GAUSS AND THE HEPTADECAGON

TOM RIKE   OAKLAND HIGH SCHOOL

Background

At the Bay Area Math Meet at USF in 2004, the final problem on the *Test of Ingenuity* was included mainly to ensure that there would be no perfect papers. The statement of the problem is as follows.

$$\text{Let } \theta = 2\pi/17. \text{ Compute } \cos\theta + \cos 4\theta + \cos 9\theta + \cdots + \cos\ 15^2\theta + \cos\ 16^2\theta.$$

Upon seeing the number 17, I immediately thought of the Gauss construction of the heptadecagon. When I got home, I went to my well-worn volume of *100 Great Problems of Elementary Mathematics* by Dörrie [5]. Gabriel Carroll once told me that he read it over the summer when he was in the eighth grade. I myself have only been able to work my way through about twenty of the problems in the past 35 years. In any case, by just following the method of Gauss through the first stage of the heptadecagon construction, I was able to solve the problem. However, I was mystified by how someone could dream up such a procedure, especially since it involves the product of a sum of 8 complex numbers times another sum of 8 complex numbers which results in 64 complex numbers that miraculously sum to a integer. When I saw Paul Zeitz later in the year at ARML, I mentioned my solution to him and he told me that he had not used this method. In fact, his problem can be solved for any prime of the form $4k+1$. This talk then, is to share with you the results of my research in this area in an attempt to understand these mysteries.

A Review of Some Preliminaries

From Euler, we have $e^{i\theta} = \cos\theta + i\sin\theta$. See [**Problem 1**]. It is then easy to see that $e^{i\theta} + e^{-i\theta} = 2\cos\theta$ and $(e^{i\theta})^n = e^{ni\theta} = \cos n\theta + i\sin n\theta$. (DeMoivre's Theorem.) Summing a geometric sequence gives $1+z+z^2+z^3+\cdots+z^{n-1} = (z^n-1)/(z-1)$. Therefore, $z^n-1 = (z-1)(z^{n-1}+z^{n-2}+\cdots+z^2+z+1)$. Note that $e^{2\pi ki/n}$ is a solution of $z^n-1=0$ for all $k\in\mathbb{N}$. For n distinct solutions take $k\in\{0,1,2,3,\ldots,n-1\}$ or for n odd, $k\in\{0,\pm1,\pm2,\ldots,\pm(n-1)/2\}$. If k is relatively prime to n, $e^{2\pi ki/n}$ is called a primitive n^{th} root of unity. Using the mod notation introduced by Gauss in *Disquisitiones Arithmeticae* [7] we have that $e^{2\pi ki/n} = e^{2\pi mi/n}$ if $k\equiv m \pmod n$. ($a\equiv b \pmod n$ iff $a-b$ is a multiple of n.) Note that the sum of the solutions is 0 and $(-1)^n$ times the product of the solutions is -1. The graph of these solutions in the plane, with the x-axis as the real axis and the y-axis as the imaginary axis, is a set of n points on the unit circle, starting at $(1,0)$ and spaced equally around the circle. In other words, these solutions are the vertices of a regular n-gon. If $\cos 2\pi/n$ can be constructed with a straightedge and compass then the regular n-gon can be constructed by constructing a perpendicular to the x-axis at $\cos 2\pi/n$. The intersections with the unit circle are the vertices of the n-gon adjacent to $(1,0)$. The notation $\mathbb{Z}/17\mathbb{Z}$ will refer to the set of numbers $\{1,2,3,\ldots,17\}$ with multiplication being defined modulo 17. For example $\mathbf{13}\cdot\mathbf{5} = 65 \equiv \mathbf{14} \pmod{17}$.

Constructibility

A figure can be constructed with a straightedge and a compass if and only if the points required are located by using only the following three constructions: the intersection of two lines, the intersection of a line and a circle, or the intersection of two circles. This is equivalent to saying the coordinates of the points are sums, differences, products, quotients, and iterated square roots of coordinates of previously located points. For example $\sqrt[3]{2}$ **is not** constructible since it requires a **cube** root, but the following number **is** constructible since it only uses **square** roots: $\dfrac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\right)$. See [**Problem 2**]. For more information on constructibility see Dickson [3] and Martin [13]. When Gauss was 18 years old on March 30, 1796, he discovered that regular polygons with a prime number of sides are constructible if that prime is of the form $2^{2^n}+1$. In *Disquisitiones Arithmeticae* he writes " It is certainly astonishing that although the geometric divisibility of the circle into three parts and five parts was already known in Euclid's time, nothing was added to this discovery for 2000 years. And all geometers had asserted that, except for those sections and the ones that derive directly from them (that is division

