Constructing the 17-gon:
In these notes, I'll give 1.999999 proofs that the 17-gon is constructible. Showing that the regular 17-gon is constructible is the same as showing that $\cos(2\pi/17)$ and $\sin(2\pi/17)$ are constructible numbers.

First (Almost) Proof: This is a cheap shot. You can verify computationally that

$$\cos(2\pi/17) =$$

$$\frac{1}{16}\left(\begin{array}{c} -1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+ \\ \sqrt{68+12\sqrt{17}+2\sqrt{578-34\sqrt{17}}-2\sqrt{34-2\sqrt{17}}-16\sqrt{34+2\sqrt{17}}} \end{array}\right).$$

Therefore $\cos(2\pi/17)$ is constructible. Since $\cos^2+\sin^2 = 1$, we see that $\sin(2\pi/17)$ is constructible as well.

You might ask *how* you verify computationally that the two sides of the equation are equal. You can plug it into a powerful calculator and see that both sides agree up to (say) 1000000 decimal places. But, if you think about it, this probably isn't enough. You either have to go through and work out the algebra or else you have to prove some result to the effect that very simple expressions which agree to 1000000 decimal places are equal. So, the above is not quite a proof.

Where does that equation come from? I found these numbers by tracing through the steps in the second proof. The second proof is an honest proof, and goes all the way.

The Second Proof: Before launching into the second proof, I want to explain the ideas behind the proof. First of all, it is more convenient to work with complex numbers, so the first part of the proof shows that it suffices to deal with complex numbers. Part 2 of the proof, the main part, shows that the 17th root of unity $\exp(2\pi i/17)$ is constructible in a complex sense, and this suffices by part 1.

For the main part of the proof, the idea is to consider subgroups of the order 16 group $G = (\boldsymbol{Z}/17)^*$. To each subset of G, you can associate a certain sum of 17th roots of unity. It turns out that there are subgroups $\boldsymbol{Z}/2 \subset \boldsymbol{Z}/4 \subset \boldsymbol{Z}/8 \subset \boldsymbol{Z}/16 = (\boldsymbol{Z}/17)^*$ and by looking at the sums associated to these subgroups and their cosets we'll find a way to construct $\exp(2\pi i/17)$. Here we go...

Definition: A complex number ω is *real constructible* (RC) if its real and imaginary parts are constructible. ω is *complex constructible* (CC) if there is a tower of fields $\boldsymbol{Q} = F_0 \subset ... \subset F_n \subset \boldsymbol{C}$ such that $[F_i : F_{i+1}] \leq 2$ for all $i = 0, ..., (n-1)$ and $\omega \in F_n$.

Lemma 0.1 *CC implies RC.*

Proof: Suppose ω is CC. Using the quadratic formula, we can find a sequence of complex numbers $\lambda_1, ..., \lambda_n$ and a sequence of complex numbers $\mu_0, ..., \mu_{n-1}$ such that

- $F_k = \boldsymbol{Q}(\lambda_1, ..., \lambda_k)$.
- $\lambda_k = \sqrt{\mu_{k-1}}$ where $\mu_0 \in \boldsymbol{Q}$ and $\mu_k \in \boldsymbol{Q}(\lambda_1, ..., \lambda_k)$ for $k \geq 1$.

The real and imaginary parts of ω are obtained from the real and imaginary parts of $\lambda_1, ..., \lambda_n$ and elements of $\boldsymbol{Q}$ by field operations. So, we just have to prove that $\lambda_1, ..., \lambda_n$ are RC. By the same reasoning, μ_k (for $k \geq 1$) is RC provided that $\lambda_1, ..., \lambda_{k-1}$ are RC. Also, $\mu_0 \in \boldsymbol{Q}$ is RC.

To finish the proof we have to show that if μ_{k-1} is RC then so is λ_k. Write $\mu_{k-1} = A + Bi$ and $\lambda_k = a + bi$. Expanding out $(a + bi)^2 = A + Bi$ and equating real and imaginary parts, we have

$$a^2 - b^2 = A, \qquad 2ab = B.$$

Substituting the equation $b = B/2a$ into the first equation and multiplying through by a^2 we see that

$$(a^2)^2 - (A)(a^2) - (B^2/4) = 0.$$

This shows that a^2 satisfies a quadratic equation with coefficients in $\boldsymbol{Q}(A, B)$. By the quadratic formula, a^2 is constructible. But then so is $\sqrt{a^2} = a$. Finally, so is $b = B/2a$. So, λ_k is RC. ♠

Thanks to the lemma, it suffices to prove that

$$\omega = \cos(2\pi i/17) + i \sin(2\pi i/17) \tag{1}$$

is CC. Define

$$\omega_k = \omega^{3^k}. \tag{2}$$

For instance $\omega_2 = \omega^9$ and $\omega_3 = \omega^{27} = \omega^{10}$. Why are we doing this? We're doing this because 3 is a generator for the multiplicative group $(\boldsymbol{Z}/17)^*$ and the set $\{3^k\}$ gives the whole group mod 17.

