Mathematics W4043 Algebraic Number Theory
Assignment # 5

Benjamin Church

Worked With Matthew Lerner-Brecher

October 18, 2017

1. We first define two quantities,

$$r_k(m) = \left|\{(x_1, \ldots, x_n) \in \mathbb{Z}^k \mid x_1^2 + \cdots + x_n^2 = m\}\right|$$

and

$$N_k(m) = \left|\{(x_1, \ldots, x_n) \in \mathbb{N}^k \mid x_1^2 + \cdots + x_n^2 = m \text{ and } x_i \text{ is odd}\}\right|$$

(a) I can't figure this out. Please have mercy upon my soul.

(b) Any solution to $x_1^2 + x_2^2 + x_3^2 + x_4^2 = m$ in $N_4(m)$ i.e. every x_i is odd and nonnegative. Thus, $x_i \equiv 1 \bmod 4$ so there is a bijection between the solutions in $N_4(m)$ and the pairs of solutions (x_1, x_2) and $(x_3, x_)$ to $x_1^2 + x_2^2 = m_1$ and $x_3^2 + x_4^2 = m_2$ with $m_1 \equiv m_2 \equiv 2 \bmod 4$ and $m_1 + m_2 = m$. Thus, each solution in $N_4(m)$ corresponds to a unique pair of solutions in $N_2(m_1)$ and $N_2(m_2)$ with $(m_1, m_2) \in R$. Therefore,

$$N_4(m) = \sum_R N_2(m_1) N_2(m_2)$$

Using the result of (a),

$$N_4(m) = \sum_R \sum_{a \mid m_1} \chi(a) \sum_{c \mid m_2} \chi(c)$$

Whenever a is even, the character $\chi(a) = 0$ so we can ignore all even divisors. The same holds for c. Since m_1 and m_2 are even we can write them as $2ab = m_1$ and $2dc = m_2$ which is possible because the divisors a and c are not even. Also, $m_1 \equiv m_2 \equiv 2 \bmod 4$ so they are not divisible by 4 and thus a, b, c, d are all odd. The set of odd divisors of m_1 and m_2 for all m_1 and m_2 satisfying the required properties is therefore in bijection with the set of odd positive integers (a, b, c, d) with $2ab + 2cd = m$. We call this set S. Thus,

$$N_4(m) = \sum_S \chi(a)\chi(c)$$

For odd x, the character is $\chi(x) = (-1)^{\frac{x-1}{2}}$ so

$$N_4(m) = \sum_S (-1)^{\frac{a-1}{2}} (-1)^{\frac{c-1}{2}}$$

but $(-1)^x = (-1)^{-x}$ so

$$N_4(m) = \sum_S (-1)^{\frac{a-1}{2}} (-1)^{\frac{1-c}{2}} = \sum_S (-1)^{\frac{a-c}{2}}$$

(c) Let $a = x + y$, $b = z - t$, $c = x - y$, and $d = z + t$. We solve to get $x = \frac{1}{2}(a + c)$, $y = \frac{1}{2}(a - c)$, $z = \frac{1}{2}(b + d)$, $t = \frac{1}{2}(d - b)$. We need to show that this mapping is a bijection between S and S'. Since we can easily invert the mapping, it must be a bijection if both directions are well defined. Take $a, b, c, d > 0$ then $|y| < x$ and $|t| < z$. We also know that a, b, c, d are odd and that $2ab + 2cd = m$. Therefore,

$$\begin{aligned}(xz - yt) &= 4\frac{1}{4}\left((a + c) \cdot (b + d) - (a - c) \cdot (d - b)\right) \\ &= (ab + cb + ad + cd - ad - cb + cd + ab \\ &= 2ab + 2cd = m\end{aligned}$$

But, $|y| < x$ because $a, c > 0$ and $|t| < z$ because $b, d > 0$. Also, a, b, c, d are odd so $x = y + c$ implies that x and y have different parity and, similarly, $z = t + b$ so z and t have different parity. Thus, $StoS'$ is well defined. Each of these demonstrations can be applied in the opposite direction to show that $S' \to S$ is a bijection. From above, $(xz - yt) = 2ab + 2cd$ so $(xy - yt) = m \iff 2ab + 2cd = m$. Also if $|y| < x$ then $-a - c < a - c < a + c$ so $a > 0$ and $c > 0$ similarly, $|t| < z \implies b, d > 0$. Finally, if x and y have different parity then $a = x + y$ and $c = x - y$ are odd. Likewise for b and d. Thus these sets are in bijection so using part (b),