Date: **January 5, 2010**   **Berkeley Math Circle**.

into $15, 3 \cdot 2^\mu, 5, 5 \cdot 2^\mu$ and 2^μ parts), there are no others that can be effected by geometric constructions." Gauss was so taken with this discovery that he changed his field of study from Philology to Mathematics and requested that a regular $2^{2^2}+1$ sided polygon by engraved on his tombstone. Although his wishes were not carried out, at the base of a statue of Gauss in his birthplace, Brunswick, there is a golden regular stellated 17-gon formed from the longest diagonals of a regular 17-gon.

Fermat Numbers

Fermat conjectured the sequence of Fermat numbers, $F_n = 2^{2^n}+1$ generated prime numbers for $n \geq 0$. He died in 1665 still believing this was true. Euler, in 1730, showed that $2^{2^5}+1 = 4,294,967,297$ is not prime, ironically, by using a technique that Fermat himself had discovered. Euler was able to show that an odd prime divisor of $2^{2^n}+1$ must be of the form $2^{n+1}k+1$. See [**Problem 3**]. So Euler began looking at $\{64k+1\} = \{65, 129, 193, 257, 321, 385, 449, 513, 577, 641, \dots\}$. Those which are prime are 193, 257, 449, 577, and 641. Dividing these numbers successively into $2^{2^5}+1$, Euler discovered upon the fifth division that $2^{2^5}+1 = 641 \cdot 6700417$. In 1877, Edward Lucas proved that the k must be even, so only primes of the form $128k+1$ need be checked. There are only 21 numbers of this form less than $\sqrt{6700417}$ and only 6 of them are prime. Therefore after 6 divisions one can conclude that the other factor, 6700417, is prime and $2^{32}+1 = 641 \cdot 6700417$ is completely factored. As an exercise, see how long it takes you to follow these steps.

Fermat also claimed to have a proof that every prime of the form $4k+1$ has a unique representation as a sum of two squares. Euler in 1749, published a proof. Note that $2^{2^5}+1 = (2^{16})^2+1^2 = 20449^2+62264^2$. Since $2^{2^5}+1$ is one more than a multiple of 4 and primes of this form have only one decomposition into the sum of two squares, this proves that it is not prime without any division. (Of course the question is, where did 20449 and 62264 come from?) For another proof that $2^{2^5}+1$ is composite that also does not require any division see [**Problem 4**]. An apocryphal story that has been around for over one hundred years is that Fermat was aware that the Chinese had a conjecture that $n|2^n-2$ implies n is prime. It is discussed in the 1973 book by Honsberger [10] . To see how this conjecture would prove Fermat's claim see [**Problem 5**]. Empirical evidence would certainly support the conjecture. It is true for integers less than 341 and 2^{341} has 103 digits. However, $2^{341}-2 = 2(2^{340}-1) = 2((2^{10})^{34}-1^{34}) = 2(2^{10}-1)(\cdots) = 2(1023)(\cdots) = 2(3 \cdot 341)(\cdots)$ and $341 = 11 \cdot 31$ is not prime. Numbers such as 341 are called *pseudoprimes*. See Honsberger [10] for more details. I believed the story about Fermat and the Chinese conjecture until recently, when I read in *The* New *Book of Prime Number Records* by Ribenboim [15] that it is not true. Ribenboim also describes how the story originated in the late 19th Century in China and how this conjecture came to be known in the West as an "old Chinese" theorem.

In any case, Fermat could not have been more wrong. In the intervening years, no other prime Fermat numbers have turned up. $F_5, F_6, F_7, \dots, F_{32}$ are known to be composite. There are 221 Fermat numbers that are known to be composite. The smallest Fermat number of unknown status is F_{33}. The largest known composite Fermat number is $F_{2478782}$. The number that tells how many digits $F_{2478782}$ has is a number with 746188 digits. For example, if a number has a million digits, then it takes a seven digit number, $1,000,000$ to tell this. The up-to-date information on the Fermat Numbers as well as the history can be found at the `http://www.prothsearch.net/fermat.html` website. There are many interesting facts about Fermat numbers and I originally planned to talk about many of them, but the details of constructing regular polygons and time constraints has displaced them. I highly recommend the book *17 Lectures on Fermat Numbers* by Křížek et.al. [12] to those interested in pursuing the topic.

