Constructions with Compass and Straightedge

A thing constructed can only be loved after it is constructed: but a thing created is loved before it exists. – Gilbert Keith Chesterton

1. Constructible Numbers

Definition 6.1. A length is constructible if it can be obtained from a finite number of applications of a compass and straightedge.

A constructible number is a constructible length or the negative of a constructible length.

To get things started, we assume we can construct a segment of length 1.

Example 6.1. The square root of two is constructible as the hypotenuse of a square who side length is 1. By several arguments given in class, \( \sqrt{2} \) is not a rational number.

Theorem 6.1. With a straightedge and compass, we can construct the following geometric objects:

(a) [perpendiculars] Given a line \( \ell \) and a point \( P \), we can construct the line \( m \) through \( P \) and perpendicular to \( \ell \).

(b) [parallels] Given a line \( \ell \) and a point \( P \) not on \( \ell \), we can construct the line \( m \) through \( P \) and parallel to \( \ell \).

(c) [angle bisectors] We can construct the angle bisector of a given angle.

(d) [midpoints] We can construct the midpoint of a given segment.

The next theorem shows that the set of constructible numbers forms a field of real numbers.
**Theorem 6.2.** If \(a\) and \(b\) are constructible, then so are \(a + b, a - b, a \times b,\) and \(a \div b.\)

To illustrate the way you might go about proving this theorem, we show how to construct the rational numbers one third and two thirds.

**Constructing \(\frac{1}{3}\) and \(\frac{2}{3}\)**

Step 1. Construct four collinear points \(A, B, C,\) and \(D\) such that \(AB = BC = CD = 1.\)

Step 2. Draw a line \(m\) through \(A\) perpendicular to \(AB.\)

Step 3. Use your compass to mark a point \(E\) on \(m\) such that \(AE = 1.\)

Step 4. Construct a line parallel to \(DE\) through the point \(B\) which intersects \(AB\) at a point \(X.\)

Step 5. Construct a line parallel to \(DE\) through the point \(C\) which intersects \(AB\) at a point \(Y.\)

Step 6. \(AX = \frac{1}{3}\) and \(AY = \frac{2}{3}.\) \(\square\)

**Theorem 6.3.** If \(r\) is constructible, then so is \(\sqrt{r}.\)

Suppose \(r\) is a constructible number. We will show how to construct \(\sqrt{r}.\)

Step 1. Construct a segment of length \(|r - 1|\).

Step 2. Construct the midpoint of this segment, to obtain a segment \(AB\) of length \(\frac{|r-1|}{2}.\)

Step 3. Construct a ray \(BP\) perpendicular to \(AB\) at \(B.\)

Step 4. Draw a circle of radius \(\frac{r+1}{2}\) centered at \(A.\) This circle will intersect \(BP\) at a point \(C.\)
Step 5. Consider the triangle $\triangle ABC$.

![Diagram of triangle ABC](image)

Step 6. By the Pythagorean Theorem,

$$BC^2 = AC^2 - AB^2 = \left(\frac{r+1}{2}\right)^2 - \left(\frac{r-1}{2}\right)^2 = \frac{r^2 + 2r + 1 - (r^2 - 2r + 1)}{4} = r.$$  

Step 7. Thus $BC = \sqrt{r}$. □

A set of real numbers $F$ is called a field if and only if it is closed with respect to the four operations $+,-,\times,$ and $\div$. The set of rationals $\mathbb{Q}$ is a field since the sum, difference, product, and quotient of two rationals is again a rational number. If $F$ is a field of real numbers and $\sqrt{r} \notin F$, then the extension field $E$ obtained by adjoining $\sqrt{r}$ to $F$ consists of all numbers of the form $a + b\sqrt{r}$, where $a$ and $b$ lie in the original field $F$.

Every constructible number can be obtained from the rationals by first adding the square root $\sqrt{r_1}$ of some rational number $r_1$ and allowing all sums, differences, products, and quotients (not dividing by 0). This gives a new field $E_1$. We can pick an element $r_2$ out of $E_1$ and add its square root $\sqrt{r_2}$ to $E_1$ and allow all sums, differences, products, and quotients, thereby obtaining a bigger extension field $E_2$. Keeping this up we get the following procession of bigger and bigger sets:

<table>
<thead>
<tr>
<th>Chain of Extension Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Q}$</td>
</tr>
</tbody>
</table>

Each extension field $E_i$ is closed under the four operations $+,-,\times$, and $\div$ and contains $\sqrt{r_i}$, where $r_i$ is an element from the previous set $E_{i-1}$ (but $\sqrt{r_i}$ is not in $E_{i-1}$).

