The Galios Group of Cyclotomic Fields of Fermat Primes

Brown, David Madden, Daniel

August 10, 2001

Contents

1 Introduction

This paper is a discussion of the research done by the authors over the summer of 2001. It discusses the calculation of nice, real expressions involving nothing worse than radicals for $\cos\left(\frac{2\pi}{p}\right)$ where p is a Fermat prime. Algorithms for the ruler and compass constructions of the corresponding regular n-gons are given as well.

2 History

Plato considered the straight line and circle the only "perfect" geometrical figures, and this restricted the tools available for the constructions of ancient Greek geometry to two: the unmarked ruler and the compass. The restrictions were that a line could be drawn through any two points and a circle could be drawn centered at any point and with a radius equal to the distance between any two points. Any intersection of lines or circles was considered a new point. The Greeks were able to perform a wide range of constructions with these self-imposed limitations including dividing a line into arbitrarily many equal segments, perpendicular and parallel lines, and constructing a square with area equal to any given polygon. Unfortunately, they never formulated their ideas algebraically and there remained many unanswered questions, such as how does one trisect an angle or construct a square with area equal to that of a circle and for which values of n the regular n-gon was constructible.

Impossibility proofs were eventually given for the first two of these unanswered problems. As for the third, ruler and compass constructions for the regular 3, 5, and 15-gon, and for any 2n-gon given the construction of an n-gon, were know to the ancient Greeks. The solution progressed little until March 30, 1796 when a young Gauss discovered that the regular 17-gon could be constructed. He was nineteen years old at the time and was so pleased with his discovery that he decided to dedicate his life to mathematics, previously unable to decide between that and the study of languages. Gauss later proceeded to definitively show in his *Disquisitiones Arithmeticae*, reprinted as Gauss [1], the exact values of n for which ruler and compass constructions of the regular n-gon were constructible; he showed that a regular n-gon is constructible if and only if

$$n = 2^r p_1 \dots p_s$$

where $p_i = 2^{2^n} + 1$ (p_i is a Fermat prime) and $n, r, s \in \mathbb{N}$.

Thus, the problem reduced to one of number theory: which Fermat numbers are prime? Pierre de Fermat made the observation in 1640 that the first five Fermat numbers, 3, 5, 17, 257, and 65537 were all prime and conjectured that all Fermat numbers were prime, but this was proved false by Euler in 1732. These remain the only know Fermat primes, and a proof of such would finally solve the ancient Greek question of for which values of n is the regular n-gon is constructible.

3 Constructing an n-gon

The vertices of a regular n-gon are precisely the n^{th} roots of unity in the complex plane. If the first root can be constructed then the remaining roots can be constructed by redefining the axes through the origin and the constructed vertex and repeating the procedure on the new axes. Now, Euler's formula gives $\zeta_n = \exp^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, so if the point $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ can be constructed, then the entire n-gon can as well. Also, if just the point $(\cos\frac{2\pi}{n}, 0)$ can be constructed, then the intersection of a line perpendicular to the x-axis through this point and a circle centered at the origin with a radius of one gives the desired vertex.

Formulated algebraically, a ruler and compass construction allows the following actions: addition, subtraction, multiplication and division of any two points, taking the inverse and square root of a point, and the solution of a quadratic or linear equation using coefficients of any constructible points, in addition to the operations mentioned in section 2. Also, given two points, an axes can be constructed through them using one point as the origin and another as the point (1,0). Examples of some of these procedures are given in [2].

Given the points (0,0) and (1,0), we would like to construct the point $(\cos\frac{2\pi}{n}, 0)$. This can be done if and only if $\cos\frac{2\pi}{n}$ is at worst a radical expression. If a radical expression is given or found then a rather unaesthetic construction of the n-gon is to simply construct the sum of rationals and roots which make up this expression. The problem thus reduces to finding a radical expression for $\cos\frac{2\pi}{n}$ and this will be center of this paper. Only the cases where n is a single fermat prime will be considered, since constructions of products of the primes and powers of two can be easily derived from constructions of p-gons.

Again, constructions for the 3 and 5-gons are simple and were known to the ancient Greeks. Since then, many constructions for the 17-gon have been given, the earliest published being that of Huguenin [3] in 1803. Richelot [4] published a series of papers under a very long title concerning the construction of a regular 257-gon. His manuscript was huge, but his construction was eventually verified. Bell [5] mentions an overzealous research student being given the construction of the 65537-gon as a project to get him out of his professors hair and returning with one twenty years later. Though this story is a bit apocryphal, it is not far from the truth; Professor Hermes of Linger spent ten years working on this problem. The last line of his transcript translates as "I am done," but many argue that in his dialect the more accurate translation is "I give up." Needless to say his manuscript has yet to be verified, and the problem of actually constructing a 65537-gon remains open.

