U}_{16} & \\ 7 \arrow[r] & 1 & 15 \arrow[l] \\ 3 \arrow[r] & 9 \arrow[u] & 13 \arrow[l] \\ 5 \arrow[ur] & & 11 \arrow[ul] \end{tikzcd}$$

$$\begin{tikzcd} & \mathcal{U}_{20} & \\ 11 \arrow[r] & 1 & 19 \arrow[l] \\ 3 \arrow[r] & 9 \arrow[u] & 13 \arrow[l] \\ 17 \arrow[ur] & & 7 \arrow[ul] \end{tikzcd}
\qquad
\begin{tikzcd} & \mathcal{U}_{30} & \\ 11 \arrow[r] & 1 & 29 \arrow[l] \\ 7 \arrow[r] & 19 \arrow[u] & 17 \arrow[l] \\ 23 \arrow[ur] & & 13 \arrow[ul] \end{tikzcd}$$

Figure 1.0.5.

2. An Algebraic Method for Constructing $e^{ik\pi/n}$

In this section we describe the repeated partitioning of $\mathcal{U}_{2n}$ into cosets with the number of elements per coset successively equal to $1,\ 2,\ 2^2, \dots,\ 2^m = \phi(2n)$. The *cosums* (sums of zeros of Ψ_n, $\Sigma_j\ e^{iu_j\pi/n}$, where the u_j belong to a coset of $\mathcal{U}_{2n}$) are studied as they are influenced by the introduction of a multiple, m, into the exponent, $e^{imu_j\pi/n}$. It is found that m sends a cosum to itself, to another cosum of the same size belonging to Ψ_n, to a number of copies of a cosum belonging to Ψ_s, where s divides n, or to a reflection in the imaginary axis of one of these.

It is shown that the sum of all the zeros of Ψ_n is an integer. Then begins the investigation of the expressions for the cosums consisting of a particular half of the zeros, quarter of the zeros, and so forth. To this end a tabular form of a sum of two squares of cosums (those whose u_j belong to the first and to the second half of $\mathcal{U}_{2n}$ as partitioned by the preceding method) is set up. The table is repeatedly referred to for each size (measured by the number of summands) of cosum considered. It permits the expression of the value of any cosum to be given in terms of a constructible expression using sums of larger cosums of Ψ_n, cosums of Ψ_s, where s divides n, or their reflections. This chain of constructible expressions is followed to its conclusion in the constructible expression for $e^{iu\pi/n}$, $u \in \mathcal{U}_{2n}$. It is noted that $e^{ik\pi/n}$, for any integer k, is similarly constructible.

Examples are worked for all the zeros of Ψ_5, having unique expressions, and two different expressions for $e^{i\pi/n}$ of Ψ_n are worked for each of $n = 8$, 10 and 15.

2.1. **Forming the Cosets of $\mathcal{U}_{2n}$.** The elements of $\mathcal{U}_{2n}$ are to be repeatedly partitioned into cosets. The first subgroup, coset containing unity, is simply $\{1\}$ and each other element has a coset to itself. The second subgroup is formed by the union of the first subgroup with another coset containing a square root of unity. Say α is a square root of unity, $\alpha^2 \equiv 1 \pmod{2n}$, then the second subgroup is $\{1,\ \alpha\}$. The third subgroup is formed by the union of the second subgroup with another coset containing a square root of either 1 or α, that is with a square root of any element of the second subgroup. If $\beta^2 \equiv 1 \pmod{2n}$ or $\beta^2 \equiv \alpha \pmod{2n}$ then the third subgroup is $\{1,\ \alpha,\ \beta,\ \alpha\beta\}$. Let γ be a square root of an element in the third subgroup. Then the fourth subgroup is $\{1,\ \alpha,\ \beta,\ \alpha\beta\ \gamma,\ \alpha\gamma,\ \beta\gamma,\ \alpha\beta\gamma\}$. This process is continued until the subgroup so made contains all the elements of $\mathcal{U}_{2n}$. (The elements of a subgroup are unordered. We order them to form the habit of doing so because later we shall use the fact that a subgroup and its cosets *can* be so ordered.) For example, in $\mathcal{U}_{30}$, beginning with the formation of the second subgroup, let $\alpha = 29$, partitioning the group into subgroup $\{1,\ 29\}$ and other cosets $\{11,\ 19\}$, $\{7,\ 23\}$ and $\{13,\ 17\}$. (At this stage the ordering of the elements within a coset other than the subgroup is not unique.) Next let $\beta = 19$ producing cosets $\{1,\ 29,\ 19,\ 11\}$ and $\{7,\ 23,\ 13,\ 17\}$. Letting $\gamma = 13$ will unite all the elements again in one coset, $\{1,\ 29,\ 19,\ 11\ 13,\ 17,\ 7,\ 23\}$, which is equal to the whole group. Other choices for α, β and γ were of course possible. This process of repeatedly forming cosets is formalized in the following proposition.

Proposition 2.1.1. *The elements of $\mathcal{U}_{2n}$ can be repeatedly partitioned into cosets with the number of elements per coset successively equal to* $1,\ 2,\ 2^2, \dots,\ 2^m = \phi(2n)$ *by forming the union of two cosets at each stage. The coset to be united with the subgroup is determined by that coset containing an element which is a square root of any element of the subgroup. Thus a new larger subgroup and its cosets are formed. This process may be continued until the subgroup so made consists of all the elements of $\mathcal{U}_{2n}$.*

Proof. The union of a subgroup with another coset containing a square root of an element of the subgroup does produce a new subgroup: it is closed under the operation of the group. Let ζ be such a square root and u_j be an element of the old subgroup. Because the old subgroup is closed ζu_j is in the coset of ζ. The products of an element of the ζ coset with another element of the ζ coset, $\zeta^2 u_1 u_2$, is an element of the old subgroup. And a product of an element of the ζ coset with an element of the old subgroup, $\zeta u_1 u_2$, is in the ζ coset. Therefore the new subgroup is closed.

The supply of candidate square roots is sufficient to complete the process. By specification of $\mathcal{U}_{2n}$ any element, say ζ proceeds by a chain of squares to unity, $\zeta^{2^j} \equiv 1 \pmod{2^k}$, 2^j is the least such power. Say ζ is not in the old subgroup then some element in the list $\zeta,\ \zeta^2,\ \zeta^4, \dots,\ \zeta^{2^j} = 1$, from left to right, is the first element to be in the old subgroup. The element immediately to that element's left is a candidate square root whose coset may be united with the old subgroup to make the new subgroup. So long as there exists an element, ζ, not already in the old subgroup then there exists an element which is a candidate square root with which to make the next subgroup. □

2.2. **Cosums and their Reflections.** The process, already performed, of forming the subgroups and other cosets used the fact that multiplying the elements of a coset by an element, u, of $\mathcal{U}_{2n}$ produces another coset. The same coset is produced if u is an element of the subgroup else a different coset is produced. It will assist in the understanding of the theorems of this subsection to first study the effect of multiplying the cosets of $\mathcal{U}_{2n}$ by an even integer, w, taken modulo $2n$, with $\gcd(w,\ n) = 1$. To this end we depict some integers modulo $2n$ in a radial display, figure 2.2.1.

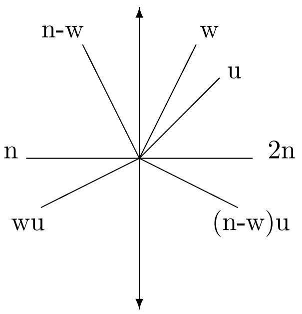

Figure 2.2.1.

Lemma 2.2.2. *When the elements, u_j, of a coset of $\mathcal{U}_{2n}$ are multiplied by an even integer, w, taken modulo $2n$, and $\gcd(w,\ n) = 1$ the coset is sent to the reflection, in the vertical axis of the radial display of integers modulo $2n$, of a coset of $\mathcal{U}_{2n}$.*

Proof. Multiplying u by w is equivalent to multiplying u by the reflection of w in the vertical axis (see figure 2.2.1) and then reflecting the result. Reflection is achieved by subtraction from n. $n - (n-w)u = n(1-u) + wu \equiv wu \pmod{2n}$, as required, because $1 - u \pmod{2n}$ is even. Also $\gcd(n-w,\ n) = 1$, taken modulo $2n$. (To see this note that $\gcd(w,\ n) = 1 \Leftrightarrow aw + bn = 1$ for some integers $a,\ b$ and that for $w < n$, $(n-w)(-a) + n(a+b) = aw + bn = 1$ and for $n < w < 2n$, $(2n + n - w)(-a) + n(3a + b) = aw + bn = 1$.) So $n - w \pmod{2n}$ is an element of $\mathcal{U}_{2n}$ and multiplication by $(n-w)$ sends u and its coset members to themselves or to another coset. Subtraction from n produces the reflection of that result. □

We now consider the effects on the exponents of zeros of Ψ_n of an integer multiple, but first a definition.

Definition 2.2.3. A *cosum* is a sum of zeros with form $\Sigma_j\ e^{iu_j\pi/n}$ of Ψ_n whose exponent u_j's belong to a coset of $\mathcal{U}_{2n}$.

Theorem 2.2.4. *When the exponents of a cosum are multiplied by an integer, m, taken modulo $2n$, and $\gcd(m,\ n) = 1$ the cosum is sent to a cosum (of the same size) of Ψ_n or to the reflection, in the imaginary axis of the complex plane, of a cosum of Ψ_n.*

Proof. If m is odd then it is an element of $\mathcal{U}_{2n}$ and it sends the cosum to the same or another cosum just as it sends a coset to the same or another coset. If m is even then n is odd and also $\gcd(n-m,\ n) = 1$, taken modulo $2n$, using the same arguments used for cosets in lemma 2.2.2. $n - m$ or, equivalently $2n + n - m$ if $n - m < 0$, is an element of $\mathcal{U}_{2n}$ and on multiplication of a cosum's exponents by even m the cosum is sent either to a reflection of itself in the imaginary axis (when $n - m$ is an element of the subgroup) or to a reflection of another cosum. □

Theorem 2.2.5. *When the exponents of a cosum are multiplied by an integer, m, taken modulo $2n$, and $\gcd(m,\ n) \neq 1$ the cosum is sent to so many copies of a cosum (of some size) of Ψ_s or to the reflections, in the imaginary axis of the complex plane, of so many copies of a cosum of Ψ_s, where m/n in lowest terms is equal to r/s.*

Proof. Now $\gcd(r,\ s) = 1$. For u a coset member we have $\gcd(u,\ n) = 1$, by group membership. s is a divisor of n implies that further $\gcd(u,\ s) = 1$. Because u is always odd $\gcd(u,\ 2s) = 1$ and $u \pmod{2s} \in \mathcal{U}_{2s}$. If $mu = kn$ for some k then n divides m, because $m = kn/u = rn$ for some r, and $s = 1$. In general if r is odd then the collection $u_j r$, where u_j are the elements of a coset, amounts to so many copies of a coset of $\mathcal{U}_{2s}$. Compare the theorem 2.2.4. (See also remark 2.2.6 following.) If r is even then s is odd and we have again the reflections, this time of so many copies of a coset of $\mathcal{U}_{2s}$. These results for cosets translate directly into the results for cosums. □

Remark 2.2.6. When s divides n the square roots chosen for forming the cosets of $\mathcal{U}_{2n}$ retain their square root property, when taken modulo $2s$, in the group $\mathcal{U}_{2s}$. $\beta^2 \equiv \alpha \pmod{2n} \Leftrightarrow \beta^2 = \alpha + k2n$. $st = n \Rightarrow \beta^2 = \alpha + k2st \Leftrightarrow \beta^2 \equiv \alpha \pmod{2s}$. Therefore when $\alpha^2 \equiv 1 \pmod{2n}$ also $\alpha^2 \equiv 1 \pmod{2s}$, when $\beta^2 \equiv \alpha \pmod{2n}$ also $\beta^2 \equiv \alpha \pmod{2s}$ and when $\beta^2 \equiv 1 \pmod{2n}$ also $\beta^2 \equiv 1 \pmod{2s}$ but possibly $\alpha \equiv 1 \pmod{2s}$, $\beta \equiv \alpha \pmod{2s}$ or $\beta \equiv 1 \pmod{2s}$. So there are several ways of making so many copies of a $\mathcal{U}_{2s}$ coset by taking modulo $2s$ the $\mathcal{U}_{2n}$ coset $\{1,\ \alpha,\ \beta,\ \alpha\beta \pmod{2n}\}$. Depending on the actual values involved it might be equivalent to

$$\begin{aligned}
&\{1,\ \alpha \pmod{2s},\ \beta \pmod{2s},\ \alpha\beta \pmod{2s}\}\\
\text{or }&\{1,\ \alpha \pmod{2s},\ 1 \pmod{2s},\ \alpha \pmod{2s}\}\\
\text{or }&\{1,\ \alpha \pmod{2s},\ \alpha \pmod{2s},\ 1 \pmod{2s}\}\\
\text{or }&\{1,\ 1 \pmod{2s},\ \alpha \pmod{2s},\ \alpha \pmod{2s}\}\\
\text{or }&\{1,\ 1 \pmod{2s},\ \beta \pmod{2s},\ \beta \pmod{2s}\}\\
\text{or }&\{1,\ 1 \pmod{2s},\ 1 \pmod{2s},\ 1 \pmod{2s}\},
\end{aligned}$$

the second, third and fourth in the list being, of course, equivalent to each other.