### 6.1 Exercises

1. Use an actual compass and a straightedge (a ruler will do as long as you ignore the markings on it) to perform the four constructions listed in Theorem 6.1.
2. What are the two extension fields needed to obtain $\alpha = \sqrt{1 + \sqrt{3}}$? Show how to construct $\alpha$ with a straightedge and compass. What polynomial equation does $\alpha$ satisfy?

3. What are the two extension fields needed to obtain $\beta = \sqrt{3} + \sqrt{5}$? What polynomial equation does $\beta$ satisfy?

4. Suppose $\alpha = 2 + 3\sqrt{5}$ and $\beta = 4 - \sqrt{5}$ lie in the extension field $E = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$. Compute (a) $\alpha + \beta$, (b) $\alpha - \beta$, (c) $\alpha \times \beta$, and (d) $\frac{\alpha}{\beta}$. Hint for (d): multiply by $\frac{4 + \sqrt{5}}{4 + \sqrt{5}}$.

2. Tools from Algebra

Given a real number, how do we know whether it is constructible or not? You might think that the cube root of 2, to take an example, is not constructible, since its description involves a cube root and not a square root. But, maybe if we add enough square roots to the rationals, we might end up with a field that contains $\sqrt[3]{2}$. For all that goes, how do we know that $\sqrt[3]{2}$ isn’t rational? Since $\sqrt[3]{2}$ satisfies the cubic equation $x^3 - 2 = 0$, we ask whether a chain of square roots could ever produce a solution to a cubic equation? It turns out that we need three algebraic tools in our work with constructible numbers and cubic equations.

2.1. The Rational Root Theorem. We state an important theorem from college algebra:

Theorem 6.4 (The Rational Root Theorem). If you have a polynomial with integer coefficients, then all rational roots must have the form

$$\frac{m}{n}$$

where the numerator $m$ divides the constant coefficient of the polynomial, and the denominator $n$ divides the leading coefficient of the polynomial.

You can find a proof in any college algebra book.

We could have used the Rational Root Theorem to prove that the square root of 2 is irrational, since the only possible rational roots of $f(x) = x^2 - 2$ are 1, 2, -1, and -2, none of which satisfy $f(x) = 0$. 

2. The Plus or Minus Theorem. Solutions to polynomials containing square roots come in pairs. In general, you get one solution by adding the square root and you get another solution by subtracting it. This is what the “plus or minus” means in the quadratic formula: “minus b plus or minus the square root of b^2 - 4ac, all divided by 2a” that you memorized in high school. (A colleague once told me that his 85 year old grandmother recited this formula to him in her nursing home and asked him what it in the world it meant.) This same behavior holds for solutions to cubic equations, and is a key fact in showing that specific real numbers are not constructible.

**Theorem 6.5 (Plus or Minus Theorem).** Given the cubic equation \( f(x) = x^3 + cx + d = 0 \), where \( c \) and \( d \) are integers. Assume that \( F \) is a field of real numbers and that \( a, b, \) and \( r \) lies in \( F \), but \( \sqrt{r} \) does not lie in \( F \). If \( a + b\sqrt{r} \) is a solution to the equation \( f(x) = 0 \), then \( a - b\sqrt{r} \) is also a solution.

**Proof.** Assume \( x = a + b\sqrt{r} \) is a solution to \( f(x) = x^3 + cx + d = 0 \). Cube \( x = a + b\sqrt{r} \) using the formula:

\[
(A + B)^3 = A^3 + 3A^2B + 3AB^2 + B^3.
\]

So

\[
x^3 = (a + b\sqrt{r})^3 = a^3 + 3a^2b\sqrt{r} + 3a(b\sqrt{r})^2 + (b\sqrt{r})^3
\]

\[
= a^3 + 3a^2b\sqrt{r} + 3ab^2r + b^3r\sqrt{r}
\]

\[
= (a^3 + 3ab^2r) + (3a^2b + b^3r)\sqrt{r}.
\]

Adding \( cx + d = c(a + b\sqrt{r}) + d \) to \( x^3 \), we have

\[
x^3 + cx + d = A + B\sqrt{r} = 0,
\]

where

\[
A = a^3 + 3ab^2r + ca + d \quad \text{and} \quad B = 3a^2b + b^3r + b.
\]

