Quadratic Congruences, the Quadratic Formula, and Euler's Criterion

R. C. Daileda

Trinity University

Number Theory

Introduction

Let R be a (commutative) ring in which $2 = 1_R + 1_R \in R^\times$. Consider a quadratic equation of the form

$$ax^2 + bx + c = 0, \quad a \in R^\times. \tag{1}$$

In this situation we can complete the square in the usual way:

$$ax^2+bx+c = a(x^2+ba^{-1}x)+c = a(x+ba^{-1}2^{-1})^2+c-b^2a^{-1}2^{-2}$$

Equating with zero, adding $b^2a^{-1}2^{-2} - c$ to both sides and multiplying both sides by 2^2a, (1) becomes

$$4a^2(x + ba^{-1}2^{-1})^2 = b^2 - 4ac. \tag{2}$$

Here we have used the fact that

$$2^2 = (1_R + 1_R)(1_R + 1_R) = 1_R + 1_R + 1_R + 1_R = 4.$$

The Quadratic Formula

It follows that (2) (and hence (1)) has solutions iff

$$\Delta = \underbrace{b^2 - 4ac}_{\text{the discriminant}} = k^2, \;\; k \in R. \tag{3}$$

We then have

$$2a(x + ba^{-1}2^{-1}) = \sqrt{b^2 - 4ac} \;\Leftrightarrow\; 2ax + b = \sqrt{b^2 - 4ac}$$
$$\Leftrightarrow \boxed{x = (2a)^{-1}\left(-b + \sqrt{b^2 - 4ac}\right)},$$

where $k = \sqrt{b^2 - 4ac}$ denotes any solution to (3).

This is the familiar *quadratic formula* for the solutions to (1), valid in any ring R in which $2a \in R^{\times}$.

Quadratic Congruences

A *quadratic congruence* has the form

$$ax^2 + bx + c \equiv 0 \pmod{n}, \quad a, b, c \in \mathbb{Z}.$$

To solve this congruence we will view it as an *equation* in $\mathbb{Z}/n\mathbb{Z}$.

Write $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ with p_i distinct primes and $m_i \in \mathbb{N}$.

Recall the ring isomorphism of the CRT:

$$\rho : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}/p_i^{m_i}\mathbb{Z},$$
$$r + n\mathbb{Z} \mapsto (r + p_i^{m_i}\mathbb{Z})_{i=1}^{k}.$$

Given a ring R, we can interpret any $t \in \mathbb{Z}$ as an element of R by setting $t = t \cdot 1_R$. We then let

$$\mathcal{S}(R) = \{r \in R \,|\, ar^2 + br + c = 0\}.$$

If $\sigma : R \to R'$ is a ring isomorphism, one can show that

$$\sigma : \mathcal{S}(R) \to \mathcal{S}(R')$$

is a bijection.

One can also show that

$$\mathcal{S}(R_1 \times R_2 \times \cdots \times R_k) = \mathcal{S}(R_1) \times \mathcal{S}(R_2) \times \cdots \times \mathcal{S}(R_k).$$

Applying these observations to ρ and $\mathbb{Z}/n\mathbb{Z}$ we find that we have a bijection

$$\rho : \mathcal{S}(\mathbb{Z}/n\mathbb{Z}) \to \prod_{i=1}^{k} \mathcal{S}(\mathbb{Z}/p_i^{m_i}\mathbb{Z}).$$

This proves the following result.

Theorem

The solutions to the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{n}$$

can be found by solving

$$ax^2 + bx + c \equiv 0 \pmod{p_i^{m_i}}, \quad i = 1, 2, \ldots, k,$$

and "gluing" tuples of solutions together using the CRT.

Corollary

The number of solutions (modulo n) to the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{n}$$

is the product of the numbers of solutions (modulo $p_i^{m_i}$*) to*

$$ax^2 + bx + c \equiv 0 \pmod{p_i^{m_i}}, \quad i = 1, 2, \ldots, k.$$

We have therefore reduced the study of quadratic congruences to the case of prime power modulus, p^m.