Theorem 2.2.7. *When the exponents of a cosum are multiplied by an integer, m, taken modulo $2n$, the cosum is sent to a cosum (of the same size) of Ψ_n, to the reflection, in the imaginary axis of the complex plane, of a cosum of Ψ_n, to so many copies of a cosum (of some size) of Ψ_s or to the reflections, in the imaginary axis of the complex plane, of so many copies of a cosum of Ψ_s, where m/n in lowest terms is equal to r/s.*

Proof. This theorem is merely a combination of theorems 2.2.4 and 2.2.5 above. □

2.3. **Constructible Expressions for Cosums.**

Theorem 2.3.1. *The sum of the zeros of Ψ_n is equal to* 0, 1 *or* -1.

Proof. The negative cyclotomic polynomial, $x^n + 1$, has a sum of zeros equal to 0. (Its x^{n-1} term has coefficient 0.) Its zeros have the form $e^{i(2j-1)\pi/n}$, $1 \le j \le n$. x^p+1, with p an odd prime, has a single polynomial factor, $\Psi_1 = x+1$. (Ψ_p has zeros $e^{iu\pi/p}$ where $\gcd(u, 2p) = 1, 1 \le u < 2p$.) Ψ_1 has only one zero, $e^{i\pi} = -1$, so Ψ_p has a sum of zeros equal to $0-(-1) = 1$. $x^{p_1p_2}+1$ has polynomial factors Ψ_1, Ψ_{p_1} and Ψ_{p_2} which implies that the sum of zeros if $\Psi_{p_1p_2}$ is equal to $0 - (-1) - 2(1) = -1$. $x^{p_1p_2p_3} + 1$ has polynomial factors Ψ_1, Ψ_{p_2}, Ψ_{p_3}, $\Psi_{p_1p_2}$, $\Psi_{p_1p_3}$ and $\Psi_{p_2p_3}$ which implies that the sum of zeros if $\Psi_{p_1p_2p_3}$ is equal to $0 - (-1) - 3(1) - 3(-1) = 1$. Generally when $n = p_1p_2 \cdots p_k$, a product of distinct odd primes, the sum of zeros of Ψ_n is equal to $\binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \ldots \pm \binom{k}{k-1} = \pm 1$. It is equal to 1 when k is odd and -1 when k is even. This series for each k coincides with the coefficients of $(x-1)^k$ excepting the constant term. That unity is a zero of these polynomials proves that each series has the required total. So the sum of zeros of Ψ_n, when n is odd, is equal to ± 1.

When n is even and $n/2$ is odd $\Psi_2 = x^2 + 1$ is a polynomial factor of $x^n + 1$. After removal of Ψ_2 from $x^n + 1$ when $n/2$ is odd, and for $x^n + 1$ when $n/2$ is even, the (remaining) zeros are in collections of four, one in each quadrant of the complex plane. Say $e^{iu\pi/n}$ is in the first quadrant then we have also, besides the exponent using u, the exponents using $n-u$, $n+u$ and $2n-u$. When one of these is relatively prime to $2n$ all are, by similar arguments to those used in lemma 2.2.2. The sum of these four zeros is equal to 0. So the sum of zeros for any number of collections of four zeros of this type is equal to 0, that is the sum of zeros of Ψ_n for even n is equal to 0. □

Remark 2.3.2. Any two complex values, say x_1 and x_2, can be made the zeros of a monic quadratic polynomial with coefficients in the field of complex numbers. $(x-x_1)(x-x_2) = x^2-(x_1+x_2)x+x_1x_2$, and the expressions are $x_1,\ x_2 = [(x_1+x_2)\pm\sqrt{[(x_1+x_2)^2-4x_1x_2]}]/2$ or, using Newton's identities, $x_1x_2 = [(x_1+x_2)^2-(x_1^2+x_2^2)]/2$ giving $x_1,\ x_2 = [(x_1+x_2)\pm\sqrt{[2(x_1^2+x_2^2)-(x_1+x_2)^2]}]/2$. All we shall then require in order to have a constructible expression for x_1 and x_2 is that the sum of the zeros of the quadratic polynomial and the sum of their squares be constructible values.

We now consider constructible expressions for cosums smaller than the sum of all the zeros of Ψ_n. We adopt the notation $[\zeta]$ to represent $e^{i\zeta\pi/n}$. Taking the cosets in the reverse order to that in which we made them in section 2.1 and using the general example with eight elements in $\mathcal{U}_{2n}$, we attend now to the cosets $\{1,\ \alpha,\ \beta,\ \alpha\beta\}$ and $\{\gamma,\ \alpha\gamma,\ \beta\gamma,\ \alpha\beta\gamma\}$ and the cosums corresponding to them $[1]+[\alpha]+[\beta]+[\alpha\beta]$ and $[\gamma]+[\alpha\gamma]+[\beta\gamma]+[\alpha\beta\gamma]$.

Obviously the sum $x_1+x_2 = ([1]+[\alpha]+[\beta]+[\alpha\beta])+([\gamma]+[\alpha\gamma]+[\beta\gamma]+[\alpha\beta\gamma])$ is equal to an integer because it is just the sum of all the zeros again. We need to find the sum of these two values squared, $x_1^2+x_2^2$, and if this value is constructible then so are x_1 and x_2 by remark 2.3.2.

After that we can consider separately the pairs $([1]+[\alpha])$, $([\beta]+[\alpha\beta])$ and $([\gamma]+[\alpha\gamma])$, $([\beta\gamma]+[\alpha\beta\gamma])$, distinguished respectively by the notation $x_{1(2)},\ x_{2(2)}$, and $x_{3(2)},\ x_{4(2)}$, the subscript number in parenthesis meaning *of level 2*. In keeping with this notation we rename the previous sums of four zeros, $x_{1(1)}$ and $x_{2(1)}$, and the sum of all the zeros, $x_{1(0)}$. The sum of the first pair of cosums, $x_{1(2)}+x_{2(2)}$, is equal to $x_{1(1)}$ and the sum of the second pair of cosums, $x_{3(2)}+x_{4(2)}$, is equal to $x_{2(1)}$. If we can express the sum of squares in terms of rational functions of $x_{1(1)}$ and $x_{2(1)}$ then these second level pairs of cosums will also be constructible values. This process may be continued until we have expressions for $[1]$, $[\alpha]$, and so forth individually.

To find expressions for the sums of squares of pairs of cosums we create and use a table, one we shall refer to at each level of this process and also again in the proof of the numeric method. This table is intended to have eight columns and four rows. For reason of space the fifth to eighth columns appear further down the page.

Table 2.3.3. $x_{1(1)}^2+x_{2(1)}^2 = ([1]+[\alpha]+[\beta]+[\alpha\beta])^2+([\gamma]+[\alpha\gamma]+[\beta\gamma]+[\alpha\beta\gamma])^2$

$=$	$[2]$	$+$	$[2\alpha]$	$+$	$[2\beta]$	$+$	$[2\alpha\beta]$
$+$	$[1+\alpha]$	$+$	$[(1+\alpha)\alpha]$	$+$	$[(1+\alpha)\beta]$	$+$	$[(1+\alpha)\alpha\beta]$
$+$	$[1+\beta]$	$+$	$[(1+\beta)\alpha]$	$+$	$[(1+\beta)\beta]$	$+$	$[(1+\beta)\alpha\beta]$
$+$	$[1+\alpha\beta]$	$+$	$[(1+\alpha\beta)\alpha]$	$+$	$[(1+\alpha\beta)\beta]$	$+$	$[(1+\alpha\beta)\alpha\beta]$

$+$	$[2\gamma]$	$+$	$[2\alpha\gamma]$	$+$	$[2\beta\gamma]$	$+$	$[2\alpha\beta\gamma]$
$+$	$[(1+\alpha)\gamma]$	$+$	$[(1+\alpha)\alpha\gamma]$	$+$	$[(1+\alpha)\beta\gamma]$	$+$	$[(1+\alpha)\alpha\beta\gamma]$
$+$	$[(1+\beta)\gamma]$	$+$	$[(1+\beta)\alpha\gamma]$	$+$	$[(1+\beta)\beta\gamma]$	$+$	$[(1+\beta)\alpha\beta\gamma]$
$+$	$[(1+\alpha\beta)\gamma]$	$+$	$[(1+\alpha\beta)\alpha\gamma]$	$+$	$[(1+\alpha\beta)\beta\gamma]$	$+$	$[(1+\alpha\beta)\alpha\beta\gamma]$.

The left half of the table, first to fourth columns, consists of the summands of $x^2_{1(1)}$ and the right half, fifth to eights columns (lower on the page), of the summands of $x^2_{2(1)}$. The table is filled in by column. The first column contains, in order from row 1 to row 4, the first term of the first round bracket multiplied by itself, $[1][1] = [2]$, the first term by the second term, $[1][\alpha] = [1+\alpha]$, the first term by the third term, $[1][\beta] = [1+\beta]$, and the first term by the fourth term, $[1][\alpha\beta] = [1+\alpha\beta]$. The second column contains, in *some* order, the second term of the first round bracket by each of the terms in that bracket. And so on for each term in the first round bracket, a column for each; and then for each term in the second round bracket (multiplied by each term in that bracket), a column for each. The first column is column 1, the second column is the α column, the third column is the β column, the fourth column is the $\alpha\beta$ column, the fifth column is the γ column, and so forth. The rows are known by their first terms, the first row is the $1+1$ row, the second row is the $1+\alpha$ row, the third row is the $1+\beta$ row and the fourth row is the $1+\alpha\beta$ row.

Remark 2.3.4. To see that each product of two terms of a round bracket can be so expressed, consider the arbitrary ζ column. We seek the correct row for the product $[\zeta][u_1]$ where $\zeta,\ u_1 \in \mathcal{U}_{2n}$. We need to find u_2 such that $\zeta + u_1 = (1+u_2)\zeta = \zeta + u_2\zeta \Rightarrow u_1 = u_2\zeta \Leftrightarrow u_2 = u_1\zeta^{-1}$. That $\mathcal{U}_{2n}$ is a group ensures the existence and uniqueness of u_2 and we put the product in the $1+u_2$ row. u_2 is in the first half of the elements, in order $1,\ \alpha,\ \beta,\ \alpha\beta,\dots,\alpha\beta\gamma$ because u_1 and ζ belong to the same half of the elements.

