Construction of regular polygons

Ancient Greeks could do it for

\[ n = 3, 2^2, 5, 2^3, 15, 2^4 \]

~1796 Gauss (age 19) did it for

\[ n = 17 \]

or more generally

and prime of the form \( 2^n + 1 \)

Then \( 2^n + 1 \) is a prime \( \# \) only if

\[ n = 2^k \]

Proof: \[ x^3 + 1 = (x+1)(x^2 - x + 1) \]

\[ x^5 + 1 = (x+1)(x^4 - x^3 + x^2 - x + 1) \]
In general, \( x \text{ odd} + 1 = (x+1)(\ldots) \)

Let \( x = 2 \)

\[ 2 + 1 = 3 \]

\[ x = 4 \]

\[ 4 + 1 = 5 \] (---)

\[ 2 \cdot \text{odd} + 1 = 5 \] (---)

Similarly, if \( n \) is not a power of 2, then

\[ n = (2^k + 1) 2^i \]

and

\[ 2^n = (2^i)^{2^k} \text{ odd} \]

\[ 2^n + 1 = (2^i + 1)(\ldots) \]

\[ 2^n + 1 \] is not a prime if \( i > 0 \).

QED
Def: A **Mersenne prime** is one that is 1 less than a power of 2.

Thm: $2^n - 1$ is prime only if $n$ is prime.

Proof: $2^n - 1 = (2-1)(2^{n-1} + 2^{n-2} + \ldots + 1)$

$n = 2$ $2^2 - 1 = 3$ - prime

$n = 4$ $4^2 - 1 = 15$ - not prime if $n > 1$

$n = 8$ $8^2 - 1 = 63$ - not prime if $n > 1$
\[2^{3^n} - 1 = 7 \cdot (\text{---})\]

\[2^{p^2} - 1 = (2^p - 1)(\text{---})\]

not prime if \(p, q \geq 2\)

\[2^m - 1 \text{ can be prime only if } m \text{ is prime} \]

QED

Exercise

If \(p\) is a prime and \(2^p - 1\) is divisible by another prime \(l\), then \(l = 1 \mod p\).
A ring $R$ is a set equipped with addition, subtraction, and multiplication.

*Example:* $\mathbb{Z} =$ integers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$$

*Example:* $(2+3i)(1+4i) = 2 + 2i + 3i - 3$

$$= -1 + 5i$$

German integers:

$\mathbb{Z}[\sqrt{n}]$
Thm 6.1.13 (Abelian Test)
A nonempty subset $S$ of a ring $R$ is itself a ring iff $\forall a, b \in S$

i) $a - b \in S$

ii) $ab \in S$.

Note
A ring need not contain 1.

Proof Why do we not need addition

i) $\Rightarrow a - a \in S \Rightarrow 0 \in S$

0 - 0 = -0 \in S \Rightarrow -0 \in S$
$$a - (-b) = a + b \in S$$

$S$ is closed under addition.

QED

**Def.** An integral domain $D$ is a ring with no zero divisors, i.e., if $a, b \in D$ and $ab = 0$, then $a = 0$ or $b = 0$.

**Example** $R = \mathbb{Z}/(10)$. This ring is not a domain.

$$3 \cdot 7 = 1$$

$$4 \cdot 5 = 0$$
Thm 6.2.11 A subset $S$ of a domain $D$ is itself a domain $\iff$

1) $S$ is a subring
2) $1 \in S$

Def A field is a ring in which every nonzero elt has a multiplicative inverse.

e.g. $\mathbb{R} = \text{real} \#$

$\mathbb{Q} = \text{rational} \#$

$\mathbb{C} = \text{complex} \#$
2/4 where \( p \) is prime

E.g. \( 2/5 = 50, 1, 2, 3, 4 \)

\[ 1 \cdot 1 = 1, \quad 4 \cdot 4 = 1, \quad 2 \cdot 3 = 1 \]

Later we will see there is a unique field with \( p^n \) elements for any prime \( p \) and integer \( n > 0 \).

**Thm 6.3.14** Every finite integral domain \( D \) is a field.

If \( y \neq 0 \in D \) want to show there is a \( z \in D \) such that \( xy = 1 \)
Consider the set $\{x \alpha : \alpha \in D\} = X$

Let $\#D = n$, claim the elements in $I$ are all different, so there are $n$ of them. Suppose 2 of them are the same, i.e.

$$x_a_1 = x_{a_2} \text{ for } a_1 \neq a_2$$

Then $x_{a_1} - x_{a_2} = 0$

$$x(a_1 - a_2) = 0$$

So $a_1 - a_2 = 0 \Rightarrow a_1 = a_2$

Hence $X = D$ so $1 \in X$, i.e.
there is an $a \in D$ with $xa = 1$, so $a = x^{-1}$. Hence $D$ is a field.

$\text{QED}$

Theorem 6.3.17 (Subfield Test). A subset $S$ of a field $F$ is a subfield if $S$ satisfies:

1) $a, b \in S$
2) $a + b \in S$
3) $ab \in S$

Proof omitted.
Def: A *division ring* (or *skew field*) is a "field" where multiplication need not be commutative.

E.g. \( H = \text{Quaternions} \) (1843)

\[ i^2 = j^2 = k^2 = ij \cdot k = -1 \]

\[ H = \{ a + b i + c j + d k : a, b, c, d \in \mathbb{R} \} \]

\[ ji = -1, \quad ji = -k, \]

\[ ik = -k, \quad ik = -j, \]

\[ kj = -j, \quad kj = -i. \]
Def 6.3.24 A ring $R$ has characteristic $n$ if $n \cdot x = 0$ for all $x \in R$, and $n$ is the smallest integer with this property.

(If there is no such $n$, we say $R$ has characteristic 0.)

e.g. $\mathbb{Z}$ has char $0$

$\mathbb{Z}/p\mathbb{Z}$

Theorem If $D$ is a domain then char $(D) = 0$ or $p$ where $p$ is prime.
Proof: If \( \text{char } (D) \neq \text{prime }, \text{ say } \text{char } (D) = 8 \), then \( 8 \cdot 1 = 0 \) but \( 4 \cdot 2 \neq 0 \) as \( 4 \cdot 2 = 8 \) and zero divisors and \( D \) is not a domain.

Let \( R \xrightarrow{\phi} R' \) be a ring homomorphism

i.e. \( \phi(a + b) = \phi(a) + \phi(b) \)
\( \phi(ab) = \phi(a) \phi(b) \)
\( \ker 0 = \{ x \in R : 0(x) = 0 \} \)

It is a subgroup under addition.

If \( a, b \in \ker 0 \) and \( b \in R \), then

\[ 0(ab) = 0(a) \circ 0(b) = 0 \cdot 0(b) = 0 \]

\[ 0(ba) = 0 \]

**Def.** An ideal \( I \) in a ring \( R \)

is a subgroup with the above property,

i.e., if \( x \in I \) and \( y \in R \) then \( xy, yx \in I \).