$$-1 = \left(\frac{-1}{p}\right) = \left(\frac{\ell}{p}\right) = (-1)^{\frac{\ell-1}{2}}\left(\frac{p}{\ell}\right) = \left(\frac{-p}{\ell}\right) = +1,$$

was ein Widerspruch ist. ($-p = b^2-4ac$, d.h. $-p$ quadratischer Rest mod ℓ !)

Schließlich ist

$$\Gamma := \{z \in \Lambda \mid gz = z\} = \left\{\tfrac{1}{\sqrt{2a}}(x,y,\dots,y) \in \tfrac{1}{\sqrt{2a}}\mathbb{Z}^{p+1} \;\middle|\; x \equiv by \bmod 2a\right\},$$

d.h.

$$\det \Gamma = \begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} = p;$$

mit dem Zusatz b) folgt daher

(iii) $g-1$ induziert einen Automorphismus von Λ^*/Λ.

Nach dem Satz existiert daher eine Modulform f auf $SL_2\mathbb{Z}$ vom Gewicht $\frac{p+1}{2}$ mit p-ganzen Koeffizienten, sodaß

$$\Theta_{[a,b,c]} \equiv f \bmod p.$$

Da der Vektorraum der Modulformen von $SL_2\mathbb{Z}$ vom Gewicht $\frac{p+1}{2}$ eine Basis von Funktionen mit Fourierkoeffizienten in $\mathbb{Z}$ besitzt, folgt leicht, daß f als Modulform mit ~~Fourier~~ ganz-rationalen Fourierkoeffizienten gewählt werden kann.