CHARLES VANDEN EYNDEN - ELEMENTARY NUMBER THEORY - SECOND EDITION

5.5 Flipping a Coin over the Telephone

The Proof of Lemma 5.11

Our first order of business is to prove the lemma of the last section from which we derived the law of quadratic reciprocity.

Lemma 5.11. *Let $a > 0$, and let p and q be odd primes not dividing a. Then $(a/p) = (a/q)$ if $p \equiv q \pmod{4a}$ or if $p \equiv -q \pmod{4a}$.*

Proof. As with our evaluations of $(2/p)$ and $(3/p)$, we will employ Gauss's lemma. Let $h = (p-1)/2$, and consider the integers

$$a, 2a, 3a, \ldots, ha.$$

These fall into the open intervals

$$\left(0, \frac{p}{2}\right), \left(\frac{p}{2}, \frac{2p}{2}\right), \left(\frac{2p}{2}, \frac{3p}{2}\right), \left(\frac{3p}{2}, \frac{4p}{2}\right), \ldots, \tag{5.12}$$

where, as is customary, we are denoting the set of real numbers X such that $A < X < B$ by (A, B). Since

$$ha = \frac{(p-1)a}{2} < \frac{pa}{2} < \frac{(p+1)a}{2} = (h+1)a,$$

the last interval we need consider is $((a-1)p/2, ap/2)$. A total of a intervals are involved, so that the number of intervals does not depend on p.

Notice that the endpoints of the intervals listed in (5.12) are either nonintegers or else multiples of p. Thus none of the integers $a, 2a, \ldots, ha$ falls on one of these endpoints, since $p \nmid a$ and $h < p$.

As in Section 5.4, we define x^* by $x^* \equiv ax \pmod{p}$, $-h \le x^* \le h$. By Gauss's lemma the value of (a/p) depends on whether the number of negative x^* is even or odd. The integer x^* will be negative when ax falls in half the intervals listed in (5.12), namely, the intervals

$$\left(\frac{p}{2}, \frac{2p}{2}\right), \left(\frac{3p}{2}, \frac{4p}{2}\right), \left(\frac{5p}{2}, \frac{6p}{2}\right), \ldots.$$

Thus in a typical interval we want to count the number of integers x such that

$$\frac{(2k-1)p}{2} < ax < \frac{2kp}{2},$$

or

$$\frac{(2k-1)p}{2a} < x < \frac{2kp}{2a}. \tag{5.13}$$

Now assume q is an odd prime such that $q \equiv p \pmod{4a}$. Then $q = p + 4at$ for some integer t. If we try to evaluate (a/q) by Gauss's lemma in the same way, a typical interval in which we would be counting integers would be define by the inequalities

$$\frac{(2k-1)q}{2a} < y < \frac{2kq}{2a}. \tag{5.1}$$

Plugging $q = p + 4at$ into this leads to

$$\frac{(2k-1)p}{2a} + (2k-1)2t < y < \frac{2kp}{2a} + 4kt. \tag{5.1}$$

(We leave it to the reader to check the algebra.)

If we compare the endpoints of the intervals defined by the inequalities (5.1 and (5.15) we see that the left endpoints differ by even integers, as do the rig endpoints. Thus the number of integers in the corresponding intervals diffe by a multiple of 2; it is even in both cases or odd in both cases. By using th same argument for each value of k and applying Gauss's lemma we conclud that $(a/p) = (a/q)$.

Now we consider the case when $q \equiv -p \pmod{4a}$. Then $q = -p + 4at$ f some integer t. Plugging this into (5.14) produces

$$\frac{-(2k-1)p}{2a} + (2k-1)2t < y < \frac{-2kp}{2a} + 4kt.$$

Multiplying through by -1 produces a symmetric interval on the other side 0 that contains the same number of integers:

$$\frac{(2k-1)p}{2a} - (2k-1)2t > y' > \frac{2kp}{2a} - 4kt.$$

In fact, the same number of integers are in the interval shifted $4kt$ units to t right:

$$\frac{(2k-1)p}{2a} + 2t > y'' > \frac{2kp}{2a},$$

which can be written

$$\frac{2kp}{2a} < y'' < \frac{(2k-1)p}{2a} + 2t. \tag{5.1}$$

We would like to show that the number of integers y'' satisfying these i equalities is even or odd the same as the number of x satisfying (5.13). B (5.16) and (5.13) define adjacent intervals, and the number of integers in th union is the number of z satisfying

$$\frac{(2k-1)p}{2a} < z < \frac{(2k-1)p}{2a} + 2t.$$

(Recall that the endpoints of our interval are never hit so we need not wor about x equaling the common endpoint of the two intervals.)

The last inequalities define an interval of length $2t$ with nonintegral en points. It must contain an even number of integers. Thus the number of intege satisfying (5.13) and (5.16) must be even in both cases or odd in both cas Again, using this argument for all values of k and applying Gauss's lemma, see that $(a/q) = (a/p)$.