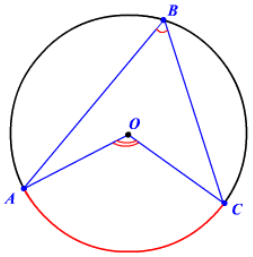
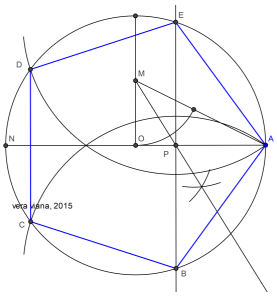
1. Sia $n \geq 2$ e sia $\Phi_n(X)$ l'ennesimo polinomio ciclotomico.
   (a) Dimostrare che $\Phi_n(0) = 1$.
   (b) Dimostrare che $\Phi_n(X)$ è un polinomio *palindromo*. In altre parole, si ha che $\Phi_n(X) = X^{\phi(n)}\Phi_n(1/X)$.
   (c) Dimostrare che, se n è potenza di un primo p, allora $\Phi_n(1) = p$; altrimenti $\Phi_n(1) = 1$.
2. Sia $n \geq 1$, sia $a \in \mathbf{Z}$ e sia p un divisore primo di $\Phi_n(a)$.
   (a) Dimostrare che, se p divide anche $\Phi_d(a)$ per un divisore proprio d di n, allora a è uno zero doppio di $X^n - 1$ modulo p.
   (b) Dimostrare che p divide n oppure p è congruo a 1 (mod n).
   (c) Fattorizzare i numeri $\Phi_3(7)$, $7^3 - 1$, $3^5 - 1$, $2^9 - 1$.
3. Dimostrare il teorema visualizzato qui accanto: consideriamo due punti A e C su una circonferenza di centro O. Allora per ogni punto B sulla circonferenza, l'angolo AOC è due volte l'angolo ABC. In particolare, se A, O e C stanno su una retta, l'angolo ABC è di 90 gradi.



4. Nel disegno qui a destra, 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, B e E (e quindi anche C e D) sono vertici di un pentagono regolare inscritto nella circonferenza.



5. Dimostrare che è possibile costruire con riga e compasso un angolo di 3 gradi, ma non è possibile costruirne uno di 1 grado.
6. (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 $q \equiv 1$ (mod 2^{k+2}).
7. Sia p un numero primo, sia ζ_p una radice primitiva p-esima dell'unità.
   (a) Sia $\sigma : \mathbf{Q}(\zeta_p) \longrightarrow \mathbf{Q}(\zeta_p)$ un omomorfismo. Dimostrare che σ è biiettivo ed è quindi un *automorfismo* di $\mathbf{Q}(\zeta_p)$.
   (b) Dimostrare che gli automorfismi di $\mathbf{Q}(\zeta_p)$ formano un gruppo G per la composizione.
   (c) Dimostrare che un automorfismo σ di $\mathbf{Q}(\zeta_p)$ è determinato da $\sigma(\zeta_p)$.
   (d) Dimostrare che per ogni $i \in \mathbf{Z}_p^*$ esiste un automorfismo σ con $\sigma(\zeta_p) = \zeta_p^i$.
   (e) Dimostrare che G è isomorfo a $\mathbf{Z}_p^*$.