Un primo di Fermat è un numero della forma $F_k = 2^{2^k} + 1$ per $k = 0, 1, 2, \ldots$. Per $k = 0, 1, 2, 3, 4$ abbiamo che $F_k = 3$, 5, 17, 257 e 65537 sono tutti primi. Per $5 \leq k \leq 32$ i numeri di Fermat F_k *non* sono primi. Per $k = 33, 34, 35$ e infiniti altri valori non si sa se gli F_k sono primi o meno.

Teorema 1. *Un poligono regolare di n lati è costruibile con riga e compasso se e solo se n è una potenza di 2 moltiplicata per un prodotto di numeri di Fermat distinti.*

Per esempio, per $n = 3$, 4, 5, 6, 8, 10, 12, 15, 16, 17, ... un poligono regolare di n lati è costruibile, ma per $n = 7$, 9, 11, 13, 14, 18, ... non è così.

Un poligono regolare di n lati è costruibile con riga e compasso se e solo se il numero complesso $e^{\frac{2\pi i}{n}}$ è *costruibile*. Come è stato spiegato in classe, i numeri complessi costruibili formano un sottocampo C_{cost} di $\mathbf{C}$. Il campo C_{cost} ha la proprietà che se $z \in C_{\text{cost}}$, allora anche $\overline{z}$ e $\sqrt{z}$ sono in C_{cost}.

Lemma 2. *Siano $r, s \in \mathbf{Z}_{>0}$.*
(a) Se $e^{\frac{2\pi i}{r}}$ è costruibile, allora per ogni divisore s di r anche $e^{\frac{2\pi i}{s}}$ lo è.
(b) Se $\text{mcd}(r, s) = 1$ e i numeri $e^{\frac{2\pi i}{r}}$ e $e^{\frac{2\pi i}{s}}$ sono costruibili, anche $e^{\frac{2\pi i}{rs}}$ lo è.

Dimostrazione. Il lemma segue dal fatto che C_{cost} è un campo e quindi chiuso rispetto alla moltiplicazione. Per la parte (a) basta osservare che $e^{\frac{2\pi i}{s}}$ è la r/s-esima potenza di $e^{\frac{2\pi i}{r}}$. Per la parte (b) siano $u, v \in \mathbf{Z}$ tali che $ur + vs = 1$ e quindi $u/s + v/r = 1/rs$. Questo implica che

$$e^{\frac{2\pi i}{rs}} = (e^{\frac{2\pi i}{r}})^u (e^{\frac{2\pi i}{s}})^v,$$

come richiesto.

Dal lemma segue che la seguente proposizione implica il Teorema 1.

Proposizione 3. *Sia p un primo e sia n una potenza di p. Allora $e^{\frac{2\pi i}{n}}$ è costruibile se e solo se $p = 2$ oppure $n = p$ è un primo di Fermat.*

Useremo la seguente caratterizzazione del campo C_{cost}.

Proposizione 4. *Un numero complesso z è contenuto in C_{cost} se e solo se esiste una catena di sottocampi di $\mathbf{C}$*

$$F_0 \subset F_1 \subset F_1 \subset \ldots \subset F_{n-1} \subset F_n$$

con $F_0 = \mathbf{Q}$ e $[F_k : F_{k-1}] = 2$ per ogni $k = 1, 2, \ldots, n$ con la proprietà che $z \in F_n$.

La proposizione segue dal fatto che le equazioni cartesiane delle rette e delle circonferenze che appaiono nelle costruzioni con riga e compasso hanno grado ≤ 2. Calcolare punti di intersezione porta sempre ad equazioni di grado ≤ 2 e i risultati coinvolgono "soltanto" radici quadrate.

Dimostriamo adesso la Proposizione 3. Supponiamo che p sia primo e che $n = p^a$ per qualche $a \geq 1$. Allora il polinomio minimo di $e^{\frac{2\pi i}{n}}$ è di Eisenstein ed ha grado $\varphi(n) = p^{a-1}(p-1)$. Se $e^{\frac{2\pi i}{n}}$ è costruibile, la Proposizione 4 implica che il grado $[\mathbf{Q}(e^{\frac{2\pi i}{n}}) : \mathbf{Q}]$ è una potenza di 2. Si ha quindi che $p^{a-1}(p-1)$ è una potenza di 2. Questo implica che $p = 2$, oppure p è un primo di Fermat e l'esponente a è uguale a 1.

Per dimostrare il viceversa, basta dimostrare che per n una potenza di 2 oppure un primo di Fermat esiste per $z = e^{\frac{2\pi i}{n}}$ una catena di sottocampi di $\mathbf{C}$ come nella Proposizione 4. Per $n = 2^a$ questo è facile. Abbiamo la catena di sottocampi

$$\mathbf{Q} \subset \mathbf{Q}(i) \subset \mathbf{Q}(e^{\frac{2\pi i}{8}}) \subset \mathbf{Q}(e^{\frac{2\pi i}{16}}) \subset \ldots.$$

Ogni campo nella catena ha grado 2 sul suo predecessore. Anche per $p = 3$ e $p = 5$ è facile esibire una catena. Infatti, per $p = 3$ abbiamo che $e^{\frac{2\pi i}{3}} = (-1 + \sqrt{-3})/2$ e l'estensione

$$\mathbf{Q} \subset \mathbf{Q}(e^{\frac{2\pi i}{3}})$$

ha quindi grado 2. Per $p = 5$, sia $\zeta = e^{\frac{2\pi i}{5}}$. Allora si ha che $\zeta^2+\zeta+1+\zeta^{-1}+\zeta^{-2} = 0$ e quindi $\eta = \zeta + \zeta^{-1}$ è uno zero del polinomio $X^2 + X - 1$. Questo implica che $\eta = (-1 + \sqrt{5})/2$. Poiché ζ soddisfa $\zeta^2 - \eta\zeta + 1 = 0$, una catena del tipo voluto è data da