Observe that \( A \) and \( B \) are elements of the field \( F \), since \( a, b, c, d, \) and \( r \) lie in \( F \) and the field \( F \) is closed with respect to +, -, \( \times \), and \( \div \). If \( B \neq 0 \), then \( \sqrt{r} = -A/B \), which violates our assumption that \( \sqrt{r} \) does not lie in \( F \). It follows that \( B \) must have the value 0, and therefore \( A \) must also be 0. If we write \( \overline{x} = a - b\sqrt{r} \), then to evaluate \( f(\overline{x}) \) we simply replace \( b \) by \(-b\) in the formulas for \( A \) and \( B \), to get

\[
\overline{x}^3 + c\overline{x} + d = A - B\sqrt{r} = 0 - 0\sqrt{r} = 0.
\]

Thus \( \overline{x} \) is also a solution to the cubic equation, as the theorem claims. \( \square \)
2.3. The Constant Term Theorem.

**Theorem 6.6 (Constant Term Theorem).** Given the cubic equation \( f(x) = x^3 + cx + d = 0 \), where \( c \) and \( d \) are integers. Assume that \( \alpha, \beta, \) and \( \gamma \) are the three solutions to \( f(x) = 0 \). Then the product

\[
\alpha \cdot \beta \cdot \gamma = -d.
\]

**Proof.** Since \( f(\alpha) = 0 \), the expression \( x - \alpha \) must divide the cubic polynomial \( f(x) = x^3 + cx + d \). Similarly \( x - \beta \) and \( x - \gamma \) also divide \( f(x) \), so \( f(x) \) factors as

\[
x^3 + cx + d = (x - \alpha)(x - \beta)(x - \gamma).
\]

If we multiply out the three terms on the right hand side of the equation, we find that the constant term is the product \(-\alpha \cdot \beta \cdot \gamma\). Comparing this product with the constant term \( d \) on the left hand side of the equation proves the theorem. \( \Box \)

**6.2 Exercises**

1. This exercise answers the question: Can a number of the form \( a + b\sqrt{r} \) ever be a solution to a cubic equation? Show that \( 3 + \sqrt{6} \) is a solution to \( f(x) = x^3 - 5x^2 - 3x + 3 = 0 \). Find the other two roots of \( f(x) \).

2. Is the Plus or Minus Theorem true if we allow \( r \) to be \(-1\)? Does our extension field consist of real numbers in this case?

3. Find three roots of the equation \( x^3 = 1 \).

**3. Duplicating a Cube**

**Theorem 6.7.** The cube root of 2 is not constructible.

**Proof.** Suppose \( \sqrt[3]{2} \) could be obtained by adding a finite procession of square roots to the rational numbers, as diagrammed above in the Chain of Extension Fields.

Let \( \sqrt{r} \) be the last square root added to obtain \( E_n \). Now suppose that \( \alpha \) is an element in \( E_n \) and that

\[
\alpha^3 = 2.
\]

We know that \( \alpha \) must look like

\[
\alpha = a + b\sqrt{r}
\]
where $a$ and $b$ come from the previous set $E_{n-1}$. By the *Plus or Minus* Theorem, $\beta = a - b\sqrt{r}$ also satisfies $\beta^3 = 2$. We have constructed two different real numbers whose cubes are 2. But this is impossible. The graph of $y = x^3$ is always increasing, so there is exactly one real number whose cube is 2.

\[ \text{Theorem 6.8 (Duplicating the cube).} \text{ It is impossible with compass and straightedge to duplicate the cube, i.e., to construct a cube with side length $y$ whose volume is twice $x^3$ (where $x$ is a constructible number).} \]

\[ \text{Proof.} \text{ If you could construct $y$, then since } y = \sqrt[3]{2}x, \text{ you could construct the quotient } \frac{y}{x} = \sqrt[3]{2}. \]

6.3 Exercises

1. If $x$ is a constructible number, could you construct a number $y$ such that the volume of the cube with side length $y$ is precisely 5 times the volume of the cube with side length $x$? What about 8 times the volume of the cube with side length $x$?

2. \[ \text{Golden Ratio} \text{ The golden ratio } \phi \text{ satisfies the equation } \phi^2 - \phi - 1 = 0. \text{ (Refer back to Problem #6 in Exercise Set 5.5.) Show that the golden ratio is a constructible number.} \]

4. Trisecting an Angle.

We know that we can bisect an arbitrary angle, using just a straightedge and compass. A natural question is: Can we trisect a given angle?