Now consider each row over the whole table. The $1+\zeta$ row contains zeros corresponding to the whole group but with exponents multiplied by $1+\zeta$, an even number. By theorems 2.2.7 and 2.3.1 each row is equal to an integer, if $\gcd(1+\zeta,\ n) = 1$, or to so many copies of a cosum of Ψ_s, where $(1+\zeta)/n = r/s$ in lowest terms. (In the proof of the numeric method in section 3 we shall see that the full row totals are always equal to an integer.) For the moment we have to say that the full rows of the table are constructible if all the cosums of Ψ_s are constructible. If they are constructible then so is the table as a whole which represents $x^2_{1(1)} + x^2_{2(1)}$ and by remark 2.3.2 so are $x_{1(1)}$ and $x_{2(1)}$. $x_{1(1)},\ x_{2(1)} = [x_{1(0)} \pm \sqrt{[2(x^2_{1(1)} + x^2_{2(1)}) - x^2_{1(0)}}]]/2$.

Now to yet smaller cosums. $x^2_{1(2)} + x^2_{2(2)} = ([1]+[\alpha])^2 + ([\beta]+[\alpha\beta])^2$ which corresponds to the upper left quarter, four columns by two rows, of table 2.3.3, generated at level 1. And $(x_{1(2)} + x_{2(2)})^2 = x^2_{1(1)}$ corresponds to the left half, four columns by four rows, of the table. To express $x_{1(2)}$ or $x_{2(2)}$ we need the radicand $2(x^2_{1(2)} + x^2_{2(2)}) - (x_{1(2)} + x_{2(2)})^2$ which corresponds to the upper left quarter of the table minus the lower left quarter of the table. In similar manner $x_{3(2)}$ and $x_{4(2)}$ use the radicand made from the upper right quarter minus the lower right quarter. Each one of these shortened rows must equal $x_{1(1)},\ x_{2(1)}$, so many copies of a cosum of Ψ_s or the reflection of one of these, by theorem 2.2.7.

At level 3, the final level for the eight zero example, we use the quarters *of* the upper right (left) quarters of table 2.3.3 and these even shorter rows must be equal to a cosum of Ψ_n of the previous level, so many copies of a cosum of Ψs or to the reflection of one of these. Generally, subsequent levels continue in this way until $x_{j(k)}$, where $2^k = \phi(2n)$, are the subject.

Proposition 2.3.5. *A constructible expression for $e^{iu\pi/n}$, where $u \in \mathcal{U}_{2n}$, may be found by the algebraic method described herein.*

Proof. From the existence of the tabular process described it follows that if the cosums of Ψ_s are constructible then so are the cosums of Ψ_n. The cosums of $\Psi_1,\ \Psi_2$

and Ψ_p, where p is an odd prime restricted as usual, are certainly constructible without reference to the cosums of any other polynomial, Ψ_s, by theorem 2.2.4. Once the cosums of Ψ_2 have been constructed then the cosums of Ψ_4 can be constructed and so on to the cosums of Ψ_{2^k}, for any positive integer k. Likewise we can first construct the cosums of the Ψ_{p_i}, for the odd prime components, p_i, of n and for products involving any number of p_i and any power of 2 which forms a factor of n; and thence to the cosums and to $e^{iu\pi/n}$ of Ψ_n. □

Proposition 2.3.6. *A constructible expression for $e^{ik\pi/n}$, for any integer k and n restricted as usual, may be found by an analogous method to that for $e^{iu\pi/n}$.*

Proof. The problem of finding a constructible expression for $e^{iku\pi/n}$ is similar to finding one for $e^{iu\pi/n}$. The table is found in the same way.

Table 2.3.7. $x^2_{1(1)}+x^2_{2(1)} = ([k]+[k\alpha]+[k\beta]+[k\alpha\beta])^2+([k\gamma]+[k\alpha\gamma]+[k\beta\gamma]+[k\alpha\beta\gamma])^2$

$$
\begin{array}{lllllllll}
=[2k] & + & [2k\alpha] & + & [2k\beta] & + & \dots & + & [2k\alpha\beta\gamma] \\
+[k(1+\alpha)] & + & [k(1+\alpha)\alpha] & + & [k(1+\alpha)\beta] & + & \dots & + & [k(1+\alpha)\alpha\beta\gamma] \\
+[k(1+\beta)] & + & [k(1+\beta)\alpha] & + & [k(1+\beta)\beta] & + & \dots & + & [k(1+\beta)\alpha\beta\gamma] \\
+[k(1+\alpha\beta)] & + & [k(1+\alpha\beta)\alpha] & + & [k(1+\alpha\beta)\beta] & + & \dots & + & [k(1+\alpha\beta)\alpha\beta\gamma].
\end{array}
$$

Now $x_{1(0)}$ is found after consideration of $\gcd(k,\ n)$. It will be shown later, in the proof of the numeric method, that $x_{1(0)}$ is still equal to an integer but at this stage we allow that it may be equal to so many copies of some cosum of Ψ_s. The process of locating the relevant section of table 2.3.7 and making the radicand from a sum of shortened rows is done in an analogous way to the preceding description. When k is even and n is prime all reflections are avoided. $e^{iku\pi/n}$ can be styled simply $e^{ik\pi/n}$. □

2.4. **Examples of the Algebraic Method.**

Remark 2.4.1. A Note on Reflection. To reflect a cosum, in the imaginary axis of the complex plane we multiply the real parts by -1. For real cosums this is very simple. And it is always possible to have nothing but real cosums to reflect. This is achieved by setting $\alpha = 2n - 1 \equiv -1 \pmod{2n}$, something one must do for $\mathcal{U}_{2p}$, where p is prime, but which is optional for non-primes. Then $[\zeta] + [-\zeta] = 2\cos(\zeta\pi/n)$ and all subsequent cosums are also real. However, if this is not done then the expression for a cosum may contain a square root of a complex value and care needs to be taken in finding the value of the reflected cosum. The reflection of $\sqrt{}(a+ib)$ is equal to $\pm\sqrt{}(a - ib)$, plus or minus depending on the convention used in allocating the positive square root, for example it might be chosen 'first square root come to going anti-clockwise from the positive x-axis' or it might be chosen 'positive real part'. To avoid confusion, the expression for a square root of a complex value should have the quadrant of the complex plane in which it is found identified. No matter how complicated the constructible expression for a cosum (as produced by the algebraic method herein) the reflection can always be achieved and merely by changes of sign in the expression. (That the sum of shortened rows is constructible is guaranteed by the form of the expression produced by the numeric method (described in the next section), no matter what choice, in keeping with proposition 2.1.1, is made for $\alpha,\ \beta,\ \gamma$ and so forth.) The reader may at this stage make some sketches in the complex plane to see that the reflection in the imaginary axis can always be achieved by changes of sign alone.

Example 2.4.2. 5-gon Let $\alpha = 9,\ \beta = 3$. Only one distinct sequence of partitions exists for $\mathcal{U}_p$, where p is prime.

Level 0. $x_{1(0)} = 1$, because 5 is an odd prime.

Level 1. $x_{1(1)}^2 + x_{2(1)}^2 = ([1]+[9])^2 + ([3]+[7])^2$

$$\begin{array}{lllllllll} = & [2] & + & [2\cdot 9] & + & [2\cdot 3] & + & [2\cdot 7] \\ + & [1+9] & + & [(1+9)9] & + & [(1+9)3] & + & [(1+9)7]. \end{array}$$

$1st$ row $= -1$, by reflection of $x_{1(0)}$.
$2nd$ row $= 4$, by $1+9 \equiv 0 \pmod{10}$, $e^{i0} = 1$.
Row total $= 3$.
$x_{1(1)},\ x_{2(1)} = [1 \pm \sqrt{(2\cdot 3 - 1^2)}]/2$. Consultation of a diagram in the complex plane distinguishes these values: $x_{1(1)} = (1+\sqrt{5})/2$ and $x_{2(1)} = (1-\sqrt{5})/2$.
Level 2. $2(x_{1(2)}^2 + x_{2(2)}^2) - (x_{1(2)} + x_{2(2)})^2$

$$\begin{array}{lllll} = & [2] & + & [2\cdot 9] \\ - & [1+9] & - & [(1+9)9]. \end{array}$$

$1st$ row $= (-1+\sqrt{5})/2$, by reflection of $x_{2(1)}$, coset containing reflection of 2, $5-2=3 \pmod{10}$.
$2nd$ row $= -2$, by $1+9 \equiv 0 \pmod{10}$, $e^{i0} = 1$.
Row total $= (-5+\sqrt{5})/2$.
$x_{1(2)},\ x_{2(2)} = [(1+\sqrt{5})/2 \pm \sqrt{[(-5+\sqrt{5})/2]}]/2 = [1+\sqrt{5} \pm i\sqrt{[10-2\sqrt{5}]}]/4$. Consultation of a diagram in the complex plane shows that $x_{1(2)} = [1+\sqrt{5}+i\sqrt{[10-2\sqrt{5}]}]/4 = e^{i\pi/5} = cos(\pi/5) + isin(\pi/5)$.
$x_{3(2)}$ and $x_{4(2)}$ are found similarly.
$2(x_{3(2)}^2 + x_{4(2)}^2) - (x_{3(2)} + x_{4(2)})^2$

$$\begin{array}{lllll} = & [2\cdot 3] & + & [2\cdot 7] \\ - & [(1+9)3] & - & [(1+9)7]. \end{array}$$

$1st$ row $= (-1-\sqrt{5})/2$, by reflection of $x_{1(1)}$, coset containing reflection of 6, $5-6=9 \pmod{10}$.
$2nd$ row $= -2$, by $1+9 \equiv 0 \pmod{10}$, $e^{i0} = 1$.
Row total $= (-5-\sqrt{5})/2$.
$x_{3(2)},\ x_{4(2)} = [1-\sqrt{5} \pm i\sqrt{[10+2\sqrt{5}]}]/2$. Consultation of a diagram in the complex plane shows that $x_{3(2)} = [1-\sqrt{5}+i\sqrt{[10+2\sqrt{5}]}]/2 = e^{i3\pi/5} = cos(3\pi/5) + isin(3\pi/5)$.

Example 2.4.3. 8-gon, version 1. We assume to have already produced constructible expressions for $\Psi_1,\ \Psi_2$ and Ψ_4 by each distinct method of partition of the relevant group. Let $\alpha = 15,\ \beta = 9,\ \gamma = 3$, providing $\alpha\beta = 7$.
Level 0. $x_{1(0)} = 0$, because 8 is even.
Level 1. $x_{1(1)}^2 + x_{2(1)}^2 = ([1]+[15]+[9]+[7])^2 + ([3]+[13]+[11]+[5])^2$

$$\begin{aligned} &= [2]+[2\cdot 15]+[2\cdot 9]+[2\cdot 7]+[2\cdot 3]+[2\cdot 13]+[2\cdot 11]+[2\cdot 5] \\ &+ [1+15]+\dots \\ &+ [1+9]+\dots \\ &+ [1+7]+\dots. \end{aligned}$$

$1st$ row $= 0$, by $2/8 = 1/4$, then $7/4,\ 1/4,\ 7/4,\ 3/4,\ 5/4,\ 3/4,\ 5/4$, providing 2 copies of Ψ_4 zeros.
$2nd$ row $= 8$, by $1+15 \equiv 0 \pmod{16}$, $e^{i0} = 1$.
$3rd$ row $= 0$, by $10/8 = 5/4$, exponents as row 1 multiplied by 5.
$4th$ row $= -8$, by $8/8 = 1,\ e^{i\pi} = -1$.

