CHAPTER II

Class Field Theory

2.1. Introduction.

2.2. l-adic Fourier series.

2.3. Gauss, Ramanujan and Kloosterman sums. [HW79]

A function g(n) is *multiplicative* when the g.c.d. of n and n′ is 1 implies

$$g(nn') = g(n)g(n'). \tag{1}$$

We will write e[t] for $e^{2\pi it}$. Then

$$e[m/n] = e[m'/n]$$

if and only if $m = m' \pmod n$.

Gauss's sum is defined as

$$S(m, n) = \sum_{k=0}^{n-1} e^{2\pi i k^2 m/n} = \sum_{k=0}^{n-1} e\left[\frac{k^2 m}{n}\right], \tag{2}$$

and because for any u

$$e\left[\frac{(k+un)^2 m}{n}\right] = e\left[\frac{k^2 m}{n}\right],$$

we obtain whenever $k = k' \pmod n$

$$e\left[\frac{k^2 m}{n}\right] = e\left[\frac{k'^2 m}{n}\right],$$

so that we are able to put

$$S(m, n) = \sum_{k(n)} e\left[\frac{k^2 m}{n}\right],$$

where by k(n) we mean that k runs through all residues (mod n). If the meaning is clear we will usually shorten k(n) in this sum to k.

Lemma 2.3.1. *If the g.c.d. of* n *and* n′ *is* 1, *and* a *runs through all residues* (mod n), *whereas* a′ *runs through all residues* (mod n′), *then* a′n + an′ *runs through all residues* (mod nn′).

Proof. The number of (a′n + an′) is nn′, and if

$$a_1'n + a_1n' = a_2'n + a_2n'$$

this implies

$$a_1n' = a_2n' \pmod n,$$

giving

$$a_1 = a_2 \pmod n.$$

Likewise

$$a'_1 = a'_2 \pmod{n'},$$

so that all these nn′ numbers differ (mod nn′). □

Corollary 2.3.2. *If the g.c.d. of* n *and* n′ *is* 1, *then* a *runs through all residues coprime to* n *and* a′ *runs through all residues coprime to* n′ *if and only if* a′n + an′ *runs through all residues coprime to* nn′.

Proof. (a′n + an′) is coprime to nn′ and therefore to n and n′ separately, so an′ is coprime to n and a′n coprime to n′, so a is coprime to n and a′ is coprime to n′, and conversely. □

Theorem 2.3.3. *If the g.c.d. of* n *and* n′ *is* 1, *then*

$S(m, nn') = S(mn', n)S(mn, n')$.

Proof. Let k, k′ run through all the residues for (mod n) and (mod n′) respectively, so by the previous lemma

$K = kn' + k'n$

runs through all residues (mod nn′). Further,

$mK^2 = m(kn' + k'n)^2 = mk^2n'^2 + mk'^2n \pmod{nn'}$,

so that

$$S(mn', n)S(mn, n') = \sum_k e\left[\frac{k^2mn'}{n}\right]\sum_{k'} e\left[\frac{k'^2mn}{n'}\right]$$
$$= \sum_{k,k'} e\left[\frac{k^2mn'}{n} + \frac{k'^2mn}{n'}\right] = \sum_{k,k'} e\left[\frac{m(k^2n'^2 + k'^2n^2)}{nn'}\right]$$
$$= \sum_K e\left[\frac{mK^2}{nn'}\right] = S(m, nn'). \square$$

Ramanujan's sum is

$$c_q(m) = \sum_{k^*(q)} e\left[\frac{km}{q}\right], \tag{3}$$

where k*(q) indicates that k runs through residues coprime to q. On occasion we will replace k*(q) by k.

Using the primitive complex qth root of unity $\omega_q = e^{2\pi iq}$, so that $\omega_q{}^q = 1$, we can rewrite Ramanujan's sum as

$c_q(m) = \sum_k \omega^m$.

Theorem 2.3.4. *If the g.c.d. of* q *and* q′ *is* 1, *then*

$c_{qq'}(m) = c_q(m)c_{q'}(m)$.

Proof. By corollary 1.4.2

$$c_q(m)c_{q'}(m) = \sum_{k,k'} e\left[m\left(\frac{k}{q} + \frac{k'}{q'}\right)\right] = \sum_{kk'} e\left[\frac{m(kq'+k'q)}{qq'}\right] = c_{qq'}(m). \square$$

Lemma 2.3.5. *If the g.c.d. of* k *and* n *is* 1, *the congruence*

$ky = ky' \pmod n$

holds if and only if

$y = y' \pmod n$.

Note that we cannot infer in general that $ky = ky' \pmod n$ implies $y = y' \pmod n$, since

$2 \times 3 = 2 \times 6 \pmod 6$,

but

$3 \neq 6 \pmod 6$.

Proof. $k(y - y') = 0 \pmod n$. Since $k \neq 0 \pmod n$, $y - y' \neq 0 \pmod n$ is a contradiction. $\square$

Corollary 2.3.6. *If* y, y′, ... are all incongruent residues (mod n) and the g.c.d. of k and n is 1, then ky, ky′, ... are also all incongruent residues.

