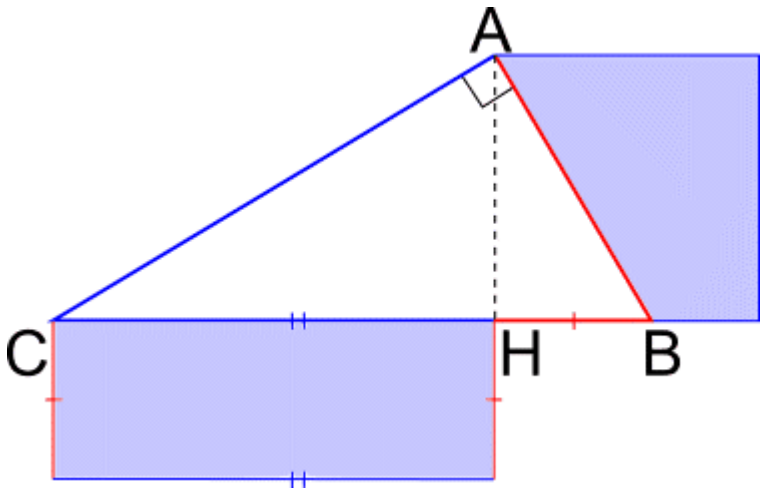
Algebra n. 3 - NOTE ALLA LEZIONE 16

Dimostrazione della **Proposizione 16.3**

Con il nome di *Secondo Teorema di Euclide* (Libro VI, Proposizione 8 degli *Elementi*) si indica solitamente il seguente enunciato di geometria elementare del piano:

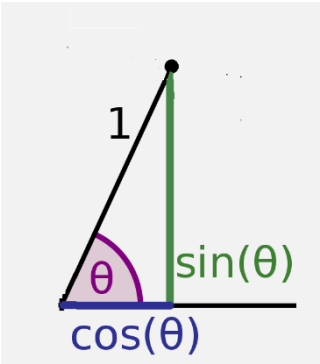


Vale l'identità: $AH^2 = CH \cdot HB$.

Nota storica

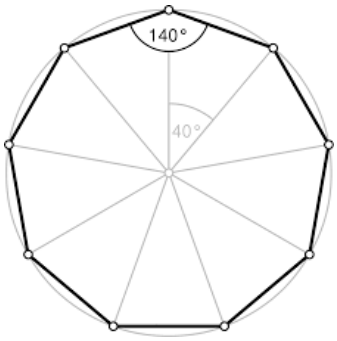
Se $\sqrt{\pi}$ fosse algebrico, allora il campo $\mathbb{Q}(\sqrt{\pi})$ avrebbe grado finito su $\mathbb{Q}$, e quindi sarebbe un'estensione algebrica di $\mathbb{Q}$. Ad essa, tuttavia, appartiene π, che dunque risulterebbe a sua volta algebrico su $\mathbb{Q}$.

Dimostrazione del **Corollario 16.9**



Una volta costruito un angolo di ampiezza θ, delimitato da due semirette (v. figura) si tracci, con centro nel suo vertice, una circonferenza di raggio unitario. Dal suo punto di intersezione con uno dei lati dell'angolo si conduca quindi la perpendicolare (in verde) all'altro lato. Il piede della perpendicolare avrà distanza $\cos\theta$ dal vertice dell'angolo. Viceversa, assegnato, su una semiretta, un punto avente distanza $\cos\theta$ dal suo estremo, si conduca da tale punto la perpendicolare alla semiretta, e la si intersechi con la circonferenza di raggio unitario avente centro nell'estremo della semiretta. Si tracci infine la semiretta congiungente l'estremo con tale punto di intersezione. Questa racchiuderà, con la semiretta assegnata, un angolo di ampiezza θ.

Dimostrazione del **Corollario 16.10**



Ogni poligono regolare è inscrivibile in una circonferenza. Il centro di quest'ultima si trova, ad esempio, come punto di intersezione tra le bisettrici di due angoli interni consecutivi. Queste determinano, allo stesso tempo, uno degli angoli al centro.