Row total $= 0$.
$x_{1(1)},\ x_{2(1)} = [0 \pm \surd(2(0) - 0^2)]/2 = 0$.
Level 2. $2(x_{1(2)}^2 + x_{2(2)}^2) - (x_{1(2)} + x_{2(2)})^2$

$$
\begin{aligned}
=&[2] + [2\cdot 15] + [2\cdot 9] + [2\cdot 7]\\
+&[1+15] + \ldots\\
-&[1+9] - \ldots\\
-&[1+7] - \ldots.
\end{aligned}
$$

$1st$ row $= 2\surd 2$, by 2 copies of elements of $\mathcal{U}_8$ coset $\{1,\ 7\}$ in numerators of exponents making Ψ_4 cosums.
$2nd$ row $= 4$, by $1 + 15 \equiv 0 \pmod{16}$, $e^{i0} = 1$.
$3rd$ row $= 2\surd 2$, by 2 copies of elements of $\mathcal{U}_8$ coset $\{3,\ 5\}$ in numerators
$4th$ row $= 4$, by $8/8 = 1,\ e^{i\pi} = -1$.
Row total $= 4(2 + \surd 2)$.
$x_{1(2)},\ x_{2(2)} = [0 \pm 2\surd[(2 + \surd 2)]]/2 = \pm\surd[2 + \surd 2]$. Consultation of a diagram in the complex plane shows that $x_{1(2)} = \surd[2 + \surd 2] = 2cos(\pi/8)$.
Level 3. $2(x_{1(2)}^2 + x_{2(2)}^2) - (x_{1(2)} + x_{2(2)})^2$

$$
\begin{aligned}
=&[2] + [2\cdot 15]\\
-&[1+15] - \ldots
\end{aligned}
$$

$1st$ row $= \surd 2$, by elements of $\mathcal{U}_8$ coset $\{1,\ 7\}$ in numerators of exponents making Ψ_4 cosum.
$2nd$ row $= -2$, by $1 + 15 \equiv 0 \pmod{16}$, $e^{i0} = 1$.
Row total $= -2 + \surd 2$.
$x_{1(3)},\ x_{2(3)} = [\surd(2 + \surd 2) \pm i\surd(2 - \surd 2)]/2$. Consultation of a diagram in the complex plane shows that $x_{1(3)} = [\surd(2+\surd 2)+i\surd(2-\surd 2)]/2 = cos(\pi/8)+isin(\pi/8)$.

Example 2.4.4. 8-gon, version 2. We assume to have already produced constructible expressions for $\Psi_1,\ \Psi_2$ and Ψ_4 by each distinct method of partition of the relevant group. Let $\alpha = 9,\ \beta = 3,\ \gamma = 7$, providing $\alpha\beta = 11$.
Level 0. $x_{1(0)} = 0$, because 8 is even.
Level 1. $x_{1(1)}^2 + x_{2(1)}^2 = ([1] + [9] + [3] + [11])^2 + ([7] + [15] + [5] + [13])^2$

$$
\begin{aligned}
=&[2] + [2\cdot 9] + [2\cdot 3] + [2\cdot 11] + [2\cdot 7] + [2\cdot 15] + [2\cdot 5] + [2\cdot 13]\\
+&[1+9] + \ldots\\
+&[1+3] + \ldots\\
+&[1+11].
\end{aligned}
$$

$1st$ row $= 0$, by $2/8 = 1/4$, then $7/4,\ 1/4,\ 7/4,\ 3/4,\ 5/4,\ 3/4,\ 5/4$, providing 2 copies of Ψ_4 zeros.
$2nd$ row $= 0$, by $10/8 = 5/4$, exponents as row 1 multiplied by 5.
$3rd$ row $= 0$, by $4/8 = 1/2$, then $1/2,\ 3/2,\ 3/2, \ldots$, 4 copies of Ψ_2 zeros.
$4th$ row $= 0$, by $12/8 = 3/2$, row 3 exponents multiplied by 3.
Row total $= 0$.
$x_{1(1)},\ x_{2(1)} = [0 \pm \surd(2(0) - 0^2)]/2 = 0$.
Level 2. $2(x_{1(2)}^2 + x_{2(2)}^2) - (x_{1(2)} + x_{2(2)})^2$

$$\begin{aligned}
=&[2]+[2\cdot 9]+[2\cdot 3]+[2\cdot 11]\\
&+[1+9]+\dots\\
&-[1+3]-\dots\\
&-[1+11]-\dots.
\end{aligned}$$

$1st$ row $=i2\surd 2$, by $1/4,\ 1/4,\ 3/4,\ 3/4$ in exponents making 2 copies of a Ψ_4 cosum.

$2nd$ row $=-i2\surd 2$, by $5/4,\ 5/4,\ 7/4,\ 7/4$ in exponents making 2 copies of a Ψ_4 cosum.

$3rd$ row $=0$, by $1/2,\ 1/2,\ 3/2,\ 3/2$ in exponents making 2 copies of Ψ_2 zeros.

$4th$ row $=0$, by $3/2,\ 3/2,\ 1/2,\ 1/2$ in exponents making 2 copies of Ψ_2 zeros.

Row total $=0$.

$x_{1(2)},\ x_{2(2)}=[0\pm\surd(2(0)-0^2)]/2=0$.

Level 3. $2(x_{1(2)}^2+x_{2(2)}^2)-(x_{1(2)}+x_{2(2)})^2$

$$\begin{aligned}
=&[2]+[2\cdot 9]\\
&-[1+9]-\dots
\end{aligned}$$

$1st$ row $=\surd 2+i\surd 2$, by $1/4,\ 1/4$ in exponents making a Ψ_4 cosum.

$2nd$ row $=\surd 2+i\surd 2$, by $5/4,\ 5/4$ in exponents making a Ψ_4 cosum.

Row total $=2\surd 2+i2\surd 2$.

$x_{1(3)},\ x_{2(3)}=[0\pm\surd(2\surd 2+i2\surd 2)]/2$. Consultation of a diagram in the complex plane shows $x_{1(3)}$ to be the first quadrant square root and $x_{2(3)}$ to be the third quadrant square root. This result is equivalent to that found by version 1. $[\surd(2+\surd 2)+i\surd(2-\surd 2)]^2=2+\surd 2-2+\surd 2+2i\surd[(2+\surd 2)(2-\surd 2)]=2\surd 2+i2\surd 2$. For the zeros of Ψ_8 yet other choices of cosets are possible but they give the same results.

Example 2.4.5. 10-gon, version 1. We assume to have already produced constructible expressions for $\Psi_1,\ \Psi_2$ and Ψ_5 by each distinct method of partition of the relevant group. Let $\alpha=9,\ \beta=3,\ \gamma=11$, providing $\alpha\beta=7$.

Level 0. $x_{1(0)}=0$, because 10 is even.

Level 1. $x_{1(1)}^2+x_{2(1)}^2=([1]+[9]+[3]+[7])^2+([11]+[19]+[13]+[17])^2$

$$\begin{aligned}
=&[2]+[2\cdot 9]+[2\cdot 3]+[2\cdot 7]+[2\cdot 11]+[2\cdot 19]+[2\cdot 13]+[2\cdot 17]\\
&+[1+9]+\dots\\
&+[1+3]+\dots\\
&+[1+7]+\dots.
\end{aligned}$$

$1st$ row $=2$, by $2/10=1/5$, then $9/5,\ 3/5,\ 7/5,\ 1/5,\ 9/5,\ 3/5,\ 7/5$, providing 2 copies of Ψ_5 zeros.

$2nd$ row $=-8$, by $10/10=1,\ e^{i\pi}=-1$.

$3rd$ row $=-2$, by $4/10=2/5$, 2 copies of reflection of Ψ_5 zeros.

$4th$ row $=-2$, by $8/10=4/5$, 2 copies of reflection of Ψ_5 zeros.

Row total $=-10$.

$x_{1(1)},\ x_{2(1)}=[0\pm\surd(-20-0^2)]/2=\pm i\surd 5$.

Consultation of a diagram in the complex plane distinguishes these values: $x_{1(1)}=i\surd 5$ and $x_{2(1)}=-i\surd 5$.

Level 2. $2(x_{1(2)}^2+x_{2(2)}^2)-(x_{1(2)}+x_{2(2)})^2$

$$\begin{aligned}
=&[2]+[2\cdot 9]+[2\cdot 3]+[2\cdot 7]\\
+&[1+9]+\dots\\
-&[1+3]-\dots\\
-&[1+7]-\dots.
\end{aligned}$$

$1st$ row $=1$, by $1/5,\ 3/5,\ 7/5,\ 9/5$ in exponents making Ψ_5 zeros.

$2nd$ row $=-4$, by $10/10=1,\ e^{i\pi}=-1$.

$3rd$ row $=1$, by $4/10=2/5$ then $6/5,\ 4/5,\ 8/5$ in exponents making reflection of Ψ_5 zeros.

$4th$ row $=1$, by $8/10=4/5$ then $2/5,\ 8/5,\ 6/5$ in exponents making reflection of Ψ_5 zeros.

Row total $=-1$.

$x_{1(2)},\ x_{2(2)}=[i\sqrt{}5\pm i]/2$.

Consultation of a diagram in the complex plane shows that $x_{1(2)}=i(-1+\sqrt{}5)/2$.

Level 3. $2(x^2_{1(2)}+x^2_{2(2)})-(x_{1(2)}+x_{2(2)})^2$

$$\begin{aligned}
=&[2]+[2\cdot 9]\\
-&[1+9]-\dots
\end{aligned}$$

$1st$ row $=(1+\sqrt{}5)/2$, by $1/5,\ 9/5$ in exponents making a Ψ_5 cosum.

$2nd$ row $=2$, by $10/10=1,\ e^{i\pi}=-1$.

Row total $=(5+\sqrt{}5)/2$.

$x_{1(3)},\ x_{2(3)}=[i(-1+\sqrt{}5)/2\pm\sqrt{}[(5+\sqrt{}5)/2]]/2=[i(-1+\sqrt{}5)\pm\sqrt{}(10+2\sqrt{}5)]/4$. Consultation of a diagram in the complex plane shows $x_{1(3)}=[\sqrt{}(10+2\sqrt{}5)+i(-1+\sqrt{}5)]/4=cos(\pi/10)+isin(\pi/10)$.

Example 2.4.6. 10-gon, version 2. We assume to have already produced constructible expressions for $\Psi_1,\ \Psi_2$ and Ψ_5 by each distinct method of partition of the relevant group. Let $\alpha=19,\ \beta=9,\ \gamma=3$, providing $\alpha\beta=11$.

Level 0. $x_{1(0)}=0$, because 10 is even.

Level 1. $x^2_{1(1)}+x^2_{2(1)}=([1]+[19]+[9]+[11])^2+([3]+[17]+[7]+[13])^2$

$$\begin{aligned}
=&[2]+[2\cdot 19]+[2\cdot 9]+[2\cdot 11]+[2\cdot 3]+[2\cdot 17]+[2\cdot 7]+[2\cdot 13]\\
+&[1+19]+\dots\\
+&[1+9]+\dots\\
+&[1+11]+\dots.
\end{aligned}$$

$1st$ row $=2$, by $2/10=1/5$, then $9/5,\ 9/5,\ 1/5,\ 3/5,\ 7/5,\ 7/5,\ 3/5$, providing 2 copies of Ψ_5 zeros.

$2nd$ row $=8$, by $1+19\equiv 0 \pmod{20}$, $e^{i0}=1$.

$3rd$ row $=-8$, by $10/10=1,\ e^{i\pi}=-1$.

$4th$ row $=-2$, by $12/10=6/5$, then $4/5,\ 4/5,\ 6/5,\dots$, 2 copies of reflection of Ψ_5 zeros.

Row total $=0$.

$x_{1(1)},\ x_{2(1)}=[0\pm\sqrt{}(2(0)-0^2)]/2=0$.

