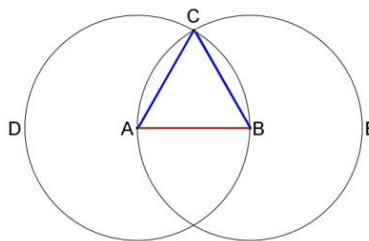


[DynamicsOfPolygons.org](https://DynamicsOfPolygons.org)

# Construction of regular polygons

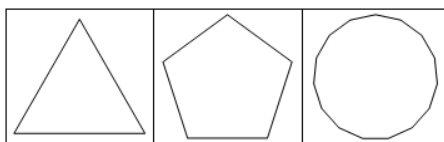
A constructible regular polygon is one that can be constructed with compass and (unmarked) straightedge. For example the construction on the right below consists of two circles of equal radii. The center of the second circle at B is chosen to lie anywhere on the first circle, so the triangle ABC is equilateral – and hence equiangular.



Compass and straightedge constructions date back to Euclid of Alexandria who was born in about 300 B.C. The Greeks developed methods for constructing the regular triangle, square and pentagon, but these were the only ‘prime’ regular polygons that they could construct. They also knew how to double the sides of a given polygon or combine two polygons together – as long as the sides were relatively prime, so a regular pentagon could be drawn together with a regular triangle to get a regular 15-gon. Therefore the polygons they could construct were of the form

$$N = 2^m 3^k 5^j \text{ where } m \text{ is a nonnegative integer and } j \text{ and } k \text{ are either } 0 \text{ or } 1.$$

The constructible regular polygons were 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 32, 40, 48, ... but the only odd polygons in this list are 3, 5 and 15.



*The triangle, pentagon and 15-gon are the only regular polygons with odd sides which the Greeks could construct.*

If  $n = p_1 p_2 \dots p_k$  where the  $p_i$  are odd primes then  $n$  is constructible iff each  $p_i$  is constructible, so a regular 21-gon can be constructed iff both the triangle and regular 7-gon can be constructed. This does not settle the question of constructing polygons with  $p^k$  sides for  $k > 1$  and this issue will be addressed below.

That was where things stood for about 2000 years, when 19 year-old Carl Friedrich Gauss showed that a regular 17-gon was constructible in 1796. He did this by showing that the solution to the cyclotomic equation  $x^{17} = 1$  can be reduced to a succession of nested quadratic equations. He published this discovery five years later in *Disquisitiones Arithmeticae* and generalized the process to show that a prime regular polygon was constructible whenever it was of the form  $p = 2^k - 1$  because  $k$  must be a power of 2. This guaranteed that there will be a sequence of nested quadratic equations for the construction.

Primes of this type are called Fermat primes. Pierre de Fermat (1601- 1655) mistakenly assumed that they would all be prime. They are all of the form  $F_n = 2^{2^n} + 1$ , but there are only 5 such primes known. They are  $F_0 = 3$ ,  $F_1 = 5$ ,  $F_2 = 17$ ,  $F_3 = 257$ ,  $F_4 = 65537$ .

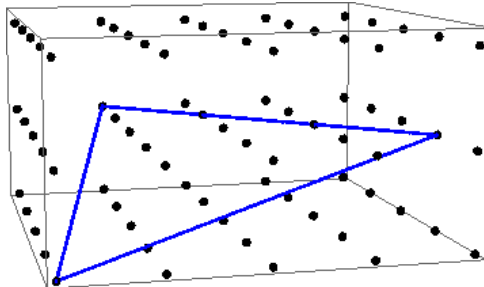
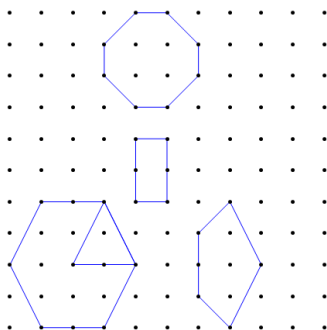
Gauss conjectured that the constructability condition was also necessary but this was not proven until 1837 by Pierre Wantzel. This converse was not trivial because it required a proof that a regular polygons of the form  $p^k$  with  $p$  prime cannot be constructed if  $k > 1$ . This is easy to see for  $n = 9$  because a  $40^\circ$  angle cannot be constructed. For a prime polygon to be constructible, the critical fact is that the irreducible equation for  $\cos(2\pi/p) + i\sin(2\pi/p)$  is degree  $\phi(p) = p-1$  and this has to be of the form  $2^k$ . Replacing  $p$  with  $p^m$ , it can be shown that the irreducible equation has degree  $\phi(p^m)$  which is  $2^{m-1}(p-1)$  and this is never of the form  $2^k$  when  $m > 1$ .

Therefore unless new Fermat primes are discovered, there are only 5 prime regular polygons which can be constructed. The rule is “A regular  $n$ -gon can be constructed with compass and straightedge iff  $n$  is the product of a power of 2 and any number of distinct Fermat primes.”

$n = 2^m p_1 p_2 \dots p_k$  where  $m$  is a non-negative integer and each  $p_j$  is either 1 or the  $j$ th Fermat prime. The number of constructible regular primes with an odd number of vertices is now  $2^5 - 1 = 31$ .

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Constructible?	Y	Y	Y	Y	N	Y	N	Y	N	Y	N	N	Y	Y	Y

The ultimate level of constructability would be a lattice polygon where the vertices lie on an integer lattice as shown on the left below. However the only regular lattice polygon is the square – although the octagon shown here is equiangular. There are no other equiangular lattice polygons besides the rectangle and octagon. (Using Pythagorean triples, equilateral lattice polygons are easy to construct, but they must have an even number of sides. This means there is an equilateral octagon and an equiangular octagon, but never at the same time.) The hexagon shown here at bottom left and the embedded triangle are almost equiangular. Allowing vertices in the rationals  $\mathbb{Q}$  clearly makes no difference, but allowing one more dimension yields a regular triangle and regular hexagon. On the right is a regular triangle in  $\mathbb{Z}^3$  with coordinates  $\{0,0,0\}$ ,  $\{4,1,1\}$  &  $\{1,4,1\}$ . Going beyond 3 dimensions does not yield new regular lattice polygons. See [LatticePolygons.pdf](#).



Basic construction techniques:



A compass and straightedge construction assumes a compass and unmarked straightedge. Each step consists of one of the following:

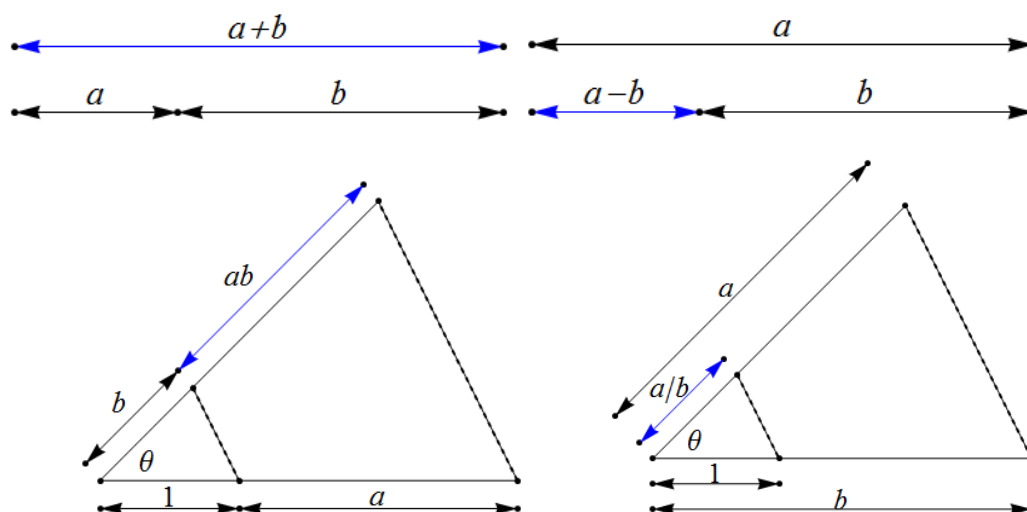
1. Drawing a line between 2 points
2. Constructing a circle with a given radius and given center
3. Finding the points of intersection of two lines, 2 circles or a line and a circle

The issues that have been of interest since the time of the Greeks are

- (i) Which numbers are constructible?
- (ii) Which angles are constructible?
- (iii) Which polygons are constructible?

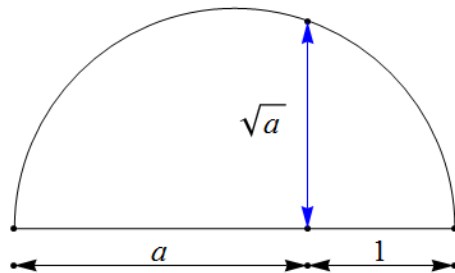
To determine which number are constructible:

The Greeks assumed (as we do today) that in any given construction, there is a basic line segment with length 1 and all other lengths are relative to this line segment. If  $a$  and  $b$  are known lengths, then  $a + b$ ,  $a - b$ ,  $ab$  and  $a/b$  can be constructed with just a straightedge as shown below. (In the last two diagrams, the angle  $\theta$  is arbitrary and the dashed lines are parallel.)



If the compass is just used to mark off lengths, the set of numbers constructible is the rationals  $\mathbb{Q}$ . The rationals are known as a ‘number field’ because they are closed under the ‘rational’ operations of addition, subtraction, multiplication and division (by non-zero elements). Other examples of number fields are the reals and the complex numbers.

This is the first ‘level’ of constructability so the ‘base’ field is  $F_0 = \mathbb{Q}$ . The second level involves picking any non-square element  $z$  of  $F_0$  and setting  $F_1 = \{a + b\sqrt{z} : a, b \text{ in } F_0\}$ . The elements of  $F_1$  are constructible because  $\sqrt{z}$  is constructable with straightedge and compass as shown below:



It is easy to see that  $F_1$  is also a number field and it contains  $F_0$  as a subfield, so it is an extension field of  $F_0$ . This process can be continued to any depth to achieve a sequence  $F_0, F_1, \dots, F_n$  of nested number fields where  $F_0 = \mathbb{Q}$  and  $F_{j+1}$  is the extension field of  $F_j$  obtained by adjoining  $\sqrt{z}$  to  $F_j$  where  $z$  is in  $F_j$  (so  $F_{j+1}$  can be written  $F_j[\sqrt{z}]$ ).

No construction with straightedge and compass can ever yield numbers outside these nested chains of fields because the equations for intersection of lines and/or circles are never worse than quadratic. Therefore every constructible number must be in one of the extension fields  $F_j$  and conversely every element of a field  $F_j$  must be constructible. These are called Euclidean numbers.

**Example:** At depth  $n = 3$ , an expression such as  $\sqrt{3 + \sqrt{2 - \sqrt{7}}}$  can be obtained with  $K_1 = \mathbb{Q}[\sqrt{7}]$ ,  $K_2 = K_1[\sqrt{2 - \sqrt{7}}]$  and  $K_3 = K_2[\sqrt{3 + \sqrt{2 - \sqrt{7}}}]$ . In terms of straightedge and compass, each number is constructible from the previous.