Final Problem on the Test of Ingenuity at BAMM 2004

Now we will look at the solution to the BAMM problem that Paul Zeitz sketched for me. Let $\theta = 2\pi/17$, $\zeta = e^{i\theta}$, and let $N = \cos\theta + \cos 4\theta + \cos 9\theta + \cdots + \cos 15^2\theta + \cos\ 16^2\theta$. Then $2N = 2\cos\theta + 2\cos 4\theta + 2\cos 9\theta + \cdots + 2\cos 15^2\theta + 2\cos\ 16^2\theta$. Since $2\cos\theta = e^{i\theta}+e^{-i\theta}$, this gives $2N = \zeta+\zeta^{-1}+\zeta^4+\zeta^{-4}+\zeta^9+\zeta^{-9}+\cdots+\zeta^{15^2}+\zeta^{-15^2}+\zeta^{16^2}+\zeta^{-16^2}$. But $\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2\} = \{1, 4, -8, -1, 8, 2, -2, -4, -4, -2, 2, 8, -1, -8, 4, 1\}$ mod 17. The other 16 values are the same numbers with the signs reversed, so $N = \zeta+\zeta^4+\zeta^9+\cdots+\zeta^{15^2}+\zeta^{16^2}$. Paul now suggests adding 1 and squaring, so that $(1+N)^2 = (\zeta^0+\zeta+\zeta^4+\zeta^9+\cdots+\zeta^{15^2}+\zeta^{16^2})^2$. He says, "You are now looking at sums of $\zeta^{m^2+n^2}$, where $0 \leq m, n \leq 16$ and the exponents are evaluated modulo $17\dots$. Now you can cleverly count out the incidences of $0, 1, 2, \dots, 16$ among the exponents and you deduce that the non-zero values all occur with the same frequency, but 0 occurs more often (17 more times), giving a total squared sum of 17." (Recall that the sum of all the roots is 0). Therefore $1+N = \sqrt{17}$ and the answer to the question is $N = \boldsymbol{\sqrt{17}-1}$.

This idea is not restricted to Fermat primes or even primes of the form $4k+1$. Gauss began investigating the problem in *Disquisitiones Arithmeticae*, where in article 356 he proves for any integer k not divisible by

p where Q is the set of all positive quadratic residues less than p and N is the set of all non-residues

$$\begin{aligned}\sum \cos \frac{kQ\pi}{p} - \sum \cos \frac{kN\pi}{n} &= \pm\sqrt{p} \\ \sum \sin \frac{kQ\pi}{p} - \sum \sin \frac{kN\pi}{n} &= \quad 0\end{aligned}$$

for $p \equiv 1 \pmod 4$. On the other hand for $p \equiv 3 \pmod 4$ the first difference will be 0 and the second $= \pm\sqrt{p}$. Gauss then goes on to say, " These theorems are so elegant that they deserve special note. We observe that the upper signs always hold when for k we take unity or a quadratic residue of p and the lower when k is a nonresidue. These theorems retain the same or even greater elegance when they are extended to composite values of p. But these matters are of a higher level of investigation, and we will reserve their consideration for another occasion." It took Gauss from May 1801 until August 1805 to determine the sign of what are now called *Gauss Sums.* For more information see Savitt [16], Rademacher [14], Dirichlet [4], Davenport [2], and Ireland [11] in order of increasing reading difficulty. I have found no easy introduction to the subject.

