Modular Quadratic Formula

To derive: $x \equiv \dfrac{-b \pm \sqrt{b^2 - 4c}}{2a}$ (mod m)

The starting point is the general quadratic congruence in one unknown:

$$ax^2 + bx + c \equiv 0 \text{ (mod } m).$$

If we can divide through by a we might get $x^2 + \frac{b}{a}x + \frac{c}{a} \equiv 0$. This step is permissible and correct under a variety of conditions. Sufficient, for instance, would be if a is a modulo-m euler unit. If a is a unit that divides b and c but is not an euler then ax^2 becomes $\omega_a x^2$ instead of just x^2 (unless we can assume that $a \mid x^2$) so one would probably proceed by replacing x by $y = x \cdot \sqrt{\omega}_a$ and solving for y (group identity-elements are always squares so $\sqrt{\omega}_a$ always exists, but beware: ω_a may not be the only value for $\sqrt{\omega}_a$). Another family of cases assumes a is a modal integer that divides both b and c (mod m) — although in those cases the resulting congruence (including the normalized coefficient of x^2) is not unique. The most general is the necessary condition that b and c be in the trace T_a (*i.e.* the center c_a euclidean-divides the centers c_b and c_c).

Next we rewrite the congruence in the form $[x + \frac{(b/a)}{2}]^2 + \frac{c}{a} - [\frac{b/a}{2}]^2 \equiv 0$ — subject to the additional assumption that $2 \mid (b/a)$ (mod m). One assumption that would guarantee 2 to divide b/a is for 2 be an euler unit (mod m); an alternative would be to assume simply that b/a is in the trace T_2 of modal cluster C_2. Either condition might or might not be satisfied, depending upon $a, b,$ and m.

The next step requires calculating the square root d of $(\frac{b/a}{2})^2 - \frac{c}{a}$ to obtain $x + \frac{b/a}{2} \equiv d$. There is a possibility that the square root may not exist (although modular roots surely exist if real integer roots exist). Of course, whenever there are *any* modular square roots, there are commonly *more* than the two in the real case.

Ignoring derivation issues

The results are still interesting if we just naively calculate the real integer formula using modular arithmetic. In Example 5, the congruence to be solved is

$$x^2 + x - 12 \equiv 0 \pmod{72}$$

so the real-integer quadratic formula is

$$x \equiv (-1 \pm \sqrt{49})/2.$$

To evaluate the formula modulo 72 requires residue 49 to have roots, and also requires the numerator to be divisible by 2.

Sqrt(49) has eight values: 7, 11, 25, 29, 43, 47, 61, and 65 (49 is an euler, so all its square roots are eulers). The last four are the negatives of the first four, *e.g.* $65 \equiv -7$. All of them are odd, so $-1 + \sqrt{49}$ is always in the trace of C_2 (mod 72) hence divisible by 2 — and each produces two alternative values since 2 is an integer modulo 72.
Thus, evaluating the quadratic formula modulo 72 yields:

$x \equiv$ any of **3**, 39, 5, 41, **12**, 48, 14, 50, 21, 57, 23, **59**, 30, 66, 32, and **68**

Four of those actually comprise the complete set of all solutions of the target congruence:

$x \equiv$ **3**, **12**, **59**, and **68**.

None of the other twelve satisfy the congruence — presumably because some of the neglected validity conditions that should have been imposed on the modular calculations had some teeth.

Another example — more complicated but with similar results:

$$14x^2 + 27x + 247 \equiv 0 \pmod{464}$$

The residue system Z_{464} supports four unit groups (C_1 , C_{16}, C_{29}, and C_{464}) along with three modal integer clusters (C_2, C_4, and C_8) and three mixed clusters (C_{58}, C_{116}, and C_{232}).

(The results are similar to Example 5 in that the naive quadratic formula finds all the actual solutions but, as is starting to seem normal, the congruence has way fewer actual solutions than the formula proposes.)