

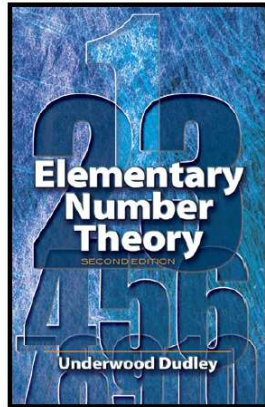
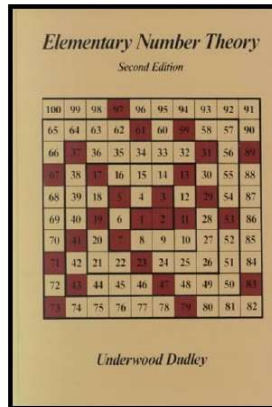
Theorem 11.1

Theorem 11.1. Suppose that p is an odd prime. If $p \nmid a$, then $x^2 \equiv a \pmod{p}$ has exactly two (least residue) solutions or no solutions.

Proof. Notice that $a \not\equiv 0 \pmod{p}$, since $p \nmid a$. Suppose that the congruence has a solution, say r . Then $p - r$ is a solution too, since $(p - r)^2 \equiv p^2 - 2pr + r^2 \equiv r^2 \equiv a \pmod{p}$. If $r = p - r \pmod{p}$, then $2r \equiv 0 \pmod{p}$; but $(2, p) = 1$ so by Theorem 4.4 we have $r \equiv 0 \pmod{p}$, contradicting the fact that $a \not\equiv 0 \pmod{p}$. So r and $p - r$ are different solutions. Let s be any (least residue) solution. Then $r^2 \equiv s^2 \pmod{p}$, whence $p \mid (r - s)(r + s)$. Thus, by Euclid's Lemma (Lemma 2.5), $p \mid (r - s)$ or $p \mid (r + s)$. If $p \mid (r - s)$ then $r \equiv s \pmod{p}$. If $p \mid (r + s)$ then $s \equiv p - r \pmod{p}$. Since s , r , and $p - r$ are all least residues, we have either $s = r$ or $s = p - r$, and these are the only solutions. That is, there are either no solutions or exactly two (least residue) solutions, as claimed. \square

Elementary Number Theory

Section 11. Quadratic Congruences—Proofs of Theorems



Theorem 11.2. Euler's Criterion

Theorem 11.2. Euler's Criterion.

If p is an odd prime and $p \nmid a$, then $x^2 \equiv a \pmod{p}$ has a solution or no solution depending on whether $a^{(p-1)/2} \equiv 1 \pmod{p}$, or $a^{(p-1)/2} \equiv -1 \pmod{p}$, respectively.

Proof. Let g be a primitive root of the odd prime p (there are $\varphi(p-1)$ primitive roots of p , by Theorem 10.6). Since g is a primitive root of p , then by the definition of "primitive root" it has order $\varphi(p) = p-1$. Then $a \equiv g^k \pmod{p}$ for some k (since $a \not\equiv 0 \pmod{p}$).

If k is even, then $x^2 \equiv a \pmod{p}$ has a solution, namely the least residue of $g^{k/2}$. By Fermat's (Little) Theorem, Theorem 6.1, $g^{p-1} \equiv 1 \pmod{p}$, so we have

$$a^{(p-1)/2} \equiv (g^k)^{(p-1)/2} \equiv (g^{k/2})^{(p-1)} \equiv (g^{(p-1)})^{k/2} \equiv 1 \pmod{p}.$$

So $a^{(p-1)/2} \equiv 1 \pmod{p}$ and $x^2 \equiv a \pmod{p}$ has a solution (namely $x = g^{k/2}$), as claimed.

Theorem 11.2. Euler's Criterion (continued)

Theorem 11.2. Euler's Criterion.

If p is an odd prime and $p \nmid a$, then $x^2 \equiv a \pmod{p}$ has a solution or no solution depending on whether $a^{(p-1)/2} \equiv 1 \pmod{p}$, or $a^{(p-1)/2} \equiv -1 \pmod{p}$, respectively.