Since the quadratic formula only holds when $2a \in (\mathbb{Z}/p^m\mathbb{Z})^\times$, we will assume p is odd and $p \nmid a$.

Euler's Criterion

Looking at the quadratic formula, we see that we are faced with two questions:

- How can we tell if Δ is a square in $(\mathbb{Z}/p^m\mathbb{Z})^\times$?
- How can we find all of the values of $\sqrt{\Delta}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$?

Because $(\mathbb{Z}/p^m\mathbb{Z})^\times$ is cyclic, the first question has a straightforward answer.

Theorem (Euler's Criterion)

Let G be a finite cyclic group of even order and $a \in G$. Write $G(2) = \{e, h\}$. Then

$$a^{|G|/2} = \begin{cases} e & \text{if } a = b^2 \text{ for some } b \in G, \\ h & \text{otherwise.} \end{cases}$$

Proof.

Notice that

$$(a^{|G|/2})^2 = a^{|G|} = e \;\Rightarrow\; a^{|G|/2} \in G(2) = \{e, h\}.$$

It therefore suffices to prove that $a^{|G|/2} = e$ iff $a = b^2$.

($\Leftarrow$) If $a = b^2$, then $a^{|G|/2} = (b^2)^{|G|/2} = b^{|G|} = e$.

($\Rightarrow$) Write $G = \langle g \rangle$, $a = g^k$. If $a^{|G|/2} = e$, then $(g^k)^{|G|/2} = e$ and

$$g^{k|G|/2} = e \;\Rightarrow\; |G| \,\Big|\, \frac{k|G|}{2} \;\Rightarrow\; 2|G| \,\Big|\, k|G| \;\Rightarrow\; 2|k.$$

Writing $k = 2m$ we have

$$a = g^k = g^{2m} = (g^m)^2.$$

Recall that for an odd prime p, if $G = (\mathbb{Z}/p^m\mathbb{Z})^\times$, then $1 + p^m\mathbb{Z} \neq -1 + p^m\mathbb{Z}$ are the two elements of $G(2)$.

Corollary (Euler's Criterion $\pmod{p^m}$)

Let p be an odd prime and $m \in \mathbb{N}$. If $p \nmid a$, then

$$a^{p^{m-1}(p-1)/2} \equiv \begin{cases} 1 \pmod{p^m} & \text{if } a \equiv b^2 \pmod{p^m} \text{ for some } b, \\ -1 \pmod{p^m} & \text{otherwise.} \end{cases}$$

Remarks:

- Because we have an efficient way to compute powers modulo p^m, Euler's criterion is a very effective way to detect squares modulo p^m.
- One can state the corollary a bit more generally, replacing p^m with any n for which $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic and using the exponent $\varphi(n)/2$ instead.

Example

Determine if 784967 is a square modulo 37^5. What about 19754611?

We use repeated squaring to compute

$$784967^{37^4\cdot 18} \equiv 1 \pmod{37^5},$$
$$19754611^{37^4\cdot 18} \equiv -1 \pmod{37^5}.$$

Hence the former is a square $\pmod{37}$ while the latter is not.

Remark: Euler's criterion does not tell us what the square roots of 784967 $\pmod{37^5}$ actually em are. They turn out to be ± 47205606.

How Many Squares?

The proof of Euler's Criterion also establishes the following useful result.

Corollary

Let $G = \langle g \rangle$ be a finite cyclic group of even order. Then $a \in G$ is a square if and only if it is an even power of g. In particular, exactly half of the elements of G are squares.

Proof.

The only thing we need to establish is the final sentence.

The elements of G are $e, g, g^2, g^3, \ldots, g^{|G|-1}$.

(cont.)

According to the first part of the corollary:

- the $|G|/2$ even exponents $0, 2, 4, \ldots, |G| - 2$ yield squares;
- the $|G|/2$ odd exponents $1, 3, 5, \ldots, |G| - 1$ do not.

□

Now that we have an effective way of detecting squares modulo p^m, we turn to the question of how many square roots there are.