It is clear how to construct an equilateral triangle who side lengths are all 1 unit long. Any angle of this equilateral triangle gives us an angle of measure 60. If we could trisect any angle, then we could trisect this angle of measure 60, giving us an angle of measure 20. By using the unit circle, we could then construct the number

\[ \alpha = \cos 20. \]

Our goal is to show that $\cos 20$ is not constructible, and consequently that it is impossible to trisect an arbitrary angle with straightedge and compass. We proceed in much the same way as when we argued that $\sqrt[3]{2}$ is not constructible. Our first task is to find an equation satisfied by $\cos 20$. This job requires some trigonometry, which we briefly review:
The “Big Three” Trig Formulas:

\[ \cos^2 \theta + \sin^2 \theta = 1 \]
\[ \cos(A + B) = \cos A \cos B - \sin A \sin B \]
\[ \sin(A + B) = \sin A \cos B + \cos A \sin B \]

The double angle formulas:

\[ \cos(2x) = \cos(x + x) = \cos^2 x - \sin^2 x \]
\[ \sin(2x) = \sin(x + x) = 2 \sin x \cos x \]

A triple angle formula: From the double angle formulas, we have

\[
\begin{align*}
\cos(3x) &= \cos(2x + x) = \cos(2x) \cos x - \sin(2x) \sin x \\
&= (\cos^2 x - \sin^2 x) \cos x - (2 \sin x \cos x) \sin x \\
&= \cos^3 x - 3 \sin^2 x \cos x \\
&= \cos^3 x - 3(1 - \cos^2 x) \cos x \\
&= \cos^3 x - 3 \cos x + 3 \cos^3 \\
&= 4 \cos^3 x - 3 \cos x.
\end{align*}
\]

Now substitute \( x = 20 \) to get

\[ 4 \cos^3 20 - 3 \cos 20 - \cos 60 = 0, \]

or, since \( \cos 60 = \frac{1}{2} \),

\[ 4 \cos^3 20 - 3 \cos 20 - \frac{1}{2} = 0. \]

Multiplying by 2,

\[ 8 \cos^3 20 - 6 \cos 20 - 1 = 0. \]

Thus \( x = \cos 20 \) satisfies the cubic equation

\[ 8x^3 - 6x - 1 = 0. \]

If \( x \) is constructible, then so is \( \alpha = \frac{1}{2} x \), since we can always construct the midpoint of a segment of length \( x \). Furthermore \( \alpha = \frac{1}{2} x \) satisfies the somewhat simpler cubic equation

\[ \alpha^3 - 3\alpha - 1 = 0. \]

Our goal is to prove that

**Theorem 6.9.** \( \frac{1}{2} \cos 20 \) is not a constructible number.
4. TRISECTING AN ANGLE. 171

Proof. First we determine that $\alpha = \frac{1}{2} \cos 20$ is not rational by showing that the cubic $x^3 - 3x - 1$ has no rational roots. By the Rational Root Theorem, the only possible rational roots of the polynomial $x^3 - 3x - 1$ are 1 and $-1$, neither of which is a solution.

Suppose we can obtain the real number $\frac{1}{2} \cos 20$ by successively adding more and more square roots to the rational numbers. We will assume that at the last stage $E_n$ we have

$$\alpha = a + b\sqrt{r},$$

where the real number $r = r_n$ comes from the previous set $E_{n-1}$. Then by the Plus or Minus Theorem, $\beta = a - b\sqrt{r}$ is also a root of the cubic $x^3 - 3x - 1 = 0$.

We have two different solutions $\alpha$ and $\beta$ to the cubic equation $x^3 - 3x - 1 = 0$. Unfortunately, this is not a contradiction, because a graphing calculator easily shows that this cubic polynomial does in fact have three real roots, that is, its graph crosses the x-axis in three distinct locations, unlike the graph of $y = x^3 - 2$ which only crosses the x-axis once.

Let $\gamma$ be the name of the third root. Since the constant term of $x^3 - 3x - 1$ is $-1$, it follows from the Constant Term Theorem that

$$\gamma = \frac{-1}{\alpha \cdot \beta} = \frac{-1}{(a + b\sqrt{r})(a - b\sqrt{r})} = \frac{-1}{a^2 - b^2r}.$$

Since $a$, $b$, and $r$ all lie in the previous field $E_{n-1}$, we are forced to conclude that the third root $\gamma$ also lies in $E_{n-1}$, which means that the third root $\gamma$ is also a constructible number. By our earlier observation that $f(x) = 0$ has no rational solutions, we know that $\gamma$ is not a rational. It follow that $\gamma = a' + b'\sqrt{s}$, where $s = r_k$ belongs to a previous field $E_{k-1}$ $(1 \leq k \leq n - 1)$. Using the Plus or Minus Theorem again, we get a fourth solution $a' - b'\sqrt{s}$ to the polynomial $x^3 - 3x - 1$. But a cubic has at most three roots. So a fourth root is one too many and we have a contradiction. This contradiction arises from our assumption that $\alpha = \frac{1}{2} \cos 20$ is constructible. Conclusion: we cannot construct $\frac{1}{2} \cos 20$.

