ALGEBRAIC NUMBER THEORY

LECTURE 12 NOTES

1. Section 5.5

Note that $\tau(1)^2 = (\frac{-1}{p})$ holds in characteristic 0 as well as characteristic q (set $w = e^{2\pi i/p}$), since it doesn't use any property of finite fields. It allows us to see what the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is: start with a generator $\zeta_p = w$ of $\mathbb{Q}(\zeta_p)$ and symmetrize with respect to the unique subgroup of index 2 of the Galois group (which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$ under $a \in (\mathbb{Z}/p\mathbb{Z})^* \mapsto (\zeta_p \mapsto \zeta_p^a)$). The subgroup consists of the squares in $(\mathbb{Z}/p\mathbb{Z})^*$, so the quadratic extension is generated by $\sum_{a\in(\mathbb{F}_p^*)^2} \zeta_p^{a^2}$ if the sum is nonzero. This sum equals

$$\sum_{a\in\mathbb{F}_p^*} \frac{1}{2}\left(1 + \left(\frac{a}{p}\right)\right)\zeta_p^a = -\frac{1}{2} + \frac{1}{2}\sum_{a\in\mathbb{F}_p^*}\left(\frac{a}{p}\right)\zeta_p^a = \frac{\tau(1)-1}{2}.$$

This sum is nonzero since $|\tau(1)| = \sqrt{p}$. So the quadratic subfield in question is indeed $\mathbb{Q}(\sqrt{(\frac{-1}{p})p})$ which is $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \bmod 4$ and $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \bmod 4$.

We know the Gauss sum up to sign since we know its square. For the computation of the sign see for example Flath's book on number theory, which has a nice proof using the finite Fourier transform. For a good introduction to Gauss and Jacobi sums see Ireland and Rosen's book.

2. Section 5.6

To see that if n is a sum of two squares then every prime which is 3 mod 4 divides n to an even power we argue by contradiction. Let n be a smallest counterexample and let $p \equiv 3 \bmod 4$ divide n to an odd power. Write $n = a^2 + b^2$ and notice that p cannot divide a or b since then it would have to divide both (sum of their squares is divisible by p), and then $n/p^2 = (a/p)^2 + (b/p)^2$ would furnish a smaller counterexample. So $p \nmid b$ in particular, and so $(ab^{-1})^2 \equiv -1 \bmod p$, which contradicts $p \equiv 3 \bmod 4$.

3. Section 5.7

Proof of four squares theorem. By multiplicativity of quaternion norms, it's enough to see that every prime is a sum of four squares. Since this is trivial for 2, assume

p is an odd prime. Now, the Chevalley-Warning theorem shows that for every p, there are integers a, b such that $a^2 + b^2 + 1 \equiv 0 \bmod p$. So let's assume we have

$$x^2 + y^2 + z^2 + w^2 = mp$$

for some positive integer m. We can reduce x, y, z, w mod p to assume their absolute values are less than $p/2$ (since p is odd). Then the LHS is less than $4(p/2)^2 = p^2$, so $m < p$. If $m = 1$ we are done. So assume $m > 1$. We will then produce another solution with smaller m. Since there are only finitely many positive integers less than m, eventually we will reach $m = 1$. Now if x, y, z, w are all divisible by m then we get after dividing my m^2 that $p/m = (x/m)^2 + (y/m)^2 + (z/m)^2 + (w/m)^2$. But the RHS is an integer and the LHS is not, since $1 < m < p$, so that's impossible.

So reduce x, y, z, w mod m to get x', y', z', w' with absolute values less than or equal to $m/2$. We then have $x'^2 + y'^2 + z'^2 + w'^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0$ mod m. Also $x'^2 + y'^2 + z'^2 + w'^2 \leq 4(m/2)^2 = m^2$. In fact we can assume that strict inequality holds, since if m is even and x', y', z', w' all have absolute value $m/2$, then they are all $\pm m/2$ and so are congruent mod m to $m/2$. Hence so are x, y, z, w, so in particular x, y, z, w are all even or all odd. Then we can replace x, y, z, w by $(x+y)/2, (x-y)/2, (z+w)/2, (z-w)/2$ and whose sum of squares is just $(x^2 + y^2 + z^2 + w^2)/2 = (m/2)p$ to reduce m. So now we can assume that $x'^2 + y'^2 + z'^2 + w'^2 = km$ with $0 < k < m$ and with $x \equiv x'$ mod m etc.

