Improving Gauss's Method for Finding Roots of Unity by Finding Radical Expressions For Arbitrary Members Of The Cyclotomic Field and Its Extensions

Eric R. Binnendyk
ericabq@gmail.com

May 27, 2020

Abstract

We introduce a new method to find radical expressions for roots of unity; that is, complex numbers that yield 1 when raised to some integer power. This method yields more compact expressions than previous methods suggested by Carl Gauss and Andreas Weber. Under a particular metric for the size of a radical expression, we develop a recursive formula for the size of the expressions for each root of unity. The method involves generalizing the problem to finding equally compact radical expressions for arbitrary members of the cyclotomic field (the minimal field, for each n, containing nth roots of unity) and their extensions. We develop an algorithm to express a value recursively in terms of values from either subfields or field extensions, and show that this recursion eventually reduces to the field of rationals, yielding a radical expression.

Radical expressions for roots of unity lead to radical expressions for $\cos(n\pi)$ and $\sin(n\pi)$ for all rational numbers n, which can be applied to the geometric construction of regular polygons using a compass, straightedge, and marked ruler. The theory behind such expressions can also be a pedagogical tool for explaining why certain trigonometric functions result in simple values (e.g. $\cos(\pi/3) = \frac{1}{2}$ and $\cos(\pi/5) = \frac{1+\sqrt{5}}{4}$).

1 Introduction and History

The result presented here derives heavily from earlier research.

The study of radical expressions for roots of unity began with Gauss's discovery of an expression for 17th roots of unity using only square roots [2]. Gauss went on to prove that all roots of unity could be expressed in radicals and developed an algorithm to find a radical expression for pth roots of unity whenever p was prime [3]. A similar method was also developed by Vandermonde [4]. Gauss's method and the theory behind it lay the basis for our research.

Later research on improvements to the algorithm was done by Andreas Weber in 1995 [6]. He developed an improved algorithm for calculating radical expressions that takes advantage of the redundancy of the different sums of periods that need to be calculated. A similar calculation of the 29th roots of unity was described in a paper by Lau Jing Feng [7]. However, for large n, the expressions for the nth roots of unity produced by both of these methods are long and cannot practically be written out in full. They are often presented by using variables to represent auxilliary expressions.

We present a new method, based on Galois theory, that avoids the need to multiply radical expressions directly. We generalize the problem of finding pth roots of unity, where p is prime, to finding radical expressions for every member of the pth cyclotomic field (the minimal field containing the pth roots of unity) as well as extensions to this field formed by adjoining other roots of unity. The resulting algorithm produces radical expressions with a simple tree-like structure; recursively speaking, they are either rational numbers (base case) or sums of rational numbers together with radical roots of simpler expressions of the same type. We also develop a formula to determine the complexity of a radical expression and analyze the complexity of expressions produced by our algorithm compared to expressions produced by previous algorithms.

2 Preliminaries

2.1 Radical expressions

Let $\mathbb{Q}[x]$ be the set of all polynomials with rational coefficients. Let $p \in \mathbb{Q}[x]$ and let $r \in \mathbb{C}$ be a particular root of p. (In other words, r is an *algebraic* complex number.) A **radical expression** for r is a particular formula evaluating to r using only of sums of rational numbers with nth roots of simpler radical expressions, where n can be any positive integer greater than 1.

Formally, the set R of radical expressions can be defined recursively as follows:

- If $expr$ is a single integer, as a formula, then $expr \in R$.
- If $expr \in R$ and $n \in \mathbb{N}$, $n > 1$, then $\sqrt[n]{expr} \in R$ for all choices of complex nth root. These choices may be denoted $\beta^j \sqrt[n]{expr}$, where j ranges from 0 to $n-1$ and β is a primitive nth root of unity (as described below). By convention, if $n = 2$, we can write $\sqrt{expr}$ instead of $\sqrt[2]{expr}$.
- If $expr1, expr2 \in R$, then $(expr1) + (expr2), (expr1) - (expr2), (expr1) * (expr2), (expr1)/(expr2) \in R$. Note that not all valid expressions correspond to numbers; for example, if $expr2$ evaluates to 0, then $(expr1)/(expr2)$ does not have a defined value.

The parentheses in any expression can be removed if they are part of a chain of associative operators, like addition or multiplication. For example, we can write $\sqrt[3]{2} + \sqrt[5]{4} + \sqrt{6}$ instead of $\sqrt[3]{2} + (\sqrt[5]{4} + \sqrt{6})$ or $(\sqrt[3]{2} + \sqrt[5]{4}) + \sqrt{6}$.

Radical expressions are a more intuitive, constructive way to understand algebraic numbers compared to the traditional method of describing them as roots of a particular polynomial. However, not all algebraic numbers even have radical expressions. As proved by Abel in 1824, there is no general formula for the roots of a polynomial of degree 5 or above in terms of radical expressions of the coefficients. In 1830, Galois identified the class of polynomials in $\mathbb{Q}[x]$ whose roots have radical expressions; they are precisely the polynomials whose Galois group is isomorphic to a product of cyclic groups.

The radical expressions produced by our algorithm belong to a specific subset of the class described above. We call this the set of **radical-sum expressions**. This subset R' can be defined by:

- If $expr$ is an integer, then $expr \in R'$ is a radical expression.

- If $expr \in R'$ and $n \in \mathbb{N}$, $n > 1$, then $\beta^j \sqrt[n]{expr} \in R'$ for all j from 0 to $n-1$.
- If $expr1, expr2 \in R'$ and $n \in \mathbb{N}$, then $(expr1) + (expr2), (expr1) - (expr2), (expr1)/(n) \in R'$.

Every radical-sum expression consists of a sum of one or more rational numbers and values under radicals, possibly divided by an integer. For example, $\sqrt{2}$, $\sqrt{\frac{3}{2}}+1$, and $\frac{\frac{1}{3}-\beta^2\sqrt[3]{1+\sqrt{-2}}}{3}$ are all in R', but $\frac{\sqrt{3}}{\sqrt{2}}+1$ and $\sqrt{2}(1+\sqrt[3]{5})$ are not.

2.2 Roots of unity

For a positive integer n, an nth **root of unity** ζ is a complex number of the form $\zeta = e^{2k\pi i/n} = \cos(2k\pi/n) + i\sin(2k\pi/n)$ for some integer k. As a consequence of this definition, we have $|\zeta| = 1$, $\arg\zeta = 2\pi k/n$, and $\zeta^n = 1$. A **primitive** nth root of unity requires additionally that k and n be relatively prime. From this definition, a primitive nth root of unity is not an mth root of unity for any $m < n$.

If ζ is an nth root of unity, then ζ satisfies the polynomial $\zeta^n - 1$. This polynomial is factorizable as $(\zeta-1)(\sum_{k=0}^{n-1}\zeta^k)$. Thus, if $\zeta \neq 1$, ζ also satisfies $\sum_{k=0}^{n-1}\zeta^k$. A polynomial satisfied uniquely by all primitive nth roots of unity, for some n, is called a *cyclotomic polynomial.* If p is prime, then all pth roots of unity besides 1 are primitive. Thus, the expression $\sum_{k=0}^{p-1}\zeta^k$ is satisfied by all, and only by, primitive pth roots of unity. It follows that if p is prime, the previous expression is the pth cyclotomic polynomial.

We know that radical expressions exist for all roots of unity. For example, to get the nth roots of unity, we can just write $\beta^j \sqrt[n]{1}$ for all n choices of the complex nth root. However, this expression is not desirable for several reasons:

1. It describes all nth roots of unity, not just the primitive ones, obtained in the previous expression when $k = 0$.
2. It is not written in the form $\frac{a+b}{c}$, where a and c are real and b is pure imaginary.
3. It is described in terms of the n choices of the complex nth root, which only differ from each other by factors of the nth roots of unity. Depending on the context of evaluation, the expression may be considered a circular definition.
4. There exist radical expressions for the nth roots of unity using only radicals with degree less than n, as will be explained below.

An example of an expression that does not have these problems is

$$e^{2\pi i/5} = \frac{-1+\sqrt{5}+\sqrt{-10-2\sqrt{5}}}{4}$$

This is an expression for a primitive 5th root of unity as the root of the cyclotomic polynomial $x^4+x^3+x^2+x^1+1$, which is satisfied by all four primitive 5th roots of unity. Changing the signs on this expressions yields the other three primitive 5th roots, but not 1.

$$e^{4\pi i/5} = \frac{-1-\sqrt{5}+\sqrt{-10+2\sqrt{5}}}{4}$$

$$e^{6\pi i/5} = \frac{-1-\sqrt{5}-\sqrt{-10+2\sqrt{5}}}{4}$$

$$e^{8\pi i/5} = \frac{-1+\sqrt{5}-\sqrt{-10-2\sqrt{5}}}{4}$$

As it turns out, every cyclotomic polynomial has a Galois group that can be expressed as a product of cyclic groups. Thus, nth roots of unity are always expressible by radicals of degree less than n, where different primitive roots can be found by using different choices of roots. In fact, this existence was known before Galois and was published by Gauss in *Disquisitiones Arithmeticae* [1].

2.3 Sums of roots of unity

Consider the field extension $\mathbb{Q}[\zeta]$ of the rationals extended with a primitive nth root of unity ζ. This is called the nth **cyclotomic field**. Any member x of this set can be expressed as $x = \sum_{j=0}^{n-1} a_j \zeta^j$ where all $a_j \in \mathbb{Q}$. We will simply call this type of expression a **sum** or **sum of roots of unity**.