4 Calculating the Radical Expression for $\cos\left(\frac{2\pi}{p}\right)$

Appealing to Euler and his formula relating imaginary arguments of exponents and the cos and sin functions provides a starting point for the calculation of a

radical expression for $\cos(\frac{2\pi}{p})$. A consequence of Euler's formula is the relation

$$2\cos(\frac{2\pi}{p}) = e^{\frac{2\pi i}{p}} + e^{-\frac{2\pi i}{p}} = \zeta_p + \zeta_p^{-1}.$$

Euler's formula gives another useful result:

$$\zeta_p = e^{\frac{2\pi i}{p}} = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p}),$$

therefore

$$(\zeta_p)^p = (e^{\frac{2\pi i}{p}})^p = e^{\frac{2\pi ip}{p}} = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1,$$

and

$$\frac{(\zeta_p)^p - 1}{\zeta_p - 1} = (\zeta_p^{p-1} + \ldots + \zeta_p + 1) = 0. \quad (1)$$

Thus, if the expression $(\zeta_p^{p-1} + \ldots + \zeta_p + 1)$ can be manipulated such that $\zeta_p + \zeta_p^{-1}$ is the solution of a quadratic equation then the problem is solved. When appropriate, we will work in terms of polynomials in x evaluated at ζ_p.

4.1 Solving for $\cos(\frac{2\pi}{3})$ and $\cos(\frac{2\pi}{5})$

For the $p = 3$ and $p = 5$ cases it is simple to do this through mere algebraic manipulation. For the $p = 3$ case, we have

$$x^2 + x + 1 = x((x + x^{-1}) + 1) = 0$$

and $(x + x^{-1})$ is a solution of the linear equation $y + 1 = 0$, or

$$\cos(\frac{2\pi}{3}) = \frac{x + x^{-1}}{2} = -\frac{1}{2}$$

which is consistent with what one is taught in an elementary trigonometry class.

Next is the $p = 5$ case:

$$x^4 + x^3 + x^2 + x + 1 = x^2((x + x^{-1})^2 + (x + x^{-1}) - 1) = 0$$

and $(x + x^{-1})$ is a solution of the quadratic equation $y^2 + y + 1 = 0$, and

$$\cos(\frac{2\pi}{5}) = \frac{x + x^{-1}}{2} = \frac{\sqrt{5} - 1}{4}$$

4.2 Solving for $\cos(\frac{2\pi}{17})$

Unfortunately, repeating this procedure for the $p = 17$ and larger cases is trickier. Mimicking the above procedure exactly gives the following:

$$x^{16}+..+x+1 = (x-1)x^8((x+x^{-1})^8+(x+x^{-1})^7-7(x+x^{-1})^6+..+(x+x^{-1})-1) = 0$$

therefore $(x+x^{-1})$ is a solution of an octic equation. There is no simple formula for the solution of an octic equation, but this is a special case. Gauss says that a nice alternate expression exists, so it must be possible to solve this one way or another.

To achieve this, it is necessary construct a tower of quadratic expressions of the form

$$\alpha_1^2 - \alpha_0\alpha_1 + \beta_1 = 0$$
$$\alpha_2^2 - \alpha_1\alpha_2 + \beta_2 = 0$$
$$\dots$$
$$\alpha_i^2 - \alpha_{i-1}\alpha_i + \beta_i = 0,$$

where each α_i is of the form

$$\alpha_i = \sum_{k=0}^{2^{2^n-i}-1} \zeta_p^{g^{2^i k}}$$

where $n \in \mathbb{N}$ and g is a quadratic nonresidue modulo p. The importance of g being a quadratic nonresidue is that g is then primitive and will generate the set $\mathbb{Z}_p\backslash\{0\}$. Hence, the portion of $\{\zeta, \dots, \zeta^{16}\}$ covered by each α_i is a subset of that covered by α_{i-1}, and has half as many elements. Likewise, the set of unique $\mathbb{Q}$ automorphisms of $\mathbb{Q}(\alpha_i)$ is a subset of the set of unique $\mathbb{Q}$ automorphisms of $\mathbb{Q}(\alpha_{i+1})$, and the set of invariants over $\mathbb{Q}(\alpha_{i+1})$ is a subset of the set of invariants over $\mathbb{Q}(\alpha_i)$. This can be better explained once the τ function is introduced in section 4.3.1.

By Fermat's little theorem $m^{p-1} \bmod p = 1$, where $m \in \mathbb{Z}$, and by the definition of quadratic nonresidues $g^{\frac{p-1}{2}} \bmod p = -1$, so another important consequence is that

$$\alpha_{2^n-1} = \sum_{k=0}^{1} (\zeta^{g^{2^{2^n-1}k}}) = \zeta^{g^0} + \zeta^{\frac{2^{2^n}}{2}} = \zeta^{g^0} + \zeta^{\frac{p-1}{2}} = \zeta + \zeta^{-1} = 2\cos\frac{2\pi}{p}.$$

Also, ζ and ζ^{-1} are complex conjugates, so their sum is a real number, and since each α_i is built from $\zeta + \zeta^{-1}$ or multiples of $\zeta + \zeta^{-1}$, they are all real numbers.