Construction of Regular Polygons

To get a better idea of regular polygon construction based on the complex roots of unity, let's first construct a regular pentagon. The vertices are the graph of the solutions to $z^5-1 = (z-1)(z^4+z^3+z^2+z+1) = 0$. Let $\theta = 2\pi/5$ and $\zeta = e^{i\theta}$. Then the solutions to the equation are $\{\zeta^0, \zeta^1, \zeta^2, \zeta^3, \zeta^4\}$. Note that $\zeta^1+\zeta^4 = \zeta^1+\zeta^{-1}$ and $\zeta^2+\zeta^3 = \zeta^2+\zeta^{-2}$, Letting $z = \zeta^1$, the equation becomes $\zeta^4+\zeta^3+\zeta^2+\zeta^1+1 = 0$, or $\zeta^{-1}+\zeta^{-2}+\zeta^2+\zeta^1+1 = 0$. Since $(a+a^{-1})^2 = a^2+2+a^{-2}$, the equation can be rewritten as $(\zeta^1+\zeta^{-1})^2 + (\zeta^1+\zeta^{-1}) - 1 = 0$. This is a quadratic equation and so $\zeta^1+\zeta^{-1} = \frac{-1\pm\sqrt{5}}{2}$. But $\zeta^1+\zeta^{-1} = 2\cos 2\pi/5$. Since $\cos 2\pi/5 > 0$, $\cos 2\pi/5 = \frac{-1+\sqrt{5}}{4}$. Now construct a perpendicular to the x-axis at $\cos 2\pi/5$. The intersection of the perpendicular with the unit circle gives the vertices of the pentagon adjacent to $(1,0)$.

Now to tackle the heptadecagon. The procedure is taken from Stewart [18] who based it on Hardy [8]. As before the vertices are the graph of the solutions to $z^{17}-1 = (z-1)(z^{16}+z^{15}+z^{14}+\cdots+z+1) = 0$, Let $\theta = 2\pi/17$, $\zeta = e^{i\theta}$, and ζ^k for $k \in \{0, \pm1, \pm2, \ldots, \pm8\}$ are the solutions. If a number $a \in \mathbb{Z}/17\mathbb{Z}$ generates $\mathbb{Z}/17\mathbb{Z}$, that is, $\{a, a^2, a^3, \ldots, a^{16}\} = \mathbb{Z}/17\mathbb{Z}$, then a is called a primitive root of $\mathbb{Z}/17\mathbb{Z}$. (Gauss proved that $\mathbb{Z}/p\mathbb{Z}$ has a primitive root a when p is equal to 2, 4, the power of an odd prime, or twice the power of an odd prime.) 3 is a primitive root of $\mathbb{Z}/17\mathbb{Z}$. Then using the powers of 3 for exponents we have $\{\zeta^{3^1}, \zeta^{3^2}, \zeta^{3^3}, \zeta^{3^4}, \zeta^{3^5}, \ldots, \zeta^{3^{13}}, \zeta^{3^{14}}, \zeta^{3^{15}}, \zeta^{3^{16}}\} = \{\zeta^3, \zeta^9, \zeta^{10}, \zeta^{13}, \zeta^5, \zeta^{15}, \zeta^{11}, \zeta^{16}, \zeta^{14}, \zeta^8, \zeta^7, \zeta^4, \zeta^{12}, \zeta^2, \zeta^6, \zeta^1\}$. Now Gauss defines two periods of length 8 using every other term.

$$\begin{aligned}x_1 &= \zeta^9+\zeta^{13}+\zeta^{15}+\zeta^{16}+\zeta^8+\zeta^4+\zeta^2+\zeta^1 \\ x_2 &= \zeta^3+\zeta^{10}+\zeta^5+\zeta^{11}+\zeta^{14}+\zeta^7+\zeta^{12}+\zeta^6\end{aligned}$$

[Note that x_1 consists of all the powers that are squares in $\mathbb{Z}/17\mathbb{Z}$.] Also notice that $x_1+x_2 = -1$ since x_1+x_2 is the sum of all the roots except $\zeta^0 = 1$. Now comes the amazing step of multiplying $x_1 \cdot x_2$. After long thought and much research I finally found in Rademacher [14] a clear way to show the 64 terms in the product sum to give $x_1 \cdot x_2 = -4$. This means that x_1 and x_2 are the roots of the quadratic equation $X^2+X-4 = 0$. Since it is clear geometrically that $x_1 > 0$, we have $x_1 = \frac{-1+\sqrt{17}}{2}$ and $x_2 = \frac{-1-\sqrt{17}}{2}$. (At this point the solution to the BAMM problem has been found since $N = 2x_1 = -1+\sqrt{17}$.) The next step in the Gauss construction is to set up periods of length 4, taking every other term in x_1 and x_2.

