Quadratic Congruences

It is natural to look at quadratic congruences

$$Ax^2 + Bx + C \equiv 0 \mod m$$

In this section, we will restrict the modulo to an odd prime p

$$Ax^2 + Bx + C \equiv 0 \mod p$$

We know that there is an integer A' such that $AA' \equiv 1 \mod p$. Therefore, the congruence can be rewritten as

$$\begin{aligned} Ax^2 + Bx + C &\equiv 0 \mod p \\ x^2 + A'Bx + A'C &\equiv 0 \mod p \end{aligned}$$

If $A'B$ is even, then we can complete the square to get

$$\begin{aligned} 0 &\equiv x^2 + A'Bx + A'C \mod p \\ 0 &\equiv x^2 + A'Bx + \left(\frac{A'B}{2}\right)^2 - \left(\frac{A'B}{2}\right)^2 + A'C \mod p \\ \left(x + \frac{A'B}{2}\right)^2 &\equiv \left(\frac{A'B}{2}\right)^2 - A'C \mod p \end{aligned}$$

If $A'B$ i odd, change it to $A'B + p$ and then complete the square

$$\begin{aligned} 0 &\equiv x^2 + (A'Bx + p) + A'C \mod p \\ 0 &\equiv x^2 + (A'Bx + p) + \left(\frac{A'B + p}{2}\right)^2 - \left(\frac{A'B + p}{2}\right)^2 + A'C \mod p \\ \left(x + \frac{A'B + p}{2}\right)^2 &\equiv \left(\frac{A'B + p}{2}\right)^2 - A'C \mod p \end{aligned}$$

In either case, we have replaced

$$Ax^2 + Bx + C \equiv 0 \mod p$$

With an equivalent quadratic congruence of the form

$$y^2 \equiv a \mod p$$

Example

Find all the solutions of the congruence $2x^2 + 3x + 1 \equiv 0 \mod 5$.

The multiplicative inverse of 2 modulo 5 is 3. Thus,

$$\begin{aligned} 0 &\equiv 2x^2 + 3x + 1 \mod 5 \\ &\equiv x^2 + 4x + 3 \mod 5 \\ &\equiv x^2 + 4x + 4 - 4 + 3 \mod 5 \\ &\equiv (x + 2)^2 - 1 \mod 5 \\ (x + 2)^2 &\equiv 1 \mod 5 \end{aligned}$$

By inspection, we see that $x = 2$ and $x = 4$ are solutions.

Such quadratic congruences do not always have solutions

$$\begin{aligned} 0^2 &\equiv 0 \mod 5 \\ 1^2 &\equiv 1 \mod 5 \\ 2^2 &\equiv 4 \mod 5 \\ 3^2 &\equiv 4 \mod 5 \\ 4^2 &\equiv 1 \mod 5 \end{aligned}$$

Therefore, there is no solution for $x^2 \equiv 2 \mod 5$ or $x^2 \equiv 3 \mod 5$

Theorem : (11.1)

Suppose that p is an odd prime. If $p \nmid a$, then $x^2 \equiv a \mod p$ has exactly two solutions or has no solutions.

Proof. Suppose that the congruence has a solution, call the solution r. Then, notice that $p - r$ is also a solution since

$$\begin{aligned} (p-r)^2 &\equiv p^2 - 2pr + r^2 \mod p \\ &\equiv r^2 \mod p \\ &\equiv 1 \mod p \end{aligned}$$

If s is any solution, then $r^2 \equiv s^2 \mod p$. Therefore,

$$p \mid (r-s)(r+s)$$

Since p is prime, either $p \mid (r-s)$ or $p \mid (r+s)$. In the first case, this gives that $s \equiv r \mod p$, so $s = r$. In the second case, this gives that $s \equiv p - r \mod p$, so $s = p - r$. □

Example

Find all solutions of the congruence $x^2 \equiv 1 \mod 8$.

From inspection, we see that

$$\begin{aligned} 1^2 &\equiv 1 \mod 8 \\ 3^2 &\equiv 1 \mod 8 \\ 5^2 &\equiv 1 \mod 8 \\ 7^2 &\equiv 1 \mod 8 \end{aligned}$$

Therefore, if m is not prime, there can be more than 2 solutions (although they still come in pairs, 1 and 7, and, 3 and 5).

Suppose a is chosen from the integers $1, 2, \ldots, p-1$. Then, $x^2 \equiv a \mod p$ will have two solutions for $\frac{(p-1)}{2}$ values of a. Also, $x^2 \equiv a \mod p$ has no solutions for the other $\frac{(p-1)}{2}$ values of a.

For example, if $p = 11$, then x^2 is of the entries in the table

x	1	2	3	4	5	6	7	8	9	10
$x^2 \mod 11$	1	4	9	5	3	3	5	9	4	1

Therefore, $x^2 \equiv a \mod 11$ will have solutions for: $a \in \{1, 3, 4, 5, 9\}$.

The entries are symmetric about $\frac{p}{2}$ and the same $\frac{p-1}{2}$ least residues appear in each half. For the $\frac{p-1}{2}$ least residues in the first half, there are two solutions. For the $\frac{p-1}{2}$ least residues in the second half, there are no solutions.

Example

For what values of a does $x^2 \equiv a \mod 7$ have two solutions?

The values of a that have two solutions are:

$$\begin{aligned} 1^2 &\equiv 1 \mod 7 \\ 2^2 &\equiv 4 \mod 7 \\ 3^2 &\equiv 2 \mod 7 \end{aligned}$$

So, $a \in \{1, 2, 4\}$ have solutions.

Definition : Quadratic Residues

If $x^2 \equiv a \mod m$ has a solution, then a is called a quadratic residue modulo m.

If $x^2 \equiv a \mod m$ has no solution, then a is called a quadratic non-residue modulo m.

Theorem : Euler's Criterion (11.2)

If p is an odd prime and $p \nmid a$, then $x^2 \equiv a \mod p$ has a solution or no respectively, if

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

or

$$a^{\frac{p-1}{2}} \equiv -1 \mod p$$

Proof. Let g be a primitive root of p, which exist by Theorem 10.6. By the definition of primitive roots, $a = g^k \mod p$ for some k. If k is even, then $x^2 \equiv a \mod p$ has a solution, which is $g^{\frac{k}{2}}$. Furthermore, by Fermat's Theorem we have that

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \left(g^k\right)^{\frac{p-1}{2}} \mod p \\ &\equiv \left(g^{\frac{k}{2}}\right)^{p-1} \mod p \\ &\equiv 1 \mod p \end{aligned}$$

If k is odd, then by Fermat's Theorem we have that

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \left(g^k\right)^{\frac{p-1}{2}} \mod p \\ &\equiv \left(g^{\frac{p-1}{2}}\right)^2 \mod p \\ &\equiv (-1)^k \mod p \\ &\equiv -1 \mod p \end{aligned}$$

Also, $x^2 \equiv a \mod p$ has no solution. If it did have one, say r, then

$$\begin{aligned} 1 &\equiv r^{p-1} \mod p \\ &\equiv \left(r^2\right)^{\frac{p-1}{2}} \\ &\equiv a^{\frac{p-1}{2}} \mod p \\ &\equiv -1 \mod p \end{aligned}$$

Since p is an odd prime, $1 \equiv -1 \mod p$, which a contradiction. So this has no solutions. □