Level 2. $2(x^2_{1(2)}+x^2_{2(2)})-(x_{1(2)}+x_{2(2)})^2$

$$\begin{aligned}&=[2]+[2\cdot 19]+[2\cdot 9]+[2\cdot 11]\\&+[1+19]+\dots\\&-[1+9]-\dots\\&-[1+11]-\dots.\end{aligned}$$

$1st$ row $= 1+\sqrt{5}$, by 2 copies of a Ψ_5 cosum.
$2nd$ row $= 4$, by $1+19 \equiv 0 \pmod{20}$, $e^{i0} = 1$.
$3rd$ row $= 4$, by $10/10 = 1$, $e^{i\pi} = -1$.
$4th$ row $= 1+\sqrt{5}$, by 2 copies of a reflection of a Ψ_5 cosum.
Row total $= 10 + 2\sqrt{5}$.
$x_{1(2)},\ x_{2(2)} = [0 \pm \sqrt{(10+2\sqrt{5})}]/2$.
Consultation of a diagram in the complex plane shows that $x_{1(2)} = \sqrt{(10 + 2\sqrt{5})}/2$.
Level 3. $2(x^2_{1(2)} + x^2_{2(2)}) - (x_{1(2)} + x_{2(2)})^2$

$$\begin{aligned}&=[2]+[2\cdot 19]\\&-[1+19]-\dots\end{aligned}$$

$1st$ row $= (1+\sqrt{5})/2$, by $1/5,\ 9/5$ in exponents making a Ψ_5 cosum.
$2nd$ row $= -2$ by $1+19 \equiv 0 \pmod{20}$, $e^{i0} = 1$.
Row total $= (-3+\sqrt{5})/2$.
$x_{1(3)},\ x_{2(3)} = [\sqrt{(10+2\sqrt{5})}/2 \pm \sqrt{[(-3+\sqrt{5})/2]}]/2 = [\sqrt{(10+2\sqrt{5})} \pm i\sqrt{(6 - 2\sqrt{5})}]/4$. Consultation of a diagram in the complex plane shows $x_{1(3)} = [\sqrt{(10 + 2\sqrt{5})} + i(-1+\sqrt{5})]/4 = cos(\pi/10) + isin(\pi/10)$.

Example 2.4.7. 15-gon, version 1. We assume to have already produced constructible expressions for Ψ_1, Ψ_3 and Ψ_5 by each distinct method of partition of the relevant group. Let $\alpha = 19$, $\beta = 7$, $\gamma = 29$, providing $\alpha\beta = 13$.
Level 0. $x_{1(0)} = -1$, because 15 is is a product of two odd primes.
Level 1. $x^2_{1(1)} + x^2_{2(1)} = ([1] + [19] + [7] + [13])^2 + ([29] + [11] + [23] + [17])^2$

$$\begin{aligned}&=[2]+[2\cdot 19]+[2\cdot 7]+[2\cdot 13]+[2\cdot 29]+[2\cdot 11]+[2\cdot 23]+[2\cdot 17]\\&+[1+19]+\dots\\&+[1+7]+\dots\\&+[1+13]+\dots.\end{aligned}$$

$1st$ row $= 1$, by reflection of zeros corresponding to whole group $\mathcal{U}_{30}$.
$2nd$ row $= -4$, by $20/15 = 4/3$, then $4/3,\ 4/3,\ 4/3,\ 2/3, \dots$, 4 copies of the reflections of Ψ_3 zeros.
$3rd$ row $= 1$, by $1+7 = 8$. 8 reflected is 7. $7 \in \mathcal{U}_{30}$. Reflection of whole group.
$4th$ row $= 1$, by $1+13 = 14$. 14 reflected is 1. $1 \in \mathcal{U}_{30}$. Reflection of whole group.
Row total $= -1$.
$x_{1(1)},\ x_{2(1)} = [-1 \pm \sqrt{(2(-1) - (-1)^2)}]/2 = (-1 \pm i\sqrt{3})/2$.
Consultation of a diagram in the complex plane distinguishes these values: $x_{1(1)} = (-1+i\sqrt{3})/2$ and $x_{2(1)} = (-1-i\sqrt{3})/2$.
Level 2. $2(x^2_{1(2)} + x^2_{2(2)}) - (x_{1(2)} + x_{2(2)})^2$

$$
\begin{aligned}
=&[2] + [2\cdot 19] + [2\cdot 7] + [2\cdot 13]\\
+&[1+19] + \dots\\
-&[1+7] - \dots\\
-&[1+13] - \dots .
\end{aligned}
$$

$1st$ row $= (1+i\sqrt{3})/2$, by reflection of cosum corresponding to level 1 coset containing reflection of 2. $15-2=13$. So we require reflection of $x_{1(1)}$. Remember to multiply only the real part by -1.

$2nd$ row $= -2-i2\sqrt{3}$, by 4 copies of reflection of a cosum of Ψ_3 which is the reflection of 4 in $\mathcal{U}_6$ (or simply of $e^{i4\pi/3}$.

$3rd$ row $= (-1-i\sqrt{3})/2$, by reflection of cosum corresponding to level 1 coset containing reflection of 8. $15-8=7$. So we require reflection of $x_{1(1)}$.

$4th$ row $= (-1-i\sqrt{3})/2$, by reflection of cosum corresponding to level 1 coset containing reflection of 14. $15-14=1$. So we require reflection of $x_{1(1)}$.

Row total $= (-5-i5\sqrt{3})/2$.

$x_{1(2)},\ x_{2(2)} = [-1+i\sqrt{3} \pm \sqrt{(}-10-i10\sqrt{3})]/4$.

Consultation of a diagram in the complex plane shows that $x_{1(2)}$ uses $4th$ quadrant square root and $x_{2(2)}$ uses $2nd$ quadrant square root. $x_{1(2)} = [-1+i\sqrt{3} + q_4\sqrt{(}-10-i10\sqrt{3})]/4$, where q_4 indicates the $4th$ quadrant. (Although $\pm\sqrt{(}-10-i10\sqrt{3}) = \pm(\sqrt{5}-i\sqrt{15})$ We wish to demonstrate a reflection of a square root of a complex value in level 3, so it is left unsimplified.)

Level 3. $2(x_{1(2)}^2 + x_{2(2)}^2) - (x_{1(2)} + x_{2(2)})^2$

$$
\begin{aligned}
=&[2] + [2\cdot 19]\\
-&[1+19] - \dots
\end{aligned}
$$

$1st$ row $= [1+i\sqrt{3} + q_1\sqrt{(}-10+i10\sqrt{3})]/4$, by reflection of a cosum of level 2 corresponding to the coset containing the reflection of 2, that is of $x_{2(2)}$.

$2nd$ row $= 1+i\sqrt{3}$ by $4/3,\ 4/3$ in exponents.

Row total $= [5+i5\sqrt{3} + q_1\sqrt{(}-10+i10\sqrt{3})]/4$.

$x_{1(3)},\ x_{2(3)} = [-1+i\sqrt{3} + q_4\sqrt{(}-10-i10\sqrt{3}) \pm 2\sqrt{[}5+i5\sqrt{3}+q_1\sqrt{(}-10+i10\sqrt{3})]]/8$. Consultation of a diagram in the complex plane shows $x_{1(3)}$ to have its square root in the first quadrant and $x_{2(3)}$ to have its in the third quadrant. $x_{1(3)} = [-1+i\sqrt{3}+q_4\sqrt{(}-10-i10\sqrt{3})+q_1 2\sqrt{[}5+i5\sqrt{3}+q_1\sqrt{(}-10+i10\sqrt{3})]]/8 = e^{i\pi/15}$.

Example 2.4.8. 15-gon, version 2. We assume to have already produced constructible expressions for $\Psi_1,\ \Psi_3$ and Ψ_5 by each distinct method of partition of the relevant group. Let $\alpha = 29,\ \beta = 19,\ \gamma = 7$, providing $\alpha\beta = 11$.

Level 0. $x_{1(0)} = -1$, because 15 is is a product of two odd primes.

Level 1. $x_{1(1)}^2 + x_{2(1)}^2 = ([1]+[29]+[19]+[11])^2 + ([7]+[23]+[13]+[17])^2$

$$
\begin{aligned}
=&[2] + [2\cdot 29] + [2\cdot 19] + [2\cdot 11] + [2\cdot 7] + [2\cdot 23] + [2\cdot 13] + [2\cdot 17]\\
+&[1+29] + \dots\\
+&[1+19] + \dots\\
+&[1+11] + \dots .
\end{aligned}
$$

$1st$ row $= 1$, by reflection of zeros corresponding to whole group $\mathcal{U}_{30}$.

$2nd$ row $= 8$, by $1+29 \equiv 0 \pmod{30}$, $e^{i0} = 1$.

$3rd$ row $= -4$, by $20/15 = 4/3$, then $2/3,\ 4/3,\ 2/3, \ldots$, 4 copies of reflection of Ψ_3 zeros.

$4th$ row $= -2$, by $12/15 = 4/5$, then $6/5,\ 6/5,\ 4/5,\ 8/5,\ 2/5,\ 2/5,\ 8/5$, 2 copies of reflection of Ψ_5 zeros.

Row total $= 3$.

$x_{1(1)},\ x_{2(1)} = [-1 \pm \sqrt{(2 \cdot 3 - (-1)^2)}]/2 = (-1 \pm \sqrt{5})/2$.

Consultation of a diagram in the complex plane distinguishes these values: $x_{1(1)} = (-1+\sqrt{5})/2$ and $x_{2(1)} = (-1-\sqrt{5})/2$.

Level 2. $2(x_{1(2)}^2 + x_{2(2)}^2) - (x_{1(2)} + x_{2(2)})^2$

$$\begin{aligned}&=[2] + [2 \cdot 29] + [2 \cdot 19] + [2 \cdot 11]\\ &+[1+29] + \ldots\\ &-[1+19] - \ldots\\ &-[1+11] - \ldots.\end{aligned}$$

$1st$ row $= (1+\sqrt{5})/2$, by reflection of cosum corresponding to level 1 coset containing reflection of 2. $15 - 2 = 13$. So we require reflection of $x_{2(1)}$.

$2nd$ row $= 4$, by $1 + 29 \equiv 0 \pmod{30}$, $e^{i0} = 1$.

$3rd$ row $= 2$, by $4/3,\ 2/3,\ 4/3,\ 2/3$ in exponents.

$4th$ row $= 1+\sqrt{5}$, by $4/5,\ 6/5,\ 6/5,\ 4/5$ in exponents.

Row total $= (15 + 3\sqrt{5})/2$.

$x_{1(2)},\ x_{2(2)} = [-1 + \sqrt{5} \pm \sqrt{(30 + 6\sqrt{5})}]/4$.

Consultation of a diagram in the complex plane shows that $x_{1(2)} = [-1+\sqrt{5} + \sqrt{(30+6\sqrt{5})}]/4$.

This time we will need $x_{3(2)}$ and $x_{4(2)}$ also. $2(x_{3(2)}^2 + x_{4(2)}^2) - (x_{3(2)} + x_{4(2)})^2$

$$\begin{aligned}&=[2 \cdot 7] + [2 \cdot 23] + [2 \cdot 13] + [2 \cdot 17]\\ &+[(1+29)7] + \ldots\\ &-[(1+19)7] - \ldots\\ &-[(1+11)7] - \ldots.\end{aligned}$$

$1st$ row $= (1-\sqrt{5})/2$, by reflection of cosum corresponding to level 1 coset containing reflection of 14. $15 - 14 = 1$. So we require reflection of $x_{1(1)}$.

$2nd$ row $= 4$, by $1 + 29 \equiv 0 \pmod{30}$, $e^{i0} = 1$.

$3rd$ row $= 2$, by $4/3,\ 2/3,\ 4/3,\ 2/3$ in exponents.

$4th$ row $= 1-\sqrt{5}$, by $8/5,\ 2/5,\ 2/5,\ 8/5$ in exponents.

Row total $= (15 - 3\sqrt{5})/2$.

$x_{3(2)},\ x_{4(2)} = [-1 - \sqrt{5} \pm \sqrt{(30 - 6\sqrt{5})}]/4$.