$$N_4(m) = \sum_{S'} (-1)^y$$

(d) Restricting the sum to only elements of S in which $y = 0$, we have

$$\mathcal{N}_0 = \sum_{S', y=0} (-1)^y = \sum_{S', y=0} 1 = \left|\{(x, y, z, t) \in S \mid y = 0\}\right|$$

we know that $|t| < z$ and $m = 4xz$ with x odd and t and z having different parity. There are z possible values for t so

$$\sum_{S', y=0} 1 = \sum_{m=4xz} z = \sum_{z|m/4} z$$

We can restrict z to odd divisors because $m \equiv 4 \bmod 8$. And therefore,

$$\mathcal{N}_0 = \sum_{d|m} d$$

Next, $\mathcal{N}_1 = \mathcal{N}_2$ because there is a bijective correspondence between positive solutions and negative solutions given by negating every comonent. Also, $(-1)^y = (-1)^- y$ so the sums that define $\mathcal{N}_1$ and $\mathcal{N}_2$ are equal. Next, we must check that the map from S' to itself is a bijection. In fact, it is its own inverse. Apply the transformation twice, $z'' = y' = z$ and $y'' = z' = y$ we must also check the x and t variables. For this, we need to know that the integers $u' = u$. This is true because

$$2u' - 1 < \frac{x'}{y'} < 2u' + 1$$

but

$$\frac{x'}{y'} = \frac{2uz - t}{z} = 2u - \frac{t}{z}$$

and we know that $|t| < z$ so $|\frac{t}{z}| < 1$. Therefore,

$$2u - 1 < \frac{x'}{y'} < 2u + 1$$

so $u' = u$ thus $x'' = 2uz' - t' = 2uy - (2uy - x) = x$ and $t'' = 2uy' - x' = 2uz - (2uz - t) = t$. Therefore the map is a bijection because it is invertable. Because x and y have opposite parity and z and t have opposite parity we must have $4(xy - yt) = m \equiv 4 \bmod 8$ so $xy - yt$ is odd then y and z have opposite parity. Then, we can reparametrize the sum because the map is a bijection,

$$\mathcal{N}_1 = \sum_{S', y > 0} (-1)^y = \sum_{S', y' > 0} (-1)^{y'} = \sum_{S', z > 0} (-1)^z = -\mathcal{N}_0$$

because y and z have opposite parity. Therefore, $\mathcal{N}_0 = 0$. However, it is clear from the definitions of $\mathcal{N}_0, \mathcal{N}_1, \mathcal{N}_2$ that the three possibilities $(y = 0, y > 0, y < 0)$ cover all possible cases. Thus,

$$N_4(m) = \mathcal{N}_0 + \mathcal{N}_1 + \mathcal{N}_2 = \mathcal{N}_0 = \sum_{d|m} d$$

(e) First, if we have a solution to $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2m$ then, using the given identity,

$$(x_1 + x_2)^2 + (x_1 - x_2)^2 + (x_3 + x_4)^2 + (x_3 - x_4)^2 = 4m$$

therefore, there is a bijective correspondence between solutions for $2m$ and for $4m$ since this mapping can be inverted. The reverse direction takes a solution for $4m$, say,

$${x'_1}^2 + {x'_2}^2 + {x'_3}^2 + {x'_4}^2 = 4m$$

then we can take

$$(x'_1 + x'_2)^2 + (x'_1 - x'_2)^2 + (x'_3 + x'_4)^2 + (x_3 - x_4)^2 = 8m$$

and thus,

$$\left(\frac{x'_1 + x'_2}{2}\right)^2 + \left(\frac{x'_1 - x'_2}{2}\right)^2 + \left(\frac{x'_3 + x'_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = 2m$$

which are integer solutions because the terms have the same parity. Thus the map is a bijection so the number of solutions in each case is identical, $r_4(4m) = r_4(2m)$.

Let m be odd. Then $4m \equiv 4 \bmod 8$. We prodceed by breaking up the solutions in $r_4(m)$ into two cases. Either, all x_i are odd in which case, up to sign the solution is one of $N_4(4m)$ or they are all even because their sum is 4 modulo 8. In the first case we have 4 sign choices and thus a total of $16N_4(4m)$ solutions. In the second case, because all x_i are even we divide $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4m$ by 4 to get a solution for m. Therefore, every solution is either one of $N_4(4m)$ or $r_4(m)$. Thus,

$$r_4(4m) = N_4(4m) + r_4(m)$$

Since m is odd we have $m \equiv 2, 6, 4 \bmod 8$ and, any solution to

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2m$$

must have two even parity and two odd parity squares. There are 6 ways to arrange these solutions. Also given any solution to

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2m$$

we can form

$$(x_1 + x_2)^2 + (x_1 - x_2)^2 + (x_3 + x_4)^2 + (x_3 - x_4)^2 = 2m$$

but these solutions are fixed to have the first two and last two squares having equal parity. Thus, we can only form 2 out of the 6 possible solutions for $2m$ given a solution to m. As before, this can be inverted as long as adjacent terms have the same parity. Therefore there is a bijection between the 2 out of 6 cases of solution for $2m$ in which the first two and last two have equal parity and all solutions for m. Therefore, $r_4(2m) = 3r_4(m)$.