2.3.1 Degree of a sum

Let $x \in \mathbb{Q}[\zeta]$, where ζ is a primitive pth root of unity and p is prime, and let $\sum_{j=0}^{p-1} a_j \zeta^j$ be a sum representation of x. Because p is prime, an integer g with $1 < g < p$ can be chosen so that $1, g, g^2, g^3, ..., g^{p-2}$ are all distinct values modulo p. (Due to Fermat's little theorem, $g^{p-1} \mod p = 1$ for any value of g not divisible by p.) Such a value g is called a *primitive root* modulo p (not to be confused with a primitive root of unity, which is an entirely different concept). In the following text, we will assume a particular primitive root g has been chosen.

We can talk of the unique field automorphism $\sigma : \mathbb{Q}[\zeta] \to \mathbb{Q}[\zeta]$ such that $\sigma(\zeta) = \zeta^g$, for a particular primitive root g. Because σ is an automorphism, we have $\sigma(P(\zeta)) = P(\zeta^g)$ for any polynomial P with rational coefficients, and in particular any sum. Thus, $\sigma(x) = \sum_{j=0}^{p-1} a_j \zeta^{jg}$ is a sum with the same coefficients as x in a different order. Because g is a primitive root modulo p, σ is a generator of the Galois group of automorphisms of $\mathbb{Q}[\zeta]$. For a positive integer k that divides $p-1$, if $\sigma^k(x) = x$, then we say that x is a sum with **degree** k.

The set of all sums x with degree k forms a field itself, and so is closed under addition and multiplication.

In fact, sums of pth roots of unity with degree k are roots of degree-k polynomials with rational coefficients. In particular, any sum of degree 1 is rational itself:

$$x = \sum_{k=0}^{p_j-1} (a_k \zeta^k) = a_0 + \sum_{k=1}^{p-1} (a_1 \zeta^k) \text{ (because } x = \sigma(x))$$

$$= a_0 + a_1 \sum_{k=1}^{p-1} \zeta^k$$

$$= a_0 - a_1 \text{ (because } \zeta \text{ is a root of } \sum_{k=0}^{p-1} \zeta^k)$$

2.3.2 Periods

A **period**, as identified by Gauss, is a special type of sum. A period (f, k) is a sum $\sum_{m=0}^{f-1} \zeta^{g^{dm}k}$, where $d = (p-1)/f$. This sum has degree d. Every sum of degree d can be written as a sum of these periods, as follows: $\sum_{j=0}^{d-1} a_{g^j}(f, g^j)$

If x has degree $k > 1$, some of the coefficients in the sum must be equal: $a_j = a_{jg^{nk} \bmod p}$ where $0 < n < (p-1)/k$.

2.3.3 Example

Let $p = 13$ and let ζ be any primitive 13th root of unity. It can be shown that $g = 2$ is a primitive root mod 13 because the values $2^0, 2^1, ..., 2^{11}$ mod 13 are all distinct:

$$1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7$$

Then we can define σ by $\sigma(P(\zeta)) = P(\zeta^2)$ for all rational polynomials P. For example, if

$$x = 2 - \zeta + \zeta^2 + 3\zeta^4 - \zeta^8 + \zeta^3 + 3\zeta^6 - \zeta^{12} + \zeta^{11} + 3\zeta^9 - \zeta^5 + \zeta^{10} + 3\zeta^7$$

is a sum with coefficients $a_0 = 2, a_1 = -1, a_2 = 1, a_3 = 1, a_4 = 3$... etc., then

$$\sigma(x) = 2 + 3\zeta - \zeta^2 + \zeta^4 + 3\zeta^8 - \zeta^3 + \zeta^6 + 3\zeta^{12} - \zeta^{11} + \zeta^9 + 3\zeta^5 - \zeta^{10} + \zeta^7$$

$$\sigma^2(x) = \sigma(\sigma(x)) = 2 + \zeta + 3\zeta^2 - \zeta^4 + \zeta^8 + 3\zeta^3 - \zeta^6 + \zeta^{12} + 3\zeta^{11} - \zeta^9 + \zeta^5 + 3\zeta^{10} - \zeta^7$$

$$\sigma^3(x) = 2 - \zeta + \zeta^2 + 3\zeta^4 - \zeta^8 + \zeta^3 + 3\zeta^6 - \zeta^{12} + \zeta^{11} + 3\zeta^9 - \zeta^5 + \zeta^{10} + 3\zeta^7$$

and we see that $\sigma^3(x) = x$, so x has degree 3. We also see that some of the coefficients are identical, such as: $-1 = a_1$, $-1 = a_{1 \cdot 2^3 \bmod 13} = a_8$, $-1 = a_{1 \cdot 2^6 \bmod 13} = a_{12}$, $-1 = a_{1 \cdot 2^9 \bmod 13} = a_5$.

We also can write x as a sum of periods of degree 3. Because the degree $d = 3$, we will need to take $f = (13-1)/3 = 4$:

$$(4, 2^0) = \zeta + \zeta^8 + \zeta^{12} + \zeta^5$$

$$(4, 2^1) = \zeta^2 + \zeta^3 + \zeta^{11} + \zeta^{10}$$

$$(4, 2^2) = \zeta^4 + \zeta^6 + \zeta^9 + \zeta^7$$

$$x = 2 + (-1) \cdot (4, 2^0) + 1 \cdot (4, 2^1) + 3 \cdot (4, 2^2)$$

2.4 Multisums (field extensions)

Let $p_1, p_2, ..., p_n$ be distinct primes and let $\zeta_1, \zeta_2, ..., \zeta_n$ be primitive roots of unity corresponding to each prime. Let $q = p_1 p_2 \dots p_n$ and let ζ be a primitive qth root of unity. We can express any power of ζ as $\zeta^k = \zeta_1^{k_1} \zeta_2^{k_2} \dots \zeta_n^{k_n}$ where $0 \le k_1 < p_1$, $0 \le k_2 < p_2$, etc. For any $x \in \mathbb{Q}[\zeta]$, we have

$$x = \sum_{k_1, k_2, k_3, \dots} (a_{k_1, k_2, k_3, \dots} (\zeta_1)^{k_1} (\zeta_2)^{k_2} (\zeta_3)^{k_3} \dots)$$

where k_j ranges from 0 to $p_j - 1$ and the $a_{k_1,k_2,k_3,\ldots}$ are rational coefficients. We will call this expression a **multisum**. For any prime $p_j \in \{p_1, \ldots, p_n\}$, we can rewrite the above expression as follows:

$$x = \sum_{k_j=0}^{p_j-1} (A_{k_j}(\zeta_j)^{k_j})$$

where

$$A_{k_j} = \sum_{\ldots k_{j-1},k_{j+1},\ldots} (a_{k_1,k_2,k_3\ldots}\cdots(\zeta_{j-1})^{k_{j-1}}(\zeta_{j+1})^{k_{j+1}}\ldots)$$

In other words, each multisum can be written as a single sum over p_jth roots of unity, where the coefficients are multisums over the other primes.

2.5 Degree of a multisum

As with sums, we can identify a primitive root g mod p_j and define the automorphism σ_j by $\sigma_j(P(\zeta_j)) = P(\zeta_j^g)$, where P is a polynomial whose coefficients are in the field of q/p_jth roots of unity. Then the multisum can be said to have a degree of d *with respect to* p_j if ${\sigma_j}^d(x) = x$ and d divides $p_j - 1$.

The entire degree of the multisum can be given by a tuple $(d_1, d_2, \ldots, d_n)$, where d_k is the degree with respect to p_k.

Note that when x has a degree of 1 with respect to p_j, it is actually in the field of q/p_jth roots of unity:

$$x = \sum_{k=0}^{p_j-1} (A_k(\zeta_j)^k) = A_0 + \sum_{k=1}^{p_j-1} A_1(\zeta_j)^k \text{ (by symmetry)}$$

$$= A_0 + A_1 \sum_{k=1}^{p_j-1} (\zeta_j)^k$$

$$= A_0 + A_1 \cdot (-1)$$

$$= A_0 - A_1$$

3 Gauss's method

Gauss's original method to find an expression for ζ, a pth root of unity (with g being a primitive root mod p), involved finding expressions for the periods (f, g^k) (k from 0 to $dc - 1$) given expressions for the periods (fc, g^k) (k from 0 to $d - 1$), where $p - 1 = efc$ and c is prime. Starting with the fact that $(p - 1, 1) = -1$, Gauss's method chooses prime factors c of $p - 1$ one by one and applies the method iteratively to find expressions for periods of increasing degrees until reaching $(1, g^k)$ (k from 0 to $p-2$), which are just the $p-1$ primitive pth roots of unity.

In the iteration step, Gauss finds expressions for the cycles (f, g^k) in terms of the cycles (fc, g^j) and cth roots of unity. Because $c < p$, we can assume that expressions for the cth roots of unity have already been found. In the below calculation, β is a primitive cth root of unity and k is a particular integer from 0 to $d - 1$.

Let $s_j = \sum_{m=0}^{c-1} \beta^{jm}(f, g^{k+dm})$ for j from 0 to $c-1$. (The values $s_0, s_1, \ldots, s_{c-1}$ are the discrete Fourier transform of the values $(f, g^k), (f, g^{k+d}), \ldots, (f, g^{k+(c-1)d})$.) Then $s_0 = (fc, g^k)$. Let $t_j = s_j^c$ for j from 1 to $c-1$. Both the s_j and t_j values are multisums in the field of pcth roots of unity. It can be shown that the t_j values have a degree of d with respect to p. Thus, we have $t_j = A + \sum_{m=0}^{d-1} A_m(fc, g^m)$, where A and the A_m are in the field $\mathbb{Q}[\beta]$.