The following general result provides the answer.

Theorem

Let G be a finite cyclic group of even order. If $a \in G$ is a square, then the equation $x^2 = a$ has exactly two solutions in G.

Proof.

Write $G(2) = \{e, h\}$. If a is a square, we can write $a = b^2$.

Suppose $c^2 = a$ as well. Then

$$c^2 = a = b^2 \;\Rightarrow\; b^{-2}c^2 = e \;\Rightarrow\; (b^{-1}c)^2 = e \;\Rightarrow\; b^{-1}c \in G(2).$$

Hence $b^{-1}c = e$ or $b^{-1}c = h$, i.e. $c = b$ or $c = bh$.

Therefore b and bh are the only solutions to $x^2 = a$.

Since $h \neq e$, this proves the result. □

Remark: This generalizes the result that $|G(2)| = 2$ for finite cyclic groups of even order, which is the case $a = e$.

Back to $(\mathbb{Z}/p^m\mathbb{Z})^\times$

Suppose that $a + p^m\mathbb{Z} \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ is a square.

Write $a + p^m\mathbb{Z} = (b + p^m Z)^2 = b^2 + p^m\mathbb{Z}$.

According to an earlier comment and the proof of the theorem, $\pm b + p^m\mathbb{Z}$ must be the (only) two square roots of $a + p\mathbb{Z}$.

Corollary

Let p be an odd prime, $m \in \mathbb{N}$ and $a \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ a square. Then a has exactly two square roots and they are (additive) inverses of each other.

Remark: Later we will see how to obtain a square root $\pmod{p^m}$ from one $\pmod{p}$. There exist efficient algorithms for finding square roots $\pmod{p}$, but they are a bit too tricky for us.

Back to $\mathbb{Z}/n\mathbb{Z}$

We can now strengthen our earlier statement on the number of solutions to a quadratic congruence.

Theorem

Consider the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{n}. \tag{4}$$

If $\Delta = b^2 - 4ac$ and $(2a\Delta, n) = 1$, then (4) has a solution if and only if Δ is a square modulo p^m for each prime power dividing n. In this case, (4) has exactly 2^k incongruent solutions modulo n, where k is the number of prime divisors of n.

We already know that the number of solutions $\pmod{n}$ is the product of the numbers of solutions $\pmod{p^m}$.

According to the quadratic formula and the final corollary above, the number of solutions $\pmod{p^m}$ is 2 or 0, depending on whether or not $\Delta + p^m\mathbb{Z}$ is a square in $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

So we have solutions to (4) if and only if Δ is a square $\pmod{p^m}$ for every p^m dividing n, and there will be exactly 2^k solutions in this case.

This completes the proof. □

Example

Solve the quadratic congruence

$$x^2 + 3x + 17 \equiv 0 \pmod{315}.$$

We have $a = 1$ and

$$\Delta = 3^2 - 4 \cdot 17 = 9 - 68 = -59.$$

Since $n = 315 = 3^2 \cdot 5 \cdot 7$, $(2a\Delta, n) = 1$.

Furthermore

$$\Delta \equiv 1 \equiv 1^2 \pmod{5},$$
$$\Delta \equiv 4 \equiv 2^2 \pmod{7},$$
$$\Delta \equiv 4 \equiv 2^2 \pmod{9}.$$

Hence the original congruence has 2^3 solutions.

Since the inverse of 2 is $3 \pmod 5$, $4 \pmod 7$, $5 \pmod 9$, the quadratic formula yields the solutions

$$\begin{aligned} x &\equiv 3(-3 \pm 1) \equiv 3, 4 \pmod 5, \\ x &\equiv 4(-3 \pm 2) \equiv 1, 3 \pmod 7, \\ x &\equiv 5(-3 \pm 2) \equiv 2, 4 \pmod 9, \end{aligned}$$

Using the CRT to solve the system arising from every possible combination of roots we obtain

$$\boxed{x \equiv 29, 38, 94, 148, 164, 218, 274, 283 \pmod{315}}.$$