Consultation of a diagram in the complex plane shows that $x_{3(2)} = [-1-\sqrt{5} + \sqrt{(30-6\sqrt{5})}]/4$.

Level 3. $2(x_{1(2)}^2 + x_{2(2)}^2) - (x_{1(2)} + x_{2(2)})^2$

$$\begin{aligned}&=[2] + [2 \cdot 29]\\ &-[1+29] - \ldots\end{aligned}$$

$1st$ row $= [-1 + \sqrt{5} + \sqrt{(30 - 6\sqrt{5})}]/4$, by reflection of a cosum of level 2 corresponding to the coset containing the reflection of 2, that is of $x_{4(2)}$.

$2nd$ row $= -2$, by $1 + 29 \equiv 0 \pmod{30}$, $e^{i0} = 1$.

Row total $= [-7 + \sqrt{5} + \sqrt{(30 - 6\sqrt{5})}]/4$.

$x_{1(3)},\ x_{2(3)} = [-1 - \sqrt{5} + \sqrt{(30 - 6\sqrt{5})} \pm 2\sqrt{[-7 + \sqrt{5} + \sqrt{(30 - 6\sqrt{5})]}]/8$. Consultation of a diagram in the complex plane shows $x_{1(3)} = [-1 - \sqrt{5} + \sqrt{(30 - 6\sqrt{5})} + 2\sqrt{[-7 + \sqrt{5} + \sqrt{(30 - 6\sqrt{5})]}]/8 = cos(\pi/15) + isin(\pi/15)$.

3. A Numeric Method for Constructing $e^{ik\pi/n}$

The proof of the numeric method is independent of the algebraic method of section 2 but much of that work and its notation is common to both methods. The following is assumed: section 1, section 2 subsection 2.1, subsection 2.2 (theorem 2.2.5 is optional) and subsection 2.3. Proficiency in the use of the algebraic method is not required for an understanding of the numeric method and its proof, but a good grasp of table building would be useful.

In this section first the numeric method is described. Discussion is continued of the effects of multipliers on the exponents of the cosums of Ψ_n, this time focussing on the sum of all the zeros of Ψ_n. It is shown that such multiples always produce one or more copies of complete sums of zeros though possibly belonging to Ψ_s where s divides n. Thus the result on the sum of all the zeros of application of the multiplier is again an integer.

The sequence of output numbers of the numeric method is studied. Output sequence members with higher subscripts may be thought of as evolving from those with lower subscripts by the action of two processes. Each of these processes is shown to produce only sums of complete rows, like those of table 2.3.3, provided that it acts on such a collection. Inductively we conclude that all output numbers are composed of sums of such complete rows and are therefore equal to integers. Thus the compact form assumed in the description of the numeric method holds for all constructible expressions of cosums of the polynomials, Ψ_n, belonging to the constructible n-gons.

3.1. Introduction.

In order to create the constructible expression for $[1] = e^{i\pi/n}$ or for $2\cos(\pi/n)$, in the algebraic method of section 2, at each level we generated and appended a radical containing a sum of expressions (found from the rows of the table) each of which may have had the same form as the entire expression of the previous level, potentially producing a very complicated expression. It is easily seen that for prime cases we always do have the maximum of complication. In this section we assume, and later prove, that these expressions are always simplifiable and we call this simplified version the *compact* form.

When the total number of cosums under study is equal to 2 the compact form of their expression is $a \pm \sqrt{b}$. When the total number of cosums is equal to 4 (the number of summands per cosum having halved) the compact form is $a \pm \sqrt{b} \pm \sqrt{(c \pm \sqrt{d})}$. When the total number of cosums is equal to 8 the compact form is $a \pm \sqrt{b} \pm \sqrt{(c \pm \sqrt{d})} \pm \sqrt{(e \pm \sqrt{f} \pm \sqrt{(g \pm \sqrt{h})})}$, and so forth, where $a,\ b,\ c, \ldots,$ are rational values. At each doubling of cosum number a radical is added whose radicand has the form of the entire previous expression.

The expressions for $x_{1(3)},\ x_{2(3)}, \ldots, x_{8(3)}$ of Ψ_{17} may be expressed in the following manner, which may help to visualize the numeric method that will be described. Letting $\alpha = 33,\ \beta = 13,\ \gamma = 15$ and $\delta = 3$ supplies the entries in table 3.1.1.

Table 3.1.1.

$$
\begin{aligned}
x_{1(3)} &= [1-\surd 17+\surd(34-2\surd 17)+2\surd(17+3\surd 17+\surd(170+38\surd 17))]/8,\\
x_{5(3)} &= [1+\surd 17+\surd(34+2\surd 17)+2\surd(17-3\surd 17-\surd(170-38\surd 17))]/8,\\
x_{3(3)} &= [1-\surd 17-\surd(34-2\surd 17)-2\surd(17+3\surd 17-\surd(170+38\surd 17))]/8,\\
x_{7(3)} &= [1+\surd 17-\surd(34+2\surd 17)-2\surd(17-3\surd 17+\surd(170-38\surd 17))]/8,\\
x_{2(3)} &= [1-\surd 17+\surd(34-2\surd 17)-2\surd(17+3\surd 17+\surd(170+38\surd 17))]/8,\\
x_{6(3)} &= [1+\surd 17+\surd(34+2\surd 17)-2\surd(17-3\surd 17-\surd(170-38\surd 17))]/8,\\
x_{4(3)} &= [1-\surd 17-\surd(34-2\surd 17)+2\surd(17+3\surd 17-\surd(170+38\surd 17))]/8,\\
x_{8(3)} &= [1+\surd 17-\surd(34+2\surd 17)+2\surd(17-3\surd 17+\surd(170-38\surd 17))]/8.
\end{aligned}
$$

These expressions are not in exactly the form output by the numeric method but they have the same structure with respect to radicals, which is what matters, and so qualify as compact. Each expression has the same rational constants, varying only in signs of radicals, which is what the numeric method assumes, later proves, of its input values. (Note that the list is not long enough to include every possible variation in signs.)

In the algebraic method we worked from level 0 to level k, where $2^k = \phi(2n)$, but in the numeric method we begin with the level k values, with (approximations of) the exponential values, $[\zeta]$. At each subsequent round we produce (approximations of) the cosums of the preceding level and as many *other* values. These other values are the radicands of the final radical terms of the compact form of expression, as will be described next.

3.2. **Description of the Numeric Method.** We begin by ordering the exponential values, $[\zeta]$, on a binary system with respect to their Greek identifiers. Staying with the Ψ_{17} example we have

Table 3.2.1.

list pos.	α	β	γ	δ	
1	0	0	0	0	corresponding to [1],
2	0	0	0	1	corresponding to $[\delta] = [3]$,
3	0	0	1	0	corresponding to $[\gamma] = [15]$,
4	0	0	1	1	corresponding to $[\gamma\delta] = [11]$,
5	0	1	0	0	corresponding to $[\beta] = [13]$,
6	0	1	0	1	corresponding to $[\beta\delta] = [5]$,
7	0	1	1	0	corresponding to $[\beta\gamma] = [25]$,
8	0	1	1	1	corresponding to $[\beta\gamma\delta] = [7]$,
9	1	0	0	0	corresponding to $[\alpha] = [33]$,
10	1	0	0	1	corresponding to $[\alpha\delta] = [31]$,
11	1	0	1	0	corresponding to $[\alpha\gamma] = [19]$,
12	1	0	1	1	corresponding to $[\alpha\gamma\delta] = [23]$,
13	1	1	0	0	corresponding to $[\alpha\beta] = [21]$,
14	1	1	0	1	corresponding to $[\alpha\beta\delta] = [29]$,
15	1	1	1	0	corresponding to $[\alpha\beta\gamma] = [9]$,
16	1	1	1	1	corresponding to $[\alpha\beta\gamma\delta] = [27]$.

To make the list of approximations of the level 3 cosums of Ψ_{17} in the introduction to this section, and in the correct order, we add together $[\zeta]$ and $[\alpha\zeta]$ to make $2\cos(\zeta\pi/17)$, the summand pairs being found eight rows apart in the list of sixteen exponential values in table 3.2.1, and put the sum back in the upper (nearer the top) list position of the pair. The example cosums are then in the first eight list positions. In adding together these pairs of values we have lost the final radical, the $\pm \imath\sin(\zeta\pi/17)$. We can isolate it by subtracting the lower member from the upper member of the pair, instead of adding them. We then record the sign, plus or minus (or the quadrant if we happen to be working with square roots of complex values), of the square root, square it and put it back in the lower list position of the pair. The second half of the list, positions 9 to 16, then contain values with the form $([\zeta] - [\alpha\zeta])^2 = -4\sin^2\zeta$. We have now completed the first round of processing. This process can be continued, at each round choosing pairs (from the list of the previous round) at half the separation distance used in the previous round, putting the sum back in the upper list position and putting the difference squared back in the lower list position.

The state of the complete list after each of four rounds of forming the sums and differences squared follows in table 3.2.2.

Table 3.2.2.

list pos.	input ζ	$1st$	$2nd$	$3rd$	$4th =$ output
1	1	S_1	S_1	S_1	S_1
2	δ	S_2	S_2	S_2	$\mathbf{D_1}$
3	γ	S_3	S_3	$\mathbf{D_1}$	S_2
4	$\gamma\delta$	S_4	S_4	D_2	$\mathbf{D_2}$
5	β	S_5	$\mathbf{D_1}$	S_3	S_3
6	$\beta\delta$	S_6	D_2	S_4	$\mathbf{D_3}$
7	$\beta\gamma$	S_7	D_3	$\mathbf{D_3}$	S_4
8	$\beta\gamma\delta$	S_8	D_4	D_4	$\mathbf{D_4}$
9	α	$\mathbf{D_1}$	S_5	S_5	S_5
10	$\alpha\delta$	D_2	S_6	S_6	$\mathbf{D_5}$
11	$\alpha\gamma$	D_3	S_7	$\mathbf{D_5}$	S_6
12	$\alpha\gamma\delta$	D_4	S_8	D_6	$\mathbf{D_6}$
13	$\alpha\beta$	D_5	$\mathbf{D_5}$	S_7	S_7
14	$\alpha\beta\delta$	D_6	D_6	S_8	$\mathbf{D_7}$
15	$\alpha\beta\gamma$	D_7	D_7	$\mathbf{D_7}$	S_8
16	$\alpha\beta\gamma\delta$	D_8	D_8	D_8	$\mathbf{D_8}$

For each round S_1 indicates the first sum made, D_1 the first difference squared made, and so forth, working through the list from the first to the sixteenth position. When a result is assigned to a position that position is not accessed again for the remainder of that round. In the $2nd$ round entries in positions 1 and $1+4$ (as they appear after the $1st$ round) are summed and put in S_1, the difference squared put in D_1; similarly for positions 2 and $2+4$ whose sum is put into S_2 and difference squared into D_2; positions 3 and $3+4$ whose sum is put into S_3 and difference squared into D_3; positions 4 and $4+4$ whose sum is put into S_4 and difference squared into D_4. Positions 5 to 8 have already been accessed so we ignore them. We then come to positions 9 and $9+4$ whose sum is put into S_5 and difference squared into D_5; positions 10 and $10+4$ whose sum is put into S_6 and difference squared into D_6; positions 11 and $11+4$ whose sum is put into S_7 and difference squared into D_7; positions 12 and $12+4$ whose sum is put into S_8 and difference squared into D_8. And positions 13 to 16 have already been accessed for this round so we have completed the second round. In the $3rd$ round entries in positions 1 and $1+2$ (as they appear after the $2nd$ round) are summed and put in S_1, the difference squared put in D_1, and so forth. In the $4th$ round entries in positions 1 and $1+1$ (as they appear after the $3rd$ round) are summed and put in S_1, the difference squared put in D_1, and so forth. It is claimed that after the kth round, where $2^k = \phi(2n)$, we have a list of integers which afterwards will be put into the compact form of expression for [1]. There are yet two more considerations before we are ready to do this.

