Legendre Symbol

Example

Determine if $x^2 \equiv 7 \mod 31$ has a solution.

By Euler's Criterion, we need to check $7^{\left(\frac{31-1}{2}\right)} = 7^{15} \mod 31$

$$7^2 \equiv 49 \equiv 18 \mod 31$$

$$7^4 \equiv 18^2 \equiv 324 \equiv 14 \mod 31$$
$$7^8 \equiv 14^2 \equiv 196 \equiv 10 \mod 31$$
$$7^{16} \equiv 10^2 \equiv 100 \equiv 7 \mod 31$$
$$7^{15} \equiv \frac{7^{16}}{7} \equiv \frac{7}{7} \equiv 1 \mod 31$$

Therefore, there is a solution.

Euler's Criterion tells us when $x^2 \equiv a \mod p$ has a solution, but it does not give us a way of finding the solutions. One method is to substitute $x = 1, 2, 3, \ldots$ until a solution is found. Another, sometimes more convenient method, is adding multiples of the modulus and factoring squares.

Example

Find a solution of $x^2 \equiv 7 \mod 31$.

Adding the modulus 31 repeatedly to 7, we have that

$$\begin{aligned} x^2 &\equiv 7 \mod 31 \\ &\equiv 38 \mod 31 \\ &\equiv 69 \mod 31 \\ &\equiv 100 \mod 31 \\ &\equiv 10^2 \mod 31 \end{aligned}$$

Therefore, the congruence is satisfied when $x = 10$ or $x = 21$.

Example

Find a solution of $x^2 \equiv 41 \mod 61$.

Adding the modulus 61 repeatedly to 41, we have that

$$\begin{aligned} x^2 &\equiv 41 \mod 61 \\ &\equiv 102 \mod 61 \\ &\equiv 163 \mod 61 \\ &\equiv 224 \mod 61 \\ &\equiv 4^2 \cdot 14 \mod 61 \end{aligned}$$

Adding the modulus 61 repeatedly to 14, we have that

$$\begin{aligned} 14 &\equiv 75 \mod 61 \\ &\equiv 5^2 \cdot 3 \mod 61 \end{aligned}$$

Adding the modulus 61 repeatedly to 3, we have that

$$\begin{aligned} 3 &\equiv 64 \mod 61 \\ &\equiv 8^2 \mod 61 \end{aligned}$$

Thus we have that:

$$\begin{aligned} x^2 &\equiv 41 \mod 61 \\ &\equiv 4^2 \cdot 5^2 \cdot 8^2 \mod 61 \\ &\equiv 160^2 \mod 61 \\ &\equiv 38^2 \mod 61 \end{aligned}$$

Therefore, the congruence is satisfied when $x = 38$ or $x = 23$.

Definition : The Legendre Symbol

The Legendre symbol, denoted $\left(\frac{a}{p}\right)$, where p is an odd prime and $p \nmid a$, is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue } (\mod p) \\ -1 & \text{if } a \text{ is a quadratic nonresidue } (\mod p) \end{cases}$$

Theorem : (11.3)

The Legendre symbol has the properties:

1. If $a \equiv b \mod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$
3. If $p \nmid a$ and $p \nmid b$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof. Suppose that $x^2 \equiv a \mod p$ has a solution. If $a \equiv b \mod p$, then $x^2 \equiv b \mod p$ also has a solution. This shows that is $\left(\frac{a}{p}\right) = 1$ and $a \equiv b \mod p$, then $\left(\frac{b}{p}\right) = 1$.

Suppose that $x^2 \equiv a \mod p$ does not have a solution. If $a \equiv b \mod p$, then $x^2 \equiv b \mod p$ does not have a solution, because if it did, then $x^2 \equiv a \mod p$ would have a solution. This shows that if $\left(\frac{a}{p}\right) = -1$ and $a \equiv b \mod p$, then $\left(\frac{b}{p}\right) = -1$.

By Euler's Criterion, we have that

$$\left(a^2\right)^{\frac{p-1}{2}} \mod p \equiv a^{p-1} \mod p \equiv 1 \mod p \qquad \text{By FLT}$$

Therefore, by the definition of the Legendre symbol, $\left(\frac{a^2}{p}\right) = 1$. In terms of Legendre symbol, Euler's criterion says that

$$\left(\frac{a}{p}\right) = 1 \quad \text{if} \quad a^{\left(\frac{p-1}{2}\right)} \equiv 1 \mod p$$

$$\left(\frac{a}{p}\right) = -1 \quad \text{if} \quad a^{\left(\frac{p-1}{2}\right)} \equiv -1 \mod p$$

Comparing the 1's and -1's, we see that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$. Therefore, we have that

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

□

Example

Evaluate $\left(\frac{19}{5}\right)$ and $\left(-\frac{9}{13}\right)$.

By Theorem 11.3, we have that

$$\begin{aligned}\left(\frac{19}{5}\right) &= \left(\frac{4}{5}\right) \\ &= \left(\frac{2^2}{5}\right) \\ &= 1\end{aligned}$$

By Theorem 11.3, we have that

$$\begin{aligned}\left(\frac{-9}{13}\right) &= \left(\frac{4}{13}\right) \\ &= \left(\frac{2^2}{13}\right) \\ &= 1\end{aligned}$$