Cela vaut le coup de s'arrêter sur certains aspects de théorie des groupes liés à la paramétrisation des points distincts de $(-1,-1)$ de la conique :

$$x^2 + y^2 - xy = 1$$

par les formules :

$$x = \frac{4 - 4t - 3t^2}{4 + 3t^2}, \qquad y = \frac{4 + 4t - 3t^2}{4 + 3t^2}$$

$$t = 2\frac{y - x}{x + y + 2}$$

Je rappelle que cette paramétrisation a été obtenue en traçant la droite passant par $(-1,-1)$ et (x,y) et en notant $(1-t, 1+t)$ son intersection avec la tangente à l'ellipse au point $(1,1)$. On pourra considérer que le point $(-1,-1)$ est obtenu avec $t = \infty$, et donc que cette paramétrisation identifie les points de l'ellipse avec $\mathbb{R} \cup \{\infty\}$ et les points rationnels avec $\mathbb{Q} \cup \{\infty\}$.

La conique possède des symétries (définies sur $\mathbb{Q}$) amusantes. D'abord il y a certainement $S : (x,y) \mapsto (y,x)$. Aussi, pour x donné tel qu'il existe y avec (x,y) sur l'ellipse, l'autre racine y' de l'équation $y^2 - xy + x^2 - 1 = 0$ est telle que $y' + y = x$, donc $y' = x - y$. Ainsi $T : (x,y) \mapsto (x, x-y)$ est également une symétrie (involutive, c'est la symétrie dans la droite de pente $\frac{1}{2}$, parallèlement à la direction verticale). On a $S^2 = T^2 = 1$ (je note 1 pour l'identité), et il se trouve que le groupe engendré par S et T est fini, en fait il est d'ordre 12, et est isomorphe au groupe diédral d'ordre (cardinalité) 12 (je ne sais jamais si on note D_6 ou D_{12}). Nous allons le prouver. Pour cela posons $M = ST$, ainsi M agit par $(x,y) \mapsto (x-y, x)$.

1. Vérifier que les itérés de M agissent par

   $$(x,y) \to (x-y,x) \to (-y,x-y) \to (-x,-y) \to (y-x,-x) \to (y,y-x) \to (x,y)$$

   et donc que M est d'ordre 6.
2. Vérifier que $SMS = M^5$. En déduire que le groupe $G := \langle S, M\rangle$ est isomorphe au groupe diédral d'ordre 12 (associé à l'hexagone).
3. Représenter G par des matrices 2×2, et remarquer que le sous groupe $\langle M\rangle$ est celui des matrices de déterminant 1.
4. Montrer qu'au niveau du paramètre t, S agit par $\psi : t \mapsto -t$ et M agit par

   $$\phi : t \mapsto \frac{-6t-4}{3t-6}$$

5. Calculer les itérés ϕ^k de l'homographie ϕ. Réponse pour $k = 1, \dots, 6$: $\frac{-6t-4}{3t-6}$, $\frac{-2t-4}{3t-2}$, $\frac{-4}{3t}$, $\frac{2t-4}{3t+2}$, $\frac{6t-4}{3t+6}$, t.
6. Il est « amusant » que le déterminant $\begin{vmatrix} -6 & -4 \\ 3 & -6 \end{vmatrix}$ vaut 48, qui est intervenu dans nos problèmes de pgcd ! Bref, l'homographie ϕ peut être représentée par la matrice de déterminant +1
$$A := \sqrt{3}\begin{pmatrix} -\frac{1}{2} & -\frac{1}{3} \\ \frac{1}{4} & -\frac{1}{2} \end{pmatrix}$$
Je rappelle en effet qu'on associe à la matrice inversible $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ l'homographie $t \mapsto \frac{at+b}{ct+d}$. Calculer les puissances successives de A. En particulier vous allez obtenir $A^6 = -I_2$, et non pas l'identité ! Je rappelle à ce sujet que les homographies de la droite réelle correspondent au groupe $PGL_2(\mathbb{R}) = GL_2(\mathbb{R})/(\mathbb{R}^\times I_2)$, et non pas au sous-groupe des matrices de déterminant ± 1 ($PGL_2(\mathbb{R})$ en est le quotient par $\pm I_2$).
7. On notera B la matrice $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ de déterminant -1, qui correspond à l'homographie ψ, et vérifie $B^2 = I_2$. Que vaut BAB ? est-ce A^5 ? ou plutôt ne serait-ce pas A^{11} ? En déduire que le groupe $G' = \langle A, B \rangle$ engendré par A et B dans $GL_2(\mathbb{R})$ est isomorphe au groupe diédral d'ordre (cardinalité) 24. Son image dans $PGL_2(\mathbb{R})$ est isomorphe au groupe G.
8. Au début on avait les transformations M et S agissant linéairement sur le plan vectoriel $\mathbb{R}^2$, et engendrant dans $GL_2(\mathbb{R})$ un groupe diédral de cardinalité 12. Montrer que son image dans $PGL_2(\mathbb{R})$ est un groupe d'ordre 6 isomorphe à S_3, le groupe des permutations de trois lettres.
9. On revient à un polynôme $P = X(X-b)(X-c)$ à racines entières *distinctes* avec $b^2 + c^2 - bc$ le carré d'un entier d (forcément non nul). Montrer que les 12 images (b_g, c_g) du couple (b, c) sous l'action du groupe diédral $G = \langle M, S \rangle$ sur le plan $\mathbb{R}^2$ sont toutes distinctes. Montrer que les douze polynômes $P_g = X(X - b_g)(X - c_g)$ sont en fait six et que ce sont précisément les six polynômes de la forme $P(\pm X + n)$ avec $n \in \mathbb{Z}$ et possédant 0 parmi leurs trois racines.
10. Écrire explicitement les six polynômes obtenus à partir de $P := X(X - 9)(X - 24)$, et les douze valeurs associées du paramètre rationnel t.
11. Faites la preuve demandée à la fin de la fiche précédente que les $P(\pm X + n)$, $n \in \mathbb{Z}$, sont les seuls polynômes à racines entières distinctes, dont la dérivée a deux racines entières avec entre elles un écart minimal (14).