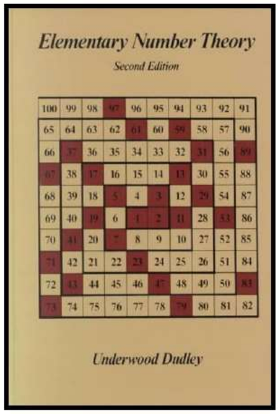
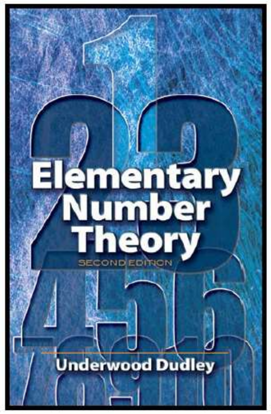
Elementary Number Theory

Section 12. Quadratic Reciprocity—Proofs of Theorems





Theorem 12.1. Gauss's Lemma

Theorem 12.1. Gauss's Lemma.
Suppose that p is an odd prime, $p \nmid a$, and there are among the least residues (mod p) of

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a$$

exactly g that are greater than $(p-1)/2$. Then $x^2 \equiv a \pmod{p}$ has a solution or no solution according as g is even or odd. That is, $(a/p) = (-1)^g$.

Proof. Let $r_1, r_2, \ldots, r_k$ denote the least residues (mod p) of $a, 2a, \ldots ((p-1)/2))a$ that are less than or equal to $(p-1)/2$, and let $s_1, s_2, \ldots, s_g$ denote those that are greater than $(p-1)/2$ (so $k + g = (p-1)/2$). By Euler's Criterion (Theorem 11.2), the claim will follow if we show that $a^{(p-1)/2} \equiv (-1)^g \pmod{p}$.

Theorem 12.1. Gauss's Lemma (continued 1)

Proof (continued). ASSUME that two of $r_1, r_2, \ldots, r_k$ are equal. Then for some $k_1 \neq k_2$ with $0 \le k_1, k_2 \le (p-1)/2$, we have $k_1 a \equiv k_2 a \pmod{p}$. Since $(a, p) = 1$ then by Theorem 4.4 we have $k_1 \equiv k_2 \pmod{p}$ and hence $k_1 = k_2$, a CONTRADICTION. So $r_1, r_2, \ldots, r_k$ must be distinct. Similarly, the $s_1, s_2, \ldots, s_g$ must be distinct. Now consider the set of number $\{r_1, r_2, \ldots, r_k, p - s_1, p - s_2, \ldots, p - s_g\}$. Each integer n in the set satisfies $1 \le n \le (p-1)/2$ and there are up to $k + g = (p-1)/2$ distinct elements in the set. We now show that the numbers in the set are actually distinct.

ASSUME that for some $1 \le i \le k$ and $1 \le j \le g$ we have $r_i \equiv p - s_j \pmod{p}$. Then $r_i + s_j \equiv p \equiv 0 \pmod{p}$. Now $r_i = ta \pmod{p}$ and $s_j = ua \pmod{p}$ for some t and u positive integers less than or equal to $(p-1)/2$. Then $r_i + s_j \equiv (t+u)a \equiv 0 \pmod{p}$ and, since $(a, p) = 1$ then by Theorem 4.4 we have $t + u \equiv 0 \pmod{p}$. But this is a CONTRADICTION since $2 \le t + u \le p - 1$. So the assumption that two of the elements in set $\{r_1, r_2, \ldots, r_k, p - s_1, p - s_2, \ldots, p - s_g\}$ are equal is false, and hence the $k + g = (p-1)/2$ elements of this set are distinct.

Theorem 12.1. Gauss's Lemma (continued 2)

Proof (continued). That is, the set $\{r_1, r_2, \ldots, r_k, p - s_1, p - s_2, \ldots, p - s_g\}$ contains exactly the elements $1, 2, \ldots, (p-1)/2$. So

$$r_1 r_2 \cdots r_k (p - s_1)(p - s_2) \cdots (p - s_g) = 1 \cdot 2 \cdot \cdots \cdot ((p-1)/2).$$

Because $p - s_j \equiv -s_j \pmod{p}$ for all j, then we have

$$r_1 r_2 \cdots r_k s_1 s_2 \cdots s_g (-1)^g \equiv \left(\frac{p-1}{2}\right)! \pmod{p}. \qquad (*)$$

Next, since $r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_g$ are (by construction) the least residues (mod p) of $a, 2a, \ldots, ((p-1)/2)a$, then the product $r_1 r_2 \cdots r_k s_1 s_2 \cdots s_g$ is congruent modulo p to $a(2a)(3a) \cdots ((p-1)/2)a = a^{(p-1)/2} \left(\frac{p-1}{2}\right)!$. So by $(*)$ we have

$$a^{(p-1)/2} (-1)^g \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Theorem 12.1. Gauss's Lemma (continued 3)

Theorem 12.1. Gauss's Lemma.
Suppose that p is an odd prime, $p \nmid a$, and there are among the least residues (mod p) of $a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a$ exactly g that are greater than $(p-1)/2$. Then $x^2 \equiv a \pmod{p}$ has a solution or no solution according as g is even or odd. That is, $(a/p) = (-1)^g$.