Once we can express the t_j in terms of degree-d cycles and cth roots of unity, we have $s_j = \beta^k \sqrt[c]{t_j}$ for j from 1 to $c-1$, for particular choices of the complex cth root as given by the value of k. (The choice of each root, as given by the complex argument of s_j, can be found by numerically evaluating the s_j values from the sums.) Then we can use the inverse discrete Fourier transform to obtain $(f, g^{k+dj}) = \frac{1}{c}\sum_{m=0}^{c-1} \beta^{-jm} s_m$ for j from 0 to $c-1$. Repeating this procedure for all k from 0 to $d-1$, we now have radical expressions for all degree-dc periods (f, g^j) in terms of degree-d periods (fc, g^j).

3.1 Example: 11th roots of unity

To find radical expressions for the 11th roots of unity, we start with $g = 2$, a primitive root mod 11. For our primitive root of unity, we choose $\zeta = e^{2\pi i/11}$, which has an argument of $2\pi/11$ radians. We start with the degree-one period

$$(p-1, g^0) = (10, 1) = -1$$

whose value -1 can be determined by the minimal polynomial for ζ.

Now we need to choose a prime factor c of $p - 1 = 10$ and compute $((p-1)/c, g^j)$ for j from 0 to $c-1$. For this step, choosing $c = 5$ is usually preferred because it will give us an expression for $(2, g^j) = 2\Re\zeta^{g^j}$, which as we will see yields an expression for ζ^{g^j} with separated real and imaginary parts.

We have $d = 1, c = 5, f = 2$, so we are looking for radical expressions for:

$$\begin{aligned}(2, g^0) &= \zeta + \zeta^{10}\\ (2, g^1) &= \zeta^2 + \zeta^9\\ (2, g^2) &= \zeta^4 + \zeta^7\\ (2, g^3) &= \zeta^8 + \zeta^3\\ (2, g^4) &= \zeta^5 + \zeta^6\end{aligned}$$

We let $\beta = e^{2\pi i/5}$, a primitive 5th root of unity. Now we compute s_0, s_1, s_2, s_3, s_4 via the Fourier transform:

As mentioned above, $s_0 = (fc, g^0) = -1$:

$$\begin{aligned}s_0 &= (2, g^0) + (2, g^1) + (2, g^2) + (2, g^3) + (2, g^4)\\ &= \sum_{m=1}^{10} \zeta^m = (10, 1) = -1\end{aligned}$$

For s_1 through s_4, we have the following multisums:

$$s_1 = (2, g^0) + \beta(2, g^1) + \beta^2(2, g^2) + \beta^3(2, g^3) + \beta^4(2, g^4)$$

$$
\begin{aligned}
&= \zeta + \beta\zeta^2 + \beta^2\zeta^4 + \beta^3\zeta^8 + \beta^4\zeta^5 + \zeta^{10} + \beta\zeta^9 + \beta^2\zeta^7 + \beta^3\zeta^3 + \beta^4\zeta^6 \\
s_2 &= (2, g^0) + \beta^2(2, g^1) + \beta^4(2, g^2) + \beta(2, g^3) + \beta^3(2, g^4) \\
s_3 &= (2, g^0) + \beta^3(2, g^1) + \beta(2, g^2) + \beta^4(2, g^3) + \beta^2(2, g^4) \\
s_4 &= (2, g^0) + \beta^4(2, g^1) + \beta^3(2, g^2) + \beta^2(2, g^3) + \beta(2, g^4)
\end{aligned}
$$

We can find the multisum for $t_1 = s_1^5$ by doing algebra on the s_1 multisum (multisums for t_2, t_3, t_4 can be found in the same manner):

$$
\begin{aligned}
t_1 &= (\zeta + \beta\zeta^2 + \beta^2\zeta^4 + \beta^3\zeta^8 + \beta^4\zeta^5 + \zeta^{10} + \beta\zeta^9 + \beta^2\zeta^7 + \beta^3\zeta^3 + \beta^4\zeta^6)^5 \\
&= \dots \\
&= (1640 + 1700\beta + 2050\beta^2 + 1800\beta^3 + 1900\beta^4) + (1836 + 1830\beta + 1795\beta^2 + 1820\beta^3 + 1810\beta^4) \sum_{m=1}^{10} \zeta^m \\
&= (1640 + 1700\beta + 2050\beta^2 + 1800\beta^3 + 1900\beta^4) + (1836 + 1830\beta + 1795\beta^2 + 1820\beta^3 + 1810\beta^4) \cdot (10, 1)
\end{aligned}
$$

Thus we see that t_1 is a multisum of degree 10 with respect to ζ, and can be expressed in terms of degree-1 cycles with coefficients in $\mathbb{Q}[\beta]$. We substitute the previously calculated value $(10, 1) = -1$ and get

$$t_1 = 196 - 130\beta + 255\beta^2 - 20\beta^3 + 90\beta^4$$

Finally, we substitute in radical expressions for the 5th roots of unity, which may also be computed by Gauss's method:

$$
\begin{aligned}
\beta &= \frac{-1 + \sqrt{5} + \sqrt{-10 - 2\sqrt{5}}}{4} \\
\beta^2 &= \frac{-1 - \sqrt{5} + \sqrt{-10 + 2\sqrt{5}}}{4} \\
\beta^3 &= \frac{-1 - \sqrt{5} - \sqrt{-10 + 2\sqrt{5}}}{4} \\
\beta^4 &= \frac{-1 + \sqrt{5} - \sqrt{-10 - 2\sqrt{5}}}{4}
\end{aligned}
$$

Using algebraic manipulations of radical expressions, this substitution yields:

$$t_1 = \frac{-979 - 275\sqrt{5} - 220\sqrt{-10 - 2\sqrt{5}} + 275\sqrt{-10 + 2\sqrt{5}}}{4}$$

Expressions for t_2, t_3, and t_4 can be found in the same manner:

$$
\begin{aligned}
t_2 &= \frac{-979 + 275\sqrt{5} - 220\sqrt{-10 + 2\sqrt{5}} - 275\sqrt{-10 - 2\sqrt{5}}}{4} \\
t_3 &= \frac{-979 + 275\sqrt{5} + 220\sqrt{-10 + 2\sqrt{5}} + 275\sqrt{-10 - 2\sqrt{5}}}{4} \\
t_4 &= \frac{-979 - 275\sqrt{5} + 220\sqrt{-10 - 2\sqrt{5}} - 275\sqrt{-10 + 2\sqrt{5}}}{4}
\end{aligned}
$$

From which we obtain radical expressions for s_1, s_2, s_3, and s_4:

$$s_1 = \sqrt[5]{\frac{-979 - 275\sqrt{5} - 220\sqrt{-10 - 2\sqrt{5}} + 275\sqrt{-10 + 2\sqrt{5}}}{4}}$$

$$s_2 = \beta^4 \sqrt[5]{\frac{-979 + 275\sqrt{5} - 220\sqrt{-10 + 2\sqrt{5}} - 275\sqrt{-10 - 2\sqrt{5}}}{4}}$$

$$s_3 = \beta \sqrt[5]{\frac{-979 + 275\sqrt{5} + 220\sqrt{-10 + 2\sqrt{5}} + 275\sqrt{-10 - 2\sqrt{5}}}{4}}$$

$$s_4 = \sqrt[5]{\frac{-979 - 275\sqrt{5} + 220\sqrt{-10 - 2\sqrt{5}} - 275\sqrt{-10 + 2\sqrt{5}}}{4}}$$

In these expressions, $\sqrt[5]{t_j}$ is the unique choice of complex 5th root with an argument in $[-\pi/5, \pi/5)$. (This choice is called the **principal** 5th root.) To obtain other choices of 5th root the expression is multiplied by a power of β. One can numerically evaluate the argument of s_1, s_2, s_3, and s_4 given their definitions above in terms of periods, to find the correct choice of 5th root.

Using the inverse discrete Fourier transform, we obtain radical expressions for $(2, g^0)$ through $(2, g^4)$:

$$(2, g^0) = \frac{s_0 + s_1 + s_2 + s_3 + s_4}{5} = \frac{-1 + s_1 + s_2 + s_3 + s_4}{5}$$

$$(2, g^1) = \frac{-1 + \beta^4 s_1 + \beta^3 s_2 + \beta^2 s_3 + \beta s_4}{5}$$

$$(2, g^2) = \frac{-1 + \beta^3 s_1 + \beta s_2 + \beta^4 s_3 + \beta^2 s_4}{5}$$

$$(2, g^3) = \frac{-1 + \beta^2 s_1 + \beta^4 s_2 + \beta s_3 + \beta^3 s_4}{5}$$

$$(2, g^4) = \frac{-1 + \beta s_1 + \beta^2 s_2 + \beta^3 s_3 + \beta^4 s_4}{5}$$

Note that although s_1 through s_4 are complex numbers with nonzero imaginary parts, the values of $(2, g^0)$ through $(2, g^4)$ are real. In fact, from Euler's formula, we have $(2, k) = 2\cos(2k\pi/11)$.

Now that we have radical expressions for the periods of degree 5, we need expressions for the periods of degree 10, which are individual roots of unity.

Taking $d = 5, c = 2, f = 1$, we see that we are looking for radical expressions for:

$$(1, g^0) = \zeta, (1, g^1) = \zeta^2, (1, g^2) = \zeta^4, (1, g^3) = \zeta^8, (1, g^4) = \zeta^5$$

$$(1, g^5) = \zeta^{10}, (1, g^6) = \zeta^9, (1, g^7) = \zeta^7, (1, g^8) = \zeta^3, (1, g^9) = \zeta^6$$

Proceeding as before, we find the Fourier transform of each pair $(1, g^k), (1, g^{k+d})$ for k from 0 to $d - 1$. Because $d = 5$, this produces 5 transforms featuring all 10 periods. Note that the discrete Fourier transform of a pair of values a, b gives $a+b, a-b$.