Then letting $u = x + yi + zj + wk$ and $v = x' + y'i + z'j + w'k$ we have $N(u) = pm, N(v) = N(\overline{v}) = km$, so $N(u\overline{v}) = pkm^2$. But also $u\overline{v} \equiv v\overline{v}$ mod $m \equiv km \equiv 0$. Hence the components of $u\overline{v}$ are all divisible by m. So we can divide out the representation as a sum of four squares $pkm^2 = N(u\overline{v})$ by m^2 to get $pk =$ sum of four squares. This completes the descent step and shows we can achieve $m = 1$ ultimately, which implies p is a sum of four squares. □

Problem. What's the fastest algorithm you can think of for expressing a given integer as a sum of four squares?

Remark. If we start counting the number of representations of n as a sum of four squares, this leads us naturally to modular forms.

For example, define $r_4(n)$ by

$$(1 + 2q + 2q^4 + 2q^9 + \dots)^4 = \sum r_4(n)q^n.$$

Then it's easy to see that $r_4(n)$ is the number of representations of n as a sum of four integer squares (positive or negative).

Now $\theta = (1 + 2q + 2q^4 + 2q^9 + \dots)$ is the theta function of the integer lattice $\mathbb{Z}$. If we plug in $q = e^{2\pi iz}$ it becomes a function of a complex variable z. Usually we let $z \in \mathcal{H}$, the upper half complex plane $\{x + iy \,|\, y > 0\}$.

So let $\vartheta_4(z) = \sum r_4(n)e^{2\pi i n z}$. Then ϑ_4 is clearly unchanged under $z \mapsto z+1$. But ϑ_4 satisfies another transformation property:

$$\vartheta_4\left(-\frac{1}{z}\right) = -z^2\vartheta_4(z).$$

We won't prove it here, but it follows by using the Poisson summation formula:

$$\sum_{x\in\Lambda} f(x) = \frac{1}{\mathrm{vol}(\Lambda)}\sum_{y\in\Lambda^*}\widehat{f}(y)$$

for any Schwarz function f on $\mathbb{R}^n$ where $\widehat{f}$ is the Fourier transform, defined by $\widehat{f}(t) = \int_{\mathbb{R}^n} f(x)e^{2\pi i t x}dx$.

These two transformation properties are enough to make ϑ_4 into a modular form for the group $SL_2(\mathbb{Z})$ of weight 2. It lies in the finite dimensional space of modular forms of weight 2 for $SL_2(\mathbb{Z})$. We can arguments from the theory of modular forms to show, for instance, that

$$r_4(n) = 8\sum_{d|n, 4\nmid d} d$$

For an introduction to modular forms, see Serre's "A course in arithmetic".

Remark. A famous theorem of Hurwitz states that the only normed algebras over $\mathbb{R}$ are $\mathbb{R}$, the complex numbers $\mathbb{C}$, the Hamiltonian quaternions $\mathbb{H}$, and the octonions or Cayley numbers $\mathbb{O}$. For the proof see Conway and Smith's book "On quaternions and octonions" or the book "Numbers" by Eddbinghaus. Hurwitz also showed that if K is a field of characteristic not equal to 2, then the only values of n for which there is an identity of the type

$$(x_1^2+\cdots+x_n^2)(y_1^2+\cdots+y_n^2) = z_1^2+\cdots+z_n^2$$

where the z_k are bilinear functions of the x_i and the y_j with coefficients in K are $n = 1, 2, 4, 8$.

But surprisingly, in 1967, Pfister showed that there is such an expression if n is any power of 2 and we allow Z_k to be linear functions of the Y_j with coefficients in the rational function field $K(X_1, \ldots, X_n)$. In particular, the product of a sume of n squares turns out to be a sum of n squares. Conversely, if n is not a power of 2, then there can be no such general identity with $Z_k \in K(X_1, \ldots, X_n, Y_1, \ldots, Y_n)$. This is a consequence of Pfister's beautiful theory of multiplicative forms.

18.786 Topics in Algebraic Number Theory
Spring 2010