Proof. By induction on lemma 1.4.5. $\square$

Lemma 2.3.7. *If the g.c.d. of* k *and* n *is* 1, *the congruence*

$ky = c \pmod n$

has exactly 1 *solution.*

Proof. This is a corollary of 1.4.6, since if there were more solutions than one, for two distinct values of y there would be a congruence relation. But there is at least one solution, since there exists a c with ky = c, and the ky are a complete set of incongruent residues. □

Kloosterman's sum is

$$S(u, v, n) = \sum_j e\left[\frac{uj+vk}{n}\right], \tag{4}$$

in which j runs through all residues coprime to n, and we define k by

$$jk = 1 \pmod{n}. \tag{5}$$

Lemma 17.2.7 shows equation (5) can be satisfied.

Theorem 2.3.8. *If the g.c.d. of* n *and* n′ *is* 1, *then*

$$S(u, V, n) = S(u, v, n)S(u, v', n'),$$

where

$$V = vn'^2 + v'n^2.$$

Proof. On putting

$$jk = 1 \pmod{n},\ j'k' = 1 \pmod{n'},$$

we obtain

$$\begin{aligned} S(u, v, n)S(u, v', n') &= \sum_{j,j'} e\left[\frac{uj+vk}{n} + \frac{uj'+v'k'}{n'}\right] \\ &= \sum_{j,j'} e\left[u\left(\frac{jn'+j'n}{nn'}\right) + \frac{vkn'+v'k'n}{nn'}\right] \\ &= \sum_{j,j'} e\left[\frac{uJ+K}{nn'}\right], \end{aligned} \tag{6}$$

in which

$$J = jn' + j'n,\ K = vkn' + v'k'n.$$

We wish to show that

$$K = VJ' \pmod{nn'}, \tag{7}$$

where J′ satisfies

$$JJ' = 1 \pmod{nn'},$$

so that equation (6) becomes

$$S(u, v, n)S(u, v', n') = \sum_J e\left[\frac{uJ+K}{nn'}\right] = S(u, V, nn').$$

But

$$(j'n + jn')J' = JJ' = 1 \pmod{nn'},$$

giving

$$jn'J' = 1 \pmod{n},\ n'J' = jkn'J' = k \pmod{n},$$

and therefore

$$n'^2J' = n'k \pmod{nn'}.$$

Correspondingly

$$n^2J' = nk \pmod{nn'},$$

so that we find

$$VJ' = (vn'^2 + v'n^2)J' = vn'k + v'nk = K \pmod{nn'}$$

and this is just equation (7), which we wished to prove. □

2.3. The Rogers-Ramanujan identities.

We can exhibit any square m^2 as

$$m^2 = 1 + 3 + 5 + \ldots + (2m - 1).$$

If we now take a partition of $n - m^2$ into m parts at most, with the parts in descending order, we obtain a partition of n into parts without repetitions or sequences, or parts whose minimal difference is 2.

On the other hand, the right hand side enumerates partitions into numbers of the form 5m + 1 and 5m + 4. Hence we obtain the purely combinatorial theorem

Theorem 2.4.1. *The number of partitions of* n *with minimal difference* 2 *is equal to the number of partitions into parts of the form* 5m + 1 *and* 5m + 4.

From this we will be able to prove

Theorem 2.4.2.

$$1 + \frac{x}{1-x} + \frac{x^4}{(1-x)(1-x^2)} + \frac{x^9}{(1-x)(1-x^2)(1-x^3)} + \cdots = \frac{1}{(1-x)(1-x^6)\cdots(1-x^4)(1-x^9)},$$

which can be expressed as

$$1 + \sum_1^\infty \frac{x^{m^2}}{(1-x)(1-x^2)\cdots(1-x^m)} = \prod_0^\infty \frac{1}{(1-x^{5m+1})\cdots(1-x^{5m+4})}.$$

There is a similar theorem to 2.3.1.

Theorem 2.4.3. *The number of partitions of* n *into parts not less than* 2, *and with minimal difference* 2 *is equal to the number of partitions into parts of the form* 5m + 2 *and* 5m + 3.

We can prove this equivalence in the same way, starting from the identity

$$m(m + 1) = 2 + 4 + 6 \ldots + 2m.$$

This leads to the analogue of theorem 2.3.2.

Theorem 2.4.4.

$$1 + \frac{x^2}{1-x} + \frac{x^4}{(1-x)(1-x^2)} + \frac{x^{12}}{(1-x)(1-x^2)(1-x^3)} + \cdots = \frac{1}{(1-x^2)(1-x^7)\cdots(1-x^3)(1-x^8)},$$

which can be put in the form

$$1 + \sum_1^\infty \frac{x^{m(m+1)}}{(1-x)(1-x^2)\cdots(1-x^m)} = \prod_0^\infty \frac{1}{(1-x^{5m+2})\cdots(1-x^{5m+3})}.$$

The interest of the formulas arises from the unexpected part played by the number 5.

It is natural to ask if there is any proof by elementary methods, and an elaborate proof was found this way by Schur. The theorems were first discovered independently by Rogers and Ramanujan, and we will provide here the proof by Rogers.

2.5. Theta functions.