Proof (continued). ...

$$a^{(p-1)/2}(-1)^g \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Since $((p-1)/2)!$ is relatively prime to p, then by Theorem 4.4 we have $a^{(p-1)/2}(-1)^g \equiv 1 \pmod{p}$, or (multiplying both sides by $(-1)^g$) $a^{(p-1)/2} \equiv (-1)^g \pmod{p}$. But we know that $a^{(p-1)/2} \equiv (a/p) \pmod{p}$ by Euler's Criterion (Theorem 4.11), so $(a/p) \equiv (-1)^g \pmod{p}$. Since p is an odd prime, this implies $(a/p) = (-1)^g$ as claimed. □

Theorem 12.2

Theorem 12.2. If p is an odd prime, then

$$(2/p) = 1 \text{ if } p \equiv 1 \text{ or } 7 \pmod{8}, \text{ or } (2/p) = -1 \text{ if } p \equiv 3 \text{ or } 5 \pmod{8}.$$

Proof. We will use Thereom 12.1, and so we consider the multiples of 2 of $2, 4, \ldots, p-1$. Let $2a$ be the first even integer greater than $(p-1)/2$. So between 2 and $(p-1)/2$ inclusive) there are $a-1$ even integers, namely $2, 4, 6, \ldots, 2a-2$. Now the total number of even integers between 2 and $p-1$ is $(p-1)/2$, so the number of even numbers greater than $(p-1)/2$ and less than or equal to $p-1$ is $g = (p-1)/2 - (a-1)$. But since $2a$ is the smallest integer greater than $(p-1)/2$, then a is the smallest integer greater than $(p-1)/4$ and hence $a-1$ is the smallest integer greater than $(p-5)/4$. This implies that $-(a-1)$ is the *largest* integer *less* than $-(p-5)/4$, and so $g = (p-1)/2 - (a-1)$ is the largest integer less than $(p+3)/4$.

Theorem 12.2 (continued 1)

Theorem 12.2. If p is an odd prime, then

$$(2/p) = 1 \text{ if } p \equiv 1 \text{ or } 7 \pmod{8}, \text{ or } (2/p) = -1 \text{ if } p \equiv 3 \text{ or } 5 \pmod{8}.$$

Proof (continued). Consider the case when $p \equiv 1 \pmod{8}$. Then $p = 8k+1$ for some k, and $(p+3)/4 = (8k+4)/4 = 2k+1$. Since g is the largest integer less than $(p+3)/4$, then $g = 2k$ and $(-1)^g = (-1)^{2k} = 1$. By Theorem 12.1, $(2/p) = 1$ if $p \equiv 1 \pmod{8}$.

Consider the case when $p \equiv 3 \pmod{8}$. Then $p = 8k+3$ for some k, and $(p+3)/4 = (8k+6)/4 = 2k+3/2$. Since g is the largest integer less than $(p+3)/4$, then $g = 2k+1$ and $(-1)^g = (-1)^{2k+1} = -1$. By Theorem 12.1, $(2/p) = -1$ if $p \equiv 3 \pmod{8}$.

Theorem 12.2 (continued 2)

Theorem 12.2. If p is an odd prime, then

$$(2/p) = 1 \text{ if } p \equiv 1 \text{ or } 7 \pmod{8}, \text{ or } (2/p) = -1 \text{ if } p \equiv 3 \text{ or } 5 \pmod{8}.$$

Proof (continued). Consider the case when $p \equiv 5 \pmod{8}$. Then $p = 8k+4$ for some k, and $(p+3)/4 = (8k+8)/4 = 2k+2$. Since g is the largest integer less than $(p+3)/4$, then $g = 2k+1$ and $(-1)^g = (-1)^{2k+1} = -1$. By Theorem 12.1, $(2/p) = -1$ if $p \equiv 5 \pmod{8}$.