$$y_1 = \zeta^{13}+\zeta^{16}+\zeta^4+\zeta^1 \qquad y_2 = \zeta^9+\zeta^{15}+\zeta^8+\zeta^2 \qquad y_3 = \zeta^3+\zeta^5+\zeta^{14}+\zeta^{12} \qquad y_4 = \zeta^{10}+\zeta^{11}+\zeta^7+\zeta^6$$

Now $y_1+y_2 = x_1$ and $y_1 \cdot y_2 = -1$ with $y_1 > y_2$ so that y_1 and y_2 are roots of the equation $Y^2 - x_1Y - 1 = 0$. Similarly, $y_3+y_4 = x_2$ and $y_3 \cdot y_4 = -1$ with $y_3 > y_4$ so that y_3 and y_4 are roots of the equation $Y^2 - x_2Y - 1 = 0$ Note that $y_1 = \zeta^1+\zeta^{-4}+\zeta^{-1}+\zeta^4 = 2\cos\theta + 2\cos 4\theta$ and $y_3 = \zeta^3+\zeta^5+\zeta^{-3}+\zeta^{-5} = 2(\cos 3\theta + \cos 5\theta) = 4\cos\theta\cos 4\theta$. So that $z_1 = 2\cos\theta$ and $z_2 = 2\cos 4\theta$ are the roots of the equation $Z^2 - y_1Z + y_3$ with $z_1 > z_2$. (To avoid the trigonometry see **Problem 6**.) Use the values of x_1 and x_2 to solve for y_1 and y_3. Then use these values to solve for $z_1/2 = \cos 2\pi/17 = \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-16\sqrt{34+2\sqrt{17}}-2(1-\sqrt{17})\sqrt{34-2\sqrt{17}}}\right)$. Although this value is constructible [**Problem 7**], an elegant solution was discovered in 1893 by H. W. Richmond that comes from substituting $\tan 4\phi = 4$ into the first quadratic $X^2+X-4 = 0$ to get $X^2+4X\cot 4\phi - 4 = 0$. Then $x_1 = 2\tan 2\phi$ and $x_2 = -2\cot 2\phi$. As a final problem, show that $y_1 = \tan(\phi+\pi/4)$, $y_2 = \tan(\phi-\pi/4)$, $y_3 = \tan\phi$, $y_4 = -\cot\phi$, so that $2(\cos 3\theta + \cos 5\theta) = \tan\phi$ and $4(\cos 3\theta\cos 5\theta) = \tan(\phi-\pi/4)$. See Stewart [18], Baragar [1], Tignol [19], and Hartshorne [9] for the Galois connection that completes the story on constructible regular polygons by proving the claim of Gauss that no other regular n-gons can be constructed beyond those he showed to be constructible. This was first proved in 1837 by Pierre Wantzel at the same time he proved that, in general, angle trisection and cube duplication with a straightedge and compass are also impossible. See Smith [17] for another construction and see the handout for Richmond's method.

Some Problems

(1) With $x = i\theta$, use the power series representations , $e^x = 1 + x/1! + x^2/2! + x^3/3! + \cdots$, $\cos x = 1 - x^2/2! + x^4/4! - \cdots$, and $\sin x = x/1! - x^3/3! + x^5/5! - \cdots$ to prove $e^{i\theta} = \cos\theta + i \sin\theta$.

(2) Consider $\frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\right)$. Convince yourself that it is constructible by constructing $17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}$.

(3) If a is even and p is a prime that is not a factor of a and $p|a^2+1$ (the notation $a|b$ stands for a divides b), then $p = 4k+1$ for some integer k. To show this, note that p is odd since it is not a factor a. Therefore $p = 4k+1$ or $4k+3$. Suppose $p = 4k+3$. By Fermat's little theorem, $p|a^{p-1}-1 = a^{4k+3-1}-1 = a^{4k+2}-1$. But $a^{4k+2}+1 = (a^2)^{2k+1}-1 = (a^2+1)[(a^2)^{2k-2}-(a^2)^{2k-3}+\cdots-a^2+1]$. Since $p|a^2+1$ we have $a^{4k+2}+1$ is a multiple of p. Therefore the difference of two multiples of p, $(a^{4k+2}+1)-(a^{4k+2}-1) = 2$, is a multiple of p. But p is odd, so the assumption that $p = 4k+3$ is incorrect and $p = 4k+1$. □

Using this fact and similar reasoning, write out the proof of the statement: If a is even and p is a prime such that $p \nmid a$ and p divides a^4+1, then $p = 8k+1$. Using strong induction show that: If a is even and p is a prime such that $p \nmid a$ and $p|a^{2^n}+1$, then $p = 2^{n+1}k+1$ for some integer k. For more detail see Dunham pp. 239-235 [6].