Proof (continued). If k is odd, then (since $a \equiv g^k \pmod{p}$). Now $x^2 \equiv 1 \pmod{p}$ has two solutions (by Theorem 11.1), namely 1 and $p-1$. We know that $g^{(p-1)} \equiv 1 \pmod{p}$, so $g^{(p-1)/2}$ must have least residue 1 or $p-1$; it can't be 1, or else the order of g is less than $p-1$ and g is not a primitive root of p . So it must be that $g^{(p-1)/2} \equiv p-1 \equiv -1 \pmod{p}$. Therefore $a^{(p-1)/2} \equiv (g^k)^{(p-1)/2} \equiv (g^{(p-1)/2})^k \equiv (-1)^k \equiv -1 \pmod{p}$. Now if $x^2 \equiv a \pmod{p}$ has a solution, say r , then we would have

$$1 \equiv r^{p-1} \equiv (r^2)^{(p-1)/2} \equiv a^{(p-1)/2} \equiv -1 \pmod{p},$$

a contradiction. So there is no solution to $x^2 \equiv a \pmod{p}$. That is, $a^{(p-1)/2} \equiv -1 \pmod{p}$ and $x^2 \equiv a \pmod{p}$ has no solution, as claimed. Since this covers both parities of k , the result holds. \square

Theorem 11.3

Theorem 11.3. The Legendre symbol has the properties

- (A) if $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$,
- (B) if $p \nmid a$, then $(a^2/p) = 1$, and
- (C) if $p \nmid a$ and $p \nmid b$, then $(ab/p) = (a/p)(b/p)$.

Proof. (A) Suppose $(a/p) = 1$, so that $x^2 \equiv a \pmod{p}$ has a solution. Since $a \equiv b \pmod{p}$, then $x^2 \equiv b \pmod{p}$ also has a solution; namely, the same solution as $x^2 \equiv a \pmod{p}$ has. Hence $(b/p) = 1$, as claimed.

Suppose $(a/p) = -1$, so that $x^2 \equiv a \pmod{p}$ does not have a solution. If $(b/p) = 1$ then $x^2 \equiv b \pmod{p}$ has a solution and, as just shown, this would also be a solution to $x^2 \equiv a \pmod{p}$ since $a \equiv b \pmod{p}$, a contradiction. So it must be that $x^2 \equiv b \pmod{p}$ does not have a solution and so $(b/p) = -1$, as claimed.

Theorem 11.5

Theorem 11.5. If p is an odd prime, then

$$(-1/p) = 1 \text{ if } p \equiv 1 \pmod{4}, \text{ and } (-1/p) = -1 \text{ if } p \equiv 3 \pmod{4}.$$

Proof. As observed in the proof of Theorem 11.3, Euler's Criterion (Theorem 11.2) gives $(a/p) \equiv a^{(p-1)/2} \pmod{p}$. So we have

$$(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Since $(p-1)/2$ is even for $p \equiv 1 \pmod{4}$, then in this case we have $(-1/p) = 1$, as claimed. Since $(p-1)/2$ is odd if $p \equiv 3 \pmod{4}$, then in this case we have $(-1/p) = -1$, as claimed. \square

Theorem 11.3 (continued)

Theorem 11.3. The Legendre symbol has the properties

- (B) if $p \nmid a$, then $(a^2/p) = 1$, and
- (C) if $p \nmid a$ and $p \nmid b$, then $(ab/p) = (a/p)(b/p)$.

Proof (continued). (B) The least residue of $a \pmod{p}$ is a solution to the equation $x^2 \equiv a^2 \pmod{p}$. Hence $(a^2/p) = 1$, as claimed.

(C) Notice that the Legendre symbol is only defined for p and odd prime, so we are assuming that property of p . By Euler's Criterion (Theorem 11.2) we have that $(a/p) = 1$ if $a^{(p-1)/2} \equiv 1 \pmod{p}$, and $(a/p) = -1$ if $a^{(p-1)/2} \equiv -1 \pmod{p}$. So $(a/p) \equiv a^{(p-1)/2} \pmod{p}$. Since $(xy)^n \equiv x^n y^n \pmod{p}$ for any x and y , then we have

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}.$$

Since the three Legendre symbols in this equivalence are either 1 or -1 , the only way the two sides of this congruence can be the same is if the left-hand side equals the right-hand side, as claimed. \square