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(e^{\frac{2\pi i}{5}}).$$

In generale, sia $p = 2^{2^k}+1$ un primo di Fermat e sia $\zeta = e^{\frac{2\pi i}{p}}$. Come spieghiamo brevemente alla fine di questa nota, per ogni $u \in \mathbf{Z}_p^*$ abbiamo l'automorfismo

$$\sigma_u : \mathbf{Q}(\zeta) \longrightarrow \mathbf{Q}(\zeta)$$

determinato da $\sigma_u(\zeta) = \zeta^u$. Poiché $\sigma_u\sigma_v = \sigma_{uv}$, la mappa $\mathbf{Z}_p^* \longrightarrow \{\sigma_u : u \in \mathbf{Z}_p^*\}$ che manda u in σ_u è un isomorfismo di gruppi. Il gruppo $\mathbf{Z}_p^*$ è ciclico di ordine $p - 1 = 2^{2^k}$. Per $j = 0, 1, 2, 3, \ldots, 2^k$, sia $H_j \subset \mathbf{Z}_p^*$ l'unico sottogruppo di ordine 2^{2^k-j}. I sottogruppi H_j sono contenuti uno dentro l'altro e formano una catena di sottogruppi di $\mathbf{Z}_p^*$:

$$\{1\} = H_{2^k} \subset H_{2^k-1} \subset \ldots \subset H_2 \subset H_1 \subset H_0 = \mathbf{Z}_p^*.$$

Per $j = 0, 1, 2, 3, \ldots, 2^k$ sia

$$F_j = \{x \in \mathbf{Q}(\zeta) : \sigma_u(x) = x \text{ per ogni } u \in H_j\}.$$

Per ogni j l'insieme F_j è un sottocampo di $\mathbf{Q}(\zeta)$. I sottocampi F_j sono contenuti uno dentro l'altro e formano una catena di sottocampi di $\mathbf{C}$:

$$F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_{2^k-1} \subset F_{2^k} = \mathbf{Q}(\zeta).$$

Affermiamo che

$$F_{j-1} \underset{\neq}{\subset} F_j, \qquad \text{per } 1 \leq j \leq 2^k.$$

Infatti, per simmetria l'elemento $\eta = \sum_{u \in H_j} \sigma_u(\zeta) = \sum_{u \in H_j} \zeta^u$ è contenuto in F_j, ma $\eta \notin F_{j-1}$. Infatti, se $\eta \in F_{j-1}$, allora $\sigma_v(\eta) = \eta$ per ogni $v \in H_{j-1}$. Sia $v \in H_{j-1} - H_j$. Abbiamo quindi la relazione

$$\sum_{u \in H_j} \zeta^u = \sum_{u \in H_j} \zeta^{vu}.$$

con esponenti u e uv nell'insieme $\{1, 2, \ldots, p-1\}$ tutti distinti. Dividendo per ζ troviamo una relazione polinomiale in ζ di grado $\leq p-2$. Poiché il polinomio minimo su $\mathbf{Q}$ di ζ ha grado $p-1$, questo implica che la relazione è identicamente zero, il che è assurdo.

I campi F_i sono quindi tutti distinti. In particolare abbiamo che $[F_j : F_{j-1}] \geq 2$ per $j = 1, 2, 3, \ldots, 2^k$. Il fatto che $[\mathbf{Q}(\zeta) : \mathbf{Q}]$ è uguale a $p - 1 = 2^{2^k}$ implica adesso che abbiamo sempre uguaglianza, vale a dire $[F_j : F_{j-1}] = 2$ per $j = 1, 2, 3, \ldots, 2^k$ ed abbiamo che $F_0 = \mathbf{Q}$. I campi F_j formano quindi una catena della forma cercata. Questo dimostra la Proposizione 3.

Concludiamo questa nota con una breve discussione degli automorfisi σ_k di $\mathbf{Q}(\zeta)$. Sia p un primo. Il polinomio minimo di $\zeta = e^{\frac{2\pi i}{p}}$ su $\mathbf{Q}$ è $\Phi_p(X) = (X^p - 1)/(X - 1) = X^{p-1} + \ldots + X + 1$. La mappa $\mathbf{Q}[X] \longrightarrow \mathbf{Q}(\zeta)$ data da $f \mapsto f(\zeta)$ induce un isomorfismo di campi

$$j : \mathbf{Q}[X]/(\Phi_p(X)) \xrightarrow{\cong} \mathbf{Q}(\zeta).$$

Per ogni $k \in \mathbf{Z}_p^*$ il polinomio $\Phi_p(X)$ è anche il polinomio minimo di ζ^k. Questo implica che il nucleo dell'omomorfismo $\mathbf{Q}[X] \longrightarrow \mathbf{Q}(\zeta)$ dato da $f \mapsto f(\zeta^k)$ è l'ideale generato da $\Phi_p(X)$ e che la mappa indotta

$$\mathbf{Q}[X]/(\Phi_p(X)) \longrightarrow \mathbf{Q}(\zeta)$$

è un isomorfismo. La composizione con l'omomorfismo j^{-1} è l'automorfismo σ_k di $\mathbf{Q}(\zeta)$ determinato da $\sigma(\zeta) = \zeta^k$.