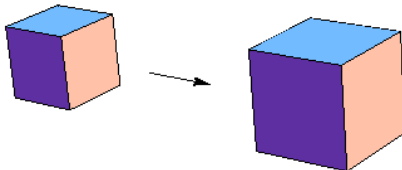
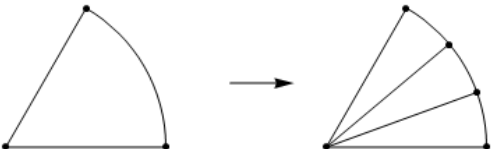
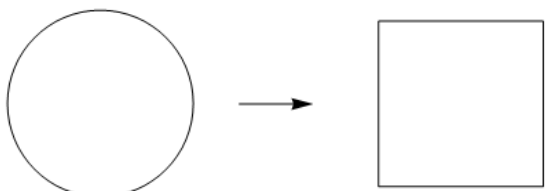
All even roots can be found by this method but how about odd roots? Suppose there is a finite tower of constructible extensions:  $F_0 \subset F_1 \subset F_2 \subset \dots \subset F_k$ . At each stage the extension must be degree 2 (quadratic) and it is easy to prove that the degrees are multiplicative, so  $F_k$  would have to be degree  $2^k$  in  $F_0$ , which we usually assume is  $\mathbb{Q}$ . (Richard Dedekind introduced the concept of the degree of an extension in 1873 and at that time he proved the multiplicative property.)

So the roots of a cubic equation are only constructible if there is at least one rational root, because then this root can be factored out leaving a quadratic. If the cubic is not reducible in this fashion then it is not possible to construct the roots. This means it is impossible to double the

volume of a cube with compass and straightedge. Assuming an original edge length is 1, the new cube would have a side  $x$ , where  $x^3 = 2$ . This equation is not reducible so  $\sqrt[3]{2}$  is not a constructable number.

The Wikipedia definition: [constructible numbers](#) (those that, starting with a unit length, can be constructed with straightedge and compass). These include all quadratic surds, all rational numbers, and all numbers that can be formed from these using the basic arithmetic operations and the extraction of square roots.

The three classic Greek problems that could not be solved by Euclid's methods are:

Doubling the volume of a cube	
Trisecting an arbitrary angle	
Finding a square with area equal to a circle	

Clearly an angle  $\theta$  is constructible if and only if  $\cos(\theta)$  is constructible. To prove that it is impossible to trisect  $60^\circ$  with compass and straightedge, note that any solution  $\theta$  must satisfy  $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$  but when  $x = 2\cos 20^\circ$ , this becomes  $x^3 - 3x - 1 = 0$  which is irreducible. Since  $\cos 20^\circ$  is not constructible,  $20^\circ$  is not constructible.

It is more difficult to show the impossibility of 'squaring' a circle with straightedge and compass. Assuming that the circle has radius 1, the square would have side  $x = \sqrt{\pi}$ . In 1768 Joanne Lambert proved that  $\pi$  was not rational and he conjectured that  $\pi$  and  $e$  were both 'transcendental' and hence not constructible. Recall that the algebraic numbers are defined to be the real (or complex) numbers which are solutions to a polynomial equation of degree  $n$  with integer coefficients. The transcendental numbers are the complement of this set. However in 1768, no number had been proven to be transcendental. In 1873 Charles Hermite showed that  $e$  was transcendental.

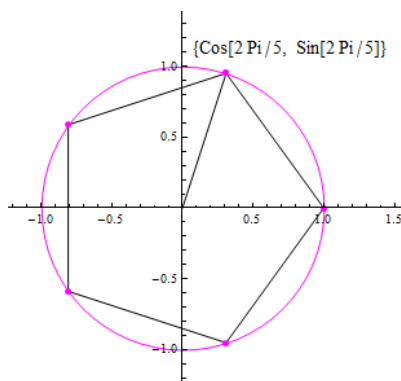
In 1882 Ferdinand von Lindermann used Hermite's result and Euler's identity  $e^{i\pi} = -1$  to show that  $\pi$  was transcendental. The first person to actually construct a transcendental number was J.

Liouville in 1851. Later, Georg Cantor (1845,1918) showed that the set of algebraic numbers is countable, so the set of transcendental real numbers is uncountable. (For this outrage he was branded a "scientific charlatan", and a "corrupter of youth" by such notable mathematicians as Henri Poincare and Leopold Kronecker.)

Since the constructible numbers are a subset of the algebraic numbers, transcendental numbers such as  $\pi$  and  $e$  and  $2^{\sqrt{2}}$  are certainly not constructible. In fact  $a^b$  is transcendental whenever  $a$  is algebraic and not 0 or 1, and  $b$  is any irrational algebraic number.

### Constructible Regular Polygons – Cyclotomic Fields

Constructing a regular polygon with  $n$  sides is the same as dividing a circle into  $n$  equal parts, and this is the same as finding  $\cos(2\pi/n)$  or  $\sin(2\pi/n)$ .



Most trigonometric expressions are transcendental, so there was interest in those which are algebraic. Mathematica will attempt to make this distinction. For example **Element[Cos[2 Degree], Algebraics] = False** but **Element[Cos[2Pi/7],Algebraics] = True**




The vertices of a regular polygon are always algebraic because they are (complex) solutions to  $z^n = 1$ . This is called the *n*th cyclotomic equation. Of course only certain algebraic numbers are constructible and Gauss realized that  $\cos(2\pi/17)$  is one of them.

We will look at Gauss's technique in detail. It is covered in his *Disquisitiones Arithmeticae* (Arithmetical Investigations) which was published in 1801 but it still very readable today. Gauss started work on it 1796 when he was 19 years old and in his first year at the university of Göttingen. This was the winter that he realized that for a prime  $p$ , the roots of the (reduced) cyclotomic equation could be partitioned in a natural way using modular arithmetic and "I was able to make on the spot the special application to the 17-gon and verify it numerically." (Gauss was a calculation wizard who also made good use of trigonometric tables and logarithms.)

The constructability of the regular 17-gon was merely one application of the general theory concerning congruences of the form  $a^n \equiv 1 \pmod{p}$  and in particular  $x^{p-1} - 1 \equiv 0 \pmod{p}$ . He discovered that the set of permutations that map the roots to themselves (known today as the

Galois group) provide a natural decomposition of the roots. The bulk of *Disquisitiones Arithmeticae* is an thorough investigation of modular arithmetic and its applications. For its methods and results, this was one of the most influential books of the early 19<sup>th</sup> century and it laid the foundations for algebraic number theory, abstract algebra, and analytic number theory.

Gauss's suggestion that cyclotomic theory could be extended to the lemniscate became a key issue in the work of Neils Able (1802–1829), on elliptic functions. Able read *Disquisitiones Arithmeticae* as a schoolboy in Norway and at age 19 he extended the techniques of Joseph-Louis Lagrange (1736-1813) and Gauss to prove that the quintic was not solvable by radicals. He was making progress in the general case of solvability before he died of tuberculosis at age 27. By 1809 *Disquisitiones Arithmeticae* was translated into French and Evariste Galois (1811–1832) generalized both Gauss's techniques and those of Abel to obtain results about solvability for equations in general. Abel and Galois independently invented the language of group theory and Galois showed that field extensions and groups of automorphisms were the key to understanding solvability. This area of study is now known as Galois Theory.

		
C.F. Gauss (1777-1855)	Niels Able (1802–1829)	Evariste Galois 1811–1832)

We will briefly discuss the theory of cyclotomic equations and then look at Gauss's original work. Following that we will state the fundamental theorem of Galois theory and compare this approach to solving cyclotomic equations. The 'base' field for most investigations will be the field of rational numbers,  $\mathbb{Q}$ .

A field  $K$  is an extension field of a field  $F$ , if  $F$  is a subfield of  $K$ . Therefore the extension field is usually written as  $K/F$ . The complex numbers  $\mathbb{C}$  are an extension field of the reals and the reals are an extension field of the rationals  $\mathbb{Q}$ . Every field extension  $K/F$  is also a vector space over  $F$ , where the 'scalars' are elements of  $F$ .  $[K:F]$  denotes the dimension (or degree) of this vector space. For example  $[\mathbb{C}:\mathbb{R}]$  is degree 2 with basis  $\{1, i\}$  and  $[\mathbb{R}:\mathbb{Q}]$  is an extension with degree equal to the cardinality of the continuum because it would be necessary to adjoin a continuum of numbers to the rationals to get the Reals.



A 'simple' extension of a field  $F$  is formed by adjoining a single element  $\zeta$ . In this case the extension can be written as  $F(\zeta)$ . For example the complex numbers are a simple extension of the reals so  $\mathbb{C} = \mathbb{R}(\zeta)$  where  $\zeta = \sqrt{-1}$ . This is also called an *algebraic extension* because  $\zeta^2 + 1 = 0$ . (If there is no such polynomial with coefficients in the 'base' field, the extension is transcendental.) The resulting field is also called a 'splitting field' because the polynomial  $\zeta^2 + 1$  can be factored. As indicated earlier, the numbers that can be generated in this fashion using  $\mathbb{Q}$  as the root field are called algebraic numbers and the remaining numbers are transcendental.

**Definition:** An *algebraic number* is a number that is a root of a non-zero polynomial in one variable with rational coefficients. The *minimal polynomial* of an algebraic number  $z$  is the unique irreducible polynomial  $p(x)$  with rational coefficients and leading coefficient 1, such that  $p(z) = 0$ .

**Definition:** A *number field* is a finite algebraic extension of  $\mathbb{Q}$

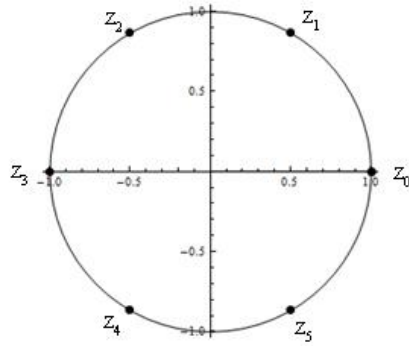
So  $\mathbb{Q}$  itself is a number field. The extension field  $\mathbb{Q}(\sqrt{2})$  consists of all numbers of the form  $\{a + b\sqrt{2}\}$  where  $a$  and  $b$  are rational. This field supports all the 'rational' operations of addition, subtraction, multiplication and division by non-zero elements. It contains  $\mathbb{Q}$  and is degree 2 so it is called a (real) quadratic field. Every number in this field is constructible and this is true for any even root. Every number field is of the form  $\mathbb{Q}(z)$  for some  $z$  so all number fields are simple extensions of  $\mathbb{Q}$ . The cyclotomic fields are a very important class of number fields.

**Definition:** The *nth cyclotomic field* is  $K_n = \mathbb{Q}(z)$  where  $z$  is a primitive  $n$ th root of unity.

The corresponding *cyclotomic equation* is  $z^n = 1$ . There are always  $n$  (complex) solutions which can be written as  $z_k = \cos(2\pi k/n) + i\sin(2\pi k/n)$  for  $k = 0, 1, 2, \dots, n-1$ . The primitive roots of the cyclotomic equation are those where  $z^n = 1$  and  $n$  is the smallest positive integer with this property. There are always  $\phi(n)$  primitive roots and any one of them can be used to generate the cyclotomic field  $K_n$ . They share the same minimal polynomial so they are called Galois conjugates. The corresponding minimal polynomial is called the *nth cyclotomic polynomial*  $\Phi(n)$ .

