Number Theory Notes
November 22 and 24, 2021

1 Gauss's Theorema Aureum Quadratic Reciprocity Law

This was regarded as a gem of number theory by Gauss and he gave six proofs as he considered it to be of prime importance. There have been many proofs (essentially varying only in details but not in the ideas) by many many mathematicians - one paper in the American Mathematical Monthly purports to give the "152nd proof". We will give 5 or 6 proofs before giving various applications. Using algebraic number theory, more natural proofs can be given.

First, we roughly describe what QRL is about. The question of whether a is a square mod b for coprime integers a, b reduces to that of primes. Then, for odd primes $p \neq q$, it turns out that the question of whether p is a square mod q is intimately connected to that of whether q is a square mod p. This is the reason for the name 'reciprocity'. For an odd prime p and a coprime to p, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be 1 or -1 according as to whether a is a square or not mod p. For convenience, one sometimes defines the symbol also when $p|a$ in which case it is defined to be 0.

Recall a general result proved earlier about whether a congruence of the form $x^n \equiv a \bmod m$ can be solved (where primitive roots mod m exist) is easily determined. In particular, when p is a prime, we have:
(Euler.) For $(a, p) = 1$, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$. In particular, a is a square or not mod p according as to whether $a^{(p-1)/2} \equiv 1$ or $-1 \bmod p$.

1.1 The Gauss Lemma

Let p be an odd prime and let $S = \{1, 2, \cdots, (p-1)/2\}$. Note that $S \sqcup (-S)$ is a reduced residue system mod p. Fix a coprime to p. For each $s \in S$, note that we may write $as \equiv e_s s_a \bmod p$ where $s_a \in S$ is unique and $e_s = \pm 1$.

That is, $e_s(a) = 1$ if $as \bmod p$ is in S and -1 if $as \bmod p$ is in $-S$. Then, we have:

Gauss's lemma. $\left(\frac{a}{p}\right) = \prod_{s\in S} e_s(a) = (-1)^\mu$, where

$$\mu = |\{s \in S : e_s(a) = -1\}|.$$

Proof. Note that $as \equiv e_s(a)s_a$ and the map $s \mapsto s_a$ is a bijection because $s_a = t_a$ implies $t \equiv \pm s \bmod p$, which is impossible as both s, t are $\leq (p-1)/2$. Therefore, multiplying the congruences $as \equiv e_s(a)s_a \bmod p$ over all $s \in S$, we get

$$a^{(p-1)/2} \prod_{s\in S} s \equiv \prod_{s\in S} (as) = \prod_{s\in S} (e_s s_a) \equiv (-1)^\mu \prod_{s\in S} s.$$

Cancelling off $\prod_{s\in S} s$, we obtain the lemma.

Remark. (Once we have defined the notion of the sign of a permutation, we can check that) $\left(\frac{a}{p}\right)$ is the sign of the permutation $t \mapsto at$ on $\mathbb{Z}_p^*$.

1.1.1 Quadratic residue of 2

Applying Gauss lemma to $a = 2$ and an odd prime p, we obtain $\left(\frac{2}{p}\right) = (-1)^\mu$ where

$$\mu = |\{s \leq (p-1)/2 : 2s > (p-1)/2\}|.$$

We can easily count the cardinality μ and obtain 1 if $p \equiv \pm 1 \bmod 8$ and -1 if $p \equiv \pm 3 \bmod 8$.

1.1.2 QRL - Trigonometric Proof

Quadratic Reciprocity Law. Let $p \neq q$ be odd primes. Then,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Further,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

We already proved the second assertion directly from Gauss's lemma. Now, we proceed to give a beautiful proof of the first assertion due to Eisenstein.

(Eisenstein was a student of Gauss and was rated by Gauss to be among the 3 topmost mathematicians of all time - the other two being Newton and Archimedes).

Trigonometric Proof. In the identity

$$\frac{x^{2r+1} - 1/x^{2r+1}}{x - 1/x} = (x - 1/x)^{2r} + \sum_{d=0}^{r-1} a_{d,r}(x - 1/x)^{2d}$$

proved by induction on r where $a_{i,j}$ are integers, we put $x = e^{iy}$ to obtain

$$\frac{\sin(2r+1)y}{\sin y} = (2i)^{2r} \sin^{2r} y + \sum_{d=1}^{r-1} a_{d,r}(2i)^{2d} \sin^{2d} y.$$