An immediate consequence of Theorem 6.9 is

**Theorem 6.10.** [Trisection with Straightedge and Compass] You cannot trisect an arbitrary angle using just a straightedge and compass.

Now you can see why the Greeks couldn’t determine that trisecting an angle with straightedge and compass is impossible. Our solution requires a lot of algebra that was just not available 2000 years ago.

Two common misconceptions by students about Theorem 6.10:
1. Students often believe Theorem 6.10 asserts that no angle can be trisected with a straightedge and compass. Wrong. The statement “not all Americans are millionaires” does not mean that there are no millionaires in the United States. In particular, a right angle can be trisected into three 30 degree angles; to make an angle of measure 30 just bisect an angle of measure 60 (which can be constructed).

2. Students often believe this theorem asserts that there is simply no way to trisect a given angle. That’s right if the only tools we are allowed to use are a straightedge and compass. But if we can use other tools, then we can trisect angles.

**Question.** How do we trisect an angle?

The answer is that we can trisect an angle if we are allowed to use a straightedge with two marks on it which are exactly one unit apart.

Assume that $A$ and $B$ are points on the unit circle (of radius 1) with center $O$. We will show how to trisect $\angle AOB$. Place the “marked” straightedge on the unit circle so that $\overrightarrow{CD} = 1$ and the line $\overrightarrow{CD}$ intersects the circle at the points $D$ and $A$ and intersects the line $\overrightarrow{OB}$ at $C$.

The first exercise is to give a geometric proof that the measure of $\angle DCO$ is one third the measure of $\angle AOB$.

### 6.4 Exercises

1. Referring to the diagram above, show that $\text{m}\angle DCO = \frac{1}{3}\text{m}\angle AOB$. 

2. Show that it is possible with a straightedge and compass to find an angle whose measure is one fourth of the measure of a given angle. Construct an angle of measure 15.

5. Constructible Regular Polygons Worksheet

**Definition 6.2.** A positive integer \( p > 1 \) is called **prime** if and only if it is divisible by no other numbers than 1 and itself. An integer \( n > 1 \) which is not prime is called **composite**.

For example, 2, 3, 5, 7, 11, and 8157530567 (the Math Department phone number at Northern Illinois University) are prime, while 4, 6, 21, and \( 2^{347} - 1 \) are not.

It turns out the question

Which regular \( n \)-gons can be constructed?

is intimately connected with the question

When is \( 2^n + 1 \) a prime?

**Fermat Number Worksheet**

Here is a short list of the factors of \( 2^n + 1 \):

<table>
<thead>
<tr>
<th>( n )</th>
<th>factors</th>
<th>( n )</th>
<th>factors</th>
<th>( n )</th>
<th>factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>11</td>
<td>3 · 683</td>
<td>21</td>
<td>( 3^2 · 43 · 5419 )</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>12</td>
<td>17 · 241</td>
<td>22</td>
<td>5 · 397 · 2113</td>
</tr>
<tr>
<td>3</td>
<td>3 · 3</td>
<td>13</td>
<td>3 · 2731</td>
<td>23</td>
<td>3 · 2796203</td>
</tr>
<tr>
<td>4</td>
<td>17</td>
<td>14</td>
<td>5 · 29 · 113</td>
<td>24</td>
<td>97 · 257 · 673</td>
</tr>
<tr>
<td>5</td>
<td>3 · 11</td>
<td>15</td>
<td>3 · 3 · 11 · 331</td>
<td>25</td>
<td>3 · 11 · 251 · 4051</td>
</tr>
<tr>
<td>6</td>
<td>5 · 13</td>
<td>16</td>
<td>65537</td>
<td>26</td>
<td>5 · 53 · 157 · 1613</td>
</tr>
<tr>
<td>7</td>
<td>3 · 43</td>
<td>17</td>
<td>3 · 43691</td>
<td>27</td>
<td>( 3^4 · 19 · 87211 )</td>
</tr>
<tr>
<td>8</td>
<td>257</td>
<td>18</td>
<td>5 · 13 · 37 · 109</td>
<td>28</td>
<td>17 · 15790321</td>
</tr>
<tr>
<td>9</td>
<td>3 · 3 · 3 · 19</td>
<td>19</td>
<td>3 · 174763</td>
<td>29</td>
<td>3 · 59 · 3033169</td>
</tr>
<tr>
<td>10</td>
<td>5 · 5 · 41</td>
<td>20</td>
<td>17 · 61681</td>
<td>30</td>
<td>5 · 13 · 41 · 61 · 1321</td>
</tr>
</tbody>
</table>
(a) For each prime in the table below, fill in all values of $n$ (up to $n = 30$) for which $p$ divides $F_n$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$n : p$ divides $F_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td></td>
</tr>
</tbody>
</table>