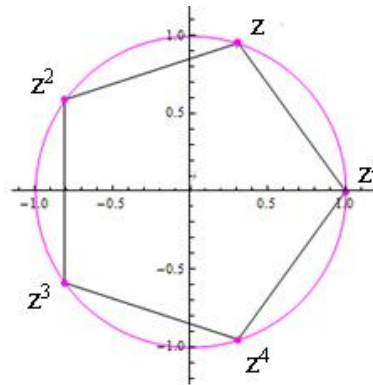
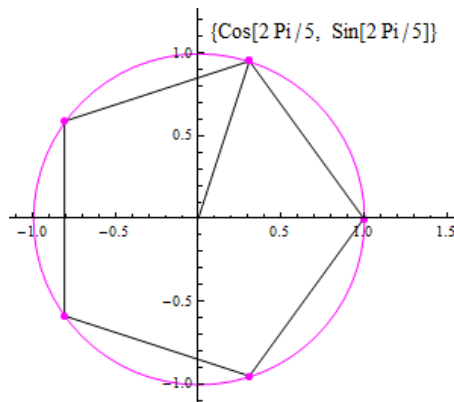
**Definition:** The *nth cyclotomic polynomial* is  $\Phi_n(x) = \prod_{k=1}^n (x - z_k)$  ( $z_k$  primitive)

**Example:** For  $n = 6$ ,  $z_1$  and  $z_5$  are the only primitive roots, so the minimal cyclotomic polynomial  $\Phi_6(x) = (x - z_1)(x - z_5) = x^2 - x + 1$  since  $z_1 + z_5 = 2\cos(2\pi/6) = 1$  and  $z_1 z_5 = 1$ .



In Mathematica: **Cyclotomic[6,x]** yields  $1-x+x^2$ . Note also that **Cyclotomic[6,x]\*Cyclotomic[3,x]\*Cyclotomic[2,x]\*Cyclotomic[1,x]** =  $(-1+x)(1+x)(1-x+x^2)(1+x+x^2) = x^6-1$ . (By convention **Cyclotomic[1,x]** =  $x-1$ ). This is always true, so  $\Phi_n$  can be obtained by dividing  $x^n-1$  by the product of the  $\Phi_d$ 's where  $d$  is a divisor of  $n$  (excluding  $n$ ). When  $n$  is prime, the only divisor is  $\Phi_1(x) = x-1$ .

**Example:** When  $n = 5$ , there are four primitive roots. Setting  $z = \cos(2\pi/5) + i\sin(2\pi/5)$  the remaining roots can be written as powers of  $z$ .

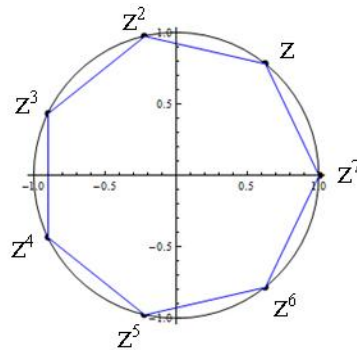


For constructability, it is just necessary to find  $\cos(2\pi/5)$ . The Greeks could do this easily using the Pythagorean Theorem to obtain  $\cos(2\pi/5) = \frac{1}{4}(-1+\sqrt{5})$ . We will use this example to illustrate the general procedure for solving cyclotomic polynomials. The first step is to divide  $z^5 = 1$  by  $z-1$  to get the irreducible cyclotomic polynomial:  $\Phi_5(z) = z^4 + z^3 + z^2 + z + 1 = 0$ .

Choose a primitive root such as  $z = \cos(2\pi/5) + i\sin(2\pi/5)$ . The complete set of primitive roots is  $\{z, z^2, z^3, z^4\}$ . Note that the four roots can be paired off into complex conjugates, so define  $s_1 = z + z^4$  and  $s_2 = z^2 + z^3$ . Both  $s_1$  and  $s_2$  are real, and in fact  $s_1 = 2\cos(2\pi/5)$ . To get an equation for  $s_1$ , note that  $s_1 + s_2 = -1$  and  $s_1 s_2 = -1$ . This yields the polynomial  $x^2 + x - 1 = 0$  whose roots are  $s_1$  and  $s_2$ , so  $s_1 = (\sqrt{5}-1)/2$ . It must be the positive root since  $\cos(2\pi/5)$  is positive. This implies that  $\cos(2\pi/5) = (\sqrt{5}-1)/4$  and is therefore constructible.

This procedure is much more general than the Pythagorean Theorem and it can be extended to all regular polygons. The prime cases are the most important, but of only a few yield nested quadratic equations which can be constructed. Let's see what goes wrong with  $n = 7$ .

**Example 2:** For  $z^7 = 1$ , the cyclotomic polynomial is  $\Phi_7(z) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$  and again we assume  $z = \cos(2\pi/7) + i\sin(2\pi/7)$  as shown below



Set  $s_1 = z + z^6$ ,  $s_2 = z^2 + z^5$ ,  $s_3 = z^3 + z^4$  Then  $s_1 + s_2 + s_3 = -1$  and  $s_1s_2 + s_1s_3 + s_2s_3 = -1 + -1 = -2$  and  $s_1s_2s_3 = 1$ .

This implies that  $s_1, s_2$  and  $s_3$  satisfy  $x^3 + x^2 - 2x - 1 = 0$ . Any roots of this equation would have to be integers and also divide  $-1$ , but neither  $1$  nor  $-1$  are roots, so this is the minimal equation for  $2\cos(2\pi/7)$ . The minimal polynomial for  $\cos(2\pi/7)$  is therefore  $8x^3 + 4x^2 - 4x - 1 = 0$ , which is also irreducible. Since this is a cubic, the roots cannot be constructed and the regular heptagon is not constructible.

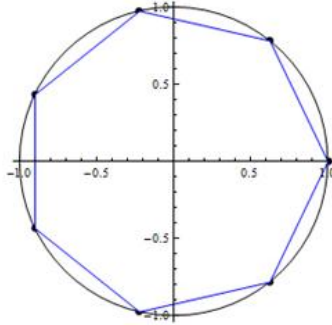
To do this with Mathematica: **V = ComplexExpand/@Roots[z^7==1,z]:**

$z = 1 \parallel z = i\cos[\frac{3\pi}{14}] + \sin[\frac{3\pi}{14}] \parallel z = i\cos[\frac{\pi}{14}] - \sin[\frac{\pi}{14}] \parallel z = -\cos[\frac{\pi}{7}] + i\sin[\frac{\pi}{7}]$   
 $\parallel z = -\cos[\frac{\pi}{7}] - i\sin[\frac{\pi}{7}] \parallel z = -i\cos[\frac{\pi}{14}] - \sin[\frac{\pi}{14}] \parallel z = -i\cos[\frac{3\pi}{14}] + \sin[\frac{3\pi}{14}]$

By convention, the list starts with  $z = 1$ . The second element is  $i\cos[3\pi/14] + \sin(3\pi/14)$  which is the same as  $z = \cos[2\pi/7] + i\sin[2\pi/7]$ , so this list matches the diagram above.

To extract the roots from V: **Roots= Table[V[[k]][[2]],{k,1,7}];**  
**Vertices= Table[{Re[#],Im[#]}&/@ Roots];**

**Graphics[{Circle[], AbsolutePointSize[6.0], Point[Vertices], EdgeForm[Blue],**  
**FaceForm[White], Polygon[Vertices]}, Axes->True]**



To get the minimal polynomial for  $\cos(2\pi/7)$  :

$$\text{MinimalPolynomial}[\text{Cos}[2*\text{Pi}/7]] = -1 - 4\#1 + 4\#1^2 + 8\#1^3 \&$$

In Mathematica  $\#k$  represents the  $k$ th argument to a (pure) function. For example a pure function can be defined as  $f = \#1 + \#2^3 \&$  where ' $\&$ ' says to apply this function to what follows, so  $f[2,3]$  is the same as  $\#1 + \#2^3 \& [2,3]$  which gives 29. The result above tells us that the answer is a pure function of degree 3 with a single argument. To get the answer as a function of  $x$ :

$$-1 - 4\#1 + 4\#1^2 + 8\#1^3 \&[x] = 8x^3 + 4x^2 - 4x - 1 = 0 \text{ as we discovered earlier.}$$

This equation is irreducible over  $\mathbb{Q}$  but the Fundamental Theorem of Algebra guarantees that roots exist. For a cubic, these formulas are well known. In Mathematica, **Solve** $[x^3 + x^2 - 2x - 1 == 0, x]$  will use traditional formulas (which have the peculiar property that the real roots are expressed in terms of imaginary radicals. This can be avoided by using trigonometric forms, but we already know the trigonometric form of the vertices.)

$$\{x \rightarrow \frac{1}{3}(-1 + \frac{7^{2/3}}{(\frac{1}{2}(1+3i\sqrt{3}))^{1/3}} + (\frac{7}{2}(1+3i\sqrt{3}))^{1/3})\}, \quad (= s_1 = 2*\text{Cos}[2\text{Pi}/7] \approx 1.2469796037)$$

$$\{x \rightarrow -\frac{1}{3} - \frac{7^{2/3}(1+i\sqrt{3})}{32^{2/3}(1+3i\sqrt{3})^{1/3}} - \frac{1}{6}(1-i\sqrt{3})(\frac{7}{2}(1+3i\sqrt{3}))^{1/3}\},$$

$$\{x \rightarrow -\frac{1}{3} - \frac{7^{2/3}(1-i\sqrt{3})}{32^{2/3}(1+3i\sqrt{3})^{1/3}} - \frac{1}{6}(1+i\sqrt{3})(\frac{7}{2}(1+3i\sqrt{3}))^{1/3}\}$$

Galois Theory shows that any cyclotomic (or cyclic) polynomial is explicitly solvable by radicals over  $\mathbb{Q}$ . In fact the roots above can be obtained without using formulas by applying the theory of symmetric functions. To back up to  $\Phi(z)$  we can solve  $s_1 = z + z^6$  for  $z$ . This is quadratic because  $z^6 = 1/z$ , so the resulting equation is degree 6 as it must be.

There are formulas for the minimal polynomials of  $\cos(2\pi/n)$  and  $\sin(2\pi/n)$ . These polynomials are closely related to the Chebyshev polynomials of the second kind. In Mathematica type **MinimalPolynomial[Cos[2Pi/n]]** or **MinimalPolynomial[Sin[2Pi/n]]**

When  $n$  is prime, the primitive roots form an even number of conjugate pairs and this guarantees that the degree of the minimal polynomial for  $\cos(2\pi/n)$  will be  $\phi(n)/2$ . Since  $\cos(2\pi/n)$  and  $\sin(2\pi/n)$  are related quadratically, the degree of  $\sin(2\pi/n)$  will be  $\phi(n)$ .