Consider the case when $p \equiv 7 \pmod{8}$. Then $p = 8k+7$ for some k, and $(p+3)/4 = (8k+10)/4 = 2k+5/2$. Since g is the largest integer less than $(p+3)/4$, then $g = 2k+2$ and $(-1)^g = (-1)^{2k+2} = 1$. By Theorem 12.1, $(2/p) = 1$ if $p \equiv 7 \pmod{8}$. □

Theorem 12.3

Theorem 12.3. If p and $4p+1$ are both primes, then 2 is a primitive root of $4p+1$.

Proof. Let $q = 4p+1$. Since q is prime by hypothesis, then $\varphi(q) = q-1 = 4p$. By Theorem 10.2, the order of 2 divides $\varphi(q)$ so that 2 has order 1, 2, 4, p, $2p$, or $4p \pmod{q}$.

Now by Euler's Criterion (Theorem 11.2) $2^{2p} \equiv 2^{(q-1)/2} \equiv (2/q) \pmod{q}$. But p is odd, so $4p \equiv 4 \pmod{8}$, and $q \equiv 4p+1 \equiv 5 \pmod{8}$ so that by Theorem 12.2 we have that $(2/q) = -1$ and hence $2^{2p} \not\equiv 1 \pmod{q}$. That is, the order of 2 is not $2p$. Next, the order of $2 \pmod{q}$ cannot be a divisor of $2p$ or else $2^{2p} \equiv 1 \pmod{q}$ (by Theorem 10.1), which we just saw is not the case. Finally, the order of $2 \pmod{q}$ cannot be 4, since $2^4 \equiv 1 \pmod{q}$ implies that prime q is 3 or 5, neither of which can be the case since $q = 4p+1$ where p is prime. So the only possible value for the order of 2 is $q-1 = 4p$ and so (by definition of "primitive root") 2 is a primitive root of $q = 4p+1$, as claimed. □

Lemma 12.1

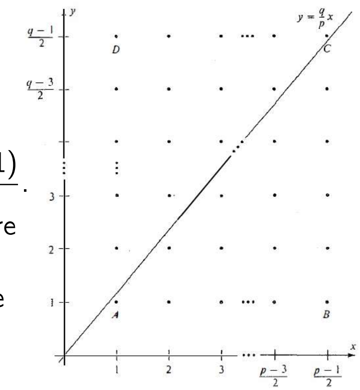
Lemma 12.1. If p and q are different odd primes, then

$$\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right] = \frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Here, $[\cdot]$ denotes the greatest integer function.

Proof.

Let $S(p,q) = \sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]$. Then the claim is $S(p,q) + S(q,p) = \frac{(p-1)(q-1)}{4}$. We give a geometric proof. The figure here has $(p-1)(q-1)/4$ points with integer coordinates. Such points lie below the line $y = px/q$ if their x coordinate is greater than their y-coordinate.



Lemma 12.1 (continued 1)

Proof (continued). The x coordinates of the lattice points are $1, 2, \ldots, (p-1)/2$ and the y coordinates are $1, 2, \ldots (q-1)/2$. There are $(q-1)/2$ lattice points with fixed x coordinate k where $1 \le k \le (p-1)/2$. Consider the line segment $\{(x,y) \mid x = k, 0 \le y \le (q-1)/2\}$. This segment intersects the line $y = qx/p$ at the point $(k, qk/p)$, and the part of the line segment below line $y = qx/p$ is $\{(x,y) \mid x = k, 0 \le y \le \min\{(q-1)/2, qk/p\}\}$. Since $1 \le k \le (p-1)/2$, then $qk/p \le q(p-1)/(2p) < q/2$ and so $[qk/p] \le (q-1)/2$. So the number of lattice points with x coordinate k is $[qk/p]$. Since k ranges from 1 to $(p-1)/2$, the total number of lattice points below the line is $S(p,q) = \sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]$. Interchanging p and q, a similar argument shows that the points to the left of the line is $S(q,p) = \sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right]$.

Lemma 12.1 (continued 2)

Lemma 12.1. If p and q are different odd primes, then

$$\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right] = \frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Here, $[\cdot]$ denotes the greatest integer function.

Proof (continued). ASSUME (a,b) is a lattice point on the line $y = qx/p$. The $b = qa/p$ or $bp = qa$; hence $p \mid qa$ and since $(p,q) = 1$ then $p \mid a$ by Euclid's Lemma (Lemma 2.5); that is, a is a multiple of p. But $1 \le a \le (p-1)/2$ since this is a lattice point, and there are no multiples of p satisfying these inequalities, a CONTRADICTION. So the assumption that there are lattice points on the line $y = qx/p$ is false, and the total number of points in the lattice is the sum of the number of those below the line $y = qx/p$ plus the number of those above the line. Since the lattice contains $(p-1)(q-1)/4$, the claim follows. □

Theorem 12.4. Quadratic Reciprocity Theorem

Theorem 12.4. The Quadratic Reciprocity Theorem.
If p and q are odd primes, then $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.