We start with $(1, g^0), (1, g^5)$ and call the transformed values $s_{0,0}, s_{0,1}$:

$$s_{0,0} = (1, g^0) + (1, g^5) = \zeta + \zeta^{10}$$

$$s_{0,1} = (1, g^0) - (1, g^5) = \zeta - \zeta^{10}$$

For $(1, g^1), (1, g^6)$:

$$s_{1,0} = \zeta^2 + \zeta^9$$

$$s_{1,1} = \zeta^2 - \zeta^9$$

Similarly, we derive the values $s_{2,0}, s_{2,1}, s_{3,0}, s_{3,1}, s_{4,0}, s_{4,1}$ from the other three pairs.

We know $s_{k,0} = (2, g^k)$, but we need to calculate $s_{k,1}$ via $t_{k,1} := s_{k,1}^2$:

$$t_{0,1} = -2 + \zeta^2 + \zeta^9 = -2 + (2, g^1)$$

$$t_{1,1} = -2 + \zeta^4 + \zeta^7 = -2 + (2, g^2)$$

$$t_{2,1} = -2 + \zeta^3 + \zeta^8 = -2 + (2, g^3)$$

$$t_{3,1} = -2 + \zeta^5 + \zeta^6 = -2 + (2, g^4)$$

$$t_{4,1} = -2 + \zeta + \zeta^{10} = -2 + (2, g^0)$$

As expected, each $t_{k,1}$ can be expressed as a sum $A + \sum_{m=0}^{d-1} A_m(fc, g^m)$, where A and the A_m values are field $\mathbb{Q}$ adjoined by a primitive 2nd root of unity. However, because the only primitive 2nd root of unity is -1, which is already in $\mathbb{Q}$, the values of A and A_m are rational.

We then have the following expressions, which can be expanded into full radical expressions by substituting expressions for s_k and β:

$$t_{0,1} = \frac{-11 + \beta^4 s_1 + \beta^3 s_2 + \beta^2 s_3 + \beta s_4}{5}$$

$$t_{1,1} = \frac{-11 + \beta^3 s_1 + \beta s_2 + \beta^4 s_3 + \beta^2 s_4}{5}$$

$$t_{2,1} = \frac{-11 + \beta^2 s_1 + \beta^4 s_2 + \beta s_3 + \beta^3 s_4}{5}$$

$$t_{3,1} = \frac{-11 + \beta s_1 + \beta^2 s_2 + \beta^3 s_3 + \beta^4 s_4}{5}$$

$$t_{4,1} = \frac{-11 + s_1 + s_2 + s_3 + s_4}{5}$$

Continuing as we did for t_0 through t_4, we then find radical expressions for $s_{k,1}$ by finding the correct sign of the square root, which is positive in all cases but one:

$$s_{0,1} = \frac{\sqrt{-55 + 5\beta^4 s_1 + 5\beta^3 s_2 + 5\beta^2 s_3 + 5\beta s_4}}{5}$$

$$s_{1,1} = \frac{\sqrt{-55 + 5\beta^3 s_1 + 5\beta s_2 + 5\beta^4 s_3 + 5\beta^2 s_4}}{5}$$
$$s_{2,1} = \frac{\sqrt{-55 + 5\beta^2 s_1 + 5\beta^4 s_2 + 5\beta s_3 + 5\beta^3 s_4}}{5}$$
$$s_{3,1} = -\frac{\sqrt{-55 + 5\beta s_1 + 5\beta^2 s_2 + 5\beta^3 s_3 + 5\beta^4 s_4}}{5}$$
$$s_{4,1} = \frac{\sqrt{-55 + 5s_1 + 5s_2 + 5s_3 + 5s_4}}{5}$$

As it happens, the s values are all pure imaginary. In fact, $s_{k,1} = 2i\sin(2g^k\pi/11)$.

Now we take the inverse discrete Fourier transform to find radical expressions for the periods:

$$(1, g^0) = \frac{s_{0,0} + s_{0,1}}{2}$$
$$(1, g^5) = \frac{s_{0,0} - s_{0,1}}{2}$$
$$(1, g^1) = \frac{s_{1,0} + s_{1,1}}{2}$$
$$(1, g^6) = \frac{s_{1,0} - s_{1,1}}{2}$$
$$(1, g^2) = \frac{s_{2,0} + s_{2,1}}{2}$$

etc.

We now have radical expressions for all 10 primitive 11th roots of unity. If the radical expression for ζ were written out in full, it would look like (after finding a common denominator of 10):

$$\frac{\begin{array}{c} -1 + \sqrt[5]{(...t_1...)} + \beta^4\sqrt[5]{(...t_2...)} + \beta\sqrt[5]{(...t_3...)} + \sqrt[5]{(...t_4...)} \\ +\sqrt{-55 + 5\beta^4\sqrt[5]{(...t_1...)} + 5\beta^2\sqrt[5]{(...t_2...)} + 5\beta^3\sqrt[5]{(...t_3...)} + 5\beta\sqrt[5]{(...t_4...)}} \end{array}}{10}$$

where $\beta = e^{2\pi i/5}$, and $(...t_1...)$ through $(...t_4...)$ are the expressions for t_1 through t_4 found above.

4 Weber's improvement

Weber realized that Gauss's algorithm could be sped up because many parts were redundant; for any given value of k from 1 to $e-1$, instead of recomputing the sum expressions for the $t_m[k] = s_m[k]^c$ values in the Fourier transform of the (f, g^{k+dm}), we could simply take the sums $t_m[0]$ from the transform (f, g^{dm}) and replace (fc, g^j) with $(fc, g^{j+k}) = \sigma((fc, g^j))$ to get $\sigma^k(t_m[0]) = t_m[k]$. This works because $\sigma^k((f, g^{dm})) = (f, g^{k+dm})$ for each k and the isomorphism σ is preserved through application of the Fourier transform and the cth power.

5 Our algorithm

The main difference in our algorithm is how the subproblem of finding an expression for a given sum is broken into subsubproblems. Previous algorithms evaluated a multisum of degree dc by expressing it in terms of periods of degree dc, which then get expressed in terms of multisums of degree d via a Fourier transform. Instead of working on a single period, our algorithm applies the Fourier transform directly to the multisums.

Starting with a multisum m of $[p_1, p_2, ..., p]$th roots of unity of degree $[d_1, d_2, ..., dc]$ (where $p - 1 = dcf$ and c is prime), we construct expressions for $\sigma^{kd}(m)$ for k from 1 to c, where σ is the automorphism $\zeta \to \zeta^g$. Taking the discrete Fourier transform of these c values produces a set of values which we can call $s_0, s_1, \dots s_{c-1}$ as above, where s_0 is a multisum of $[p_1, p_2, ..., p]$th roots of unity and s_1 through s_{c-1} are multisums of $[p_1, p_2, ..., p, c]$th roots of unity. Then the multisums ${s_1}^c$ through ${s_{c-1}}^c$ are computed. It can be shown that s_0 is a multisum of degree $[d_1, d_2, ..., d]$ while ${s_1}^c$ through ${s_{c-1}}^c$ are multisums of degree $[d_1, d_2, ..., d, c-1]$. Thus, we can express a multisum of degree $[d_1, d_2, ..., dc]$ as a radical expression in terms of multisums of degrees $[d_1, d_2, ..., d]$ and $[d_1, d_2, ..., d, c-1]$ (which, if $c = 2$, becomes a radical expression only in terms of multisums of degree $[d_1, d_2, ..., d]$.) In this way, we can start with an unevaluated pth root of unity as a degree-$[p-1]$ multisum and call the algorithm recursively to produce sums of degree $[(p-1)/2]$, and $[(p-1)/2, 1]$ $(= [(p-1)/2])$, then sums of degree $[(p-1)/(2c)]$ and $[(p-1)/(2c), c-1]$, then sums of degree $[(p-1)/(2c), (c-1)/2]$, etc. until we reach multisums of degree $[1]$, which are just rational numbers, at which point we have an entire radical expression. These rational numbers are the base case of the recursion. Is this base case always reached? We claim that it is, and we will prove this below.

Note that we cannot start with degree-1 sums as Gauss did, because we do not know which sums will be needed to express the higher-degree multisums. Each new multisum must be generated on-the-fly because its value will not be known in advance.

5.1 Proof that our method terminates

To prove that our method always reaches the base case, we associate each multisum with an ordinal as follows:

Let m be a multisum of $[p_1, \dots, p_n]$th roots of unity with degrees $[d_1, \dots, d_n]$, where p_1 through p_n are in descending order. Then m is associated the ordinal $\omega^{p_1} d_1 + \cdots + \omega^{p_n} d_n$.

Our method involves expressing a multisum m of $[p_1, p_2, ..., p]$th roots of unity of degree $[d_1, d_2, ..., dc]$ in terms of multisums s_0 is a multisum of $[p_1, p_2, ..., p]$th roots of unity of degree $[d_1, d_2, ..., d]$ and s_j of $[p_1, p_2, ..., p, c]$th roots of unity of degree $[d_1, d_2, ..., d, c-1]$. We see that s_0 and s_j correspond to smaller ordinals than m corresponds to. We also see that the ordinal is reduced by rewriting a multisum of $[p_1, \dots, p_{n-1}, p_n]$th roots of unity of degree $[d_1, \dots, d_{n-1}, 1]$ as a multisum of $[p_1, \dots, p_{n-1}]$th roots of unity of degree $[d_1, \dots, d_{n-1}]$. Finally, in the base case when the multisum is a rational number, the corresponding ordinal is 0.
Thus, the entire process can be modeled by a tree of ordinals where any node has at most two children which are associated with smaller ordinals than the node itself. By the well-ordering principle, this tree must necessarily be finite. Thus, the recursion always reaches the base case in a finite number of steps.

