MAS3008 NUMBER THEORY

GAUSS' LEMMA & QUADRATIC RECIPROCITY

Gauss' Lemma

Let p be an odd prime and let $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$. Consider the least residues mod p of the $(p-1)/2$ numbers ka, $k = 1, 2, \ldots, (p-1)/2$. (So these numbers lie in $\{-(p-1)/2, \ldots, (p-1)/2\}$.) Suppose that s of these are negative. Then

$$\left(\frac{a}{p}\right) = (-1)^s.$$

PROOF: Let these residues be $u_1, \ldots, u_r > 0$ and $-v_1, \ldots - v_s < 0$. Thus $r + s = (p-1)/2$ and $1 \leq u_1, \ldots, u_r, v_1, \ldots v_s \leq (p-1)/2$.

The numbers $u_1, \ldots, u_r, v_1, \ldots v_s$ are all different since

1. if $u_i = u_j$ with $i \neq j$ then we have $ka \equiv la \pmod{p}$ for some k, l, with $1 \leq k < l \leq (p-1)/2$, which is impossible as $p \not| a$.

2. if $v_i = v_j$ with $i \neq j$ then we have $-ka \equiv -la \pmod{p}$ for some k, l, with $1 \leq k < l \leq (p-1)/2$, which is impossible as $p \not| a$.

3. if $u_i = v_j$ for some i, j then we have $ka \equiv -la \pmod{p}$ for some k, l with $1 \leq k, l \leq (p-1)/2$. But this implies that $k + l \equiv 0 \pmod{p}$, which is again impossible.

It follows that the numbers $u_1, \ldots, u_r, v_1, \ldots v_s$ are precisely the numbers $1, 2, \ldots (p-1)/2$ in some order, so that

$$\left(\prod_{i=1}^{r} u_i\right)\left(\prod_{j=1}^{s} v_j\right) = \left(\frac{p-1}{2}\right)!.$$

Thus

$$\prod_{k=1}^{(p-1)/2} (ka) \equiv \left(\prod_{i=1}^{r} u_i\right)\left(\prod_{j=1}^{s}(-v_j)\right) \equiv (-1)^s \left(\frac{p-1}{2}\right)! \pmod{p}.$$

On the other hand, using Euler's criterion, we have

$$\begin{aligned}\prod_{k=1}^{(p-1)/2} (ka) &= a^{(p-1)/2} \prod_{k=1}^{(p-1)/2} k \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{p-1}{2}\right)!.\end{aligned}$$

Thus we have

$$\left(\frac{a}{p}\right) \equiv (-1)^s \pmod{p},$$

and this must be an equality (rather than just a congruence mod p) since both sides are ± 1. $\square$

Theorem (Quadratic Reciprocity)

Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{((p-1)/2)\cdot((q-1)/2)}.$$

PROOF:

Call a point (x, y) in the plane a **lattice point** if $x, y \in \mathbb{Z}$. We will consider the lattice points inside or on the edges of the rectangle with horizontal sides $y = 1, (q-1)/2$ and vertical sides $x = 1, (p-1)/2$. Clearly the number of such lattice points is

$$\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}.$$

The three lines shown are:

$$L: \qquad y = \frac{q}{p}x, \qquad \text{i.e.} \quad x = \frac{p}{q}y.$$

$$L_1: \qquad y = \frac{q}{p}x + \frac{1}{2}.$$

$$L_2: \qquad x = \frac{p}{q}y + \frac{1}{2}.$$

Note that the diagram is symmetric under swapping x and y; p and q; L_1 and L_2.

None of the lattice points in or on the rectangle lie on any of the lines L, L_1, L_2: for $x, y \in \mathbb{Z}$ we have

$$(x, y) \in L \Rightarrow py = qx \Rightarrow p|x;$$

$$(x, y) \in L_1 \Rightarrow 2py = 2qx + p \Rightarrow p|x;$$

$$(x, y) \in L_2 \Rightarrow 2qx = 2py + q \Rightarrow q|y;$$

and in each case this shows that (x, y) cannot lie in or on the rectangle. Thus each of the $(p-1)/2 \cdot (q-1)/2$ lattice points is in one of the regions A, B, C_1, C_2 (where A and B include points on the edges of the rectangle).
We claim:

(i) A and B contain the same number of lattice points, m say;

(ii) C_1 contains s_1 lattice points, where $\left(\frac{q}{p}\right) = (-1)^{s_1}$;

(iii) C_2 contains s_2 lattice points, where $\left(\frac{p}{q}\right) = (-1)^{s_2}$.

Assuming this, we have

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \text{Number of lattice points in/on rectangle} = s_1+s_2+2m,$$

so

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s_1+s_2} = (-1)^{s_1+s_2+2m} = (-1)^{(p-1)/2\cdot(q-1)/2}$$

as required.

To prove the claim:

(i) A and B contain the same number of lattice points because, by symmetry, we can rotate the rectangle by 180 degrees about its centre

$$R = ((p+1)/4, (q+1)/4).$$

In detail, the transformation

$$(x, y) \mapsto (x^*, y^*) = ((p+1)/2 - x, (q+1)/2 - y)$$

takes lattice points to lattice points, and takes the rectangle to itself:

$$1 \le x \le (p-1)/2 \iff 1 \le x^* \le (p-1)/2$$

and similarly for y. This transformation interchanges A and B:

$$\begin{aligned}
(x, y) \in A &\iff y > \frac{qx}{p} + \frac{1}{2} \\
&\iff \frac{q+1}{2} - y^* > \frac{q}{p}\left(\frac{p+1}{2} - x^*\right) + \frac{1}{2} \\
&\iff x^* > \frac{p}{q}y^* + \frac{1}{2} \\
&\iff (x^*, y^*) \in B.
\end{aligned}$$

(ii) We count the lattice points in C_1. For $1 \le x \le (p-1)/2$:

$$(x, y) \in C_1 \iff \frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2}.$$

(Equality is impossible for lattice points). For each x, there is at most one y satisfying this, and

$$\begin{aligned}
\text{Such a } y \text{ exists} &\iff \frac{qx}{p} < \left\lfloor \frac{qx}{p} + \frac{1}{2} \right\rfloor \\
&\iff \left\lfloor \frac{qx}{p} \right\rfloor < \frac{qx}{p} < \left\lfloor \frac{qx}{p} + \frac{1}{2} \right\rfloor \\
&\iff \left\lfloor \frac{qx}{p} \right\rfloor + \frac{1}{2} < \frac{qx}{p} < \left\lfloor \frac{qx}{p} \right\rfloor + 1 \\
&\iff \frac{1}{2} < \frac{qx}{p} - \left\lfloor \frac{qx}{p} \right\rfloor < 1 \\
&\iff \frac{p}{2} < qx - p\left\lfloor \frac{qx}{p} \right\rfloor < p \\
&\iff \text{the least residue of } qx \bmod p \text{ is negative.}
\end{aligned}$$

By Gauss' Lemma, if s_1 is the number of x for which this occurs, then

$$\left(\frac{q}{p}\right) = (-1)^{s_1}$$

as claimed.

(iii) is similar to (ii). □

Nigel Byott
December 2002