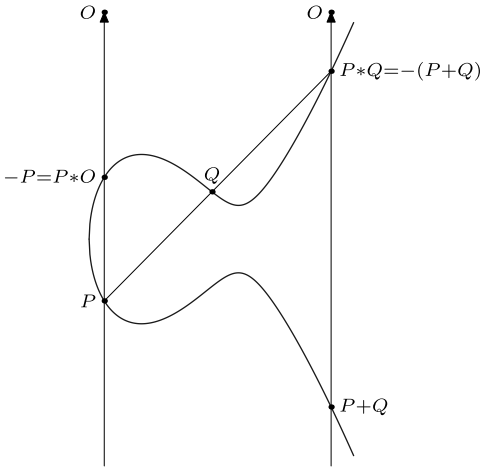
7.5.6. Uso dei flessi come elemento neutro. Se come elemento neutro O usiamo uno dei flessi della curva, abbiamo già osservato che $O * O = O$. In questo caso $-P = P * O$ e quindi $P * Q = -(P + Q)$. Questo significa che la legge di gruppo è determinata dalla scelta del flesso O e dalla proprietà che tre punti allineati hanno somma nulla. Scegliendo il flesso improprio della forma canonica, la costruzione geometrica diventa molto facile:



7.5.7. Punti di ordine 2 e 3. Scegliendo come O un flesso, abbiamo che i punti di ordine 2 della legge di gruppo sono i punti di tangenza alla cubica delle rette uscenti da O (sono quattro punti, contando O stesso); i punti di ordine 3 sono tutti e soli i punti di flesso della cubica (quindi nove punti, di nuovo contando anche O). Per i punti di ordine superiore?

7.5.8. Formule esplicite. Dalle costruzioni geometriche fatte è chiaro che la legge di composizione si potrà scrivere in modo esplicito, usando le coordinate dei punti, in termini di funzioni razionali delle coordinate dei punti di partenza. Per far capire cosa intendiamo, esplicitiamo le formule di addizione per una cubica affine liscia nella forma di Weierstrass $Y = 4X^3 - g_2X - g_3$, scegliendo il punto improprio (che è un flesso) come elemento neutro. Dato un punto affine P di coordinate $\binom{x}{y}$ è chiaro che il punto opposto $-P$ ha coordinate $\binom{x}{-y}$ (simmetria della curva rispetto all'ascissa). Dati due punti P_1 e P_2 di coordinate $\binom{x_1}{y_1}$ e $\binom{x_2}{y_2}$, vogliamo esprimere le coordinate $\binom{x}{y}$ del punto $P = P_1 + P_2$. Evidentemente basta trovare le coordinate del punto $-P = P_1 * P_2$, determinando il terzo valore di t (oltre a 0 e 1) tale che il punto di coordinate $\binom{x_1+t(x_2-x_1)}{y_1+t(y_2-y_1)}$ soddisfi all'equazione della cubica. Imponendo

$$(y_1 + t(y_2 - y_1))^2 = 4(x_1 + t(x_2 - x_1))^3 - g_2(x_1 + t(x_2 - x_1)) - g_3$$

si trova

$$4(x_2 - x_1)^3t^3 + (12x_1(x_2 - x_1)^2 - (y_2 - y_1)^2)t^2 + (12x_1^2(x_2 - x_1) - g_2(x_2 - x_1) - 2y_1(y_2 - y_1))t = 0$$

da cui si deduce che la terza radice in t vale

$$t = -\frac{12x_1(x_2 - x_1)^2 - (y_2 - y_1)^2}{4(x_2 - x_1)^3} - 1 = \frac{1}{4}\frac{(y_2 - y_1)^2}{(x_2 - x_1)^3} - \frac{2x_1 + x_2}{x_2 - x_1} .$$

Sostituendo questo valore di t si ottiene che il punto cercato $P_1 + P_2$ ha coordinate

$$x = \frac{1}{4}\frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - (x_1 + x_2)$$

$$y = -\frac{1}{4}\frac{(y_2 - y_1)^3}{(x_2 - x_1)^3} + 2\frac{x_1y_2 - x_2y_1}{x_2 - x_1} - \frac{x_1y_1 - x_2y_2}{x_2 - x_1}$$

chiaramente espressioni razionali di quelle di partenza.

7.5.9. Problemi sulla geometria delle curve ellittiche. Usiamo sempre la legge di gruppo con punto neutro un flesso.

(*a*) Tre punti su una curva ellittica sono allineati se e solo se la loro somma è zero.

(*b*) Dati tre punti allineati su una curva ellittica, le tangenti in quei punti intersecano la curva in ulteriori tre punti (detti le intersezioni residue) che risultano allineati; il viceversa non è vero. In simboli: P, Q, R allineati implica $P * P, Q * Q, R * R$ allineati.

(*c*) Dati sei punti su una curva ellittica, essi giacciono su una conica se e solo se la loro somma è nulla (suggerimento: usare un fascio di cubiche generato dalla curva ellittica e da tre rette ottenute usando a coppie i sei punti dati: i nove punti del ciclo base hanno somma zero, e i sei dati stanno su una conica sse gli altri tre sono allineati...).

(*d*) Dati sei punti su una curva ellittica, se essi giacciono su una conica allora i sei punti residui (intersezioni della cubica con le tangenti nei punti dati) stanno anch'essi su una conica. Viceversa?