In general the relationship is as follows (from Paulo Ribenboim, *Algebraic Numbers*)

$$(i) \quad \deg(\cos(2\pi/n)) = \phi(n)/2$$

$$(ii) \quad \text{If } n \neq 4 \text{ and } n = 2^r m \text{ for } m \text{ odd, } \deg(\sin(2\pi/n)) = \begin{cases} \phi(n) & \text{if } r = 0 \text{ or } 1 \\ \frac{1}{4}\phi(n) & \text{if } r = 2 \\ \frac{1}{2}\phi(n) & \text{if } r \geq 3 \end{cases}$$

For example when  $n = 12$ ,  $\phi(n) = 4$  and the minimal polynomial for  $\cos(2\pi/12)$  is  $4x^2 - 3$  while the minimal polynomial for  $\sin(2\pi/12)$  is just  $2x - 1$ . The polynomials become more unwieldy as  $n$  increases.  $N = 11$  is the first to require a quintic.

Below is a comparison of  $\Phi_n(x)$  and the corresponding minimal polynomial of  $2\cos(2\pi/n)$

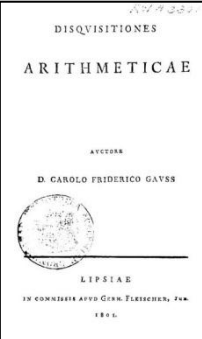
**MatrixForm[Table[{k,Cyclotomic[k,x],MinimalPolynomial[2\*Cos[2\*Pi/k]][x]},{k,3,16}]]**

3	$1 + x + x^2$	$1 + x$
4	$1 + x^2$	$x$
5	$1 + x + x^2 + x^3 + x^4$	$-1 + x + x^2$
6	$1 - x + x^2$	$-1 + x$
7	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6$	$-1 - 2x + x^2 + x^3$
8	$1 + x^4$	$-2 + x^2$
9	$1 + x^3 + x^6$	$1 - 3x + x^3$
10	$1 - x + x^2 - x^3 + x^4$	$-1 - x + x^2$
11	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10}$	$1 + 3x - 3x^2 - 4x^3 + x^4 + x^5$
12	$1 - x^2 + x^4$	$-3 + x^2$
13	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12}$	$-1 + 3x + 6x^2 - 4x^3 - 5x^4 + x^5 + x^6$
14	$1 - x + x^2 - x^3 + x^4 - x^5 + x^6$	$1 - 2x - x^2 + x^3$
15	$1 - x + x^3 - x^4 + x^5 - x^7 + x^8$	$1 + 4x - 4x^2 - x^3 + x^4$
16	$1 + x^8$	$2 - 4x^2 + x^4$

## ***Disquisitiones Arithmeticae* of C.F.Gauss (1801)**

The 19<sup>th</sup> century is often regarded as the ‘Golden Age’ of mathematics because of the great advances made by people such as Gauss, Able , Galois, Lagrange, Cauchy, Riemann, Weierstrass, Dedikind, Brouwer, Hilbert and Cantor.

Gauss completed work on *Disquisitiones Arithmeticae* 1798 when he was just 21 years old and a student at Göttingen. It was written in Latin which was still the language of choice for mathematicians in the early 19<sup>th</sup> century. We will use an English translation published by Springer Verlag in 1986. Below is the table of contents.

	Section I Congruent Numbers in General
	Section II Congruences of the First Degree
	Section III Residues of Powers
	Section IV Congruences of the Second Degree
	Section V Forms and Indeterminate Equations of the Second Degree
	Section VI Various Applications of the Preceding Discussions
	Section VII Equations Defining Sections of a Circle

Gauss was born in 1777 in Brunswick (Braunschweig), in the duchy of Braunschweig-Wolfenbüttele. His talents were recognized early and his education was supported by the Duke of Brunswick who allowed him to attend the university at Göttingen. The university was founded in 1737 by the British king George II – who was German by birth.



In 1795 when Gauss arrived at the university, he was treated to a very impressive library, where students could actually borrow books. Gauss was very adept at learning on his own. He read works of Leonhard Euler (1707-1783) and Euler’s doctoral student Joseph-Louis Lagrange (1736-1813) as well as Adrien-Marie Legendre (1752-1833). (In *Disquisitiones Arithmeticae* Gauss quotes 29 articles of Euler, 8 of Lagrange and 2 of Legendre.)

Throughout his life Gauss accumulated his own library of works – not all of which were on science and mathematics. He was interested in literature and philosophy as well. One of the first books he borrowed from the Göttingen library was *Clarissa*, by Samuel Richardson which was very popular at the time. Gauss’s calculating prowess was aided by tables of logarithms. The duke of Brunswick gave him Johann Schulze’s two volume set of books on logarithms and trigonometry. He would eventually add many more such books to his collection.

As a young man, Gauss was fascinated by number theory where his computational abilities were of great value. He was to later remark “*Mathematics is the Queen of sciences and number theory is the Queen of mathematics.*” He compiled extensive tables based on his own investigations and those of Euler and Lagrange and Legendre . The major result in *Disquisitiones Arithmeticae* is a proof of the law of quadratic reciprocity – which was first conjectured by Legendre and independently formulated by Gauss.

In Section III (Residues of Powers), Gauss begins the study of geometric progressions with the classic theorem of Fermat: (article 50):

$$a^{p-1} \equiv 1 \pmod{p} \text{ (where } p \text{ is an odd prime and } a \text{ is not a multiple of } p)$$

So  $5^6 \equiv 1 \pmod{7}$  and in fact 5 has the maximal possible period which is 6. The members of this cycle are  $\{5, 5^2, 5^3, 5^4, 5^5, 5^6\} \equiv \{5, 4, 6, 2, 3, 1\} \pmod{7}$ . In Euler’s language 5 is a ‘primitive root’ mod 7.

In modern terminology, the integers mod 7 are an example of a finite field. The additive and multiplicative tables are shown below. These are called Cayley tables after Arthur Cayley (1821-1895). The multiplicative group is called  $Z_7^*$ . It has only 6 elements, but in the table 0 is included for comparison with the additive table. In Mathematica, using the [Abstract Algebra](#) package, `SwitchStructureTo[Ring]; CayleyTables[Z[7], Mode -> Visual]`

		Add . y									Mult . y								
	x	0	1	2	3	4	5	6			0	1	2	3	4	5	6		
	0	0	1	2	3	4	5	6			0	0	0	0	0	0	0		
	1	1	2	3	4	5	6	0			1	0	1	2	3	4	5		
	2	2	3	4	5	6	0	1			2	0	2	4	6	1	3		
	3	3	4	5	6	0	1	2			3	0	3	6	2	5	1		
	4	4	5	6	0	1	2	3			4	0	4	1	5	2	6		
	5	5	6	0	1	2	3	4			5	0	5	3	1	6	4		
	6	6	0	1	2	3	4	5			6	0	6	5	4	3	2		

To see why  $5^6 \equiv 1 \pmod{7}$ , note that  $(6 \cdot 5)(5 \cdot 5)(4 \cdot 5)(3 \cdot 5)(2 \cdot 5)(1 \cdot 5) = 6!5^6$  and the numbers  $(6 \cdot 5), (5 \cdot 5), \dots, (1 \cdot 5)$  must all be distinct mod 7, because 5 and 7 are relatively prime. Therefore the left side is  $6! \pmod{7}$ . The  $6!$  term can be cancelled on both sides because  $6!$  is relatively prime with 7. The general proof of Fermat’s theorem follows these same lines.

Even though  $Z_7^*$  is a cyclic group, not all the elements are generators. The only generators of  $Z_7^*$  are 3 and 5. The number of generators is always  $\phi(p-1)$ . Of course Fermat's theorem works for the remaining elements of  $Z_7^*$ , but their prime period is less than 6. For example  $\{2, 2^2, 2^3, 2^4, 2^5, 2^6\} \equiv \{2, 4, 1, 2, 4, 1\}$ . This defines an order 3 subgroup of  $Z_7^*$ . It is easy to prove that a cyclic group  $G$  must have a subgroup for every divisor of  $\phi(G)$ . The only other non-trivial subgroup of  $Z_7^*$  is  $\{6, 1\}$  which is generated by 6.

As Gauss realized, there is a close connection between Fermat's theorem and cyclotomics via the congruence  $x^{p-1} \equiv 1 \pmod p$  for prime  $p$ . Below is a letter he wrote to Christian Gerling who was a former student:

*"Already earlier I had found everything related to the separation of the roots of the equation  $x^{p-1} - 1 \equiv 0$  into two groups on which the beautiful theorem in the D. A. on p. 637 (article 357) depends, in the winter of 1796 (during my first semester in Gottingen), without having recorded the day. By thinking with great effort about the relation of all the roots to each other with respect to their arithmetic properties, I succeeded, while I was on a vacation in Braunschweig, on that day (before I got out of bed) in seeing this relation with utmost clarity, so that I was able to make on the spot the special application to the 17-gon and to verify it numerically."*

When  $p = 17$ , the corresponding group determined by Fermat's theorem is  $Z_{17}^*$  which has 16 elements and is cyclic. The separation of the roots that Gauss discovered, was generated by the subgroup of order 8. Subsequent subgroups of order 4, 2 and 1, completed the chain of quadratic extensions necessary for construction of the 17-gon.

Gauss did not use the language of groups, but he knew the cycles and periods of congruences. These are now called Gaussian periods. He knew that 3 was a primitive root of 17 and he used this generator to find the correct partition of the roots. In modern cyclotomic theory, the group  $Z_{17}^*$  is called the Galois group for  $p = 17$ . It is the group of automorphisms which map the 16 primitive roots to themselves.

(Note that the full set of  $p$  vertices also forms a group under (complex) multiplication, but these vertices are not independent and the corresponding equation is not irreducible. Gauss was one of the first mathematicians to realize the importance of working only with irreducible equations.)

To see the connection between Fermat's result and quadratic reciprocity, suppose  $p$  is an odd prime, so it is of the form  $p = 2q + 1$ . Then Fermat's theorem says that  $a^{2q} - 1 \equiv 0 \pmod p$ , so

$$a^{2q} - 1 = (a^q - 1)(a^q + 1) \equiv 0 \pmod p$$

This gives two possibilities:  $a^q \equiv 1$  or  $a^q \equiv -1 \pmod p$  (where  $q = (p-1)/2$ ). The choice clearly depends on the relationship between  $a$  and  $p$ .



For example with  $a = 5$  and  $p = 7$ , we saw above that  $5^6 \equiv 1 \pmod{7}$  but this does not tell us whether  $5^3 \equiv 1$  or  $5^3 \equiv -1$ . In the first case, 5 is said to be a *quadratic residue* mod 7 and otherwise it is a non-residue. Here  $5^3 \equiv 6 \pmod{7} \equiv -1$ , so 5 is a non-residue mod 7. The only residues mod 7 are 1, 2 & 4 so 3, 5 & 6 are non-residues.

**Definition:** An integer  $a$  is a *quadratic residue* mod  $n$  iff there is an integer  $x$  such that  $a \equiv x^2 \pmod{n}$ .