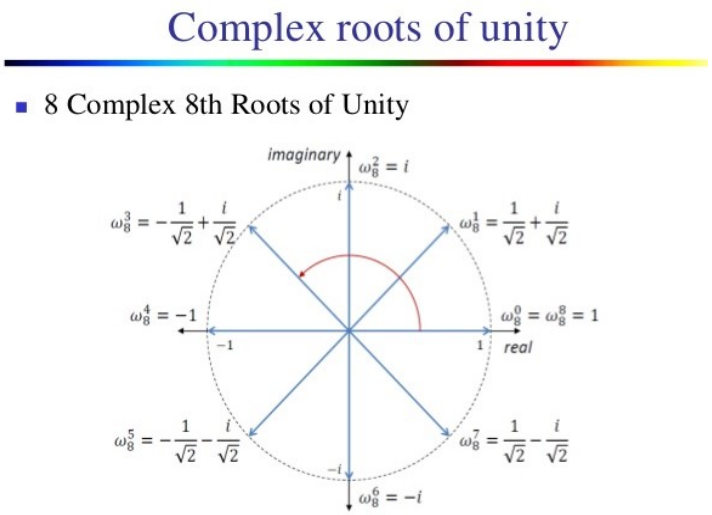
Nota

Per i riferimenti storici a Fermat e agli autori citati più avanti in questa lezione, si vedano le pagine successive a questa, contenenti brani delle loro opere originali.

Teorema 16.14

In base alla Definizione 16.13, se un numero reale è costruibile, è tale anche come numero complesso, in quanto coincide con la propria parte reale. In tal caso, secondo il Teorema 16.4, appartiene ad una estensione 2-radicale di $\mathbb{Q}$; la chiusura normale di quest'ultima è a sua volta un'estensione 2-radicale (come osservato nelle Note alla Lezione 15). Dunque il numero considerato verifica anche la tesi del Teorema 16.14.

Dimostrazione del **Teorema 16.15**



L'immagine illustra il collegamento con i poligoni regolari (qui, un ottagono) nel caso delle radici ottave dell'unità. Una volta costruito il punto che rappresenta

$$\omega = e^{\frac{2\pi i}{n}},$$

ossia il vertice che segue il punto $(1,0)$ percorrendo la circonferenza in senso antiorario, possono essere costruiti tutti gli altri vertici, semplicemente attraverso un trasporto di misura sulla circonferenza (corrispondente, a livello algebrico, alla moltiplicazione per ω, effettuata in maniera iterata).

Ora, alla luce del Teorema 16.14, il numero ω è costruibile se e solo se appartiene ad un'estensione normale di $\mathbb{Q}$ il cui grado è una potenza di 2. Questa condizione è certamente verificata se $[\mathbb{Q}(\omega):\mathbb{Q}]$ è una potenza di 2, in quanto $\mathbb{Q}(\omega)$ è un'estensione normale di $\mathbb{Q}$ (è il campo di spezzamento del polinomio $x^n - 1$). Viceversa, se ω appartiene ad un'estensione normale K di $\mathbb{Q}$ tale che $[K:\mathbb{Q}]$ sia

una potenza di 2, allora anche $[\mathbb{Q}(\omega):\mathbb{Q}]$ è una potenza di 2, in quanto questo numero, per il teorema di moltiplicazione dei gradi, è un divisore del precedente.

Lettera di Pierre de Fermat (1601-1665) a Bernard Frénicle de Bessy

FERMAT A FRENICLE (¹).

< AOUT? 1640 >

(A, f° 76.)

1. Soit par exemple la progression double depuis le binaire avec ses exposants au-dessus :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536

Je dis que, si vous augmentez les nombres de la progression de l'unité, et que vous fassiez 3, 5, 9, 17, etc., tous les dits nombres progressifs ainsi augmentés, qui se trouveront avoir pour exposants des nombres qui ne sont pas de la dite progression double, seront nombres composés.

2. Bien qu'on puisse faire une anatomie particulière qui est trop longue à décrire, il suffit de vous faire comprendre, dans l'exemple qui suit, la proposition que j'y ai faite :

Soit le nombre progressif augmenté de l'unité 8193, duquel l'exposant est 13 nombre premier. Je dis que, si vous divisez 8193 par 3, le

(¹) Fragment publié par M. Ch. Henry (*Recherches etc.*, p. 192-193) d'après le brouillon d'Arbogast. Il porte sur la copie au net le titre : *Sur les nombres premiers de Fermat à Frenicle*, et la mention : *D'après la copie de Mersenne*.

quotient ne pourra être divisé que par un nombre qui surpasse de l'unité ou le double de 13 exposant susdit, ou un multiple dudit double de 13, etc., à l'infini.

Que si l'exposant est un nombre composé, qui pourtant ne soit pas un de ceux de la progression double, je puis trouver tous les diviseurs fort aisément.

3. Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé (¹) que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme

3 5 17 257 65537 4294967297

et le suivant de 20 lettres

18446744073709551617; etc.

Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurois peine à me dédire.

Dalla lettera di Fermat a Frénicle

Commento di Fermat alla successione delle potenze di 2:

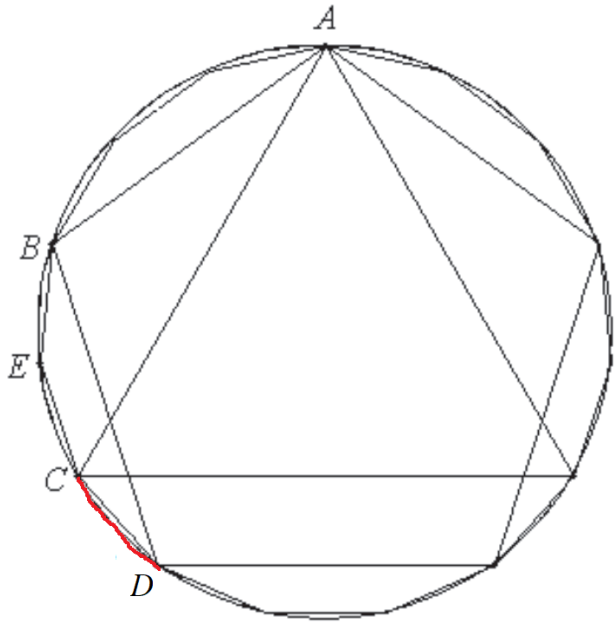
Io dico che, se aumentate i numeri della progressione di una unità, facendo 3, 5, 9, 17, ecc., tutti i numeri progressivi così aumentati, che non avranno per esponente un numero della suddetta progressione doppia, saranno numeri composti.

Questo è l'enunciato del nostro Lemma 16.12, nelle parole del famoso matematico francese.

Più sotto, a proposito del numero 8193, che è pari a $2^{13}+1$, Fermat osserva che il suo quoziente rispetto alla divisione per 3 è della forma $26k+1$, per qualche intero k. Questa sembra voler essere l'indicazione di una tecnica per la fattorizzazione dei numeri di Fermat composti. L'idea soggiacente è basata sul cosiddetto Piccolo Teorema di Fermat, e può essere così presentata in generale. Sia p un numero maggiore di 3. Allora, essendo p dispari, e $2^2 \equiv 1 \pmod 3$, si ha che $2^p+1 \equiv 0 \pmod 3$. Posto allora $2^p+1=3q$, sarà $3q \equiv 3 \pmod p$, da cui $q \equiv 1 \pmod p$. Essendo inoltre q dispari, ne consegue che $q \equiv 1 \pmod{2p}$.

Dagli *Elementi* di Euclide

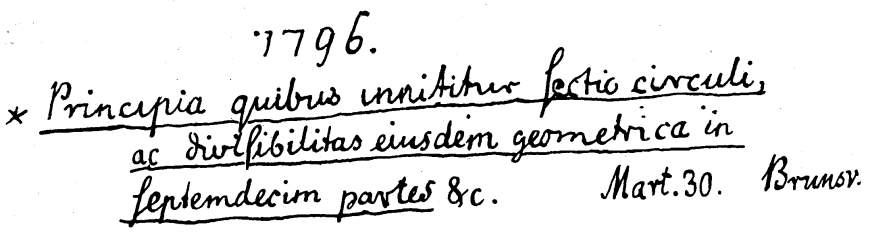
LIBRO IV, PROPOSIZIONE 16
Inscrivere in un cerchio dato un pentadecagono regolare.



Il lato del pentadecagono regolare inscritto in una circonferenza è la corda sottesa ad un arco pari alla quindicesima parte della circonferenza stessa. Questo arco si può costruire sottraendo la terza parte dal doppio della quinta parte (arco CD). Infatti $\frac{2}{5}-\frac{1}{3}=\frac{6-5}{15}$.

Carl Friedrich Gauss (1777-1855)

L'*incipit* dell'annotazione sul suo diario:


1796.
* Principia quibus innititur sectio circuli, ac divisibilitas eiusdem geometrica in septemdecim partes &c. Mart. 30. Brunsv.