5.2 Example 1: Degrees of multisums used in calculation of 11th roots of unity ($p = 11$)

A primitive 11th root of unity is a sum of 11th roots of unity of degree [10].

We choose the prime factors c of $p - 1$ in the order $2, 5$. Note that these factors can be chosen in any order, but choosing $c = 2$ first yields two separate expressions for the real and imaginary part of ζ, the 11th root of unity.

We choose $c = 2$ and reduce the problem to finding an expression for:

- A sum of 11th roots of degree 5
- A multisum of $[11, 2]$th roots of degree $[5, 1]$
  - Because the 2nd roots of unity are 1 and -1, this is equal to a second sum of 11th roots of unity of degree 5.

For each sum of 11th roots of unity of degree 5, we choose $c = 5$ and find expressions for:

- A sum of 11th roots of unity of degree 1
  - This is a rational number and its value can be found using the identity $\sum_{j=1}^{10} \zeta^j = -1$.
- A multisum of $[11, 5]$th roots of unity of degree $[1, 4]$
  - This is equal to a sum of 5th roots of unity of degree 4

For each sum of 5th roots of unity of degree 4, we choose $c = 2$ and find expressions for:

- A sum of 5th roots of unity of degree 2
- A multisum of $[5, 2]$th roots of unity of degree $[2, 1]$
  - This is equal to a sum of 5th roots of unity of degree 2

For each sum of 5th roots of unity of degree 2, we choose $c = 2$ and find expressions for:

- A sum of 5th roots of unity of degree 1
  - This is a rational number
- A multisum of $[5, 2]$th roots of unity of degree $[1, 1]$
  - This is also a rational number

Because all sums and multisums have been expressed in terms of rational numbers, we are at the end of the evaluation process.

5.3 Example 2: Degrees of multisums used in calculation of 53rd roots of unity ($p = 53$)

A primitive 53rd root of unity is a sum of 53rd roots of unity of degree 52.

For this example, we choose the prime factors c of $p - 1$ in the order $2, 13, 2$.

First we choose $c = 2$ and reduce the problem to finding an expression for:

- A sum of 53rd roots of degree 26
- A multisum of $[53, 2]$th roots of degree $[26, 1]$
  - This is equal to another sum of 53rd roots of unity of degree 26.

For each sum of 53rd roots of unity of degree 26, we choose $c = 13$ and find expressions for:

- A sum of 53rd roots of unity of degree 2
- A multisum of $[53, 13]$th roots of unity of degree $[2, 12]$

For each sum of 53rd roots of unity of degree 2, we choose $c = 2$ and find expressions for:

- A sum of 53rd roots of unity of degree 1
  - This is a rational number
- A multisum of $[53, 2]$th roots of unity of degree $[1, 1]$
  - This is also a rational number

For each multisum of $[53, 13]$th roots of unity of degree $[2, 12]$, we choose $c = 2$ and find expressions for:

- A multisum of $[53, 13]$th roots of unity of degree $[2, 6]$
- A multisum of $[53, 13, 2]$th roots of unity of degree $[2, 6, 1]$
  - This is equal to another multisum of $[53, 13]$th roots of unity of degree $[2, 6]$

For each multisum of $[53, 13]$th roots of unity of degree $[2, 6]$, we choose $c = 3$ and find expressions for:

- A multisum of $[53, 13]$th roots of unity of degree $[2, 2]$
- A multisum of $[53, 13, 3]$th roots of unity of degree $[2, 2, 2]$

For each multisum of $[53, 13]$th roots of unity of degree $[2, 2]$, we choose $c = 2$ and find expressions for:

- A multisum of $[53, 13]$th roots of unity of degree $[2, 1]$
  - This is equal to a sum of 53rd roots of unity of degree 2 (for which we can apply the rules described above).
- A multisum of $[53, 13, 2]$th roots of unity of degree $[2, 1, 1]$
  - This is also equal to a sum of 53rd roots of unity of degree 2.

For each multisum of $[53, 13, 3]$th roots of unity of degree $[2, 2, 2]$, we choose $c = 2$ and find expressions for:

- A multisum of $[53, 13, 3]$th roots of unity of degree $[2, 2, 1]$
  - This is equal to a multisum of $[53, 13]$th roots of unity of degree $[2, 2]$.
- A multisum of $[53, 13, 3, 2]$th roots of unity of degree $[2, 2, 1, 1]$
  - This is equal to another multisum of $[53, 13]$th roots of unity of degree $[2, 2]$.

We have now covered the methods to evaluate all the sums and multisums in the calculation of 53rd roots of unity.

5.4 Worked example: calculating the 11th roots of unity

An 11th root of unity ζ is a sum of degree 10. We let $c = 2$ and $d = 5$.

Let $\sigma : \mathbb{Q}[\zeta] \to \mathbb{Q}[\zeta]$ be the automorphism replacing ζ with ζ^2.

We apply the discrete Fourier transform to the values ζ and $\sigma^5(\zeta) = \zeta^{10}$:

$$s_0 := \zeta + \sigma^5(\zeta) = \zeta + \zeta^{10}$$

$$s_1 := \zeta - \sigma^5(\zeta) = \zeta - \zeta^{10}$$

Next we compute ${s_1}^c$ using algebra:

$${s_1}^c = {s_1}^2 = -2 + \zeta^2 + \zeta^9$$

Radical expression for s_0

The value s_0 is a degree-5 sum of 11th roots of unity. We let $c = 5$ and $d = 1$.

Let $\eta = e^{2\pi i/5}$ be a primitive 5th root of unity. Apply the discrete Fourier transform to the values $s_0, \sigma(s_0), \sigma^2(s_0), \sigma^3(s_0), \sigma^4(s_0)$:

$$t_0 := s_0 + \sigma(s_0) + \sigma^2(s_0) + \sigma^3(s_0) + \sigma^4(s_0) = \sum_{j=1}^{10} \zeta^j = -1$$

$$t_1 := s_0+\eta\sigma(s_0)+\eta^2\sigma^2(s_0)+\eta^3\sigma^3(s_0)+\eta^4\sigma^4(s_0) = \zeta+\zeta^{10}+\zeta^2\eta+\zeta^9\eta+\zeta^4\eta^2+\zeta^7\eta^2+\zeta^3\eta^3+\zeta^8\eta^3+\zeta^5\eta^4+\zeta^6\eta^4$$
$$t_2 := s_0+\eta^2\sigma(s_0)+\eta^4\sigma^2(s_0)+\eta\sigma^3(s_0)+\eta^3\sigma^4(s_0) = \zeta+\zeta^{10}+\zeta^2\eta^2+\zeta^9\eta^2+\zeta^4\eta^4+\zeta^7\eta^4+\zeta^3\eta+\zeta^8\eta+\zeta^5\eta^3+\zeta^6\eta^3$$
$$t_3 := s_0+\eta^3\sigma(s_0)+\eta\sigma^2(s_0)+\eta^4\sigma^3(s_0)+\eta^2\sigma^4(s_0) = \zeta+\zeta^{10}+\zeta^2\eta^3+\zeta^9\eta^3+\zeta^4\eta+\zeta^7\eta+\zeta^3\eta^4+\zeta^8\eta^4+\zeta^5\eta^2+\zeta^6\eta^2$$
$$t_4 := s_0+\eta^4\sigma(s_0)+\eta^3\sigma^2(s_0)+\eta^2\sigma^3(s_0)+\eta\sigma^4(s_0) = \zeta+\zeta^{10}+\zeta^2\eta^4+\zeta^9\eta^4+\zeta^4\eta^3+\zeta^7\eta^3+\zeta^3\eta^2+\zeta^8\eta^2+\zeta^5\eta+\zeta^6\eta$$

We see that t_0 is a sum of degree 1 and is therefore rational (equal to -1).

Find ${t_1}^5$ through ${t_4}^5$:

$${t_1}^5 = (1640 + 1700\eta + 2050\eta^2 + 1800\eta^3 + 1900\eta^4) + (1836 + 1830\eta + 1795\eta^2 + 1820\eta^3 + 1810\eta^4) \sum_{j=1}^{10} \zeta^j$$

$$= -196 - 130\eta + 255\eta^2 - 20\eta^3 + 90\eta^4$$

$$t_2{}^5 = (1640 + 1800\eta + 1700\eta^2 + 1900\eta^3 + 2050\eta^4) + (1836 + 1820\eta + 1830\eta^2 + 1810\eta^3 + 1795\eta^4)\sum_{j=1}^{10}\zeta^j$$

$$= -196 - 20\eta - 130\eta^2 + 90\eta^3 + 255\eta^4$$

$$t_3{}^5 = (1640 + 2050\eta + 1900\eta^2 + 1700\eta^3 + 1800\eta^4) + (1836 + 1795\eta + 1810\eta^2 + 1830\eta^3 + 1820\eta^4)\sum_{j=1}^{10}\zeta^j$$

$$= -196 + 255\eta + 90\eta^2 - 130\eta^3 - 20\eta^4$$

$$t_4{}^5 = (1640 + 1900\eta + 1800\eta^2 + 2050\eta^3 + 1700\eta^4) + (1836 + 1810\eta + 1820\eta^2 + 1795\eta^3 + 1830\eta^4)\sum_{j=1}^{10}\zeta^j$$

$$= -196 + 90\eta - 20\eta^2 + 255\eta^3 - 130\eta^4$$

Radical expression for $t_1{}^5$

The value $t_1{}^5$ is a degree-4 sum of 5th roots of unity. We let $c = 2$ and $d = 2$.