If $P(t) = (2i)^{2r} t^r + \sum_{d=1}^{r-1} a_{d,r}(2i)^{2d} t^d$, the above equality is

$$\frac{\sin(2r+1)y}{\sin y} = P(\sin^2 y).$$

As the LHS vanishes at $2\pi d/(2r+1)$ for $1 \leq d \leq r$, we obtain

$$P(t) = (2i)^{2r} \prod_{d=1}^{r} (t - \sin^2(2\pi d/(2r+1))).$$

Evaluating this at $t = \sin^2 y$, we obtain the trigonometric identity

$$\frac{\sin(2r+1)y}{\sin y} = (2i)^{2r} \prod_{d=1}^{r} (\sin^2 y - \sin^2(2\pi d/(2r+1))).$$

Let $p \neq q$ be odd primes; we prove QRL now.
By the notation in the Gauss lemma, $qs = e_s s_q$ for each $s \in S$.
As the sine function has period 2π, we get

$$\sin(2\pi qs/p) = e_s \sin(2\pi s_q/p).$$

Multiplying these over $s \in S$, we obtain

$$\left(\frac{q}{p}\right) = \prod_{s \in S} \frac{\sin(2\pi qs/p)}{\sin(2\pi s/p)}.$$

By the above trigonometric identity for $q = 2r + 1$, the RHS equals

$$(-4)^{(p-1)(q-1)/4} \prod_{s,t} (\sin^2(2\pi s/p) - \sin^2(2\pi t/q))$$

where s varies in $S = \{1, \cdots, (p-1)/2\}$ and t varies in $\{1, 2 \cdots, (q-1)/2\}$. So,

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{s \in S} (-4)^{(q-1)/2} \prod_{t} (\sin^2(2\pi s/p) - \sin^2(2\pi t/q)) \\ &= (-4)^{(p-1)(q-1)/4} \prod_{s,t} (\sin^2(2\pi s/p) - \sin^2(2\pi t/q)).\end{aligned}$$

Interchanging the roles of p and q, we obtain the QRL.

Later, we will prove how to explain this in a more conceptual manner.

1.2 Eisenstein's lattice point proof

Let $p \neq q$ be odd primes. Consider the line $y/x = q/p$. It has evidently no lattice points on it. We count the lattice points (x, y) with $1 \leq x \leq (p-1)/2, 1 \leq y \leq (q-1)/2$. Let M be the number of such lattice points below the line mentioned. We claim:

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

To see how, a lattice point (x, y) lies below the line if and only if $y < qx/p$. Write, for each $x \leq (p-1)/2$,

$$qx = q_x p + r_x \ (0 \leq r_x < p).$$

So, $y < qx/p$ means $y \leq q_x$. In other words,

$$M = \sum_{x=1}^{(p-1)/2} q_x = \sum_x \lfloor qx/p \rfloor.$$

Let $\alpha_1, \cdots, \alpha_\mu$ be the r_x's that are $> (p-1)/2$. Note that this $\mu = |\{s \leq (p-1)/2 : qs > (p-1)/2\}|$ is as in Gauss lemma for q (that is, $\left(\frac{q}{p}\right) = (-1)^\mu$).

We show that $M \equiv \mu \bmod 2$.

This would prove the claim.

Recall we wrote for $x \leq (p-1)/2$ that

$$qx = q_x p + r_x$$

and wrote $\alpha_1, \cdots, \alpha_\mu$ for the r_x's that are $> (p-1)/2$. Let $\beta_1, \cdots, \beta_v$ be the rest of the r_x's; hence $\mu + v = (p-1)/2$ and

$$\{p - \alpha_1, \cdots, p - \alpha_\mu, \beta_1, \cdots, \beta_v\} = \{1, 2, \cdots, (p-1)/2\}.$$

Hence, summing both sides we get

$$p\mu + \sum_j \beta_j - \sum_i \alpha_i = (p^2 - 1)/8.$$

Also, summing both sides of $qx = q_x p + r_x$, we get

$$q(p^2 - 1)/8 = p \sum_x q_x + \sum_i \alpha_i + \sum_j \beta_j = pM + \sum_i \alpha_i + \sum_j \beta_j.$$

Thus, $\frac{(q-1)(p^2-1)}{8} = p(M - \mu) + 2\sum_i \alpha_i \equiv M - \mu \bmod 2$.
This shows $M \equiv \mu \bmod 2$ as LHS is even. Hence the claim follows.

We have proved $\left(\frac{q}{p}\right) = (-1)^M$. Similarly $\left(\frac{p}{q}\right) = (-1)^N$ where N is the number of lattice points (x, y) above the line satisfying $1 \leq x \leq (p-1)/2, 1 \leq y \leq (q-1)/2$. Therefore,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N} = (-1)^{(p-1)(q-1)/4}$$

since $M + N = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$.