We give an algorithm for solving the congruence $ax^2 + bx + c \equiv 0 \pmod{n}$

1. Completing the square

We assume $a > 0$ and $n > 1$.

Case 1. b even.

$$ax^2 + bx + c \equiv 0 \pmod{n} \tag{1.1}$$
$$\iff a^2x^2 + abx + ac \equiv 0 \pmod{an}$$
$$\iff (ax + b/2)^2 \equiv d/4 \pmod{an},$$

where $d = b^2 - 4ac$.

Solve $X^2 \equiv d/4 \pmod{an}$. If this has no solutions, then (1.1) has no solutions. Otherwise let $X_0, \ldots, X_{s-1}$ be the solutions $\pmod{an}$.

For each i, solve $ax + b/2 \equiv X_i \pmod{an}$, i.e.,

$$ax \equiv X_i - b/2 \pmod{an}. \tag{1.2}$$

. If $X_i - b/2 \not\equiv 0 \pmod{a}$, then (1.2) is not soluble.

However if $X_i - b/2 \equiv 0 \pmod{a}$, then (1.2) has solution

$$x \equiv (X_i - b/2)/a \pmod{n}.$$

Case 2. b odd. Then (1.1) is equivalent to

$$X^2 \equiv d \pmod{4an},$$

where $d = b^2 - 4ac$ and $X = 2ax + b$.

If this has no solutions, then (1.1) has no solutions. Otherwise let $X_0, \ldots, X_{s-1}$ be the solutions $\pmod{an}$.

$$2ax \equiv X_i - b \pmod{4an}. \tag{1.3}$$

If $X_i - b \not\equiv 0 \pmod{2a}$, then (1.3) is not soluble.

However if $X_i - b \equiv 0 \pmod{2a}$, then (1.3) has solution

$$x \equiv (X_i - b)/2a \pmod{2n}.$$

We then have the solutions of (1.1) $\pmod{2n}$.

However if x is a solution of (1.1), so is $x + n$. So the solutions of (1.1) $\pmod{2n}$ come in pairs $\pmod{n}$.

$$x \equiv (X_i - b/2)/a \pmod{n}.$$

2. EXAMPLES

Example 1. Solve $6x^2 + 14x + 8 \equiv 0 \pmod{21}$. This has solutions 8 and 20 $\pmod{21}$.

($X_0 = 55, X_1 = 1, X_2 = -55, X_3 = -1$. $X_0 = 55$ gives $x = 8$, while $X_1 = 1$ gives $x = 20$.)

Example 2. Solve $18x^2 + 5x + 8 \equiv 0 \pmod{21}$. This has solutions 5 and 20 $\pmod{21}$.

$X_4 = 185$ gives $x = 5$, $X_5 = 725$ gives $x = 20$, $X_{10} = -31$ gives $x = -1$, $X_{11} = -571$ gives $x = -16$, so we have solutions $5, 20, -1, -16$ $\pmod{42}$.