For the case in question, $p = 17$, our tower of quadratic extensions is

$$\alpha_1^2 - \alpha_0\alpha_1 + \beta_1 = 0$$
$$\alpha_2^2 - \alpha_1\alpha_2 + \beta_2 = 0$$
$$\alpha_3^2 - \alpha_2\alpha_3 + \beta_3 = 0.$$

Gauss's proof that $\cos\frac{2\pi}{p}$ has an alternate radical expression with no worse than square roots also guarantees that this tower will exist. The solution of the bottom quadratic, or the one in terms of α_1, is a radical expression and the solution of each of the quadratics in α_i are in terms of radical expressions of $\alpha_{i-1} \dots \alpha_1$. For simplicity, we will use $g = 3$.

Consider $\alpha_1 = \sum_{k=0}^{7}(x^{3^{2k}}) = x + x^2 + x^4 + x^8 + x^{-8} + x^{-4} + x^{-2} + x^{-1}$:

$$(\alpha_1^2 + \alpha_1 - 4)x^{16} = 4\sum_{k=0}^{16}(x^k) + (x^{17} - 1)g(x) = 4(0) + (0)g(x) = 0$$

and α_1 is a root of the quadratic $y^2 + y - 4 = 0$.

Next consider $\alpha_2 = \sum_{k=0}^{3}(x^{3^{4k}}) = x + x^4 + x^{-4} + x^{-1}$:

$$(\alpha_2^2 - \alpha_1\alpha_2 - 1)x^{12} = -\sum_{k=0}^{16}(x^k) - (x^{17} - 1)(x + x^2 + x^4 + x^7) = 0$$

and α_2 is a root of the quadratic $y^2 - \alpha_1 y - 1$.

Finally, consider $\alpha_3 = \sum_{k=0}^{1}(x^{3^{8k}}) = x + x^{-1}$:

$$(2\alpha_3^2 - 2\alpha_2\alpha_3 + (\alpha_1\alpha_2 + \alpha_2 - \alpha_1 - 3)) = \sum_{k=0}^{16}(x^k) + (x^{17} - 1)(x + x^2 + x^4 + x^7) = 0$$

and $\alpha_3 = 2\cos(\frac{2\pi}{17})$ is a solution of the equation

$$\alpha_3^2 - \alpha_2\alpha_3 + \frac{1}{2}(\alpha_1\alpha_2 + \alpha_2 - \alpha_1 - 3)$$

Hence, each α_i is the solution of a quadratic equation with coefficients from the field $\mathbb{Q}(\alpha_1 \ldots \alpha_{i-1})$.

The motivation for the algebraic manipulations above are not natural or obvious, but their accuracy is easily checked using any symbolic maniuplator. The manipulations necessary for the two larger cases would be even more of a shot in the dark. A more systematic method will be used to formulate the tower of quadratic extensions necessary to solve for the alternate radical expressions of $\cos(\frac{2\pi}{257})$ and $\cos(\frac{2\pi}{65537})$, and the idea of formulating a tower of quadratic equations is central to this technique.

4.3 How to find $\cos(\frac{2\pi}{257})$ and $\cos(\frac{2\pi}{65537})$

The procedure used to solve for the radical expressions of these two expressions will be described here. To formulate the quadratic towers it is first necessary to introduce a new function.

4.3.1 The Tau Function

It is useful to define the $\mathbb{Q}$ automorphism $\tau(\zeta)$ on the field extension of the rationals $\mathbb{Q}(\zeta_p^{p-1}, \ldots, \zeta_p)$ such that $\tau^j(\zeta) = \zeta^{g^j}$, where g is the same quadratic non-residue modulo p used in the summation of α_i. Since g is a generator of the multiplicative group $\mathbb{Z}_{p-1}\backslash\{0\}$, $\tau(\zeta)$ is a generator of the set $\{\zeta, \ldots, \zeta^{16}\}$.

As mentioned above, each field extension $\mathbb{Q}(\alpha_i)$ is invariant under some set of $\mathbb{Q}$ automorphisms of the field extension $\mathbb{Q}(\zeta)$. For example, in the $p = 17$

case, $\mathbb{Q}(\alpha_0) = \mathbb{Q}(\zeta, \ldots, \zeta)$ is invariant under all $\mathbb{Q}$ automorphisms of ζ. Each $\mathbb{Q}$ automorphism sends ζ^j to a unique ζ^l, and each of the $\zeta, \ldots, \zeta^{16}$ are sent to another of the $\zeta, \ldots, \zeta^{16}$. Thus, $\mathbb{Q}(\zeta, \ldots, \zeta^{16})$ is really just $\mathbb{Q}$ in disguise, which should be true since $\mathbb{Q}(\zeta, \ldots, \zeta^{16}) = \mathbb{Q}(-1) = \mathbb{Q}$ $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^{-8} + \zeta^{-4} + \zeta^2 + \zeta^{-1})$ is invariant under τ^{2n}, where $n \in \mathbb{N}$, and in general $\mathbb{Q}(\alpha_1)$ is invariant under $\tau^{2^i n}$.