Let $\rho : \mathbb{Q}[\eta] \to \mathbb{Q}[\eta]$ be the automorphism replacing η with η^2.

Apply the discrete Fourier transform to the values $t_1{}^5$ and $\rho^2(t_1{}^5)$:

$$v_0 := t_1{}^5 + \rho^2(t_1{}^5) = -392 - 40\eta + 235\eta^2 + 235\eta^3 - 40\eta^4$$

$$v_1 := t_1{}^5 - \rho^2(t_1{}^5) = -220\eta + 275\eta^2 - 275\eta^3 + 220\eta^4$$

Find $v_1{}^2$:

$$v_1{}^2 = -248050 + 196625\eta - 72600\eta^2 - 72600\eta^3 + 196625\eta^4$$

Radical expression for v_0

The value v_0 is a degree-2 sum of 5th roots of unity. We let $c = 2$ and $d = 1$.

Apply the discrete Fourier transform to the values v_0 and $\rho(v_0)$:

$$v_0 + \rho(v_0) = -784 + 195\sum_{j=0}^{4}\eta^j = -979$$

$$v_0 - \rho(v_0) = -275\eta + 275\eta^2 + 275\eta^3 - 275\eta^4$$

Find $(v_0 - \rho(v_0))^2$:

$$(v_0 - \rho(v_0))^2 = -378125\sum_{j=0}^{4}\eta^j = 378125$$

Thus, we have $v_0 = \frac{-979-\sqrt{378125}}{2} = \frac{-979-275\sqrt{5}}{2}$.

Radical expression for $v_1{}^2$

The value $v_1{}^2$ is a degree-2 sum of 5th roots of unity. We let $c = 2$ and $d = 1$.

Apply the discrete Fourier transform to the values $v_1{}^2$ and $\rho(v_1{}^2)$:

$$v_1{}^2 + \rho(v_1{}^2) = -496100 + 124025\sum_{j=0}^{4}\eta^j = -620125$$

$$v_1{}^2 - \rho(v_1{}^2) = 269225\eta - 269225\eta^2 - 269225\eta^3 + 269225\eta^4$$

Find $(v_1{}^2 - \rho(v_1{}^2))^2$:

$$(v_1{}^2 - \rho(v_1{}^2))^2 = -362410503125\sum_{j=0}^{4}\eta^j = 362410503125$$

Thus, we have $v_1{}^2 = \frac{-620125+\sqrt{362410503125}}{2} = \frac{-620125+269225\sqrt{5}}{2}$ and $v_1 = \frac{-55\sqrt{-410+178\sqrt{5}}}{2}$.

Thus, we have $t_1{}^5 = \frac{v_0+v_1}{2} = \frac{-979-275\sqrt{5}-55\sqrt{-410+178\sqrt{5}}}{4}$ and $t_1 = \eta\sqrt[5]{\frac{-979-275\sqrt{5}-55\sqrt{-410+178\sqrt{5}}}{4}}$.

Using the same methods, we can find:

$$t_2 = \eta\sqrt[5]{\frac{-979+275\sqrt{5}-55\sqrt{-410-178\sqrt{5}}}{4}}$$

$$t_3 = \eta^4\sqrt[5]{\frac{-979+275\sqrt{5}+55\sqrt{-410-178\sqrt{5}}}{4}}$$

$$t_4 = \eta^4\sqrt[5]{\frac{-979-275\sqrt{5}+55\sqrt{-410+178\sqrt{5}}}{4}}$$

Thus, we have $s_0 = \frac{-1+t_1+t_2+t_3+t_4}{5}$, which we can expand into a full radical expression using the values above.

Radical expression for $s_1{}^2$

The value $s_1{}^2$ is also a degree-5 sum of 11th roots of unity. We let $c = 5$ and $d = 1$.

Apply the discrete Fourier transform to the values $s_1{}^2, \sigma(s_1{}^2), \sigma^2(s_1{}^2), \sigma^3(s_1{}^2), \sigma^4(s_1{}^2)$:

$$u_0 := s_1{}^2 + \sigma(s_1{}^2) + \sigma^2(s_1{}^2) + \sigma^3(s_1{}^2) + \sigma^4(s_1{}^2) = -10 + \sum_{j=1}^{1} 0\zeta^j = -11$$

$$u_1 := s_1{}^2 + \eta\sigma(s_1{}^2) + \eta^2\sigma^2(s_1{}^2) + \eta^3\sigma^3(s_1{}^2) + \eta^4\sigma^4(s_1{}^2)$$

$$= -2 + \zeta^2 + \zeta^9 - 2\eta + \zeta^4\eta + \zeta^7\eta - 2\eta^2 + \zeta^3\eta^2 + \zeta^8\eta^2 - 2\eta^3 + \zeta^5\eta^3 + \zeta^6\eta^3 - 2\eta^4 + \zeta\eta^4 + \zeta^{10}\eta^4$$

$$u_2 := {s_1}^2 + \eta^2\sigma({s_1}^2) + \eta^4\sigma^2({s_1}^2) + \eta\sigma^3({s_1}^2) + \eta^3\sigma^4({s_1}^2)$$

$$= -2 + \zeta^2 + \zeta^9 - 2\eta + \zeta^5\eta + \zeta^6\eta - 2\eta^2 + \zeta^4\eta^2 + \zeta^7\eta^2 - 2\eta^3 + \zeta\eta^3 + \zeta^{10}\eta^3 - 2\eta^4 + \zeta^3\eta^4 + \zeta^8\eta^4$$

$$u_3 := {s_1}^2 + \eta^3\sigma({s_1}^2) + \eta\sigma^2({s_1}^2) + \eta^4\sigma^3({s_1}^2) + \eta^2\sigma^4({s_1}^2)$$

$$= -2 + \zeta^2 + \zeta^9 - 2\eta + \zeta^3\eta + \zeta^8\eta - 2\eta^2 + \zeta\eta^2 + \zeta^{10}\eta^2 - 2\eta^3 + \zeta^4\eta^3 + \zeta^7\eta^3 - 2\eta^4 + \zeta^5\eta^4 + \zeta^6\eta^4$$

$$u_4 := {s_1}^2 + \eta^4\sigma({s_1}^2) + \eta^3\sigma^2({s_1}^2) + \eta^2\sigma^3({s_1}^2) + \eta\sigma^4({s_1}^2)$$

$$= -2 + \zeta^2 + \zeta^9 - 2\eta + \zeta\eta + \zeta^{10}\eta - 2\eta^2 + \zeta^5\eta^2 + \zeta^6\eta^2 - 2\eta^3 + \zeta^3\eta^3 + \zeta^8\eta^3 - 2\eta^4 + \zeta^4\eta^4 + \zeta^7\eta^4$$

We see that u_0 is a sum of degree 1 and is therefore rational (equal to -11).

Find ${u_1}^5$ through ${u_4}^5$:

$${u_1}^5 = (-29460 - 29400\eta - 29050\eta^2 - 29300\eta^3 - 29200\eta^4) + (2946 + 2940\eta + 2905\eta^2 + 2930\eta^3 + 2920\eta^4)\sum_{j=1}^{10}\zeta^j$$

$$= -32406 - 32340\eta - 31955\eta^2 - 32230\eta^3 - 32120\eta^4$$

$${u_2}^5 = (-29460 - 29300\eta - 29400\eta^2 - 29200\eta^3 - 29050\eta^4) + (2946 + 2930\eta + 2940\eta^2 + 2920\eta^3 + 2905\eta^4)\sum_{j=1}^{10}\zeta^j$$

$$= -32406 - 32230\eta - 32340\eta^2 - 32120\eta^3 - 31955\eta^4$$

$${u_3}^5 = (-29460 - 29050\eta - 29200\eta^2 - 29400\eta^3 - 29300\eta^4) + (2946 + 2905\eta + 2920\eta^2 + 2940\eta^3 + 2930\eta^4)\sum_{j=1}^{10}\zeta^j$$

$$= -32406 - 31955\eta - 32120\eta^2 - 32340\eta^3 - 32230\eta^4$$

$${u_4}^5 = (-29460 - 29200\eta - 29300\eta^2 - 29050\eta^3 - 29400\eta^4) + (2946 + 2905\eta + 2920\eta^2 + 2940\eta^3 + 2930\eta^4)\sum_{j=1}^{10}\zeta^j$$

$$= -32406 - 32120\eta - 32230\eta^2 - 31955\eta^3 - 32340\eta^4$$

Radical expression for ${u_1}^5$

The value ${u_1}^5$ is a degree-4 sum of 5th roots of unity. We let $c = 2$ and $d = 2$.

Apply the discrete Fourier transform to the values ${u_1}^5$ and $\rho^2({u_1}^5)$:

$$w_0 := {u_1}^5 + \rho^2({u_1}^5) = -64812 - 64460\eta - 64185\eta^2 - 64185\eta^3 - 64460\eta^4$$

$$w_1 := {u_1}^5 - \rho^2({u_1}^5) = -220\eta + 275\eta^2 - 275\eta^3 + 220\eta^4$$

Find ${w_1}^2$:

$${w_1}^2 = -248050 + 196625\eta - 72600\eta^2 - 72600\eta^3 + 196625\eta^4$$

The value w_0 is a degree-2 sum of 5th roots of unity. We let $c = 2$ and $d = 1$.

