Proofs of the Quadratic Reciprocity Theorems

Antarish Rautela

November 6, 2018

1 Quadratic Reciprocity Law

If the primes p and q are odd, then $(\frac{p}{q})(\frac{q}{p}) = (1)^{\frac{(p-1)(q-1)}{4}}$, or, $(1) = \frac{(p-1)(q-1)}{4}$ if and only if p $\equiv q \equiv 3(mod4), and (1)^{\frac{(p-1)(q-1)}{4}}$ otherwise.

2 Gauss's Lemma

Let p be an odd prime, q be an integer co-prime to p. Consider the set $\{q, 2q, ..., \frac{(q)(p-1)}{2}\}$ and view each member as an integer in $\{0, 1, ..., p-1\}$. Let u be the number of members in this set that are greater than $\frac{p}{2}$. Then

$$\left(\frac{q}{p}\right) = (-1)^u$$

3 Proof of Gauss's Lemma

Let $\{b_1, ..., b_t\}$ be the members of the set less than $\frac{p}{2}$, and $\{c_1, ..., c_u\}$ be the members greater than $\frac{p}{2}$. Then $u+t = \frac{p-1}{2}$. Consider the sequence $0 < b_1, ..., b_t, p-c_1, ..., p-c_u < p/2$. Each of these are distinct: clearly $b_i \neq b_j$ and $c_i \neq c_j$ whenever $i \neq j$, and if $b_i = p-c_j$, then let $b_i = rq, c_j = sq$. Then $r+s = 0$, which is a contradiction since $0 < r, s < \frac{p}{2}$. Hence they must be the numbers $\{0, 1, ..., \frac{p-1}{2}\}$ in some order. Thus, $q(2q)...(q(p-1)/2) = b_1...b_tc_1...c_u = (-1)^u b_1...b_t(p-c_1)...(p-c_u) = (-1)^u \left(\frac{p-1}{2}\right)!$ Divide both sides by $\frac{p-1}{2}!$ and we complete the proof.

4 Theorem 1

Let p be an odd prime and q be an integer coprime to p. Let $m = \lfloor q/p \rfloor + \lfloor 2q/p \rfloor + ... + \lfloor ((p-1)/2)q/p \rfloor$.Then $m = [u+q-1](mod2)$, where u is the number of elements in $\{q, 2q, ..., q(p-1)/2\}$ which have a residue greater than $\frac{p}{2}$. When q is odd $m = u(mod2)$.

4.1

Proof For any i such that i is an integer between 1, and $\frac{p-1}{2}$, inclusive, the equation $iq = p\lfloor iq/p \rfloor + r_i$ holds for some r_i such that $r_i$is an integer between 0 and p inclusive. Let b_1, b_2,..., b_t be the numbers in the set less than $\frac{p}{2}$, while c_1, c_2,..., c_t be all the other numbers. Summing two equations with b_i and c_i,
q(p$^2 - 1)/8 = pm + b_1 + ... + b_t + c_1 + ... + c_u$
$= pm + b_1 + ... + b_t + up + (p - c_1) + ... + (p - c_u)$
$= pm + up + 1 + 2 + ... + (p - 1)/2$
$= pm + up + (p^2 - 1)/8$

Since p is odd, $m = u + q - 12$.

5 Proof of Quadratic Reciprocity Law

Using the theorem before, all that's left to prove is that $m+n = (p-1)(q-1)/4$. Where n is m except when all p's are q's and vice versa. The difference $py - qx$ when x and y equal $1, 2, ..., \frac{p-1}{2}$, and $1, 2, ..., \frac{q-1}{2}$, respectively. Therefore, there are a total of $\frac{(p-1)(q-1)}{4}$ possible differences. None of them are zero and n of them are positive and m of them are negative.

6 Eisenstein's Proof

Let line L be a line that runs through (0,0) and (p,q), which can be written as $y = \frac{px}{q}$, and consider the rectangle R which has corners at (0,0), (0,$\frac{q}{2}$), ($\frac{p}{2}$,$\frac{q}{2}$), and ($\frac{p}{2}$,0).We can find the number of lattice points in R. By finding the area of the rectangle we get $\frac{(p-1)(q-1)}{4}$. Another way to count is to count the number points above and below L inside R. This is true since there are no lattice points on L since p, and q are co-prime. We can see that the points on x=1 have y coordinates $1, 2, ..., \lfloor \frac{q}{p} \rfloor$. And the points on x=2 have y coordinates $1, 2, ..., \lfloor \frac{2q}{p} \rfloor$. And the points on x=3 have y coordinates $1, 2, ..., \lfloor \frac{3q}{p} \rfloor$. So then the points on x=j have y coordinates $1, 2, ..., \lfloor \frac{jq}{p} \rfloor$. Which gives a total of m points below L in R. And there are n points above L in R.

7 Restating Eisenstein's Proof algebraically

Consider the numbers $px - qy$ for $x = 1, ..., \frac{p-1}{2}$ and $y = 1, ..., \frac{q-1}{2}$. There are a total of $(p - 1)(q - 1)/4$ numbers, not necessarily distinct. None are zero since p, and q are co-prime. We can observe n of them are positive while q of them are negative.