To demonstrate this, we will investigate some of the properties of the τ function: $\tau(xy) = \tau(x)\tau(y)$, therefore

$$\tau^j(\alpha_i) = \tau^j(\sum_{k=0}^{2^{2^{n-i}-1}} (x^{g^{(2^i)k}})) = \sum_{k=0}^{2^{2^{n-i}-1}} \tau^j(x^{g^{(2^i)k}}) = \sum_{k=0}^{2^{2^{n-i}-1}} (x^{g^{(2^i)k}})^{g^j} = \sum_{k=0}^{2^{2^{n-i}-1}} x^{g^{(2^i)k+j}}$$

where n corresponds to the index of the Fermat number. Since

$$\sum_{k=0}^{2^{2^{n-i}-1}} x^{g^{(2^i)k}} = \sum_{k=0}^{2^{2^{n-i}-1}} x^{g^{(2^i)k+2^i}},$$

there are 2^i conjugates for each α_i.

4.3.2 Calculating the Tower

This set of conjugates will become more important later, but for now the most important conjugate is $\tau^{2^{i-1}}(\alpha_i)$; it is the key in building up our tower. An important property of this conjugate is the following:

$$\alpha_i + \tau^{2^{i-1}}(\alpha_i) = \sum_{k=0}^{2^{2^{n-i}-1}} x^{g^{(2^i)k}} + \sum_{k=0}^{2^{2^{n-i}-1}} x^{g^{(2^i)k+2^{i-1}}} = \sum_{k=0}^{2^{2^{n-i+1}-1}} x^{g^{(2^{i-1})k}} = \alpha_{i-1}.$$

or simply

$$\alpha_i + \tau^{2^{i-1}}(\alpha_i) = \alpha_{i-1} \tag{2}$$

Furthermore, we define:

$$\beta_i = \alpha_i \tau^{2^{i-1}}(\alpha_i) \tag{3}$$

a constant to which more attention will be paid later. Substituting (2) into (3) gives

$$\alpha_i^2 - \alpha_{i-1}\alpha_i + \beta_i = 0 \tag{4}$$

and each α_i is a radical expression in α_{i-1} and β_i.

For this two work, our tower needs a rational foundation. In other words, α_0 and β_1 must be at worst radical expressions. From (1), $\alpha_0 = \sum_{i=1}^{p-1} = -1$. It remains to show that β_1, the other part of our foundation, is at worst a radical expression.

4.3.3 Calculating β_i From the Bottom

From here the tower will be determined if each β_i can be determined. One way to calculate each β_i is the algebraic "needle in a haystack" method used for the $p = 17$ case. However, no one in their right mind would want to do this for the $p = 257$ or $p = 65537$ case.

A better approach is to consider the field extension $\mathbb{Q}(\alpha_1)$, which forms a vector space over $\mathbb{Q}$. Likewise, $\mathbb{Q}(\alpha_i)$ forms a vector space over $\mathbb{Q}(\alpha_{i-1})$. Now, β_i lies in $\mathbb{Q}(\alpha_{i-1})$ and hence can be written as a linear combination of the elements of $\mathbb{Q}(\alpha_{i-1})$ using weights from $\mathbb{Q}(\alpha_{i-2})$.

Using the $p = 17$ case as an example will help to explain. The tower of equations is

$$\alpha_1^2 - \alpha_0\alpha_1 + \beta_1 = 0$$
$$\alpha_2^2 - \alpha_1\alpha_2 + \beta_2 = 0$$
$$\alpha_3^2 - \alpha_2\alpha_3 + \beta_3 = 0.$$

With the above in mind, β_1 is a rational, β_2 is a linear combination of the vectors 1 and α_1 over $\mathbb{Q}$, and β_3 is a linear combination of the vectors 1 and α_2 over the field $\mathbb{Q}(\alpha_1)$. Putting this more visually:

$$\beta_1 = a, a \in \mathbb{Q}$$
$$\beta_2 = b_1 + b_2\alpha_1, b_i \in \mathbb{Q}$$
$$\beta_3 = c_1 + c_2\alpha_2, c_i \in \mathbb{Q}(\alpha_1),$$

or

$$\beta_3 = d_1 + d_2\alpha_1 + d_3\alpha_2 + d_4\alpha_1\alpha_2, d_i \in \mathbb{Q},$$

and the problem is again reduced, this time to finding the rational weights.