Apply the discrete Fourier transform to the values w_0 and $\rho(w_0)$:

$$w_0 + \rho(w_0) = -129624 - 128645 \sum_{j=0}^{4} \eta^j = -979$$

$$w_0 - \rho(w_0) = -275\eta + 275\eta^2 + 275\eta^3 - 275\eta^4$$

Find $(w_0 - \rho(w_0))^2$:

$$(w_0 - \rho(w_0))^2 = -378125 \sum_{j=0}^{4} \eta^j = 378125$$

Thus, we have $w_0 = \frac{-979-\sqrt{378125}}{2} = \frac{-979-275\sqrt{5}}{2}$

Radical expression for w_1

Comparing the formula for w_1 with that of v_1, we see that $w_1 = v_1 = \frac{-55\sqrt{-410+178\sqrt{5}}}{2}$.

Thus, we have ${u_1}^5 = \frac{w_0+w_1}{2} = \frac{-979-275\sqrt{5}-55\sqrt{-410+178\sqrt{5}}}{4}$ and $u_1 = \sqrt[5]{\frac{-979-275\sqrt{5}-55\sqrt{-410+178\sqrt{5}}}{4}}$.

Using the same methods, we can find:

$$u_2 = \eta^4 \sqrt[5]{\frac{-979 + 275\sqrt{5} - 55\sqrt{-410 - 178\sqrt{5}}}{4}}$$

$$u_3 = \eta \sqrt[5]{\frac{-979 + 275\sqrt{5} + 55\sqrt{-410 - 178\sqrt{5}}}{4}}$$

$$u_4 = \sqrt[5]{\frac{-979 - 275\sqrt{5} + 55\sqrt{-410 + 178\sqrt{5}}}{4}}$$

We see that ${t_j}^5 = {u_j}^5$ for j from 1 to 4, and $u_j = \eta^{-j} t_j$

Thus, we have $s_1 = \sqrt{\frac{-11+\eta^4 t_1+\eta^3 t_2+\eta^2 t_3+\eta t_4}{5}}$, which we can expand into a full radical expression using the values above.

Finally, we can combine the expressions for s_0 and s_1 to obtain a full radical expression for $\zeta = \frac{s_0+s_1}{2}$.

If the radical expression for ζ were written out in full, it would look like:

$$\frac{-1 + \eta \sqrt[5]{{t_1}^5} + \eta \sqrt[5]{{t_2}^5} + \eta^4 \sqrt[5]{{t_3}^5} + \eta^4 \sqrt[5]{{t_4}^5} + \sqrt{-55 + 5\sqrt[5]{{t_1}^5} + 5\eta^4 \sqrt[5]{{t_2}^5} + 5\eta \sqrt[5]{{t_3}^5} + 5\sqrt[5]{{t_4}^5}}}{10}$$

with ${t_1}^5$ through ${t_4}^5$ replaced by their corresponding radical expressions.

Comparing this with the result found by Gauss's method, we see that it takes the same form consisting of a sum of four 5th roots, and then another sum, under a square root, of four 5th roots using the same radicands but different choices of root. The only difference is that the expression under the radicals has changed. Using Gauss's method, this expression was:

$$\frac{-979 \pm_a 275\sqrt{5} \pm_b (220\sqrt{-10 \pm_a 2\sqrt{5}} \pm_a 275\sqrt{-10 \mp_a 2\sqrt{5}})}{4}$$

The expression that we obtain is:

$$\frac{-979 \pm_a 275\sqrt{5} \pm_b 55\sqrt{-410 \mp_a 178\sqrt{5}}}{4}$$

Here, the $\pm_{a,b}$ represent two independent choices of sign producing four possibilities. These two expressions can be shown to be equal in each of these four cases by algebraically expanding the squares of $220\sqrt{-10 \pm_a 2\sqrt{5}} \pm_a 275\sqrt{-10 \mp_a 2\sqrt{5}}$ and $55\sqrt{-410 \mp_a 178\sqrt{5}}$. The process of squaring, simplifying, and taking the square root is a well-known technique for radical simplification. However, our method is more powerful than this simple technique because it also allows for the simplification of sums of cube roots and higher.

6 Radical expression complexity metric

When studying the radical expressions produced by the nth roots of unity, we developed a simple formula that models the complexity of any radical-sum expression:

Let R' be the set of radical-sum expressions.

- If $expr$ is an integer, then $size(expr) = 1$.
- For any $expr \in R'$, $m \in \digamma$, $n \in \mathbb{N}$ with $n > 1$, and $j \in \{0, \ldots, n-1\}$, $size(expr) = size(z\beta^j \sqrt[n]{(}expr))$.
- For any $expr1, expr2 \in R'$, $size((expr1) + (expr2)) = size((expr1) - (expr2)) = size(expr1) + size(expr2)$.
- For any $expr \in R'$ and $n \in \mathbb{N}$, $size((expr)/(n)) = size(expr)$.

Let p be prime. It follows from the above definition that the complexity of the radical expression for any degree-d sum of primitive pth roots of unity calculated via our algorithm is given by $f(p, d)$, where:

$$f(p, 1) = 1$$

$$f(p, n) = f(p, n/c) \cdot (1 + f(c, c-1) \cdot (c-1))$$

Here, c is any prime factor of n. Due to the uniqueness of prime factoring, the final value of $f(p, n)$ is independent of which prime factor is chosen.

In particular, the complexity of the radical expression for any primitive pth root of unity is given by $f(p, p-1)$.

We wrote a Python program to find radical expressions for roots of unity using Weber's method and expand out products to form radical-sum expressions. We also wrote code to obtain the length of each of the resulting expressions. The code is available at `https://github.com/ericbinnendyk/roots_of_unity/` in the files `unrefined_nth_roots_improvement_test.py` and `expr_metrics.py`. We compared the size of each expression to the size of the expression for the same value produced using our own method using our formula:

p	Size using Gauss/Weber method	Size using our method (from formula)
2	1	1
3	2	2
5	4	4
7	10	10
11	50	34
13	16	20
17	20	16
19	178	50
23	6410	682
29	920	244
31	1282	170
37	420	100
41	296	136
43	N/A	610
47	N/A	30010
53	4726	964
59	N/A	13666
61	3444	340
67	N/A	3410
73	1636	200
97	904	160
193	4172	320
257	4196	256