Proof. As with the proof of Gauss's Lemma (Theorem 12.1), we consider least residues modulo p of multiples of q, $q, 2q, 3q, \ldots((p-1)/2)q$. Denote these multiples of q less than or equal to $(p-1)/2$ as $r_1, r_2, \ldots, r_k$ and denote those greater than $(p-1)/2$ as $s_1, s_2, \ldots, 2_g$. The $k + g = (p-1)/2$ and by Gauss's Lemma we have that the Legendre symbol satisfies $(q/p) = (-1)^g$. Let R and S denote the sums $R = r_1 + r_2 + \cdots + r_k$ and $S = s_1 + s_2 + \cdots + s_g$. It was shown in the proof of Gauss's Lemma the set $\{r_1, r_2, \ldots, r_k, p - s_1, p - s_2, \ldots, p - s_g\}$ contains exactly the elements $1, 2, \ldots, (p-1)/2$. Summing these two representations of the same numbers we get:

$$\sum_{j=1}^{k} r_j + \sum_{j=1}^{g}(p - s_j) = R + pg - S \ldots$$

Theorem 12.4. Quadratic Reciprocity Theorem (cont. 1)

Proof (continued).

$$\sum_{j=1}^{(p-1)/2} j = \frac{((p-1)/2)((p-1)/2+1)}{2} = \frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8},$$

so that $R + gp - S = (p^2-1)/8$ or $R = S - gp + (p^2-1)/8$. The least residue modulo p of jq (where $j \in \{1, 2, \ldots, (p-1)/2\}$) is the remainder when we divide jq by p. We can use the greatest integer function to find the quotient as $[jq/p]$, so that $jq = [jq/p]p + t_j$ where t_j denotes the least residue (mod p) of jq. So $\sum_{j=1}^{(p-1)/2} t_j$ is the sum of the least residues of $q, 2q, \ldots, ((p-1)/2)q$, and hence

$$\sum_{j=1}^{(p-1)/2} t_j = r_1 + r_2 + \cdots r_k + s_1 + s_2 + \cdots + s_g = R + S.$$

Theorem 12.4. Quadratic Reciprocity Theorem (cont. 2)

Proof (continued). Summing both sides of $jq = [jq/p]p + t_j$ gives

$$\sum_{j=1}^{(p-1)/2} jq = \sum_{j=1}^{(p-1)/2} [jq/p]p + \sum_{j=1}^{(p-1)/2} t_j$$

$$\text{or } q \sum_{j=1}^{(p-1)/2} jq = p \sum_{j=1}^{(p-1)/2} [jq/p] + R + S,$$

or $q(p^2-1)/8 = pS(p,q) + R + S$, where $S(p,q)$ is defined in Lemma 12.1. From above, $R = S - gp + (p^2-1)/8$, we now have $q(p^2-1)/8 = pS(p,q) + 2S - gp + (p^2-1)/8$ or

$$(q-1)(p^2-1)/8 = p(S(p,q) - g) + 2S. \qquad (*)$$

Since $\sum_{j=1}^{(p-1)/2} j = (p^2-1)/8$, then $(p^2-1)/8$ is an integer and so the left-hand side of $(*)$ is even.

Theorem 12.4. Quadratic Reciprocity Theorem (cont. 3)

Theorem 12.4. The Quadratic Reciprocity Theorem.
If p and q are odd primes, then $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.

Proof (continued). So the right-hand side of $(*)$, $p(S(p,q) - g) + 2S$, is even and hence $S(p,q) - g$ is even. Hence $(-1)^{S(p,q)-g} = 1$, or $(-1)^{S(p,q)} = (-1)^g$. Since the Legendre symbol satisfies $(-1)^g = (q/p)$ by Gauss's Lemma (Theorem 12.1, with $a = q$), then $(-1)^{S(p,q)} = (-1)^g = (q/p)$. Interchanging p and q, we also get that $(-1)^{S(q,p)} = (p/q)$. Multiplying these last two equations gives $(-1)^{S(p,q)+S(q,p)} = (p/q)(q/p)$ or, by Lemma 12.1,

$$(-1)^{(p-1)(q-1)/4} = (p/q)(q/p),$$

as claimed. □