So quadratic residues are perfect squares mod  $n$ . In the case of  $n = 7$ , if there was a solution to  $5 \equiv x^2$ , then  $(x^2)^3$  would have to be 1, but we know that  $5^3 \equiv -1$ .

For a given prime  $p$ , there are only  $p-1$  possible  $a$ 's and they are evenly divided among the residues and non residues. As Gauss points out in article 107, for a given prime  $p$ , it is easy to find the residues and nonresidues by simply making a table of all possible squares that could appear mod  $p$ . Clearly we only need to compute the squares of  $1, 2, \dots, (p-1)/2 \pmod{p}$ .

In Mathematica: **Table[Mod[n^2,13], {n,1,6}] = {1,4,9,3,12,10}** gives the 6 residues mod 13.

The hard part is to determine the distribution of these residues. For example, which primes have 3 as a residue? From the table above,  $p = 13$  is one such prime because  $4^2 \equiv 3 \pmod{13}$ . Among the first six odd primes, 3 is only a residue for  $p = 11$  and  $p = 13$ . Euler, Lagrange, Legendre and Gauss were all interested in the distribution of these residues (and the distribution of primes in general). Quadratic residues have many applications. They can be used to solve second degree congruences or to factor certain large numbers. Gauss discovered that they also play a role in cyclotomic theory.

In article 108 Gauss proves that -1 is a (quadratic) residue of all primes of the form  $4k + 1$  and a non-residue of the  $4k + 3$  primes. For example  $-1 \equiv 12 \pmod{13}$  and this is in the list of residues above. Note that 13 and 17 are 'twin'  $4k + 1$  primes, and clearly 16 is a residue mod 17. Every Fermat prime  $p$  is of the form  $4k + 1$ , so  $p-1$  is always a residue.

The composite cases can be determined from the primes, so the crucial cases are when two primes are residues of each other. The fundamental theorem – Section IV, article 131:

*“If  $p$  is a prime number of the form  $4n+1$ ,  $+p$  will be a residue or nonresidue of any prime number which taken positively is a residue or non residue of  $p$ . If  $p$  is of the form  $4n+3$ ,  $-p$  will have the same property.”*

Gauss explains at the end of Section IV that this simple form of the theorem was unique, but that Euler used this fact in his work and later realized that he could not provide a proof. Legendre attempted a proof but he realized that his proof depended on propositions which he could not demonstrate. Gauss's proof is about 30 pages long and has multiple cases to consider. In Gauss's words *“The proof tortured me for the whole year and eluded the most strenuous efforts, before finally, I got the proof explained in the fourth section of Disquisitiones Arithmeticae.”*

**Example:** To find whether 3 is a quadratic residue mod 13, note that 13 is a  $4n+1$  prime so we can use reciprocity and ask the simpler question of whether 13 is a residue mod 3. The equation  $x^2 \equiv 13 \pmod{3}$  is the same as  $x^2 \equiv 1 \pmod{3}$ , and this has the trivial solution  $x = 1$ , so the answer is ‘yes, 3 is a residue mod 13 because 13 is a residue mod 3’. Given that 3 is a quadratic residue of 13, it may still be difficult to find the corresponding square. In this case the numbers are small and we already know from the table above that  $4^2 \equiv 3 \pmod{13}$ .

Equations Defining Sections of a Circle (Section VII of *Disquisitiones Arithmeticae*)

*“Among the splendid developments contributed by modern mathematicians, the theory of circular functions without a doubt holds a most important place. ...The reader might be surprised to find a discussion of this subject in the present work which deals with a discipline apparently so unrelated; but the treatment itself will make it abundantly clear that there is an intimate connection between this subject and Higher Arithmetic.”*

Gauss assumes a cyclotomic equation  $x^n = 1$ , with  $n$  an odd prime and  $X$  is the reduced cyclotomic equation:  $x^{n-1} + x^{n-2} + \dots + x + 1 = 0$  (which we call  $\Phi(n)$ )

Article 354 ( $n = 17$ ) *“Here  $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$  so the calculation will be reduced to four quadratic equations. For the positive root we will take the number 3. The least residues of its powers relative to the modulus 17 are the following:”* (\*Note that 3 will generate  $Z_{17}^*$  the multiplicative group mod 17 which is isomorphic to the Galois group  $G$ . In Appendix A, we will repeat Gauss’s steps in the framework of Galois theory. For any Fermat prime greater than 3, 3 is a quadratic nonresidue by the reciprocity theorem, so it is always a primitive root.\*)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

*“From this we derive the following distributions of the complex  $\Omega$  into two periods of 8 terms each, then four of four terms each, and eight of 2 terms.”* (Since [1] represents the root  $r^1$ , the notation (8,1) is the period 8 sum of the powers of  $r^1$ , so it is every other term in the table above:  $(8,1) = r + r^9 + r^{13} + \dots$  and (8,3) is the complement:  $r^3 + r^{10} + \dots$ . In terms of automorphisms the elements of (8,1) define a subgroup of the Galois group  $G$ .)

$$\Omega = (16,1) \left\{ \begin{array}{l} (8,1) \left\{ \begin{array}{l} (4,1) \left\{ \begin{array}{l} (2,1) \dots [1], [16] \\ (2,13) \dots [4], [13] \end{array} \right\} \\ (4,9) \left\{ \begin{array}{l} (2,9) \dots [8], [9] \\ (2,15) \dots [2], [15] \end{array} \right\} \end{array} \right\} \\ (8,3) \left\{ \begin{array}{l} (4,3) \left\{ \begin{array}{l} (2,3) \dots [3], [14] \\ (2,5) \dots [5], [12] \end{array} \right\} \\ (4,10) \left\{ \begin{array}{l} (2,10) \dots [7], [10] \\ (2,11) \dots [6], [11] \end{array} \right\} \end{array} \right\} \end{array} \right\}$$

“The equation (A) whose roots are the sums (8,1),(8,3) is found by the rules of article 351 to be  $x^2 + x - 4 = 0$ . (\* since  $(8,1) + (8,3) = -1$  and  $(8,1)(8,3) = -4$  \*) Its roots are

$$-(1/2) + \sqrt{17/2} = 1.5615528128 \text{ and } -(1/2) - \sqrt{17/2} = -2.5615528128$$

And we will set the former to be (8,1) and latter (8,3).... “

Gauss derives all the roots but he does not give details for every equation because he has already done the more difficult case of  $n=19$ . Below is a summary table for the basic equations which he calls (A),(B),(C),(D). These will generate roots [1] & [16] shown in his summery table above.

- (A)  $x^2 + x - 4 = 0$  Roots (8,1) & (8,3)
- (B)  $x^2 - (8,1)x - 1 = 0$  Roots (4,1) and (4,9)
- (C)  $x^2 - (4,1)x + (4,3) = 0$  Roots (2,1) and (2,13)
- (D)  $x^2 - (2,1)x + 1 = 0$  Roots [1] and [16]

For example to get (B):  $(4,1) = r + r^{13} + r^{16} + r^4$  and  $(4,9) = r^9 + r^{15} + r^8 + r^2$  Note that (4,1) is just every other term of (8,1). It also defines a subgroup of G1 and (4,9) is the complement . By definition  $(4,1) + (4,9) = (8,1)$ , and a little algebra shows that  $(4,1)(4,9) = -1$ .

In Article 365, Gauss sets [1] equal to  $\cos(2\pi/17) + i\sin(2\pi/17)$  so that  $\cos(2\pi/17) = \frac{1}{2}(2,1) = \frac{1}{2}([1] + [16])$  . He notes that this yields the equation given below :

$$\cos(2\pi/17) = \frac{1}{16} \left[ -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} \right]$$

Mathematica gives the same equation by nesting (A), (B) and (C) and simplifying. In the compass and straightedge construction process, equation (D) is solved automatically by placing the above length on the x-axis and moving up to a unit circle. Algebraically this process is not symmetric. The minimal cosine polynomial is order 8, but for sine, it is the full order 16. In

Mathematica, **MinimalPolynomial[ ]** yields the following for  $2\cos[2\text{Pi}/17]$  and  $2\sin[2\text{Pi}/17]$

$$1 - 4x - 10x^2 + 10x^3 + 15x^4 - 6x^5 - 7x^6 + x^7 + x^8$$

$$17 - 204x^2 + 714x^4 - 1122x^6 + 935x^8 - 442x^{10} + 119x^{12} - 17x^{14} + x^{16}$$

Gauss points out that if a prime  $n$  is of the form  $2^m + 1$ , then  $m$  must be either 2 or 1, so these powers of 2 are nested. “All values of  $n$ , therefore that can be reduced to quadratic equations are contained in the form  $2^{2^v} + 1$  . Thus the five numbers 3,5,17,257 and 65537 result from letting  $v = 0,1,2,3,4$  .”

He continues “Whenever  $n-1$  involves prime factors other than 2 we are led to equations of higher degree, namely to one or more cubic equations when 3 appears once or several times among the prime factors of  $n-1$ , to equations of the fifth degree when  $n-1$  is divisible by 5.etc... We can show with all rigor that these higher degree equations cannot be avoided in any way, nor

*can they be reduced to lower degree equations. The limits of the present work exclude this demonstration here.”*

This implies that Gauss had a proof of the necessity for Fermat primes, but it was never published. In 1837 Pierre Wantzel published a proof of the necessity. The key to that proof is the irreducibility of the cyclotomic polynomial  $\Phi(x)$  for arbitrary values of  $n$ . Gauss never used the term ‘irreducible’ but he knew the importance of this fact. In article 42 (Gauss’s Lemma) and article 341 he showed that for prime  $p$ , the cyclotomic polynomial  $\Phi(x)$  is irreducible over  $\mathbb{Q}$ . (This was generalized by Eisenstein and Schönemann in about 1850 but  $p$  still had to be prime.)

Based on this fact it is obvious that no prime polygon could be constructed unless it was a Fermat prime. Suppose  $p$  is a prime polygon which can be constructed. Then  $\cos(2\pi/p)$  is constructible. Therefore it must satisfy a polynomial which is a power of 2 and this implies that  $\cos(2\pi/p) + i\sin(2\pi/p)$  also satisfies a polynomial which is a power of 2 (one higher power). But the latter also satisfies the cyclotomic polynomial  $\Phi(x)$  which is degree  $p-1$  and irreducible. Therefore  $p-1$  is a power of 2.

As we pointed out earlier, the only other case that needs to be proven impossible is when  $n$  is of the form  $p^k$  for  $k > 1$  and  $p$  an odd prime. Gauss addresses this issue in the last article of the book, article 366. It is clear that he knew how to finish the proof, but he had not yet found general conditions for the cyclotomic polynomial  $\Phi(x)$  to be irreducible. Gauss stated in his diary that he had a proof for all values of  $n$ , but it was never published.

According to [Olaf Neumann](#) “As for the cyclotomic polynomials for arbitrary indices, Gauss claimed in entry 136 of his diary, in 1808 that he could prove their irreducibility over the rationals for composite indices too. But up to the present time (2007) no one seems to be able to reconstruct a proof in ‘Gaussian style’ “

Neumann goes on to point out that for constructions of regular polygons, it is only necessary to have a proof for powers of a prime and Alfred Lowery states that in all probability Gauss had such a proof when *Disquisitiones Arithmeticae* was published because it would only involve a “slight extension of the arguments in article 341”.