For α_i, there are 2^{i-1} unknowns, and to find 2^{i-1} unknowns we need 2^{i-1} equations. Counting the identity, there are 2^i conjugates for each α_i. However, each the coefficients of the quadratic are members of the field $\mathbb{Q}(\alpha_{i-1})$, for which there are 2^{i-1} conjugates. Hence, we can use these conjugates to turn the equation

$$\alpha_i^2 - \alpha_{i-1}\alpha_i + \beta_i = 0$$

into

$$(\tau^j(\alpha_i^2))^2 - \tau^j(\alpha_{i-1})\tau^j(\alpha_i) + \tau^j(\beta_i) = 0 \tag{5}$$

and as j runs from 0 to $2^{i-1} - 1$ we get 2^{i-1} different equations.

Unfortunately, we need exact answers to a lot of equations in a lot of unknowns. That's too bad too because approximate answers are easy to find. Fortunately, a change of basis for our vector spaces helps alleviate this problem. Instead of using $\{1, \alpha_i\}$ as a basis over the field $\mathbb{Q}(\alpha_{i-1})$, for β_i we can use $\{\alpha_{i-1}, \tau(\alpha_{i-1}), \ldots, \tau^{2^{i-1}-1}\alpha_{i-1}\}$ as our basis over the field $\mathbb{Q}$. Again, we can use (5) to formulate 2^{i-1} equations in 2^{i-1} variables.

To use this, consider any of the $\tau^j(\alpha_i)$, $\tau^5(\alpha_3)$ of the $p = 257$ case for example:

$$\tau^5(\alpha_3) = \sum_{k=0}^{31}(\cos(\frac{2\pi 3^{8k+5}}{257}) + i\sin(\frac{2\pi 3^{8k+5}}{257})).$$

However, by their construction each α_i is a real number. The imaginary parts will eventually cancel out, so why even bother with them. Hence,

$$\tau^5(\alpha_3) = \sum_{k=0}^{31}(\cos(\frac{2\pi 3^{8k+5}}{257})),$$

and a reasonably good approximation of this and the unknowns can be found using anything that handles numerical computations and large matrices.

But what good are approximate answers when we need exact ones? Each of the unknowns are integers! The basis with which we are working is not quite an intergal one, but it is close enough that the unknowns are all integers. Numerical analysis can be used to insure that the error on each unknown is less than ± 0.5 and once the approximations reach that accuracy the answers can be confidently rounded to the nearest integer.

Ideally, the basis $\{1, \alpha_i\}$ is close enough to an intergal basis that the unknowns are integers. It is close, but as section 3.2 demonstrates it is not close enough. The reason that this would be ideal is that it would only be necessary to solve for each α_i. Unfortunately, with the basis $\{\alpha_{i-1}, \tau(\alpha_{i-1}), \ldots, \tau^{2^{i-1}-1}(\alpha_{i-1})\}$ it is necessary to keep track of most of the $\tau^j(\alpha_i)$. In other words, we are working with a tree instead of just a tower. But this problem is a practical one, not a theoretical one, and enough computing power or programming technique can minimize this downside.

To further check one's answers, a symbolic manipulator can be used to actually write out the polynomials and check that they are correct. Again, this is not a small task, but it can still be done with enough computing power.

4.3.4 Calculating β_i From the Top

Unfortunately, the average personal computer cannot handle a 2^{12} by 2^{12}, and for the $p = 65537$ case some of the matrices are much larger than this. The worst case scenario would be to solicit your math department for time on a local supercomputer, but fortunately this is not necessary, at least not until someone finds another Fermat prime.

Before, we were working our way up the tower from α_1, and as we did the matrices grew continually larger. Fortunately, there is a method of working from the top as well, and this method grows more difficult to implement as we work down the tower. We hope to meet somewhere in the middle.

Consider β_7 of the $p = 257$ case. We have:

$$\alpha_7\tau_7^{64} = (x + x^{-1})(x^{16} + x^{-16}) = (x^{3^0} + x^{3^{128}})(x^{3^{64}} + x^{3^{196}}) =$$

$$x^{3^0+3^{64}} + \ldots + x^{3^{128}+3^{196}}$$

We know that each β_i is a linear combination of the τ_{i-1}^j, therefore

$$(3^0 + 3^{64}) \bmod 257 = 3^j \bmod 257.$$

Discrete modular equations are notoriously hard to solve, even to the point that they are used in cryptology. Brute force can be used to solve these equations, and there are at most p natural numbers to try. The big advantage of this method is that there are no approximations to deal with. Another advantage is that near the top of the tower this method is more efficient than using matrices. Near the middle of the tower this method takes just as long as the matrix method, but hopefully the two methods will meet before this point is reached.

A third advantage to this method is revealed in a little trick that can be used to narrow down the domain of j. Consider α_6: each exponent is of the form g^{64k}. If we raise any element to the 4^{th} power we find that

$$(g^{64k})^4 = (g^{256})^k = (1)^k.$$

Similarly, each α_i is a solution of the equation $x^{2^{2^n-i}} = 1$ over the field $\mathbb{Z}_p$, where n is the index of the Fermat number. For α_6, each of the indices $3^0, \ldots, 3^{192}$ are the numbers in $\mathbb{Z}_p$ which when raised to the fourth power give one, or solutions of the equation $x^{2^{2^3-6}} = x^4 = 1$.

