CHAPTER VIII

Modular Forms

8.1. Introduction.

Fred Diamond and Jerry Shurman's deep, accessible and extremely well-researched book *A first course in modular forms* is strongly recommended for further insight into this chapter.

The modularity theorem has been used to prove Fermat's last theorem, that for integers x, y and z, and prime p

$$x^p + y^p = z^p \qquad (1)$$

implies that xyz = 0. This took () years to solve.

The modularity theorem relates three subjects that we have touched on, Galois representation theory, the theory of lattices, and elliptic curves.

The modularity theorem connects with lattice theory, which we have seen in chapter V has a rich structure, but what is needed in lattice theory for the modularity theorem is rather basic. In fact, normally we will be dealing with lattices in two dimensions.

8.2. Galois representation theory.

In chapter VI we mentioned that Galois representation theory is equivalent to the binomial theorem, so that in the case where x, y and z are integers this is the binomial theorem in integers, and both Galois representation theory and the binomial theorem are correct. But as we mentioned there, Galois solvability theory is not the same theory as Galois representation theory, it is an incorrect model for the solution of polynomial equations, and we will not be dealing with Galois solvability theory again here.

There is also a reformulation of the binomial theorem for finite, or congruence, arithmetic dealing with Fermat's little theorem, which for transformations is known as the Frobenius automorphism, and the extension of the little theorem to Euler's totient theorem, which we met in chapter I. We repeat a proof of Fermat's little theorem again here.

Theorem 8.2.1. Fermat's little theorem states for prime p, verifiable directly for p = 2

$$x^p – x = bp. \qquad (1)$$

for some unique b dependent on x.

Proof. We prove this by induction. For x = 0

$$0^p – 0 = 0p.$$

Assume (1) holds. Then for $x \to x + 1$, by the binomial theorem and the primality of p, so p does not divide any denominator

$$(x + 1)^p – (x + 1) = x^p – x + px^{p-1} + [p(p – 1)/2]x^{p-2} + ... + 1^p – 1 = bp + cp$$

for some unique c. ☐

8.3. Quadratic, cubic and biquadratic reciprocity.

We will use Fermat's little theorem to prove for odd primes the celebrated theorem of quadratic reciprocity, and extend it to odd composite numbers. We prove the corresponding results for cubic and biquadratic reciprocity.

In order to appeal to the widest possible audience the Legendre and Jacobi symbols do not appear, and to begin with use of the mod notation has been suppressed.

Theorem 8.3.1. The law of quadratic reciprocity states there exists a unique n and m such that

$$(q^{(p-1)/2} - np)(p^{(q-1)/2} - mq) = (-1)^{(p-1)/2\ (q-1)/2}. \quad (1)$$

This can be rephrased using the Euclidean algorithm, that for any given y and for any $r > 0$ there exist unique natural numbers n and a with $a < r$ such that $y = a + nr$. On putting $r = p$ and $y = q^{(p-1)/2}$, this implies n is unique in (1) if $(q^{(p-1)/2} - np) < p$.

We will deal with squares up to equation (5), minus signs up to equation (6) and then powers up to equation (9) to establish this quadratic reciprocity theorem.

Proof. Fermat's little theorem may be rewritten from 8.2.(1) as

$$x(x^{p-1} - 1) = x[(x^2)^{(p-1)/2} - 1]$$
$$= x(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) = bp, \quad (2)$$

so that if x is not zero or another multiple of p, for some unique r, s and t, squares in x are of the form

$$x^{(p-1)/2} = 1 + rp \text{ if and only if } (x^2)^{(p-1)/2} = 1 + sp, \quad (3)$$

otherwise non-squares are of the form

$$x^{(p-1)/2} = -1 + tp. \ \square \quad (4)$$

On substituting $(q - p)$ for x, which cannot be zero or another multiple of p, we obtain from equations (3) and (4)

$$(q - p)^{(p-1)/2} = \pm 1 + up, \quad (5)$$

for some unique u. Less multiples of p, the $q^{(p-1)/2}$ term in the binomial expansion of (5) is ± 1.