(There seems to be some confusion on this issue by members of the mathematical community and as of July 2012 the Wikipedia article on [cyclotomic polynomials](#) attributes the general case to Gauss.)

A proof that the cyclotomic polynomial is always irreducible can be found in section 8.4 of van der Warden’s *Algebra*, which is based primarily on the lectures of E. Artin and E. Noether. This proof does not depend on Galois theory but it does use the uniqueness of prime factorization in principle ideal rings. Based on the irreducibility of the cyclotomic polynomial, it is easy to provide the sufficient and necessity conditions for compass and straightedge constructions. This is done in Section 8.9 of the van der Warden’s text, and the argument is given below. It is almost identical to Gauss’s argument in article 366 except that irreducibility plays an important part in setting the stage.

Assume a regular polygon with  $h$  sides and set  $\zeta = \cos(2\pi/h) + i\sin(2\pi/h)$  as the primitive  $h$ th root of unity. Then  $\zeta + \zeta^{-1} = 2\cos(2\pi/h)$ . Since this sum is carried into itself only by the substitutions  $\zeta \rightarrow \zeta$  and  $\zeta \rightarrow \zeta^{-1}$  of the Galois group of the cyclotomic field, it generates a real subfield of degree  $\phi(h)/2$ . The condition for constructability is that  $\phi(h)/2$  and hence  $\phi(h)$ , be a power of 2.

Now for  $h = 2^{v_1} q_1^{v_1} \dots q_r^{v_r}$  (where the  $q_i$  are odd primes), we have

$$\phi(h) = 2^{v_1-1} q_1^{v_1-1} \dots q_r^{v_r-1} (q_1 - 1) \dots (q_r - 1)$$

Thus the condition is that only the first powers of the odd prime factors ( $v_i = 1$ ) may divide  $h$  and furthermore that for every odd prime  $q_i$  dividing  $h$  the number  $q_i - 1$  be a power to the base 2; that is every  $q_i$  must be of the form:  $q_i = 2^k + 1$

Which are the primes of this form? Note that  $k$  cannot be divisible by an odd number except 1 because otherwise  $q_i$  would not be prime, so  $k$  must be of the form  $2^\lambda$  and therefore

$$q_i = 2^{2^\lambda} + 1$$

Only the values 0,1,2,3,4 are known to yield prime numbers: 3,5,17, 257,65537

*“As soon as the number  $h$  contains, besides powers of 2, only primes of the sequence 3,5,17,... to at most the first power, the regular polygon with  $n$  sides will be constructible (Gauss).”*

The proof of irreducibility of the cyclotomic equation for arbitrary  $n$  is more difficult than the ‘powers of a prime’ case. If Gauss felt that the full case was within reach, that could explain why he left it to others to complete the construction proof. He certainly knew that the converse was true and he did not agonize over it as he did with the formulas at the end of article 356. This article provides an important link between cyclotomic theory and quadratic residues and after publication, Gauss took 4 years to settle this issue to his satisfaction.

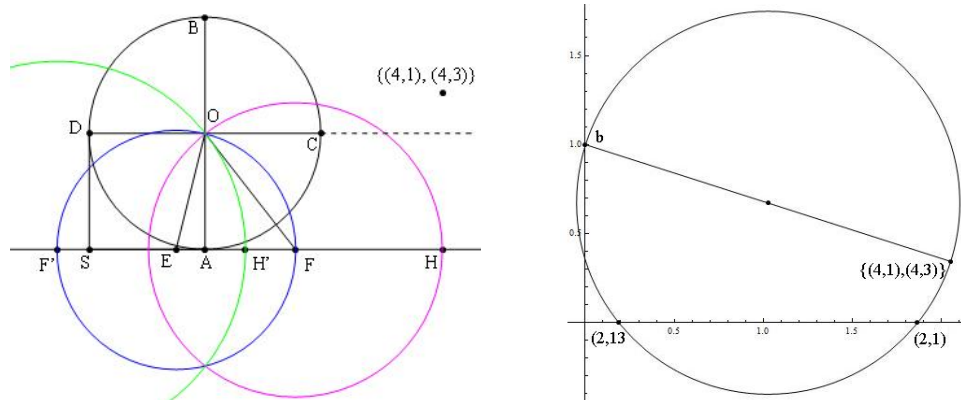
In *Disquisitiones Arithmeticae* Gauss refers to Section VIII which was never published, but after Gauss died in 1855, his student Richard Dedekind published Gauss’s notes for this section which was titled *Disquisitiones generales de congruentiis*. It was to be a study of higher congruences with respect to a prime number and as such would pave the way for a theory of function fields and higher order residue classes. These notes were written at about the same time as *Disquisitiones Arithmeticae* (c. 1797), but they had grown in size and complexity so that it was not practical to include them in the original text.

A number of mathematicians worked in this newly emerging field of algebraic number theory. These included Lejeune Dirichlet, Carl Gustav Jakob Jacobi, Gotthold Eisenstein, Richard Dedekind, Ernst Kummer, and David Hilbert. One of their goals was to generalize quadratic reciprocity for higher powers. In 1900 Hilbert proposed the problem of finding the ‘most general’ reciprocity law for an arbitrary number field. In 1927 Emil Artin found a general theorem that answered Hilbert’s proposal.

Another motivation behind algebraic number theory was to prove (or disprove) Fermat’s Last Theorem which says that there are no integer solutions to  $x^k + y^k = z^k$  for  $k > 2$ . In 1847, Gabriel Lamé outlined a proof when  $k$  is prime. His proof was based on cyclotomic theory where the factoring took place in the field of complex numbers. Unfortunately some cyclotomic fields do

The real breakthrough was the Taniyama–Shimura conjecture which provides a link between elliptic curves over  $\mathbb{Q}$  and certain modular forms. This conjecture gained credibility when it was independently discovered by André Weil in 1967. In 1986 Ken Ribet showed that Fermat’s Last Theorem was a special case of the Taniyama–Shimura conjecture. This inspired Andrew Wiles to prove that the Taniyama–Shimura conjecture was true for semistable elliptic curves and this was sufficient to show that Fermat’s Last Theorem was true. This proof was completed in 1995. The full conjecture was proven in 2001 by Brian Conrad, Fred Diamond and Chris Breuil.

Below is a very literal construction of  $2\cos(2\pi/17)$  from Benjamin Bold's Famous Problems in Geometry. It is based on Gauss's procedure and we have revised the notation to reflect that of Gauss. The construction uses only equations (A), (B) and (C). The two solutions to (C) are  $(2,1) = r + r^{16} = 2\cos(2\pi/17)$  and  $(2,13) = 2\cos(8\pi/17)$ . These values are approximately 1.864944459 and 0.1845367189 as seen on the right below. The circle on the right solves the quadratic (C):  $x^2 - (4,1)x + (4,3) = 0$ .



On the left diagram  $H = \{(4,1), -1\}$  and  $H' = \{(4,3), -1\}$ . The first step is to find  $E = (1/4)SA$ . The blue circle at  $E$  defines  $F$  and  $F'$  and the magenta circle at  $F$  defines  $H$  while the green circle at  $F'$  defines  $H'$ .

## Appendix A: Galois Theory

**Definition:** Given a field  $F$  and an extension  $K$ , the *Galois group* of the extension  $G(K/F)$  is the group of all field automorphisms  $\sigma$  which map  $F$  to itself. (If  $H$  is a subgroup of  $G(K/F)$  then the fixed field of  $H$  is the subset of  $K$  that is fixed by  $H$ .)

For a given polynomial  $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  with coefficients in  $F$ , and (complex) solutions  $z_1, z_2, \dots, z_n$ , the corresponding extension is written  $F[p(x) = 0]$  and is called a *polynomial extension*. For  $z$  in  $C$ , the *minimal polynomial* over  $F$  is the (monic) polynomial of lowest degree such that  $p(z) = 0$ .

If two numbers such as  $z_1$  and  $z_2$  share the same minimal polynomial, they are called *algebraic conjugates*. This is a generalization of the fact that complex conjugates  $z$  and  $\bar{z}$  share the same minimal polynomial.

A field extension of the form  $F[x^2 = 0]$  is called a quadratic extension and in general an extension such as  $F[x^n = 0]$  is called a *radical extension*. All radical extensions have abelian Galois groups, so any field that can be reached from  $F$  by a sequence of radical extensions has a Galois group which is itself has a nested series of abelian subgroups:

### Theorem: (The Fundamental Theorem of Galois Theory)

Let  $F$  be a field of characteristic 0 and let  $K$  be an extension field which is the root field of some irreducible polynomial  $f(x)$ . Let  $G$  be the group of automorphisms of  $K$  that fix  $F$ . Then  $G$  is called the Galois group of the extension and written  $G = G(K/F)$ .

1. For every field  $F_1$  such that  $F \subseteq F_1 \subseteq K$  there is a subgroup  $G_1$  of  $G$  consisting of those elements of  $G$  that leave fixed each element of  $F_1$  so  $G_1 = G(K:F_1)$
2. For  $G_1$  as defined in part 1, the order of  $G_1$  is the degree of  $K$  over  $F_1$  so in particular  $o(G) = [K:F]$
3. For every subgroup  $G_1$  of  $G$  there is a subfield  $F_1$  of  $K$  consisting of those elements of  $K$  left fixed by the elements of  $G_1$
4. There is a 1-1 correspondence between the subgroups of  $G$  and the extensions of  $F$

$$F \subset F_1 \subset F_2 \dots \subset F_n = K \quad \text{iff} \quad G \supset G_1 \supset G_2 \dots \supset G_n$$

A polynomial  $f(x)$  is solvable by radicals iff its Galois group  $G$  is solvable. A Galois group is solvable iff (i) the series ends at the trivial subgroup  $G_n = \{1\}$  and (ii)  $G_{i+1} \triangleleft G_i$  which means that  $G_{i+1}$  is a normal subgroup of  $G_i$  and (iii) each factor group  $G_i/G_{i+1}$  is cyclic of prime order.

**Example 1:** For  $p$  prime, the irreducible cyclotomic polynomial  $\Phi_p(z) = \frac{z^p - 1}{z - 1}$  has (primitive) roots  $\{z, z^2, \dots, z^{p-1}\}$ . The elements of the extension field  $\mathbb{Q}(z)$  are the linear combinations of these roots (along with 1), so this is a normal extension. Every automorphism of  $\mathbb{Q}(z)$  must map these roots to each other, so they are of the form  $\sigma(z) = z^k$  for  $k = 1, \dots, p-1$ . Therefore the Galois group  $G$  is a cyclic group of order  $p-1$  which is isomorphic to  $Z_{p-1}^*$ . This implies that all subgroups will be abelian and hence normal. Therefore all prime cyclic polynomials are solvable by radicals. (In fact this is true for any value of  $n$  and the corresponding Galois group will be cyclic of order  $\phi(n)$ .)