(4) Note that $641 = 2^4+5^4$ and $641 = 5\cdot 2^7+1$. Now look at the first equation multiplied by 2^{28} which shows that $641|2^{32}+5^4\cdot 2^{28}$. Use the second equation to show that $641|5^4\cdot 2^{28}-1$. If $a|b$ and $a|c$ then $a|b \pm c$. Therefore $641|2^{32}+1$. This proof is by G.T. Bennett and is an improvement on the proof in Hardy pp14-15 [8]. I mention G.T. Bennett because at least one of his discoveries (A five piece dissection of a regular octagon that forms a square) was for over 50 years ascribed to another man, who shall remain nameless.

(5) (From Honsberger [10]) Prove that $F_n|2^{F_n}-2$ for all n. It is true for $n \leq 4$ by Fermat's little theorem, since the first four Fermat numbers are prime. Note that $n+1 < 2^n$ for $n > 4$. Since $2^a|2^b$ if $a < b$, it follows that $2^{n+1}|2^{2^n}$ and $2^{2^n} = 2^{n+1}k$ for some integer k. Now look at $2^{F_n}-2 = 2^{2^{2^n}+1}-2 = 2(2^{2^{2^n}}-1) = 2(2^{2^{n+1}k}-1)$. Use the difference of two powers of k ($1 = 1^k$) to factor. Then use the difference of two squares to factor again. Since one of the final factors is F_n, the proof is completed.

(6) Let $z_1 = \zeta^1+\zeta^{-1} = 2\cos 2\pi/17$ and $z_2 = \zeta^4+\zeta^{-4}$. Show $z_1+z_2 = y_1$ and $z_1 z_2 = y_3$ so z_1 and z_2 are the roots of the equation $Z^2 - y_1 Z + y_3$ with $z_1 > z_2$ and without resorting to trigonometry.

(7) Solve the quadratic equations and show that $\cos 2\pi/17$ is equal to the value stated in the final paragraph and show by algebra that it is equal to the radical expression in problem 2 that Gauss obtained.

To comment, ask questions, or report errors contact me at tricycle222@mac.com

References

1. A. Baragar, *A Survey of Classical and Modern Geometry*, Prentice Hall, 2001.
2. H. Davenport, *Multiplicative Number Theory*, 3rd ed., Springer, 2000.
3. L. Dickson, *Monographs on Topics of Modern Mathematiics*, Ch. 8: Constructions with Ruler and Compasses, Dover, 1955.
4. P. Dirichlet, *Lectures on Number Theory*, History of Mathematics, Vol. 16, Amer. Math. Soc., 1999.
5. H. Dörrie, *100 Great Problems of Elementary Mathematics*, Dover, 1965.
6. W. Dunham, *Journey Through Genius*, Math. Assoc. of America, 1990.
7. C. Gauss, *Disquisitiones Arithmeticae*, English ed., Springer, 1985.
8. G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, 1960.
9. R. Hartshorne, *Geometry: Euclid and Beyond*, Springer, 1997.
10. R. Honsberger, *Mathematical Gems*, Ch. 1, Math. Assoc. of America, 1973.
11. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1990.
12. M. Křížek, F. Luca, and L. Somer, *17 Lectures on Fermat Numbers*, Canadian Mathematical Society, Springer, 2001.
13. G. Martin, *Geometric Constructions*, Springer, 1998.
14. H. Rademacher, *Lectures on Elementary Number Theory*, Blaisdell, 1964.
15. P. Ribenboim, *The* New *Book of Prime Number Records*, pp. 103–5, Springer, 1996.
16. D. Savitt, *The Mathematics of Gauss*, `http://math.arizona.edu/~savitt/papers/unpublished/gauss.pdf`.
17. L. Linn Smith, *A Construction of the Regular Polygon of Seventeen Sides*, Amer. Math. Monthly **27** (1920), pp. 322–26.
18. I. Stewart, *Galois Theory*, Chapman and Hall, 1973.
19. P. Tignol, *Galois' Theory of Algebraic Equations*, Longman Scientific and Technical, 1988.