**Question 1.** When does $3$ divides $2^n + 1$?

**Question 2.** When does $5$ divides $2^n + 1$?

**Question 3.** When does $17$ divides $2^n + 1$?

**Question 4.** When is $2^n + 1$ is prime?

To figure out why your observations are working out, recall the polynomial factorization:

$$x^3 + 1 = (x + 1)(x^2 - x + 1)$$

Plugging in $x = 2$ gives the integer factorization $2^3 + 1 = (2 + 1)(2^2 - 2 + 1)$ and out pops the factor $3$.

**Question 5.** What happens when you plug in $x = 2^2$? $x = 2^3$?

**Question 6.** Verify the factorization of $x^5 + 1 = (x + 1)(x^4 - x^3 + x^2 - x + 1)$.

**Question 7.** What happens when you plug in $x = 2^2$? $x = 2^3$? $x = 2^4$?

**Question 8.** Find a factorization of $x^7 + 1$, based on the factorizations of $x^3 + 1$ and $x^5 + 1$. 
Question 9. What happens when you plug in $x = 2$? $x = 2^2$?

Conclusions:

- $x + 1$ divides $x^{\text{odd}} + 1$
- $x = 2$: $2 + 1 = 3$ divides $2^{\text{odd}} + 1$
- $x = 2^2$: $2^2 + 1 = 5$ divides $2^{2\text{ odd}} + 1$
- $x = 2^4$: $2^4 + 1 = 17$ divides $2^{4\text{ odd}} + 1$
- etc.

As you can see, $2^n + 1$ factors whenever $n$ contains an odd factor. This means that the only chance $2^n + 1$ has of being prime is when the exponent $n$ itself is a power of 2. These numbers are called Fermat numbers.

**Definition 6.3.**

$$F_m = 2^{2^m} + 1$$

An examination of the previous table shows that

- $F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$
- $F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$
- $F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$
- $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 127$
- and $F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$

are prime. Fermat conjectured that all of these numbers are prime, but alas, the very next one, $F_5$, factors:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 641 \cdot 6700417.$$

**Exercise 10.** You can determine that 641 divides $F_5$ with a minimum of calculation, as follows: Start with $640 = 641 - 1$ and factor $640 = 128 \cdot 5 = 2^7 \cdot 5$. Raise both sides of the equation

$$2^7 \cdot 5 = 641 - 1$$

to the 4th four power (your answer with involve powers of 641 on the right hand side) and then use the fact that $5^4 = 641 - 2^4$. If you follow these steps you should be able to write $2^{32} + 1$ as $641 \times$ some number.

Extensive computer calculations over the past 50 years have shown that $F_5$ through $F_{32}$ are all composite. At this time no one knows whether $F_{33}$ is prime or composite, but the
safe best is that it factors. To comprehend the enormity of this innocent looking number, consider the following statistics:

- \( F_{33} \) consists of 2,585,827,973 decimal digits.
- To print it in a book would require 538,715 pages (80 columns and 60 lines).
- To print it as one line (8 characters per inch) would require over 5101 miles of tape.

It’s a really big number!

Why are these numbers so important? Well, about 200 years ago, perhaps the most famous mathematician of all time, Carl Friedrich Gauss, proved that

Theorem 6.11 (Gauss’ Theorem). A regular \( n \)-gon can be constructed with straight-edge and compass if and only if \( n \) factors into powers of 2 times distinct products of Fermat primes.