For example with  $n = 17$  the cyclic Galois group is isomorphic to  $Z_{16}^*$ , the multiplicative group mod 17 – which is order 16. As Gauss pointed out, one generator of this group is  $\sigma_3$ . (There are  $\phi(16) = 8$  such generators). Define  $\lambda_k = (\sigma_3)^k$  (where  $(\sigma_3)^0$  is the identity transformation) and the Galois group can be written as  $G = \{ \lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8, \lambda_9, \lambda_{10}, \lambda_{11}, \lambda_{12}, \lambda_{13}, \lambda_{14}, \lambda_{15} \}$ . This defines the first row of Gauss's table which is reproduced below. The second row gives the exponents after applying each element of  $G$  to  $z$ .

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

For the subgroup  $G_1$  take the even elements so  $G_1 = \{ \lambda_0, \lambda_2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}, \lambda_{12}, \lambda_{14} \}$ . To find the elements of  $\mathbb{Q}(z)$  fixed by  $G_1$  just apply each element of  $G_1$  to  $z$ . This yields Gauss's  $(8,1) = z + z^9 + z^{13} + \dots$  and  $(8,3)$  is just  $\lambda_1(8,1) = z^3 + z^{10} + \dots$ . Since  $(8,1) + (8,3) = -1$  and  $(8,1)(8,3) = -4$ , the first quadratic in the chain is  $x^2 + x - 4 = 0$ . The corresponding quadratic extension field  $F_1$  consists of the elements of  $\mathbb{Q}(z)$  left fixed by  $G_1$ , so  $F_1 = \mathbb{Q}((8,1))$ .

The resulting chain of normal subgroups is

$$G \supset G_1 = \{ \lambda_0, \lambda_2, \lambda_4, \lambda_6, \lambda_8, \lambda_{10}, \lambda_{12}, \lambda_{14} \} \supset G_2 = \{ \lambda_0, \lambda_4, \lambda_8, \lambda_{12} \} \supset G_3 = \{ \lambda_0, \lambda_8 \} \supset G_4 = \{ \lambda_0 \}$$

The corresponding fields are:  $\mathbb{Q} \subset F_1 = \mathbb{Q}((8,1)) \subset F_2 = F_1((4,1)) \subset F_3 = F_2((2,1)) \subset F_4 = F_3((1))$

So the root field of  $\Phi_n(z)$  is  $F_4$  and each extension is quadratic.

**Example 2:** The general  $n$ th order polynomial with integer coefficients has Galois group  $S_n$  which is the symmetric group on  $n$  elements. It has order  $n!$ . The alternating group  $A_n$  is a subgroup of  $S_n$  with  $n!/2$  elements and for  $n > 4$ , it is simple (and not abelian). Therefore one possible series is  $S_n \supset A_n \supset \{1\}$ . This series is not normal and the Jordan Holder Theorem says that any two composition series are equivalent. Therefore the general polynomial of order 5 or greater is not solvable by radicals. (The Galois groups  $S_1, S_2, S_3$  and  $S_4$  are all solvable.)



**Example 3:**  $N = 11$  has Galois group  $Z_{10}^* = C_{10}$  which can be generated by  $\sigma_2$  (the automorphism that maps  $z$  to  $z^2$ ). Using Gauss's notation, the period 10 table is shown below:.

0	1	2	3	4	5	6	7	8	9
$z$	$z^2$	$z^4$	$z^8$	$z^5$	$z^{10}$	$z^9$	$z^7$	$z^3$	$z^6$

The period 5 subgroup is  $C_5$  which is generated by  $\sigma_5$  and this yields every other term in the table above so  $(5,1) = \{z, z^4, z^5, z^9, z^3\}$ .  $C_5$  is a simple group so the chain of normal subgroups is very short:  $G = C_{10} \supset G_1 = C_5 \supset \{1\}$ .

The question is, what is  $F_1$  ? What field has  $C_5$  as its group of automorphisms ? This is the same as asking what is the minimal polynomial for  $2\cos(2\pi/11)$ , because that polynomial will have Galois group equal to  $C_5$ . If we ask Mathematica this question the answer is

$$\text{MinimalPolynomial}[2\text{Cos}[2\text{Pi}/11]] = 1 + 3x - 3x^2 - 4x^3 + x^4 + x^5$$

The five elements of  $G_1$  are generated by  $\sigma_5$  which clearly fixes the real numbers in  $\mathbb{Q}[\Phi(z)]$  and these have as basis the conjugate pairs  $s_1 = \{z + z^{10}\}$ ,  $s_2 = \{z^2 + z^9\}$ ,  $s_3 = \{z^3 + z^8\}$ ,  $s_4 = \{z^4 + z^7\}$ ,  $s_5 = \{z^5 + z^6\}$ . These should be the zeros of the minimal polynomial. We can verify that the polynomial given above is correct by substitution, or we can derive the coefficients by taking sums of products. For example to verify that the coefficient of  $x^3$  is -4, we need to find all products of 2 terms:  $s_1s_2 + s_1s_3 + s_1s_4 + \dots + s_4s_5$  which is  $4(z + z^2 + z^3 + \dots + z^{10})$  as given above.

## Appendix B: Trisections and Origami Paper Folding

In a 1988 article in the *American Mathematical Monthly*, Andrew Gleason discusses the issue of which regular polygons would be constructible if angles could be trisected. Not surprisingly the answer goes back to Gauss. For trisections to work there must be 'towers' of 3 in  $n-1$ , just like Gauss needed powers of 2. With both bisections and trisections it is possible to combine quadratics and cubics, so  $n$  has to be of the form  $2^k 3^j + 1$ , This means that 7 is accessible and so are 13, 17, 19, 37, ..

The number of trisections grows with  $n$ , but for 7 and 13 one trisection will suffice and 19 needs 2 (of course 17 needs none). Gleason also points out that quinsections would enable the 11-gon to be constructed. Based on results dating back to Gauss, it can be concluded that:

".. a regular  $n$ -gon can be constructed if, in addition to ruler and compass, equipment is available to  $p$ -sect any angle for every prime  $p$  that divides  $\phi(n)$ ."

## Appendix C: Origami Constructions

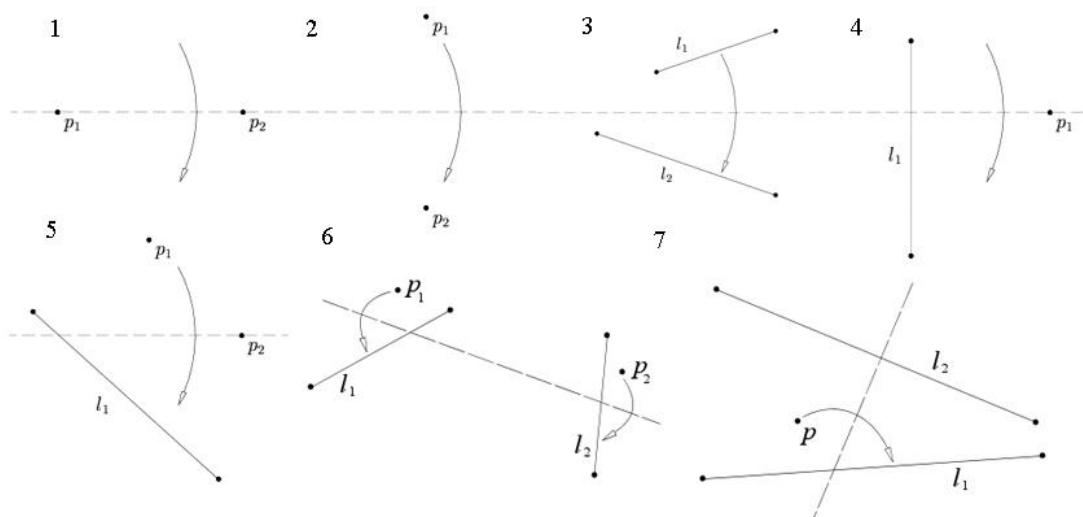
**Origami** is the art of paper folding. The name is derived from Japanese ‘ori’ for paper and ‘gami’ for folding. Origami has been an art form in Japan for more than 400 years, but paper folding as played a part in many other cultures – notably in China, Spain and Germany. The related art of kirigami allows paper to be cut and pasted as well as folded.

Origami has recently become a ‘science’ due primarily to axioms which can be used to characterize the possible constructions. Origami axioms have been proposed by a number of authors – notably Jacques Justin, Humiaki Huzita, Koshiro Hatori, Roger Alperin, David Auckly, John Cleveland, Robert Geretschlager and Robert Lang.

The most commonly recognized algorithms are the 7 Huzita-Hatori axioms shown below. They are not minimal, but they have been shown to be complete by Roger Lang who is a physicist and one of the foremost origami designers in the world today

1. Given two points  $p_1$  and  $p_2$ , there is a unique fold that passes through both of them.
2. Given two points  $p_1$  and  $p_2$ , there is a unique fold that places  $p_1$  onto  $p_2$ .
3. Given two lines  $l_1$  and  $l_2$ , there is a fold that places  $l_1$  onto  $l_2$ .
4. Given a point  $p_1$  and a line  $l_1$ , there is a unique fold perpendicular to  $l_1$  that passes through point  $p_1$ .
5. Given two points  $p_1$  and  $p_2$  and a line  $l_1$ , there is a fold that places  $p_1$  onto  $l_1$  and passes through  $p_2$ .
6. Given two points  $p_1$  and  $p_2$  and two lines  $l_1$  and  $l_2$ , there is a fold that places  $p_1$  onto  $l_1$  and  $p_2$  onto  $l_2$ .
7. Given one point  $p$  and two lines  $l_1$  and  $l_2$ , there is a fold that places  $p$  onto  $l_1$  and is perpendicular to  $l_2$ .

The 7 diagrams for these constructions are shown below – courtesy of the wikipedia site on the [Huzita-Hatori axioms](#).



These axioms are listed order of increasing ‘complexity’. Roger Alperin calls the first three axioms the Thalian constructions after Thales who was the teacher of Pythagoras. The fourth algorithm allows for bisections, and axioms 1-4 together define the Pythagorean numbers which were studied by Hilbert in his *Foundations of Geometry*. At this stage the possible origami numbers are weaker than the compass and straight edge numbers (which are called the Euclidean numbers.) David Auckly and John Cleveland discuss this case and show that:

“Everything which can be constructible with origami is constructible with a compass and straight edge, but the converse is not true.”

For example using axioms 1-4 it is not possible to construct a right triangle with hypotenuse  $\sqrt{2 + \sqrt{2}}$  and leg 1.

Axioms 1-5 together define the Euclidean numbers which are the points constructible by compass and straight edge.

Axiom 6 is known as the neusis axiom because it mimics Archimedes method for trisecting an angle. Axiom 7 has been rediscovered a number of times, but it does not add to the possible constructions.

The neusis method involved lining points up with a marked ruler and this is essentially what is done in the origami trisection process. These became known as the ‘Viète marked ruler constructions’ and the set of numbers constructible in this way are called ‘Viétens’.

