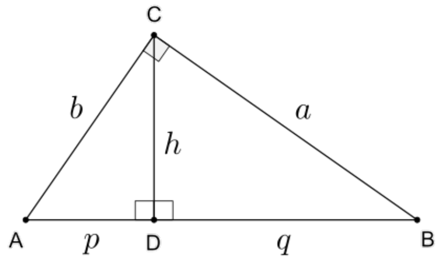
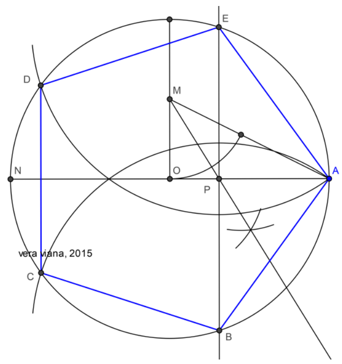
1. Nel triangolo qui accanto, dimostrare che $h^2 = pq$.



$c = p + q$

2. Nel disegno, M è il punto medio del segmento verticale che parte dal centro O della circonferenza. La retta MP è la bisettrice dell'angolo OMA. Se il raggio della circonferenza è 1, dimostrare che il segmento OP ha lunghezza $\cos\frac{2\pi}{5} = \frac{1}{4}\sqrt{5} - \frac{1}{4}$. Dedurre che A e E (e quindi anche B, C e D) sono vertici di un pentagono regolare inscritto nella circonferenza.



3. Dimostrare che non è possibile costruire con riga e compasso un angolo di 1 grado.
4. Sia p un numero primo, sia ζ_p una radice primitiva p-esima dell'unità.
   (a) Dimostrare che un automorfismo σ di $\mathbf{Q}(\zeta_p)$ è determinato da $\sigma(\zeta_p)$.
   (b) Dimostrare che per ogni $i \in \mathbf{Z}_p^*$ esiste un automorfismo σ con $\sigma(\zeta_p) = \zeta_p^i$.
   (c) Dimostrare che il gruppo degli automorfismi di $\mathbf{Q}(\zeta_p)$ è isomorfo a $\mathbf{Z}_p^*$.
5. (Numeri di Fermat).
   (a) Sia $n \geq 1$. Dimostrare che: se $2^n + 1$ è primo, allora n è potenza di 2.

   Per $k \geq 0$, sia $F_k = 2^{2^k} + 1$ il k-esimo numero di Fermat.

   (b) Sia $k \geq 2$. Dimostrare che $\zeta = 2^{2^{k-2}}$ soddisfa $\zeta^4 + 1 \equiv 0$ modulo F_k. Dimostrare che $\alpha = \zeta + \zeta^{-1}$ soddisfa $\alpha^2 \equiv 2$ e quindi $\alpha^{2^{k+1}} \equiv -1$ modulo F_k.
   (c) Sia q un divisore primo di F_k. Dimostrare che $q \equiv 1 \pmod{2^{k+2}}$.
6. Sia $p > 2$ primo, sia $H \subset \mathbf{Z}_p^*$ il sottogruppo dei quadrati e sia H' la classe laterale dei non quadrati. Sia ζ una radice primitiva p-esima dell'unità e siano $\eta, \eta' \in \mathbf{Q}(\zeta)$ i periodi di Gauss dati da

$$\eta = \sum_{a \in H} \zeta^a, \qquad \text{e} \qquad \eta' = \sum_{a \in H'} \zeta^a.$$

   (a) Dimostrare che $\eta + \eta' = -1$.
   (b) Sia $\tau = \eta - \eta'$ la cosiddetta *somma di Gauss*. Dimostrare che $\tau = \sum_{a \in \mathbf{Z}_p^*} \chi(a)\zeta^a$ dove χ è l'unico omomorfismo $\mathbf{Z}_p^* \to \{\pm 1\}$ di nucleo H.
   (c) Calcolare il polinomio minimo di τ su $\mathbf{Q}$ per $p = 3$ e per $p = 5$.
   (d) Sia $\epsilon = (-1)^{\frac{p-1}{2}}$. Dimostrare che $\tau^2 = \epsilon p$ e che quindi $\eta = -\frac{1}{2} \pm \frac{1}{2}\sqrt{\epsilon p}$. (Sugg: si ha che $\tau^2 = \sum_{a,b} \zeta^{a+b}\chi(ab)$. Il cambiamento di variabile $b = ac$ ci dà che $\tau^2 = \sum_c \chi(c) \sum_a \zeta^{a(c+1)}$. Distinguere i casi $c = -1$ e $c \neq -1$).