Given a positive integer m and $k \in \{0, ..., m-1\}$ define

$$\alpha_{mk} = \sum_{j \equiv k \ (m)} \omega_j. \tag{3}$$

The sum is over an irredundant set of j congruent to k mod m. For instance

$$\alpha_{20} = \omega_0 + \omega_2 + ... + \omega_{14} = \omega^1 + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} + \omega^8 + \omega^4 + \omega^2.$$

Group theoretically, we are summing powers with the exponents taken from various subgroups and cosets of subgroups in $(\boldsymbol{Z}/17)^*$.

Define the following fields.

- $F_0 = \boldsymbol{Q}$.
- $F_1 = F_0(\alpha_{20}, \alpha_{21})$.
- $F_{21} = F_1(\alpha_{41}, \alpha_{43})$.
- $F_2 = F_1(\alpha_{40}, \alpha_{41}, \alpha_{42}, \alpha_{43}) = F_{21}(\alpha_{40}, \alpha_{42})$.
- $F_3 = F_2(\alpha_{80}, \alpha_{84})$.
- $F_4 = F_3(\omega, \omega^{16})$.

Use the notation $A \to B$ to mean that $A \subset B$ and $[A : B] \leq 2$. The following chain proves that every element of F_4 is constructible:

$$F_0 \to F_1 \to F_{21} \to F_2 \to F_3 \to F_4. \tag{4}$$

The rest of these notes is devoted to establish this chain, one link at a time.

Lemma 0.2 $F_0 \to F_1$.

Proof: We have $\alpha_{20} + \alpha_{21} = -1$ and a calculation shows that $\alpha_{20}\alpha_{21} = -4$. Therefore α_{20} and α_{21} are roots of a degree 2 polynomial in $F_0[x]$. ♠

Lemma 0.3 $F_1 \to F_{21}$.

Proof: We have $\alpha_{41} + \alpha_{43} = \alpha_{21}$ and a calculation shows that $\alpha_{41}\alpha_{43} = -1$. Therefore α_{41} and α_{43} are roots of a degree 2 polynomial in $F_1[x]$. ♠

Lemma 0.4 $F_{21} \to F_2$.

Proof: Note that $F_2 = F_{21}[\alpha_{40}, \alpha_{42}]$. We have $\alpha_{40} + \alpha_{42} = \alpha_{20}$, and a calculation shows that $\alpha_{40}\alpha_{42} = -1$. Therefore α_{40} and α_{42} are roots of a degree 2 polynomial in $F_1[x]$. But then, *a forteriori*, α_{40} and α_{42} are roots of a degree 2 polynomial in. $F_{21}[x]$. ♠

Lemma 0.5 $F_2 \to F_3$.

Proof: We have $\alpha_{80} + \alpha_{84} = \alpha_{40}$, and a calculation shows that $\alpha_{80}\alpha_{84} = \alpha_{41}$. Therefore α_{80} and α_{84} are roots of a degree 2 polynomial in $F_2[x]$. ♠

Lemma 0.6 $F_3 \to F_4$.

Proof: Note that $\omega = \omega_0$ and $\omega^{-1} = \omega_8$. We have $\omega + \omega^{16} = \alpha_{80}$ and $\omega\omega^{-1} = 1$. So, ω and ω^{16} are roots of the degree 2 polynomial in $F_3[x]$. ♠

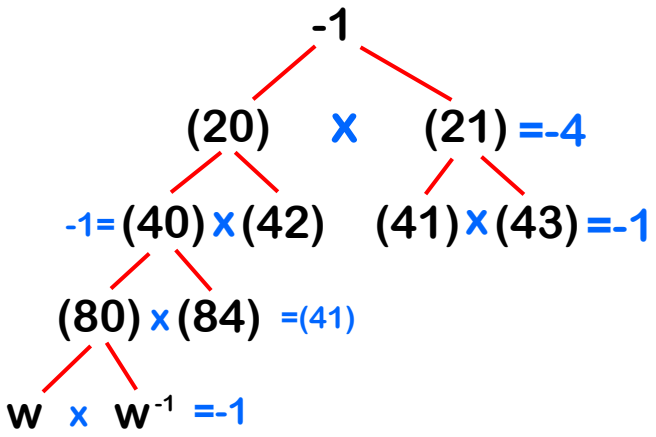

Figure 1: Summary of the proof