As pointed out above by Andrew Gleason, trisections of angles (along with the traditional compass and straight edge constructions) extends the possible regular polygon constructions to include all primes of the form  $2^{k3^j} + 1$  for non-negative integers j and k. These are known as Pierpont primes – named after the American mathematician James Pierpont (1866-1938). They clearly contain the Fermat primes as a proper subset and Gleason conjectured that there are an infinite number of Pierpont primes. The first few are

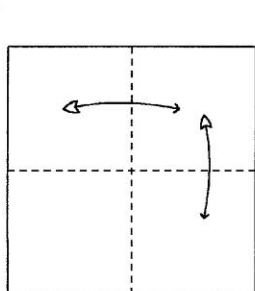
2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257 (sequence [A005109](#) in [OEIS](#))

All of these regular polygons can be constructed with origami using axioms 1-6. We will give an example of the regular heptagon by Robert Geretschlager, who has also constructed the regular 19-gon. Origami experts such as Kazuo Haga and Tomoko Fuse have also tackled the Platonic solids.

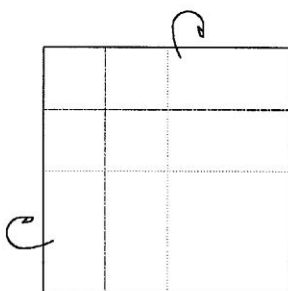
### **Construction the Regular Heptagon with Origami**

The 13-step procedure shown below is due to Robert Geretschlager. He starts with a 4 inch piece square of paper which is assumed to be centered at the origin. Using standard origami notation, the dashed lines represent ‘valley’ folds and dot-dashed lines represent ‘mountain’ folds. Thin lines represent previous folds. In the figures below, the point M is the origin. A =  $\{-1, -1/2\}$  are B

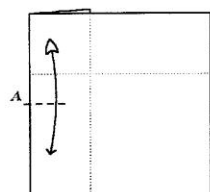
$= \{0,1\}$  are foci of parabolas (recall that cubics can generally be represented as intersections of parabolas). The point E has y coordinate  $-2\cos(2\pi/7)$ .



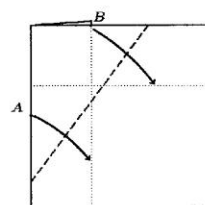
Fold and unfold twice.



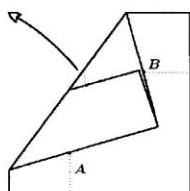
Fold back twice.



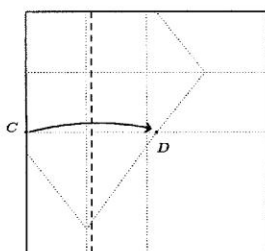
Fold and unfold, making a crease mark at point A (bisecting the side).



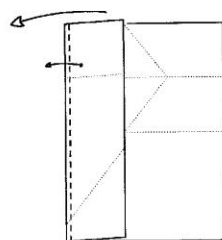
Fold such that A and B come to lie on the creases.



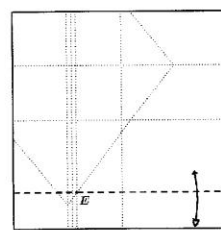
Unfold everything.



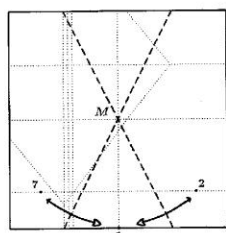
Fold C to D.



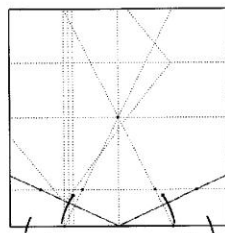
Fold and unfold both layers at crease, then unfold everything.



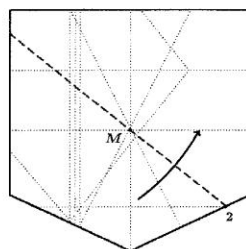
Fold horizontally through E, then unfold.



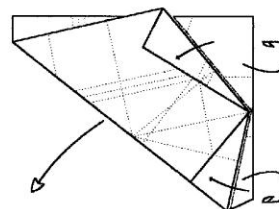
Fold through M, such that 1 lies on crease, resulting in 2 and 7 (M is the mid-point of the heptagon, 1, 2 and 7 are corners).



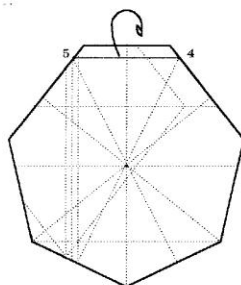
Fold back twice, so that the marked points come to lie on one another; resulting folds are first two sides of the heptagon.



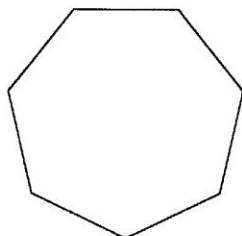
Fold through M and 2.



Fold back lower layers using edges of upper layer as guidelines; resulting folds are two more sides of the heptagon; open up fold from step 12 and repeat 11 and 12 on left side.



Fold back final edge of the heptagon through 4 and 5.

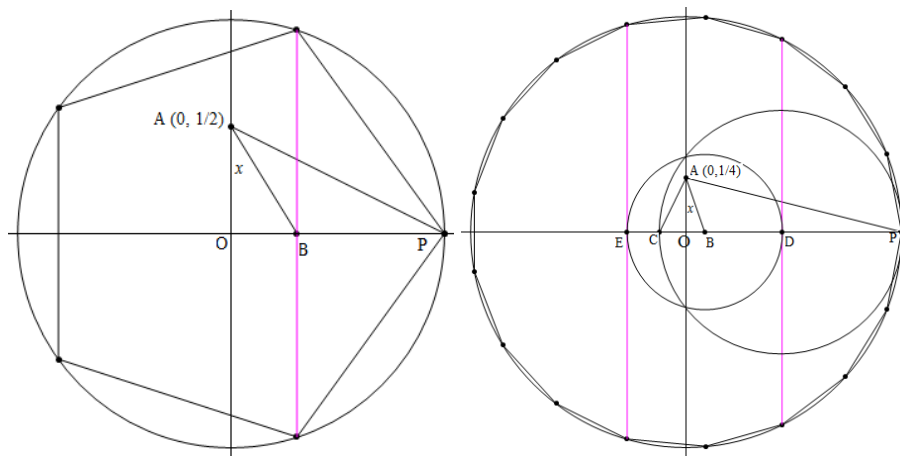


The finished heptagon.

## Appendix D: H.W. Richmonds' 1893 Constructing of the Regular 5-gon and Regular 17-gon

Over the years there have been many different constructions for the regular pentagon and regular 17-gon. The constructions shown below are due to H.W. Richmond in 1893. (See *Mathematical Recreations and Essays* by W.W. Rouse Ball and H.M.S.Coxeter.) Both constructions are based on the same principle and they are simple and elegant. The pentagon construction takes just 2 steps and the 17-gon construction takes 6 steps.

For reference we have drawn the final version of the polygons as they would appear when inscribed in a unit circle, with vertex 1 at  $\{1,0\}$ . So in both diagrams P is at  $\{1,0\}$ .



To construct the generating arc for the regular pentagon takes just 2 steps (on the left above)

- (i) Locate point A at  $(0, 1/2)$  as shown
- (ii) Bisect angle OAP to obtain angle  $x$  and this defines point B and vertex 2.

To construct the generating angle for the regular 17-gon takes 6 steps

- (i) Locate the point A at  $(0, 1/4)$
- (ii) To find B, set the angle  $x$  to  $1/4$  of angle OAP
- (iii) To find C, make the angle CAB equal to  $\pi/4$
- (iv) The point D is the center of CP and this determines vertex 4 .
- (v) Point E and vertex 6 are obtained from a circle centered at B passing through D
- (vi) Now subtract the two arcs.

In terms of the Lemoine measure of complexity for constructions, there are slightly less complex constructions using Carlyle circles, but no one knows the minimal complexity.

## Bibliography

Alperin, R.C., A Mathematical theory of origami constructions and numbers, Yew York Journal of Mathematics, Vol 6 (2000), pp 119-133

Alperin, R.C., Trisections and totally real origami, American Mathematical Monthly, Vol 112, No. 3 (March 2005), pp 200-211

Alperin, R.C., A Totally real folding of the regular heptagon, see [alperin@math.sjsu.edu](mailto:alperin@math.sjsu.edu)

Auckly D., Cleveland, J., Real origami and impossible paper folding, American Mathematical Monthly, Vol 102, No. 3, (March 1995), pp. 215-226

Ball, W.W & Coxeter H.M.S. ,*Mathematical Recreations and Essays* , Dover Publications, 1987 (13<sup>th</sup> edition of 1974 text)

Bold, B. , *Famous Problems of Geometry and How to Solve Them*, Dover Publications, 1982

Cox D.A., Shurman, J, Geometry and number theory on clovers. American Mathematical Monthly, Vol 112, No. 8,(Oct. 2005), pp.682-704)

DeTemple, D.W. Carlyle circles and the Lemoine simplicity of polygon constructions, American Mathematical Monthly, Vol 98, No.2 (1991) pp. 97-108

Fuse,T.,Unit Origami, Japan Publications, Tokyo,(1990)

Gauss, Carl Friedrich, *Disquisitiones Arithmeticae*, Springer Verlag, Berlin, 1986 (Translated by Arthur A. Clark, revised by William Waterhouse)

Gauss, Carl Friedrich; Maser, Hermann (translator into German) (1965), *Untersuchungen über höhere Arithmetik (Disquisitiones Arithmeticae & other papers on number theory) (Second edition)*, New York: Chelsea

Geretschlager, R. Euclidean constructions and the geometry of origami, Mathematics Magazine, Vol. 68, N0.5, (Dec. 1995) pp 357-371

Geretschlager, R., Folding the Regular Heptagon

Gleason, A. Angle trisection, the heptagon and the triskaidecagon, American Mathematical Monthly, Vol 95, No. 3 ,1988, pg. 185-194

Goldstein, C. Schappacher, N., Schwermer, J. (editors) , *The Shaping of Arithemtic after C.F. Gauss's Disquisitiones Arithmeticae*, Springer Verlag, 2007. [Pdf available here](#).

Hibbard A.C., Levasseur K.M. *Exploring Abstract Algebra with Mathematica*, ISBN 0-3387-98619-7, Telospub.com.

Hull, T., A note on “Impossible” paper folding, *American Mathematical Monthly*, Vol 103, No. 3 (March 1996) pp. 210-241

Jones, B.W. *Introduction to Modern Algebra*, MacMillan Publishing, 1975

Kunihiko, K, Takahama, T., *Origami for the connoisseur*, Japan Publications, Tokyo (1987)

Loewy, Alfred, Über eine algebraische Behauptung von Gauss. II. Jahresbericht der DMV 30 155-158, (1921)

Rotman, J.J. *Theory of Groups*, Allyn and Bacon, Boston, 1968

Ribenboim, Paulo, *Algebraic Numbers*, Wiley Interscience, 1972

van der Waerden, B.L. *Algebra* (vol I), Springer Verlag, Berlin, 2003 (from the 7<sup>th</sup> edition, originally translated in 1966 from the German text *Moderne Algebra* (1930-31.)