Since the only Fermat primes known are 3, 5, 17, 257, and 65537, this severely restricts the number of constructions. Here is a short list of constructible \( n \)-gons based on the factorization of \( n \), for \( n = 3 \) to 40:

<table>
<thead>
<tr>
<th>( n )</th>
<th>factors</th>
<th>( n )</th>
<th>factors</th>
<th>( n )</th>
<th>factors</th>
<th>( n )</th>
<th>factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>not poly</td>
<td>11</td>
<td>not constr</td>
<td>21</td>
<td>not constr</td>
<td>31</td>
<td>not constr</td>
</tr>
<tr>
<td>2</td>
<td>not poly</td>
<td>12</td>
<td>( 2^2 \cdot F_0 )</td>
<td>22</td>
<td>33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>( F_0 )</td>
<td>13</td>
<td>not constr</td>
<td>23</td>
<td></td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>( 2^2 )</td>
<td>14</td>
<td>not constr</td>
<td>24</td>
<td></td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>( F_1 )</td>
<td>15</td>
<td>( F_0 \cdot F_1 )</td>
<td>25</td>
<td></td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>( 2 \cdot F_0 )</td>
<td>16</td>
<td>( 2^4 )</td>
<td>26</td>
<td></td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>not constr</td>
<td>17</td>
<td>( F_2 )</td>
<td>27</td>
<td></td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>( 2^3 )</td>
<td>18</td>
<td>not constr</td>
<td>28</td>
<td></td>
<td>39</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>not constr</td>
<td>19</td>
<td>not constr</td>
<td>29</td>
<td></td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>( 2 \cdot F_1 )</td>
<td>20</td>
<td>( 2^2 \cdot F_1 )</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Do–It–Now Exercise. Complete the table above.

Question 11. For how many values of \( n \) between 3 and 100 is a regular \( n \)-gon constructible?

Problem 12. Construct the following regular polygons:
(a) triangle \( n = 3 \)  (b) hexagon \( n = 6 \)  (c) square \( n = 4 \)  (d) octogon \( n = 8 \).

Problem 13. Explain how to Construct a regular polygons with \( n = 15 \) sides. Hint: find integers \( A \) and \( B \) such that

\[
\frac{1}{15} = \frac{A}{3} + \frac{B}{5}.
\]
Problem 14. [Constructing a regular pentagon]

Given \( \triangle ABC \) in \( \mathbb{E} \) with \( \angle A = 36 \), \( \angle B = 72 \), and \( AC = 1 \).

(a) What is \( \angle C \)?

(b) What is \( AB \)?

Let \( P \) be the intersection of segment \( \overline{AC} \) and the angle bisector of \( \angle B \).

(c) Draw a picture of \( \triangle ABC \) and point \( P \).

(d) What is \( \angle ABP \)?

(e) What is \( \angle PBC \)?

(f) What is \( \angle BPC \)?

Assume that \( AP = x \).

(g) What is \( BP \) (in terms of \( x \))?  

(h) What is \( BC \)?

(i) What is \( PC \)?

(j) Explain why \( \triangle ABC \) is similar to \( \triangle BPC \).

(k) Using the fact that the two triangles in (j) are similar, explain why it follows that

\[
\frac{BC}{AC} = \frac{PC}{BC}
\]

(l) Plug in the values for \( BC, AC, \) and \( PC \) into the above equation to get an equation involving \( x \).

(m) Solve this equation for \( x \).

(n) Explain why the number \( x \) is constructible.

(o) Since \( x \) is constructible, it follows that you can construct the point \( P \) on \( \overline{AC} \) whose length from \( A \) is \( x \). Use your answers to parts (b) and (g) to explain how to construct point \( B \) once you have located points \( A, P, \) and \( C \).

(p) Explain how to use \( \triangle ABC \) to construct a regular pentagon inscribed inside the circle centered at point \( C \) with radius \( AC = 1 \). [Hint: what is the central angle of a regular pentagon?]

6. Transcendental Numbers

We return to our verbose professor and his two favorite students, Ernest and Hedda, for our final dialogue.

Ernest: That was pretty cool, Professor, how you got the cosine of 20 to satisfy that cubic equation—I forget what it was right now, but I got it in my notes. Anyway, what I was
wondering is: if someone gives me a real number, how do I go about finding out the equation it satisfies?

Hedda: That’s a good question. What about a number like π? What’s its equation?

Professor: Are you sure that it even has an equation?

Ernest: Pi is easy. Its equation is \( A = \pi r^2 \), isn’t it?