In the field $\mathbb{Z}_p$, 16 and -16 behave like i and $-i$, respectively. For other α_i, the exponents behave like the appropriate primitive roots of unity. With this in mind,

$$\alpha_7\tau_7^{64} = (x + x^{-1})(x^i + x^{-i}) = (x + x^{-1})(x^i + x^{-i}) = x^{1+i} + \ldots + x^{(-1-i)}$$

and

$$3^j = (1 + i) \bmod 257.$$

Now, the solution to this equation is no more obvious than its alternate form, but a little manipulation will show the merit of this representation. If we continually square the quantity $1 + i$, we get the following result:

$$(1 + i)^{16} = 256 = 3^{128} = -1 \tag{6}$$

and the quantity $1 + i \bmod 257$ is a primitive 32^{nd} root of unity. Taking the 16^{th} root of each side of this equation gives:

$$1 + i = (3^{128})^{1/16} = 3^{128/16} = 3^8. \tag{7}$$

Of course, since we are working in $\mathbb{Z}_p$ and $3^{256} = 1$, this is not the only solution. Equation (6) then becomes

$$(1 + i)^{16} = (3^{128})(3^{256k}) = 3^{128+256k}$$

and equation (7) becomes

$$1 + i = 3^{8+16k},$$

leaving us with only 16 values to try for j instead of 256.

It is not necessary to use i for this, for $(1+3^{64})^{16} = -1$. However, as mentioned above 3^{64} and i behave similarly, and $(1+i)^{32}$ is considerably easier to compute than $(1+3^{16384})^{32}$.

Unfortunately this procedure does not gain much for most of the α_i. For the $p = 257$ case, we find for α_7 that $1+\zeta_8 = 3^{1+2k}$ and for α_6 and below that $1+\zeta_{16} = 3^k$, which is what we already knew. For the $p = 65537$ case, we find for α_{15} that $1+i = 3^{1024+2048k}$, for α_{14} that $1+\zeta_8 = 3^{4+8k}$, for α_{12} that $1+\zeta_{16} = 3^{1+2k}$, and for $1+\zeta_{32} = 3^k$, which is again what we already knew. The merit of this trick is that helps us calculate a few β_i at the top of the tower.

4.3.5 Distinguishing Between Solutions

There is only one more aspect to discuss before the technique for finding the radical expressions is complete. α_{i-1} has only half as many conjugates as α_i. The consequence of this is that the equations

$$(\tau^j(\alpha_i^2))^2 - \tau^j(\alpha_{i-1})\tau^j(\alpha_i) + \tau^j(\beta_i) = 0$$

and

$$(\tau^{j+2^{i-1}}(\alpha_i^2))^2 - \tau^{j+2^{i-1}}(\alpha_{i-1})\tau^{j+2^{i-1}}(\alpha_i) + \tau^{j+2^{i-1}}(\beta_i) = 0$$

both have the same solution, differing by the sign in front of the radical, due to the fact that $\tau^{j+2^{i-1}}(\alpha_{i-1}) = \tau^j(\alpha_{i-1})$ (since $\tau^{2^{i-1}}(\alpha_{i-1}) = \alpha_{i-1}$).

It would seem that there should be some pattern to the signs, such as the conjugate that occurs first is the greater one, but unfortunately this intuition is wrong. In fact, we were unable to determine any kind of pattern at all, even an artificial pattern for the purpose of making data presentation easier. To determine which has which sign, it is necessary to look at the approximations for each and check which one is bigger.

A different perspective on this problem unfortunately does not help to solve this problem. The τ function is a $\mathbb{Q}$ automorphism, but our solutions are in terms of radicals, which do not lie in $\mathbb{Q}$. Considering the following, where $x \in \mathbb{Q}$:

$$(\tau(\sqrt{x}))^2 = \tau((\sqrt{x})^2) = \tau(x) = x$$

therefore

$$\tau(\sqrt{x}) = \pm\sqrt{(x)}$$

which is, of course, what we already knew. Likewise,

$$(\tau(\sqrt{\beta_i}))^2 = \tau((\sqrt{\beta_i})^2) = \tau(\beta_i)$$

therefore

$$\tau(\sqrt{\beta_i}) = \pm\sqrt{(\tau(\beta_i))},$$

which still does nothing to help distinguish between solutions.

5 Calculations Using the Tower

Here the method described in section 4.3 will be used to calculate $\cos(\frac{2\pi}{17})$, $\cos(\frac{2\pi}{257})$, and $\cos(\frac{2\pi}{65537})$. The generator used for each case will be 3, but this is arbitrary and is only used because it is the smallest generator and makes the calculations faster. Each of the following subsections will contain the calculated tower of equations, a table indicating the sign of each radical expression, and the entire radical expression. For the $p = 17$ and $p = 257$ cases, it was easy to calculate the entire tower of quadratic extensions using matrices, and the errors in the approximations were very small, even using just Maple and a personal computer. For the $p = 65537$ case, the first ten equations were easy to compute using matrices, and the top four equations were easy to compute by solving the discrete modular equations. The 11^{th} equation was difficult to calculate either way, and after a few days of computation on a personal computer, the method from the top succeeded in calculating the correct equation. Each of the equations were checked for correctness using the actual polynomials they represent.

