Can construct a regular n-gon using straightedge and compass

$\Leftrightarrow$ can construct $\zeta_n \in \mathcal{C}$.

$\Leftrightarrow$ $\frac{2\pi}{n} \in \Theta$.

Lemma: If you can construct a regular n-gon, then n must have the form $n = 2^m p_1 \cdots p_k$, where $p_1 < \cdots < p_k$ are primes with $p_i = 2^{a_i}+1$ for some $a_i \in \mathbb{N}$.

Pf: If $\zeta_n \in \mathcal{C}$ then $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ must be a power of 2.

But $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$. Suppose $n = q_1^{\alpha_1} \cdots q_\ell^{\alpha_\ell}$ for primes $q_1 < \cdots < q_\ell$, $\alpha_i \in \mathbb{N}$. Then

$$\varphi(n) = q_1^{\alpha_1 - 1}(q_1 - 1)\, q_2^{\alpha_2 - 1}(q_2 - 1) \cdots q_\ell^{\alpha_\ell - 1}(q_\ell - 1).$$

This implies the result. ☒

Facts: If p is a prime of the form 2^a+1 then p must have the form $2^{2^b}+1$ for some $b \geq 0$.

Let $F_n = 2^{2^n}+1$, $n \geq 0$. (nth Fermat numbers)

n	F_n
0	3
1	5
2	17
3	257
4	65537

prime

Conj 1: These are the only prime Fermat #'s.

Conj 2 ("easier"): There are only finitely many Fermat primes.

Lemma: If n is a Fermat prime then $\zeta_n \in \mathcal{C}$.

Pf: $\varphi(n) = n-1 = 2^a$. Also $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong C_n$

Since C_n has subgroups of orders 2^ℓ, $0 \le \ell \le a$,

by the FTGT, there are int. fields

$K_0 = \mathbb{Q} \subseteq K_1 \subseteq \cdots \subseteq K_{a-1} \subseteq K_a = \mathbb{Q}(\zeta_n)$ with

$[K_i : K_{i-1}] = 2, \ \forall i.$ ∎

Thm: A regular n-gon is constr. using stredge and compass if and only if $n = 2^m p_1 \cdots p_k$, where $p_1 < \cdots < p_k$ are primes with $p_i = 2^{a_i} + 1$.

Pf: One direction follows from lemma on previous page.

For the other, suppose $n = 2^m p_1 \cdots p_k$ as above.

We know from the prev. lem. that $\zeta_{p_1}, \ldots, \zeta_{p_k} \in \mathcal{C}$.

Let $a, b \in \mathbb{Z}$ be chosen s.t. $ap_1 + bp_2 = 1$.

Then $\left(e^{2\pi i/p_1}\right)^b \cdot \left(e^{2\pi i/p_2}\right)^a = e^{2\pi i/p_1 p_2}$

$\Rightarrow \zeta_{p_1 p_2} \in \mathcal{C}$.

Continuing in this way, $\zeta_{p_1 \cdots p_k} \in \mathcal{C}$.

By using angle bisection m times, $\zeta_n \in \mathcal{C}$. ∎

Last problem that the Greeks couldn't solve:

4) Trisecting an arbitrary angle.

Can't do it: if you could, then you trisect a $60°$ angle to make a regular 9-gon, which contradicts our theorem.

Another way: Use the triple angle formula to show that $\cos(20°)$ satisfies a cubic irred. poly. in $\mathbb{Q}[x]$.

$$e^{i3\theta} = (\cos\theta + i\sin\theta)^3 = \cdots$$

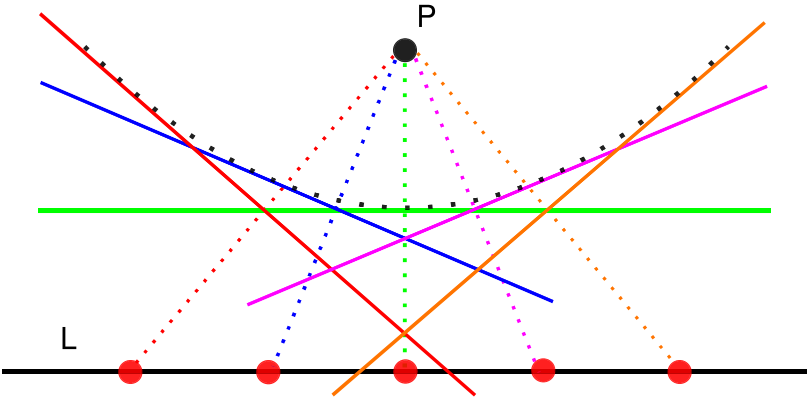
→ it follows from this that the only integer angles, measured in degrees, that can be constructed, are integer multiples of $3°$.

Note: $\frac{2\pi}{5} = 72°$, $\frac{2\pi}{6} = 60°$

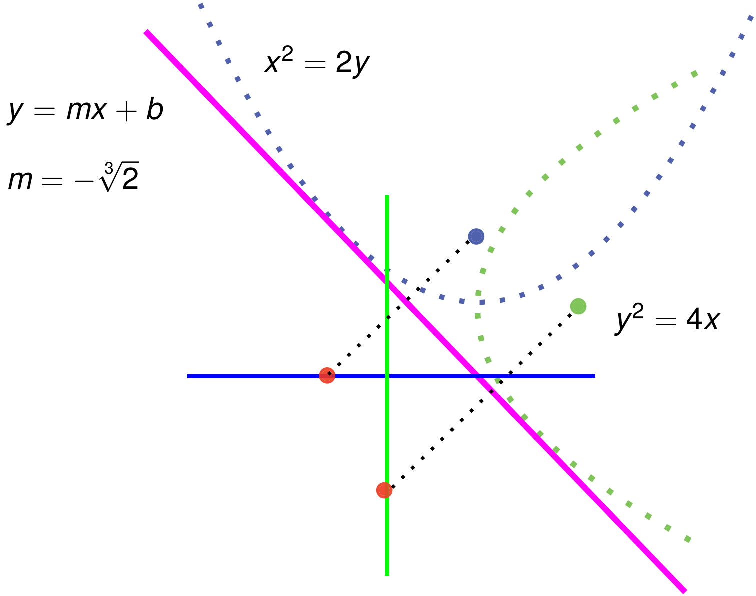
$$\frac{72° - 60°}{4} = 3°$$

(Origami folding)

Constructing tangents to a parabola



A tangent to two parabolas



Solvability

Work over $\mathbb{Q}$. A polynomial $f(x) \in \mathbb{Q}[x]$ is solvable by radicals if $\exists k \in \mathbb{N}$ and a sequence of fields $F_0 \subseteq \cdots \subseteq F_k$ s.t.:

i) $F_0 = \mathbb{Q}$ and F_k contains the splitting field of $f(x)$

ii) $\forall\, 1 \le i \le k$, $\exists\, \alpha_i \in \mathbb{C}$, $m_i \in \mathbb{N}$ s.t. $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{m_i} \in F_{i-1}$.