Le pagine delle *Disquisitiones Arithmeticae* (1801) – traduzione in francese - dedicate alla costruibilità dei poligoni regolari:

365. Nous avons ainsi réduit par les recherches précédentes la division du cercle en n parties, si n est un nombre premier, à la solution d'autant d'équations qu'il y a de facteurs dans le nombre $n-1$, et dont le degré est déterminé par la grandeur des facteurs. Ainsi, toutes les fois que $n-1$ est une puissance de 2, ce qui arrive pour les valeurs de n

$$3,\quad 5,\quad 17,\quad 257,\quad 65537,\quad \text{etc.},$$

la division du cercle est réduite à des équations du second degré seulement, et les fonctions trigonométriques des angles $\frac{P}{n}$, $\frac{2P}{n}$, etc. peuvent être exprimées par des racines quarrées plus ou moins compliquées, suivant la grandeur de n; donc, dans ces différens cas, la division du cercle en n parties, ou la description du polygone régulier de n côtés, peut s'exécuter par des constructions géométriques. Par exemple, pour $n=17$, on tire facilement des n^os 354, 361

$$\cos\frac{P}{17}=-\tfrac{1}{16}+\tfrac{1}{16}\sqrt{17}+\tfrac{1}{16}\sqrt{(34-2\sqrt{17})}-\tfrac{1}{8}\sqrt{\{(17+3\sqrt{17})-\sqrt{(34-2\sqrt{17})}-2\sqrt{(34+2\sqrt{17})}\}};$$

les cosinus des multiples de cet angle ont une forme semblable, les sinus ont un radical de plus. Il y a certainement bien lieu de s'étonner que la divisibilité du cercle en 3 et 5 parties ayant été connue dès le temps d'*Euclide*, on n'ait rien ajouté à ces découvertes dans un intervalle de deux mille ans, et que tous les géomètres aient annoncé comme certain, qu'excepté ces divisions et celles qui s'en déduisent (les divisions en 2^μ, 15, 5.2^μ, 5.2^μ, 15.2^μ parties), on ne pouvait en effectuer aucune par des constructions géométriques.

Au reste on prouve facilement que si un nombre premier n est $=2^m+1$, le nombre m lui-même ne peut avoir d'autres diviseurs que 2, et qu'il est parconséquent de la forme 2^ν. En effet si m était divisible par un nombre impair ζ plus grand que l'unité, et qu'on eût ainsi $m=\zeta n$, 2^m+1 serait divisible par 2^n+1, et partant composé. Toutes les valeurs de n qui ne conduisent qu'à des équations du second degré, sont donc contenues sous la forme $2^{2^\nu}+1$; ainsi les cinq nombres 3, 5, 17, 257, 65537 s'en déduisent en faisant $\nu=0$, 1, 2, 3, 4 ou $m=1$, 2, 4 8, 16. Mais la réciproque n'est pas vraie, et la division du cercle n'a lieu géométriquement que pour les nombres *premiers* compris dans cette formule. A la vérité *Fermat*, trompé par l'induction, avait affirmé que tous les nombres compris sous cette forme étaient nécessairement premiers; mais *Euler* a remarqué le premier que cette règle était en défaut dès la supposition $\nu=5$ ou $m=32$, qui donne

$$2^{32}+1=4294967297,$$

nombre divisible par 641.

Toutes les fois que $n-1$ renferme des facteurs différens de 2, on est toujours conduit à des équations plus élevées, par exemple, à une ou plusieurs équations du troisième degré, si 3 est une ou plusieurs fois facteur; à des équations du cinquième degré, quand $n-1$ est divisible par 5, etc., et NOUS POUVONS DÉMONTRER EN TOUTE RIGUEUR QUE CES ÉQUATIONS NE SAURAIENT EN AUCUNE MANIÈRE ÊTRE ÉVITÉES NI ABAISSÉES, et quoique les limites de cet Ouvrage ne nous permettent pas de développer ici la démonstration de cette vérité, nous avons cru devoir en avertir, pour éviter que quelqu'un ne voulût essayer de réduire à des constructions géométriques d'autres divisions que celles données par notre théorie, et n'employât inutilement son temps à cette recherche.

366. Si l'on veut diviser le cercle en a^α parties, a étant un nombre premier et $\alpha>1$, il est aisé de voir que la construction géométrique n'est possible qu'autant que $a=2$. En effet, si $a>2$, outre les équations nécessaires pour la division du cercle en a parties, il

Il coseno della 17-esima parte dell'angolo giro:

$$-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

L’impresa di Johann Gustav Hermes (1846-1912)