Note that:

if $(p - 1)/2$ is even, then $x^{(p-1)/2} = (-x)^{(p-1)/2}$,

but if $(p - 1)/2$ is odd, then $x^{(p-1)/2} = -(-x)^{(p-1)/2}$. (6)

Under the transformation of $(q - p)$ to its negative, $(p - q)$, when $(p - 1)/2$ is odd, on using equation (6) the sign ± 1 in (5) becomes reversed, but when $(p - 1)/2$ is even, the sign remains the same. □

Using the binomial theorem, by taking the $(q - 1)/2^{th}$ power at the right hand side of (5), for both $(p - 1)/2$ and $(q - 1)/2$ odd

$$[(q - p)^{(p-1)/2}]^{(q-1)/2} = (\pm 1 + up)^{(q-1)/2} = \pm 1 + vp, \quad (7)$$

for some unique v, where the ± is carried through unchanged in all expressions. Then by the remark after (5), for some unique w this is

$$q^{(p-1)/2} - wp,$$

but for $(q - 1)/2$ even, the analogue of (7) is

$$(\pm 1 + up)^{(q-1)/2} = +1 + vp. \ \square$$

Now $[(-1)^{(p-1)/2}]^{(q-1)/2}$ is -1 if and only if $(p - 1)/2$ and $(q - 1)/2$ are both odd.

Using equation (7) and the remark after (6), with both $(p - 1)/2$ and $(q - 1)/2$ odd there exists an $n = w + v$, and a similarly derived m for which

$$[(q - p)^{(p-1)/2}]^{(q-1)/2}[(p - q)^{(q-1)/2}]^{(p-1)/2} = (q^{(p-1)/2} - np)(p^{(q-1)/2} - mq)$$
$$= -1(\pm 1)^2$$

$$= (-1)^{(p-1)/2\,(q-1)/2},$$

and this version of (1) also holds when (p – 1)/2 or (q – 1)/2 are even. We prove this next.

We will write x = a + np by x ≡ a (mod p), and call a the *residue* (mod p). This notation will be used in conjunction with the Euclidean algorithm.

If x ≡ x′ (mod p) we say x and x′ are *congruent* (mod p), otherwise *incongruent* (mod p). A result we shall use is: if a general polynomial f(x) in x satisfies f(x) = x′, then the congruence

$$f(x) \equiv x' \pmod p$$

also holds.

If (p – 1)/2 is even and (q – 1)/2 is odd – the quadratic reciprocity theorem is symmetrical with respect to p and q, so this also holds when (p – 1)/2 is odd and (q – 1)/2 is even, then

$$[(q - p)^{(p-1)/2}]^{(q-1)/2} \equiv 1 \pmod p,$$

which equates to

$$(q^{(p-1)/2})^{(q-1)/2} \equiv 1 \pmod p$$

$$\equiv q^{(p-1)/2} \pmod p, \qquad (8)$$

so by the Euclidean algorithm there exists an n with

$$q^{(p-1)/2} - np = 1,$$

whereas

$$[-(q - p)^{(q-1)/2}]^{(p-1)/2} \equiv 1 \pmod q,$$

$$\equiv p^{(q-1)/2} \pmod q, \qquad (9)$$

and the product of (8) and (9) is in this particular circumstance [1 (mod p)][1 (mod q)] = 1.

If both (p – 1)/2 and (q – 1)/2 are even, clearly the product of (8) and (9) again has leading terms 1. ☐

8.4. Hyperintricate and hyperpolyticate numbers.

8.5. Eigenvalues and hyperactual numbers are J-abelian.

8.6. Two dimensional lattices and abelian groups.

Two dimensional lattices seem a simple idea, for example given in the diagram

8.7. Two dimensional lattices and Heegner numbers.

8.8. Two dimensional lattices, topology and divisors.

There is a relation of two dimensional lattices with the topology of two dimensional surfaces, in which the topology of diagram 8.6.(1) is the same as the rectangular strip below.

For the opposite edges of the strip, we can either glue the strip with arrows at the end so that the arrows fit together in opposite directions, for example as a Möbius strip, which is an antioriented manifold and we have dealt with in rich generality in chapter VII, or we can fit the arrows together in the same direction, which is an oriented manifold like a cylinder, although we can also do a rotation of π(2n + 1) radians to fit these arrows together in the same orientation, as shown in the diagram.

For this cylinder we have the option of either gluing the remaining sides of the rectangle together to form a torus, or otherwise if we wish to introduce a nondifferentiable structure, and differentiation does not concern us for finite lattices, then we can glue each side of the cylinder to itself, which topologically is a sphere with corners.