7 Pseudocode

Here is pseudocode for evaluating a multisum to radicals using our algorithm. A Python implementation of this algorithm is also available at `https://github.com/ericbinnendyk/roots_of_unity/` in the file `refined_nth_roots.py`.

```
# Auxilliary functions used in code:
#   len(a): returns the length of a 1-dimensional array
#   factorize(n): returns the prime factors of integer n in an array
#   max(a): returns the maximum element of an array
#   primitive_root(p): returns a primitive root modulo the prime p
#   sigma(A, index, g): returns a multisum which is the image of multisum A
    under the automorphism (zeta) -> (zeta)^g, where zeta is the root of
   unity described by the index-th dimension in A
#   a.insert(index, n): inserts element n into array at index i
#   epsilon - a very small positive real floating-point number
#   sum(a) - returns the sum of elements in array
#   gcd(a) - returns the GCD of all elements in array
#   multisum_power(A, n): returns a multisum equal to A^n, where A is a
   multisum
#   radical_root(n, expr): returns a radical expression for the nth root of
    expr, with attribute root_choice for the choice of complex nth root
#   evaluate(expr): evaluates expr to a complex floating-point value, where
    expr can be a radical expression or a multisum
#   abs(n): absolute value of n
#   r(n, j): returns the floating-point value of e^(2*pi*i*j/n)

# A: an n-dimensional array representing a multisum of (q_1)th, (q_2)th,
   ..., (q_n)th roots of unity (zeta_1 := e^(2*pi*i/q_1) through zeta_n :=
   e^(2*pi*i/q_n)) where q_1 through q_n are prime. Each entry is an
   integer. The entry A[k_1; k_2; ...; k_n] is the coefficient on the term
   (zeta_1)^k_1*(zeta_2)^k_2*...*(zeta_n)^k_n and the i-th index ranges
   from 0 to q_i - 1.
# dims: list of the range of each dimension of A; [q_1, q_2, ..., q_n].
   Each entry is prime.
# degrees: degrees of the sum with respect to each index. A degree of d for
    the i-th index means that the sum is invariant under d applications of
   the automorphism (zeta_i) -> (zeta_i)^g, where g is a primitive root
   modulo q_i.
def multisum_to_radicals(A, dims, degrees):
    # choose a value of q_i to reduce the degree of the multisum with
       respect to (q_i)th roots of unity. In this code, q_1 is chosen.
    # The algorithm works for any choice, but the resulting radical
       expression will be different.
    q_1 = dims[0]
    d = degrees[0]

    # Check if the sum has a degree of 1 wrt. the first index. If it is,
       the multisum can be simplified by eliminating the first index range
       and (zeta_1)^k terms.
    # BASE CASE: If there is only one index (i.e. the multisum is a sum),
       it is simplified to a single integer. This integer is the radical
       expression obtained from evaluating the sum, and is then returned.
    if d == 1 and len(dims) == 1:
        return A[0] - A[1]
    if d == 1 and len(dims) != 1:
        # Produce two subarrays containing all elements of A whose initial
           index is equal to 0 and 1, respectively.
        # Set A to the element-wise difference of these subarrays. This is
           our simplified multisum.
        A = A[0; 0..q_2 - 1; ...; 0..q_n - 1] .- A[1; 0..q_2 - 1; ...; 0..
           q_n - 1]
        # Evaluate the radical expression for the simplified multisum.
    A_radicals = multisum_to_radicals(A, dims[1..len(dims) - 1],
       degrees[1..len(degrees) - 1])
    return A_radicals

# Choose a prime factor c of d and reduce d by that factor.
# The algorithm works for any choice, but I choose 2 if d == q_1 - 1 (
   so the expression will separate into real and imaginary parts), and
   the greatest prime factor otherwise (to match the historical results
    of Gauss et al.)
# Note: the choice of 2 does not work when q_1 - 1 is odd (i.e. q_1 ==
   2), but that case has already been dealt with above.
if d == q_1 - 1:
    c = 2
else:
    facts = factorize(d)
    c = max(facts)
d = d / c

g = primitive_root(q_1)

# find the conjugates of A by applying the automorphism zeta -> zeta^g,
    k*d times, where zeta is a (q_1)th root of unity.
A_conj = Array.new(size=c)
for k from 0 to c - 1:
    A_conj[k] = sigma^(k*d)(A, index=1, g)

# find dimensions and degrees of S[0] through S[c - 1], the discrete
   Fourier transform of the values in A_conj
# S[0] and S[j]^c (for j = 1 through c - 1) all have degree d with
   respect to q_1, or 1/c of the degree of A
# Additionally, if c != 2 then S[j]^c has an extra dimension with range
    equal to c and degree equal to c - 1. (If c == 2 then the degree of
    1 means that this extra dimension can be, and is, automatically
   eliminated in the code that follows)
S_0_dims = dims
S_j_dims = dims
if c != 2:
    S_j_dims.insert(0, c)
S_0_degrees = degrees
S_0_degrees[0] = d
S_j_power_c_degrees = S_0_degrees
if c != 2:
    S_j_power_c_degrees.insert(0, c - 1)

# construct multisums for S[0] through S[c - 1]
S = Array.new(size=c)
```

```
if c == 2:
    S[0] = A_conj[0] .+ A_conj[1]
    S[1] = A_conj[0] .- A_conj[1]
else:
    S[0] = sum(A_conj)
    for j from 1 to c - 1:
        S[j] = Array.new(dims=S_j_dims)
        for k from 0 to c - 1:
            S[j][(j * k) mod c; 0..q_1 - 1; 0..q_2 - 1; ...; 0..q_n -
                1] = A_conj[k]

# calculate radical expressions for S[0] through S[c - 1]
S_radicals = Array.new(size=c)
S_radicals[0] = multisum_to_radicals(S[0], dims, S_0_degrees)
for j from 1 to c - 1:
    # find the GCD of all coefficients in S[j] and factor it out before
        finding the radical expression
    # This step is not necessary, but it allows the S[j] radical
       expressions to be things like 275*sqrt(5) instead of sqrt
       (378125)
    # Note: The GCD function must return 0 if all the coefficients are
       0
    divisor = gcd(S[j])
    if divisor == 0:
        # every coefficient in S[j] is 0
        S_radicals[j] = 0
    else:
        # divide each coefficient of S[j] by divisor
        S_j_div = (1/divisor)*S[j]
        # calculate the multisum for (1/divisor*S[j])^c
        S_j_div_power_c = multisum_power(S_j_div, c)

        # Calculate radical expression for (S[j]/div)^c and then for S[
           j]
        S_j_div_power_c_radicals = multisum_to_radicals(S_j_div_power_c
           , S_j_dims, S_j_power_c_degrees)
        S_j_div_radicals = radical_root(c, S_j_div_power_c_radicals)
        S_radicals[j] = div*S_j_div_radicals

        # Calculate the correct choice of cth root by numerically
           evaluating the multisum
        S_j_numeric = evaluate(S[j])
        S_j_radicals_numeric = evaluate(S_radicals[j])
        # multiply S_j_radicals_numeric by each (q_1)th root of unity
           until the two floating-point results are close enough to be
           considered equal
```

```
            k = 0
            while abs(S_j_numeric - S_j_radicals_numeric) > epsilon:
                if k == q_1:
                    # we have tried multiplying by all q_1 roots of unity
                    print("Error: Unable to resolve expression")
                    exit()
                S_j_radicals_numeric *= r(q_1, 1)
                k += 1
            # indicate jth choice of (q_1)th root
            S_radicals[j].root_choice = k

    # use inverse discrete Fourier transform to find radical expression for
        A
    A_radicals = sum(S_radicals) / c
    return A_radicals
```

8 Discussion

We can apply similar optimizations to our algorithm as Weber did to eliminate redundancies.

Even though we have measured the expressions generated by our algorithm to be shorter, there are a few potential issues with the expression complexity metric we used. For instance, the metric requires that the radical expression does not contain unexpanded products of sums (e.g. $(1+\sqrt{2})(\sqrt{2}+\sqrt{3})$). To measure the size of expressions produced by Gauss/Weber's method, all such products were expanded into sums, affecting the overall length of the expression. Furthermore, our method can produce radical expressions with quite large integers (a 23rd root of unity contains integers that are 98 digits long) but our size metric does not take integer size into account.

It is interesting to note that the expression is "customizable" depending on the order in which the prime factors of $p1$ are chosen. In particular, by choosing $c = 2$ when $d = p - 1$, we always produce an expression which is a sum of real and imaginary parts. We can also customize the expression for a multisum by choosing which of its degrees to reduce. The complexity of the resulting expression does not seem to depend on either of these choices.

Besides prime roots of unity, we can use this method to find a radical expression for any value contained within a field which is the product of multiple extensions to $\mathbb{Q}$ using prime roots of unity. When n is a product of distinct primes (a square-free number), every nth root of unity is equal to a product of prime roots of unity. This can be proven by repeated applications of the Chinese Remainder Theorem [8]. Thus, our method can be used to find radical expressions for nth roots of unity when n is any square-free integer.

In addition, our method can be adapted to express many trigonometric values in radicals. If $\zeta = e^{2\pi i/n}$, the values $\cos(2k\pi/n) = \frac{\zeta^k+\zeta^{-k}}{2}$ and $i\sin(2k\pi/n) = \frac{\zeta^k-\zeta^{-k}}{2}$ are in $\mathbb{Q}[\zeta]$ for every integer k from 0 to $n-1$. Due to closure under division, the values $i\tan(2k\pi/n), \sec(2k\pi/n), i\csc(2k\pi/n), i\cot(2k\pi/n) \in \mathbb{Q}[\zeta]$ as well. Thus, if n is square-free, all these values can be expressed in radicals using our method.

9 Conclusion

In this paper, we have identified a new method for finding radical expressions for roots of unity with prime degree, as well as for general members of the cyclotomic field of these roots. We have shown that this algorithm produces shorter expressions than Gauss's algorithm under a particular metric for expression complexity, and discussed possible drawbacks of using this metric. We have also discussed this method's flexibility and potential to be adapted to trigonometric functions and squarefree composite roots of unity.

When we take the nth root of a complex value, our code uses floating-point computation to identify the correct choice of complex root by comparing each approximate value to the desired result. This computation is the main limiting factor keeping our method from working for larger primes. Future work could include redesigning this part of the algorithm so that it does not use floating-point computations.

We have also not discussed the prospect of finding radical expressions for nth roots of unity when n is not squarefree. If n has a repeated prime factor p, one can of course find an nth roots of unity by taking the pth root of an n/pth root of unity. However, this method does not produce expressions of equal size for every member of the cyclotomic field. Future research could involve improving the method that we describe to produce radical expressions of uniform complexity for any cyclotomic field. By the Kronecker-Weber theorem, every algebraic number with a radical expression belongs to some cyclotomic field [9]. Thus, this method could be used to find a radical expression for every number that has one, simply by expressing it as a sum of roots of unity.

References

[1] Gauss, Carl F. *Disquisitiones Arithmeticae.* Yale University Press. pp. 359-360, 1965. ISBN 0-300-09473-6.

[2] Lynn, Ben. "Number Theory - The Heptadecagon." Stanford Applied Cryptography Group, `https://crypto.stanford.edu/pbc/notes/numbertheory/17gon.html`. Accessed August 17, 2019.

[3] Lynn, Ben. "Number Theory - Roots of Unity." Stanford Applied Cryptography Group, `https://crypto.stanford.edu/pbc/notes/numbertheory/rootsunity.html`. Accessed August 17, 2019.

[4] Lynn, Ben. "Miscellany - Roots of Unity." Stanford Applied Cryptography Group, `https://crypto.stanford.edu/pbc/notes/misc/rootsunity.html`. Accessed August 17, 2019.

[5] Weber, Andreas; Keckeisen, Michael. "Solving Cyclotomic Polynomials by Radical Expressions" (PDF). Accessed August 17, 2019.

[6] Weber, Andreas. "Computing radical expressions for roots of unity." *ACM SIGSAM Bulletin*, 30, 1996, pp. 11-20. 10.1145/240065.240070.

[7] Lau Jing Feng. "On solvable septics." *ScolarBank@NUS Repository.* January 7, 2005.

[8] Lynn, Ben. "Number Theory - The Chinese Remainder Theorem." Stanford Applied Cryptography Group, `https://crypto.stanford.edu/pbc/notes/numbertheory/crt.html`. Accessed May 11, 2020.

[9] Stover, Christopher. "Kronecker-Weber Theorem." From *MathWorld*–A Wolfram Web Resource, created by Eric W. Weisstein. `https://mathworld.wolfram.com/Kronecker-WeberTheorem.html`. Accessed May 11, 2020.