5.1 A Warmup – $\cos(\frac{2\pi}{17})$

Though this problem has been tackled many times before, the techniques of this paper will be used to again give a rational expression for $\cos(\frac{2\pi}{17})$. The calculated tower of equations used was

$$\alpha_1^2 + \alpha_1 - 4 \tag{8}$$

$$\alpha_2^2 - \alpha_1\alpha_2 - 1 \tag{9}$$

$$\alpha_3^2 - \alpha_2\alpha_3 + \tau(\alpha_2) \tag{10}$$

Table (1) gives the appropriate signs of each radical expression.

Table 1. Signs for $p = 17$

Root	Tau	Sign
1	0	+
1	1	-
2	0	+
2	1	+
2	2	-
2	3	-
3	0	+
3	1	+
3	2	-
3	3	-
3	4	-
3	5	-
3	6	+
3	7	+

Here we will demonstrate from start to finish how to formulate a real expression involving no worse than square roots using the tower of equations and table **??**. We first solve (10) for α_3 and we get the expression

$$\alpha_3 = \frac{\alpha_2}{2} \pm \frac{\sqrt{\alpha_2^2 + 4\tau(\alpha_2)}}{2}.$$

To determine the sign in front of the radical, we refer to table (1). We are solving for α_3, or $\tau^0(\alpha_3)$, so we refer to the line in the table with a '3' in the 'Root' column and a '0' in the 'Tau' column, and find that the sign is '+'. In general, for the expression $\tau^i(\alpha_j)$ we refer to the line with an 'i' in the 'Tau' column and a 'j' in the 'Root' column. Hence,

$$\alpha_3 = \frac{\alpha_2}{2} + \frac{\sqrt{\alpha_2^2 + 4\tau(\alpha_2)}}{2}.$$

Next we must solve for all of the remaining unknowns in the expression. This means we must solve for α_2 and $\tau(\alpha_2)$. For this, we solve (9) or one of its conjugates for the variable. We first have

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

Referring to the line of Table (1) with a '1' in the 'Root' column and a '0' in the 'Tau' column gives a sign of '+', therefore

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

Using the τ function, (9) can be rewritten as

$$\tau(\alpha_2)^2 - \tau(\alpha_1)\tau(\alpha_2) - 1 = 0$$

and solving for $\tau(\alpha_2)$ gives

$$\tau(\alpha_2) = \frac{\tau(\alpha_1)}{2} \pm \frac{\sqrt{\tau(\alpha_1)^2 - 4(-1)}}{2},$$

and referring to the line corresponding to a '2' in the 'Root' column and a '1' in the 'Tau' column gives a sign of '+', so

$$\tau(\alpha_2) = \frac{\tau(\alpha_1)}{2} + \frac{\sqrt{\tau(\alpha_1)^2 + 4}}{2}.$$

Substituting these into the expression for α_3 gives

$$\alpha_3 = \frac{\frac{\alpha_1}{2} + \frac{\sqrt{\alpha_1^2+4}}{2}}{2} + \frac{\sqrt{(\frac{\alpha_1}{2} + \frac{\sqrt{\alpha_1^2+4}}{2})^2 + 4(\frac{\tau(\alpha_1)}{2} + \frac{\sqrt{\tau(\alpha_1)^2+4}}{2}}}{2}.$$

Simplifying this gives

$$\alpha_3 = \frac{\alpha_1}{4} + \frac{\sqrt{\alpha_1^2+4}}{4} + \frac{1}{4}\sqrt{(\alpha_1+\sqrt{\alpha_1^2+4})^2 + 8(\tau(\alpha_1)+\sqrt{\tau(\alpha_1)^2+4})}.$$

Finally, we refer to (8) and its conjugate

$$\tau(\alpha_1)^2 + \tau(\alpha_1) - 1 = 0$$

to solve for α_1 and $\tau(\alpha_1)$. Solving gives:

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

and also

$$\tau(\alpha_1) = \frac{-1}{2} \pm \frac{\sqrt{(1)^2 - 4(-4)}}{2}.$$

Referring to Table (1) gives

$$\alpha_1 = \frac{-1}{2} + \frac{\sqrt{17}}{2}$$

and also

$$\tau(\alpha_1) = \frac{-1}{2} - \frac{\sqrt{17}}{2}.$$

Substituting these into the expression for α_3 gives:

$$\alpha_3 = \frac{(\frac{-1}{2}+\frac{\sqrt{17}}{2})}{4} + \frac{\sqrt{(\frac{-1}{2}+\frac{\sqrt{17}}{2})^2+4}}{4} +$$

$$\frac{1}{4}\sqrt{((\frac{-1}{2}+\frac{\sqrt{17}}{2})+\sqrt{(\frac{-1}{2}+\frac{\sqrt{17}}{2})^2+4})^2 + 8((\frac{-1}{2}-\frac{\sqrt{17}}{2})+\sqrt{(\frac{-1}{2}-\frac{\sqrt{17}}{2})^2+4})}.$$