Professor: Well, pi is in that equation, alright, but that’s not what we mean by the “equation satisfied by pi.” For example, \( \sqrt{2} \) is in the equation

\[
\cos 45 = \frac{\sqrt{2}}{2}
\]

but this is not how we get an equation satisfied by \( \sqrt{2} \). What we want is a polynomial \( f(x) \) so that when we plug in \( \sqrt{2} \) we get 0.

Ernest: Couldn’t you just take \( f(x) = x - \sqrt{2} \)?

Professor: That would be cheating. The polynomial must have integer coefficients.

Ernest: Now you tell us.

Hedda: You could always start with

\[
x = \sqrt{2}
\]

and then square to get

\[
x^2 = 2
\]

so the polynomial we want is

\[
f(x) = x^2 - 2.
\]

Professor: Good! Let’s take another example to see if you understand the concept. What’s the equation for

\[
x = \sqrt[3]{2} + \sqrt[3]{3}?
\]

Ernest: [goes to board] That’s easy. We can move the square root to the left, like this:

\[
x - \sqrt[3]{3} = \sqrt[3]{2}.
\]

Now cube both sides to get rid of the cube root:

\[
(x - \sqrt[3]{3})^3 = 2.
\]

I forget the formula for cubes.
Professor: Pascal’s ghost says

\[(A - B)^3 = A^3 - 3A^2B + 3AB^2 - B^3.\]

Ernest: Thanks, Mr. Ghost. So

\[x^3 - 3\sqrt{3}x^2 + 3(\sqrt{3})^2x - (\sqrt{3})^3 = 2.\]

Now I’m stuck

Professor: Can someone help Ernest?

Hedda: Well, \((\sqrt{3})^2 = 3\) and \((\sqrt{3})^3 = 3\sqrt{3}\), so we can simplify this equation to

\[x^3 - 3\sqrt{3}x^2 + 9x - 3\sqrt{3} = 2.\]

Then we can put the \(\sqrt{3}\) terms on the right, like this:

\[x^3 + 9x - 2 = 3\sqrt{3}x^2 + 3\sqrt{3}\]

or

\[x^3 + 9x - 2 = 3\sqrt{3}(x^2 + 1).\]

Now square both sides:

\[(x^3 + 9x - 2)^2 = 27(x^2 + 1)^2.\]

It’s starting to look kinda messy.

Professor: I think you’ve gone far enough. You could always multiply out the square \((x^2 + 1)(x^2 + 1)\) by FOIL and you could work out the other square \((x^3 + 9x - 2)(x^3 + 9x - 2)\) by multiplying out all the terms and collecting them together. The point is that it would start with \(x^6\) and it would have integer coefficients. If you did all this work you would end up with a sixth degree polynomial whose solution is \(\sqrt{2} + \sqrt{3}\). Now could you do something like this starting with

\[x = \pi?\]

To put it another way, can you combine the numbers

\[\pi, \pi^2, \pi^3, \pi^4, \ldots\]

in some way to get an equation equalling zero?

Ernest: You know, Professor, you’re asking us the same question that we originally asked you!

Professor: Good point, Ernest. So why don’t I just tell you the answer. A real number like \(\sqrt{2}\) or \(\cos{20}\) which satisfies a polynomial with integer coefficients is called an algebraic
**number.** All rationals are algebraic since $\frac{m}{n}$ satisfies $nx - m = 0$ and all constructible numbers are obviously algebraic. A real number which is not algebraic is called a **transcendental number.** In fact, here’s the hierarchy of the number line:

```
Real Numbers
   /\          /\  \\
 Algebraic Numbers  |  Transcendental Numbers
   |\        |\  |
 Constructible Numbers
   |\        |\  |
 Rational Numbers
   |\        |\  |
 Integers
```

Professor: It turns out that pi is a transcendental. It does not satisfy any polynomial whose coefficients are integers.

Hedda: Are there any other transcendental numbers like pi that we’ve seen before?

Professor: Well, if you’ve had calculus, the number $e$ is transcendental and logarithms are, except for special cases, transcendental. The truth is that almost all of the real numbers you have seen in your life are algebraic.

Ernest: So the transcendentals must be really rare, huh?

Professor: That’s the interesting thing. The set of polynomials with integer coefficients is a countable set, and thus the algebraic numbers are countable. As we saw when the course began, a countable set takes up zero length on the number line. The transcendental numbers outnumber the algebraic numbers by another order of infinity.

Ernest: Thanks for telling us about these transcendental numbers and giving us something to meditate about.

Professor: I get your joke, Ernest. Good day.