For the interior of a strip like (3), we can cut out a finite number of holes. We dealt with the situation for gluing holes to Möbius strips in chapter VII. In the oriented case, if the strip contains an even number of holes, then we can glue the ends of a cylinder to each pair of holes. This creates a handle on the strip. The strip can then be attached together to form a sphere with corners, as before, and the result for two holes with an attached cylinder in this case is in shape a torus, or if we glue the strip to form a torus, the result for two holes with an attached cylinder is topologically a sphere with two handles. In general, for holes in pairs, any number of handles may be attached.

We notice that a real lattice, being a finite object in congruence arithmetic, or even in the case when its nodes are spaced by integer complex numbers called Gaussian integers, in which case it has four dimensions, possesses the feature of having as well as addition, subtraction and multiplication, a division operation available to it. This is because we are dealing here with a two dimensional vector space, say of vectors with integer coefficients, where each individual vector has an algebra which is a ring, and the vectors in two dimensions form a ring too. The fact that division (of course, not for zero) is available is that in finite arithmetic the set of elements obtained under division (mod p), where p is prime, is the same set of elements obtained under multiplication. This discussion is normally not expressed in these terms, but in terms of the generalisation of vector spaces to modules.

When we have a topological structure on the lattice, so it has handles, is there a division operation there too? Well, we might expect the normal case to hold, with exceptions because of the holes. But if we have a regularly curved cylinder for the handle, if a node was inside the hole somewhere and projected upwards, then it would project upwards so one node in the hole would hit the associated handle in only one place. We would expect, topologically, that the division operation would be maintained. So with a sphere with 2n handles considered as a lattice, we expect to find on it the addition, subtraction, multiplication and division operations (mod p), suitably defined, that we found in the previous case.

When we are dealing not (mod p), but with a composite number (mod s), the appropriate description is not taken from Fermat’s little theorem, but from Euler’s totient theorem. In this case, two numbers (mod s) that are not zero can multiply to form a number which is zero, so that division is not defined for these combinations.

8.9. Two dimensional lattices and elliptic curves.

There are interesting things to say about the connection of the theory of two dimensional lattices with elliptic curves, which we introduced in chapter VII

$$w^2 = v^3 + av^2 + bv + c. \qquad (5)$$

Must these curves, which may self-intersect, always be oriented manifolds, or can they be twisted?

8.10. Two dimensional lattices and theta functions.

Theta function[edit]

One can associate to any (positive-definite) lattice Λ a theta function given by

The theta function of a lattice is then a holomorphic function on the upper half-plane. Furthermore, the theta function of an even unimodular lattice of rank n is actually a modular form of weight $n/2$. The theta function of an integral lattice is often written as a power series

in so that the coefficient of q^n gives the number of lattice vectors of norm n.

Up to normalization, there is a unique modular form of weight 4: the Eisenstein series $G_4(\tau)$. The theta function for the E_8 lattice must then be proportional to $G_4(\tau)$. The normalization can be fixed by noting that there is a unique vector of norm 0. This gives

where $\sigma_3(n)$ is the divisor function. It follows that the number of E_8 lattice vectors of norm $2n$ is 240 times the sum of the cubes of the divisors of n. The first few terms of this series are given by (sequence A004009 in the OEIS):

The E_8 theta function may be written in terms of the Jacobi theta functions as follows:

where

Theta series[edit]

One can associate to any (positive-definite) lattice Λ a theta function given by

The theta function of a lattice is then a holomorphic function on the upper half-plane. Furthermore, the theta function of an even unimodular lattice of rank n is actually a modular form of weight $n/2$ for the full modular group $PSL(2,\mathbf{Z})$. The theta function of an integral lattice is often written as a power series in so that the coefficient of q^n gives the number of lattice vectors of squared norm 2*n*. In the Leech lattice, there are 196560 vectors of squared norm 4, 16773120 vectors of squared norm 6, 398034000 vectors of squared norm 8 and so on. The theta series of the Leech lattice is

where is the normalized Eisenstein series of weight 12, is the modular discriminant, is the divisor function for exponent 11, and is the Ramanujan tau function. It follows that for $m \geq 1$ the number of vectors of squared norm 2*m* is