By assumption, each of the values in the input list may be expressed using the compact form with the same rational values, varying only in sign. One might record the whole suite of signs but in practice we need only those pertaining to the first position's input value. The sign of a radical (or quadrant if a square root of a complex value) belonging to the higher list position is recorded in another list with the same list position as that where the squared radical is to be put, that is with the position of each D_j in the scheme above. After these signs are over-written in the normal course of execution they will finally contain the signs belonging to the radicals of the first position's input value, corresponding to the bold $\mathbf{D_j}$ in the scheme above. All except the first output position (S_1 after the $4th$ round in the example) will be assigned a sign in this manner. The signs are stored in correct order for writing ahead of the (assumed) integer, S_j or D_j, stored in the same position number, after the final round, with radical symbol intervening.

We need also to divide by 2 the results of the additions and subtractions to restore the value of just one list member, for example $\cos(\zeta\pi/n)$ rather than $2\cos(\zeta\pi/n)$. We can accomplish this most easily by finding the total number of halvings applicable to each output number and writing an explicit division by a power of 2 in the output expression.

The list of explicit divisors of form 2^m is very easily accomplished and is identical for each case that uses the same number of rounds of processing. At each successive round the values (ought to) undergo halving for the S_j, and halving and squaring for the D_j. Thus we can find m by the process following in table 3.2.3, assuming an eight input example.

Table 3.2.3.

listpos.	$0th$		$1st$		$2nd$		$3rd$
1	0	$\ldots + 1 \ldots$	1	$\ldots + 1 \ldots$	2	$\ldots + 1 \ldots$	3
			·		·		$\times 2$
2			·		$\times 2$		6
			·		·		
3			$\times 2$		4	$\ldots + 1 \ldots$	5
			·				$\times 2$
4			·				10
			·				
5			2	$\ldots + 1 \ldots$	3	$\ldots + 1 \ldots$	4
					·		$\times 2$
6					$\times 2$		8
					·		
7					6	$\ldots + 1 \ldots$	7
							$\times 2$
8							14

After the $3rd$ round we have produced the list of values in output order for m of 3, 6, 5, 10, 4, 8, 7, 14, with which to write the explicit divisors of form 2^m. For cases with more inputs we need to increase the separation of the doubled numbers and increase the number of rounds of the process indicated, for example for sixteen inputs, we need to double the separation distances and add one more round.

Collating the output lists of (i) the (assumed) integers $S_1,\ D_1,\ S_2,\ D_2, \ldots, S_8,\ D_8$, (ii) the signs of the radicals belonging to the position 1 input value, that is the signs of the square roots of the bold $\mathbf{D_j}$ and (iii) the values of m for the divisors of form 2^m, we produce the completed output expression. Here is the compact constructible expression so produced for $[1] = e^{i\pi/17}$ of our example:

$$\begin{aligned} &1/2^4 - \surd(17/2^8) + \surd(17/2^7 - \surd(17/2^{14}))+ \\ &\surd(17/2^6 + \surd(153/2^{12}) + \surd(85/2^{11} + \surd(6137/2^{22})))+ \\ &\surd(-17/2^5 + \surd(17/2^{10}) + \surd(17/2^9 - \surd(17/2^{18}))+ \\ &\surd(17/2^8 + \surd(153/2^{16}) - \surd(85/2^{15} + \surd(6137/2^{30})))). \end{aligned}$$

Because the numeric method is applied symmetrically to the inputs, apart from the recording of sign, it can equally be applied to finding $[\zeta]$ or $2\cos(\zeta\pi/n)$ simply by putting this value in the first position, that using $[\zeta\delta]$ in the second position, $[\zeta\gamma]$ in the third position, and so forth, for the sixteen elements in $\mathcal{U}_{2n}$ example. We can also use it to find $[k]$ or $2\cos(k\pi/n)$, for any integer k. When $\gcd(k,\ n) \neq 1$ the numerical process is the same as when $\gcd(k,\ n) = 1$ just as the algebraic process is the same in both cases. We merely start with an adjusted table (algebraic method) or input list (numeric method). In the numeric method we are still solving for the quadratic zeros. The expression for the quadratic zeros $x_1,\ x_2 = [x_1 + x_2 \pm \surd[2(x_1^2 + x_2^2) - (x_1 + x_2)^2]]/2$ used in the algebraic method may also be put $x_1,\ x_2 = [x_1 + x_2 \pm \surd[(x_1 - x_2)^2]]/2$. In section 3.3 the numeric process is described in terms of rows of a table or tables like table 2.3.3 or table 2.3.7. So if, as will be shown, the numeric method can be used to find a compact constructible expression for $[u]$ or $2\cos(u\pi/n)$, where $u \in \mathcal{U}_{2n}$, then it can also be used to find one for $[k]$ or $2\cos(k\pi/n)$ for any integer k.

3.3. **The Numeric Method Produces Only Integers.** There is nothing to prevent us imposing the numeric method on any collection of 2^k, for any positive integer k, real or complex values but we would not generally expect the output numbers to be all equal to integers. Nor will they be for the present purpose unless the input values are in an appropriate order.

In section 2 we considered what became of cosums whose exponents were multiplied by an integer. It sufficed to know that another cosum was produced and to which polynomial it belonged, that there might be so many copies of the cosum and that it might be reflected in the imaginary axis. Now we need to investigate further the sum of all the zeros of Ψ_n when their exponents are multiplied by an integer, m. We already know by theorem 2.2.4 that when $\gcd(m,\ n) = 1$ the transformed sum is again equal to the sum of all the zeros or to the reflection in the imaginary axis of all the zeros. We wish to show that when $\gcd(m,\ n) \neq 1$ the transformed sum always contains so many copies of *all the zeros* of Ψ_s, where $m/n = r/s$ in lowest terms, and not merely that it contains so many copies of a cosum of *some size* of Ψ_s, which is all that theorem 2.2.5 provided.

Lemma 3.3.1. *When the exponents of all the zeros of Ψ_n are multiplied by an integer, m, taken modulo $2n$, and $gcd(m,\ n) \neq 1$ the zeros are sent to so many copies of all of the zeros of Ψ_s or to the reflections, in the imaginary axis of the complex plane, of so many copies of all of the zeros of Ψ_s, where m/n in lowest terms is equal to r/s.*

Proof. In the extreme case when $m = rn$ and therefore $m/n = r/1$ the numerators $u_j r$, where $u_j \in \mathcal{U}_{2n}$, in the exponents are taken modulo 2. Thus the sequence $u_j r$ is equal to $\phi(2n)$ copies of the only element of $\mathcal{U}_2$, that is of unity, when r is odd or the reflections of these, that is of $1 - 1 = 0$, when r is even. Then we have $\phi(n)$ copies of $e^{i\pi} = -1$ or of $e^{i0} = 1$. We next consider separately the cases where (i) $n = p_1 p_2 \cdots p_h$, a product of distinct odd primes of the usual form and (ii) $n = 2^v$ and then the general case with $n = p_1 p_2 \cdots p_h 2^v$.

The product of distinct odd primes case is most easily shown by using some group isomorphisms involving external direct products, symbol $\oplus$, whose operation is multiplication by components, using the appropriate modulus for each component. Generally $\mathcal{U}_{ab} \approx \mathcal{U}_a \oplus \mathcal{U}_b$, when $\gcd(a,\ b) = 1$. The mapping is $\mu :\ k \pmod{ab} \to (k \pmod{a},\ k \pmod{b})$. [ref]

So $\mathcal{U}_{2n} = \mathcal{U}_{2p_1 p_2 \cdots p_h} \approx \mathcal{U}_{p_1 p_2 \cdots p_h} \approx \mathcal{U}_{2p_1} \oplus \mathcal{U}_{p_2 \cdots p_h}$ and the sequence of elements of $\mathcal{U}_{2n}$ is equivalent to the sequence of elements of $U_{2p_1} \oplus \mathcal{U}_{p_2 \cdots p_h}$ in some order. The elements of $\mathcal{U}_{2p_1}$ occur as the first component in the external direct product representation and each occurs $\phi(p_2\cdots p_h)$ times in the whole sequence. So when $\mathcal{U}_{2s}=\mathcal{U}_{2p_1}$ or more generally $\mathcal{U}_{2s}=\mathcal{U}_{2p_1\cdots p_g}$, $g<h$, the whole group $\mathcal{U}_{2s}$ appears in the sequence u_j taken modulo $2s$, for $u_j\in\mathcal{U}_{2n}$, and it appears $\phi(p_{g+1}\cdots p_h)$ times. mu_j/n becomes ru_j/s and taking ru_j modulo $2s$ is equivalent to ignoring the second component in the external direct product representation and considering only the first component, thus producing so many copies of all the elements of $\mathcal{U}_{2s}$ in the numerators of the exponents when r is odd and the reflections of these when r is even.

The powers of 2 case is very simple. The elements of $\mathcal{U}_{2n}=\mathcal{U}_{2^v}$ consist of all the odd numbers less than 2^v and the only possible divisors, s, of n are similarly powers of 2. The elements are

$$\begin{array}{ll}
1,\ 3,\ 5,\ 7,\ 9,\ 11,\ 13,\ 15,\ldots & \text{modulo } 16,\ 32,\ldots,\\
1,\ 3,\ 5,\ 7,\ 1,\ 3,\ 5,\ 7,\ldots & \text{modulo } 8,\\
1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ldots & \text{modulo } 4,\\
1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ldots & \text{modulo } 2.
\end{array}$$

Thus $u_j \pmod{2s}$ cycle a number of times through the elements of $\mathcal{U}_{2s}$ in the course of the sequence of elements of $\mathcal{U}_{2n}$. $ru_j \pmod{2s}$, where $u_j\in\mathcal{U}_{2n}$, therefore represents so many copies of all the elements of $\mathcal{U}_{2s}$. r cannot be even because $\gcd(r,\ s)=1$ and $s=2^w$, so reflections are not possible in this case.

Combining the cases of product of odd primes and powers of 2 gives our general constructible case. Now $\mathcal{U}_{2n}=\mathcal{U}_{p_1p_2\cdots p_h2^v}\approx\mathcal{U}_{p_1p_2\cdots p_g}\oplus\mathcal{U}_{p_{g+1}\cdots p_h}\oplus\mathcal{U}_{2^v}$. Already we have dealt with the cases where $v=1$ and with $h=1,\ p_1=1$. The general combined case is susceptible of the same componentwise treatment. When $s=p_1\cdots p_g,\ g<h$ or $s=2^w,\ 1\le w<v-1$ we simply have a previous case with one extra component in the external direct product, giving yet more copies of all the elements of $\mathcal{U}_{2s}$, when the elements, u_j, of $\mathcal{U}_{2n}$ are taken modulo $2s$. When $s=p_1\cdots p_g2^w$ we need to consider two components (of the three in the external direct product), actually one component and some of the 2^v component, to find a representation for the elements of $\mathcal{U}_{2s}$, but they are all there and so many copies of all of them. Multiplying u_j by r merely either reorders or reflects, or both, these elements $u_j \pmod{2s}$. These results in terms of elements of $\mathcal{U}_{2s}$ translate immediately into the corresponding results for the zeros of Ψ_s. $\square$

Looking at the output numbers of the numeric method in terms of cosums $x_{j(l)}$, the jth cosum of level l, we find the following sequence of expressions.

