Is b^2-4ac mod m square

Conjecture: If there exists a solution of the congruence $ax^2 + bx + c \equiv 0 \pmod{m}$ then $b^2 - 4ac$ is a modular square.

Proof: unknown

Theorem: If x is a solution of the congruence $ax^2 + bx + c \equiv 0 \pmod{m}$ then $(b^2 - 4ac) \cdot \frac{x^2}{x^2}$ is a modular square.

Proof: From the hypothesis, $bx \equiv -(ax^2 + c)$

so $b^2x^2 - 4acx^2 \equiv (ax^2 - c)^2$

so $(b^2 - 4ac) \cdot x^2 \equiv (ax^2 - c)^2$

so $(b^2 - 4ac) \cdot \frac{x^2}{x^2} \equiv \frac{(ax^2 - c)^2}{x^2}$

We observe that the right hand side is square because x^2 and $(ax^2 - c)^2$ are both squares, so $(b^2 - 4ac) \cdot \omega_x$ is square. QED ■

Corollary 1: If either (i) x is an euler unit, or (ii) x^2 is a modal integer, then $b^2 - 4ac$ is a modular square.

Proof: We have $(b^2 - 4ac) \cdot \frac{x^2}{x^2} \equiv \frac{(ax^2 - c)^2}{x^2}$ (see proof of Theorem 1).

If (i) x is an euler unit then so too is x^2 so $\frac{x^2}{x^2} \equiv \omega_{x^2} \equiv 1$, so

$(b^2 - 4ac) \cdot \omega_{x^2} \equiv b^2 - 4ac \equiv \frac{(ax^2 - c)^2}{x^2}$ completing proof part (i) ▪

If (ii) x^2 is a modal integer then $\frac{x^2}{x^2} \equiv 1\Delta\frac{m}{i_{x^2}}$ which includes the case $\frac{x^2}{x^2} \equiv 1$ hence $(b^2 - 4ac) \cdot 1 \equiv b^2 - 4ac$ so proof part (ii) concludes the same as part (i). ■

Corollary 2: If x is a modal unit but not euler, then $(b^2 - 4ac) \cdot \omega_x$ is a modular square.

Corollary 3: If x is a modal unit which divides the discriminant $b^2 - 4ac$ then $b^2 - 4ac$ is a modular square.

Proof: In this case $(b^2 - 4ac) \cdot \omega_x \equiv b^2 - 4ac$ so proof concludes like part (i) Cor.1 ■

We want more

We would really like to always be rid of the baggage $\frac{x^2}{x^2}$ but the general case eludes us. Corollaries 1 and 3 come close, but examples disappoint Corollary 3 by showing that, while x does sometimes divide $b^2 - 4ac$, it does not always do so.