Simplifying this gives:

$$-\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34-2\sqrt{17}}$$
$$+\frac{1}{8}\sqrt{68+12\sqrt{17}-2\sqrt{34-2\sqrt{17}}+2\sqrt{17}\sqrt{34-2\sqrt{17}}-16\sqrt{34+2\sqrt{17}}}.$$

5.2 More Practice – $\cos(\frac{2\pi}{257})$

The rational expression for $\cos(\frac{2\pi}{257})$, and thus an algorithm for the construction of a 257-gon, has been given and verified, but never in brief form. The calculated tower is:

$$\alpha_1^2 + \alpha_1 - 64$$

$$\begin{gathered}
\alpha_2^2 - \alpha_1\alpha_2 - 16 \\
\alpha_3^2 - \alpha_2\alpha_3 + 2\alpha_2 + 5\tau(\alpha_2) + 4\tau^2(\alpha_2) + 5\tau^3(\alpha_2) \\
\alpha_4^2 - \alpha_3\alpha_4 + 2\alpha_3 + 2\tau^2(\alpha_3) + \tau^4(\alpha_3) + 2\tau^5(\alpha_3) + \tau^6(\alpha_3) \\
\alpha_5^2 - \alpha_4\alpha_5 + \alpha_4 + \tau(\alpha_4) + \tau^2(\alpha_4) + \tau^5(\alpha_4) \\
\alpha_6^2 - \alpha_5\alpha_6 + \tau(\alpha_5) + \tau^{23}(\alpha_5) \\
\alpha_7^2 - \alpha_6\alpha_7 + \tau^{56}(\alpha_6)
\end{gathered} \tag{11}$$

I left a lot of junk out here for brevity.
Finally, here is the radical expression for $\cos(\frac{2\pi}{65537})$.

6 Two Algorithms for the Construction of n-gons

Here we present two algorithms for construction of a 17, 257, and 65537-gon. The first is obvious, but rather unpleasing aesthetically. The second is more aesthetically pleasing and slightly easier to actually perform.

6.1 A Messy Algorithm

The first method is mentioned above, and it is to simply construct the point corresponding to $\cos(\frac{2\pi}{p})$ using the several page long radical expression. For the $p = 17$ case this is not easy but also not impossible. For the larger cases this is entirely unmanagable.

6.2 A Nicer Algorithm

The second method provides a method of construction which does not require the actual radical expression. Each equation in the tower is of the form

$$\alpha_i^2 - \alpha_{i-1}\alpha_i + \beta_i = 0.$$

One can rewrite this equation by completing the square:

$$(\alpha_i - \frac{\alpha_{i-1}}{2})^2 + \beta_i - (\frac{\alpha_{i-1}}{2})^2 = 0$$

and each α_i is the intersection of a circle centered at $(\frac{\alpha_{i-1}}{2})$ with radius $\sqrt{(\frac{\alpha_{i-1}}{2}) - \beta_i}$ and the x-axis. The sign of the root, and hence the left or right intersection, is still in question and must be computed or referenced from table (??). The construction is still no cake walk, for each τ_i^j which is contained in a β_{i+1} must be constructed. This is done by constructing a circle instead centered at $(\frac{\tau^j(\alpha_{i-1})}{2})$ with radius $\sqrt{(\frac{\tau^j(\alpha_{i-1})}{2}) - \tau^j(\beta_i)}$.

7 Conclusion

In this paper we have presented a method for calculation of $\cos(\frac{2\pi}{p})$, where p is a Fermat prime. With this, we have given two algorithms for the ruler and compass construction of a regular n-gon, where n is a Fermat prime, hence providing an algorithm for the ruler and compass construction of every known possible regular n-gon.

References

[1] Gauss, C. F. *Disquisitiones Arithmeticae*. New Haven: Yale University Press, 1966.

[2] Stewart, Ian. *Galois Theory, 2nd ed.* New York: Chapman and Hall, 1989.

[3] Klein, F. *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*. London: Kegan Paul, 1913.

[4] Richelot, F. J. De resolutione algebraica aequationis $x^{257} = 1$, sive de divisione circuli per bisectionam anguli septies repetitam in partes 257 inter se aequales commentatio coronata. *Crelle's Journal*. **IX**(1832) 1-26, 146-61, 209-30, 337-56.

[5] Bell, E. T. *Men of Mathematics* (2 vols). Harmondsworth, Middlesex: Penguin, 1965.

[6] Niven, Ivan and Zuckerman, Herbert S. *An Introduction to the Theory of Numbers, 4th ed.* New York: John Wiley & Sons, 1980.