Table 3.3.2.

$$\begin{aligned}
S_1 &= x_{1(0)}=x_{1(1)}+x_{2(1)},\\
D_1 &= (x_{1(1)}-x_{2(1)})^2,\\
S_2 &= (x_{1(2)}-x_{2(2)})^2+(x_{3(2)}-x_{4(2)})^2,\\
D_2 &= [(x_{1(2)}-x_{2(2)})^2-(x_{3(2)}-x_{4(2)})^2]^2,\\
S_3 &= [(x_{1(3)}-x_{2(3)})^2+(x_{3(3)}-x_{4(3)})^2]+[(x_{5(3)}-x_{6(3)})^2+(x_{7(3)}-x_{8(3)})^2],\\
D_3 &= ([(x_{1(3)}-x_{2(3)})^2+(x_{3(3)}-x_{4(3)})^2]-[(x_{5(3)}-x_{6(3)})^2+(x_{7(3)}-x_{8(3)})^2])^2,\\
S_4 &= [(x_{1(3)}-x_{2(3)})^2-(x_{3(3)}-x_{4(3)})^2]+[(x_{5(3)}-x_{6(3)})^2-(x_{7(3)}-x_{8(3)})^2],\\
D_4 &= ([(x_{1(3)}-x_{2(3)})^2-(x_{3(3)}-x_{4(3)})^2]-[(x_{5(3)}-x_{6(3)})^2-(x_{7(3)}-x_{8(3)})^2])^2,\\
&\cdots
\end{aligned}$$

We wish to show that each S_j and D_j is equivalent to a table or tables of summands similar in structure to table 2.3.3 with each row being *complete*, that is having form $\Sigma_{j=1}^{\phi(2n)} e^{imu_j\pi/n}$, where m is some integer constant for that row, $u_j \in \mathcal{U}_{2n}$ and having a 1 column, α column, β column, $\alpha\beta$ column and so forth. Table construction is to be carried on by column, just as in the description accompanying table 2.3.3.

Table 3.3.2 can be viewed as if just two processes were at work in extending it.
Process (i) Replacement of a central plus sign with a minus sign and squaring the whole expression, for example $x_{1(1)} + x_{2(1)}$ becomes $(x_{1(1)} - x_{2(1)})^2$. This process sends $S_j \to D_j$ and
Process (ii) Reducing the size of the cosum components ($x_{j(l)}$ becomes $x_{j(l+1)}$) and adding a similar part with the subscripts continuing in number order, for example $(x_{1(1)} - x_{2(1)})^2$ becomes $(x_{1(2)} - x_{2(2)})^2 + (x_{3(2)} - x_{4(2)})^2$. This process sends $S_j \to S_{2j-1}$ and $D_j \to S_{2j}$.
These processes can be continued until $x_{j(l)}$ becomes undefined.

Process (i) is immediately evident from the manner of making S_j and D_j.

To illustrate process (ii) for $S_j \to S_{2j-1}$ the reader might pencil in on table 3.2.2 the source of some S_j and S_{2j-1} of the final ($4th$) round, as they are supplied by all the previous rounds' output. It will be observed that S_j of the final round has the same structure of inputs from previous rounds as does S_{2j-1} and does S_{2j} of the last but one ($3rd$) round but that the cosums in S_j of the final round are larger (level 3 cosums for $j = 4$, level 2 cosums for $j = 2$) than those of S_{2j-1} or S_{2j} of the last but one round (level 4 cosums for $j = 4$, level 3 for $j = 2$). When S_{2j-1} and S_{2j} of the last but one round are summed in S_{2j-1} of the final round the expression (as in table 3.3.2) of S_{2j-1} of the last but one round is repeated but with contiguous cosum subscripts, as required.

Similarly, for process (ii) and $D_j \to S_{2j}$, D_j of the final ($4th$) round has the same structure of inputs from previous rounds as does D_{2j-1} and does D_{2j} of the last but one ($3rd$) round but that the cosums in D_j of the final round are larger (level 3 cosums for $j = 3$, level 2 cosums for $j = 2$) than those of D_{2j-1} or D_{2j} of the last but one round (level 4 cosums for $j = 3$, level 3 for $j = 2$). When D_{2j-1} and D_{2j} of the last but one round are summed in S_{2j} of the final round the expression (as in table 3.3.2) of D_{2j-1} of the last but one round is repeated but with contiguous cosum subscripts, again, as required.

An inductive proof follows. It will be shown that if each process acts on expressions composed of only complete rows then they each produce expressions composed of only complete rows. Because $S_1 = x_{1(0)}$ is represented by a complete row, any S_j or D_j produced by these two processes is necessarily composed of only complete rows. Then because complete rows are equal to an integer the output numbers of the numeric method are necessarily integers.

Definition 3.3.3. A *complete row* has the form $\Sigma_{j=1}^{\phi(2n)} e^{imu_j\pi/n}$, where m is some integer constant for a row and u_j are all the elements of $\mathcal{U}_{2n}$.

Lemma 3.3.4. *Process (i) of extending table 3.3.2 sends $A + B \to (A - B)^2$. If $A + B$ consists of a complete row or rows and A contains the first half of each complete row and B contains the second half of each complete row then process (i) produces only complete rows.*

Proof. The table created on multiplying out the expression made by process (i) consists of rows made from each of the two interior compound components squared and then rows made from the products of these two compound components. Thus $(A - B)^2$

$$\begin{array}{cccc} = & A^2 & + & B^2 \\ - & AB & - & BA. \end{array}$$

Here $A^2 + B^2$ represents a part table of several rows and $\phi(2n)$ columns and likewise for $-AB - BA$ except that the latter is composed of subtrahends rather than summands. Studying first the simplest case, $A = x_{1(1)},\ B = x_{2(1)}$, we have the upper half of the table identical to table 2.3.3. The lower half is filled in by continuing the columns of the upper half. Finding which row in the arbitrary ζ column in which to place a product with exponent $\zeta + u_1$ uses the same procedure as was used in table 2.3.3 and in the upper half of this table. That is we seek $u_2 \in \mathcal{U}_{2n}$ such that $\zeta + u_1 = (1 + u_2)\zeta = \zeta + u_2\zeta \Rightarrow u_2 = u_1\zeta^{-1}$ and place that product in the $1+u_2$ row. In contrast to the upper half of the table where u_2 must be in the first half of the elements in order $1,\ \alpha,\ \beta,\ \alpha\beta,\ \gamma \ldots$, in the lower half of the table u_2 must be in the second half of the elements in order because now u_1 and ζ come from different halves of the elements in order.

In more complicated cases, where A and B already represent several rows each, the first half of a row in A and the second half of a row in B, then we proceed a row at a time. Let A be represented by rows $y_{1,A}$ to $y_{k,A}$ and B by rows $y_{1,B}$ to $y_{k,B}$, where the second subscript identifies the first or second half of a complete row. Now to make the upper half of a super-table we join the half rows of $y_{1,A}y_{1,A}$ to those of $y_{1,B}y_{1,B}, \ldots,\ y_{r,A}y_{s,A}$ to those of $y_{r,B}y_{s,B}, \ldots,\ y_{k,A}y_{k,A}$ to those of $y_{k,B}y_{k,B}$. We arrange these component tables one below the other, maintaining $\phi(2n)$ columns in the super-table. To make the lower half of a super-table we join the half rows of $y_{1,A}y_{1,B}$ to those of $y_{1,B}y_{1,A}, \ldots,\ y_{r,A}y_{s,B}$ to those of $y_{r,B}y_{s,A}, \ldots,\ y_{k,A}y_{k,B}$ to those of $y_{k,B}y_{k,A}$. A product of rows, such as $y_{r,A}y_{s,B}$, while of course being ultimately commutative, directs the table builder to make columns who take their column labels from within each of the exponents of the summands of the first-written multiplicand. To find the correct row of a component table in which to place a product we have now to consider the exponent $m_1\zeta + m_2u_1$ to go in the ζ column. Here ζ comes from an $m = m_1$ row, say $y_{r,A}$, and u_1 form an $m = m_2$ row, say $y_{s,B}$. We seek u_2 such that $(m_1 + m_2u_2)\zeta = m_1\zeta + m_2u_1 \Rightarrow u_2 = u_1\zeta^{-1}$ which indicates that the product goes in the $m = m_1 + m_2u_2$ row. That each such row exists and is unique follows from $\mathcal{U}_{2n}$ being a group. Thus the super-table is composed of complete rows where the m for each row has the form $m = m_1 + m_2u_2$, that is of the required form. □

Lemma 3.3.5. *If process (ii) of extending table 3.3.2 acts on complete rows then process (ii) produces only complete rows.*

Proof. The rows of, for example, $(x_{1(1)} - x_{2(1)})^2$ have as many columns, when arranged like table 2.3.3, as $x_{1(1)} + x_{2(1)} = x_{1(0)}$ has summands and the rows of $(x_{1(2)} - x_{2(2)})^2$ have as many columns as $x_{1(2)} + x_{2(2)} = x_{1(1)}$ has summands, that is half as many columns. It also has fewer rows, some of which have their summands changed to subtrahends. This follows from the manner of constructing a table such as table 2.3.3 or the more complicated super-table of lemma 3.3.4. Recall how, in the algebraic method, the quadratic radicand for higher levels was found from smaller areas of the same table. Extending $(x_{1(2)} - x_{2(2)})^2$ by adding to it a similar expression, with consecutive subscripts, $(x_{3(2)} - x_{4(2)})^2$, extends the rows, in the prescribed manner, in its tabular representation making it contain as many columns as $x_{1(1)} + x_{2(1)} = x_{1(0)}$ has summands. The similar expression which is added on is identical to the first but that each exponent is multiplied by the next in order of $\alpha\ \beta,\ \gamma$ and so forth, so making the result consist of only complete rows. Because of the manner of table production any of the expressions in table 3.3.2, given it is composed of complete rows, will, like the example, produce only complete rows under the action of process (ii). □

Theorem 3.3.6. *The output numbers, $S_j,\ D_j$, of the numeric method are integers.*

Proof. $S_1 = x_{1(0)}$ is equal to the sum of all the zeros of Ψ_n which is an integer, by theorem 2.3.1. All S_j with $j > 1$ and D_j with $j \geq 1$ can be produced by a chain of applications of processes (i) and (ii). Process (i), after converting $S_1 \to D_1$, always acts on the output of process (ii) and process (ii) has the required form, $A+B$, for input to process (i), given that process (ii) acted on complete rows, by lemma 3.3.5. Process (ii) acts on the output of either process (i) or (ii), each of which will be composed of complete rows given they acted on input composed of complete rows, by lemmas 3.3.4 and 3.3.5. By combined induction on the two processes, each of the output numbers is then composed of a sum of complete rows, each of which rows is equal to an integer, by theorem 2.2.4 and lemma 3.3.1. Therefore each output number of the numeric method is equal to an integer. □

3.4. **Using the Numeric Method.** In the proof that the numeric method produces only integers we began consideration of the output numbers with $S_1 = x_{1(0)}$ but could have begun with any complete row or rows and finished with integers in the compact form of constructible expression. We could have used $\Sigma_{j=1}^{\phi(2n)} te^{iku_j\pi/n}$, where u_j are all the elements of $\mathcal{U}_{2n}$; $t,\ k$ are integer constants and n is restricted in the usual way to equal the number of sides of a constructible polygon, thus making the input list hold the $\phi(2n)$ summands ordered on u_j expressed as a product of $\alpha,\ \beta,\ \gamma$ and so forth. Further, we could have used $S_1 = \Sigma_{j=1}^{\phi(2n)}(t_1e^{ik_1u_j\pi/n} + t_2e^{ik_2u_j\pi/n} + \ldots + t_se^{ik_su_j\pi/n})$ with as many components in each summand as liked. For this does not alter the type of calculation needed but only increases the number of tables to be produced, which still are composed of complete rows.

The precision with which the output integers can be determined is dependent on the precision of the input values. For $n > 85$ the precision commonly available, say 18 decimal places, will be insufficient. $2\cos(\pi/85)$ has around a 16 digit integer for its final output term, D_{16} (It does not have a unique compact expression). High precision algorithms for arithmetic and trigonometric evaluation and the constant π exist and the use of such a system would be essential to produce precise integer output for larger n. [ref]

Western Australia