At last, we prove the Jacobi Four Square fomula. Take odd m,

$$3r_4(m) = r_4(2m) = r_4(4m) = 16N_4(4m) + r_4(m)$$

but we know that $N_4(m) = \sum_{d|\frac{m}{4}} d$ so,

$$2r_4(m) = 16 \sum_{d|\frac{m}{4}} d$$

and thus

$$r_4(m) = 8 \sum_{d|\frac{m}{4}} d$$

Now we consider the case that m is even. Write $m = 2m'$; if m' is odd then by above, $_4(m') = 8 \sum_{d|\frac{m'}{4}} d$ and $r_4(2m') = 3r_4(m')$ so

$$r_4(m) = 24 \sum_{d|\frac{m'}{4}} d = 24 \sum_{d|\frac{m}{2}} d$$

On the other hand, if m' is even then using $r_4(4m) = r_4(2m)$ we reduce until m' is odd or $2k$ with odd k. Then the above cases can be applied.

2. (a) As proven in class, every solution to the equation $x^2 - dy^2 = 1$ is in the form $(\pm a_n, \pm b_n)$ where $a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n$ with $a_1 + b_1\sqrt{d}$ being the positive solution $(a_1, b_1 > 0)$ with the smallest b_1. Now consider the set $\Sigma \subset \Gamma$ of $u_i = a_i - b_i\sqrt{d}$ which solve $a_i^2 - db_i^2 = \pm 1$ with $b_1 \leq b_2 \leq b_3 \ldots$. If the negative sign Pell's equaton has no solutions, then we are done because every $x \in \Gamma$ is of the form $\pm a_n \pm b_n\sqrt{d}$ but $(a_1 + b_1\sqrt{d})^{-n} = a_n - b_n\sqrt{d}$ since $(a_n - b_n\sqrt{d})(a_n + b_n\sqrt{d}) = a_n^2 - db_n^2 = 1$. Also, $a_1 - b_1\sqrt{d} = (a_1 + b_1\sqrt{d})^{-1}$ because

$(a_1 - b_1\sqrt{d})(a_1 + b_1\sqrt{d}) = a_1^2 - db_1^2 = 1$. Therefore, -1 and $a_1 - b_1\sqrt{d}$ generate every sign combination and thus the entire group of units. Now we suppose that the negative equation has solutions. There must be a u_k with minimal b_k which has norm -1 and thus solves the negative equation. If $u_1 \neq u_k$ then u_1 solves the positive equation by minimality. But $\mathrm{N}_{\mathbb{Q}}^{K}(u_k^2) = \mathrm{N}_{\mathbb{Q}}^{K}(u_k)^2 = (-1)^2 = 1$ so by the above classification, $u_k^2 = (u_1)^n$ and thus either n is even or u_1 is a square. If $u_1 = w^2$ then $\mathrm{N}_{\mathbb{Q}}^{K}(w^2) = \mathrm{N}_{\mathbb{Q}}^{K}(w)^2 = 1$ so $\mathrm{N}_{\mathbb{Q}}^{K}(w) = \pm 1$ therefore w would be a smaller solution than u_1 which contradicts minimality. Thus, n is even so $u_k = \pm(u_1)^{n/2}$ and thus,

$$\mathrm{N}_{\mathbb{Q}}^{K}(u_k) = \mathrm{N}_{\mathbb{Q}}^{K}\left(\pm(u_1)^{n/2}\right) = \mathrm{N}_{\mathbb{Q}}^{K}(u_1)^{n/2} = 1$$

But by assumption, u_k has norm -1. Thus, u_1 must have a negative norm and be minimal. Similarly, in this case, $a_1 - b_1\sqrt{d} = u_1^2$ else since u_1^2 has norm $+1$ we would have $u_1^2 = (a_1 - b_1\sqrt{d})^n$ so either n is even or u_1 is a square. But $u_1 = (a_1 - b_1\sqrt{d})^{n/2}$ is a contradiction because u_1 has norm -1 and $a_1 - b_1\sqrt{d}$ has norm $+1$ and u_1 being a square would contradict its minimality. Take $r \in \Gamma$, then r^2 has norm $+1$ and thus $r^2 = (u_1^2)^n$ because u_1^2 is the minimal solution to the positive equation. Thus, $r = \pm(u_1)^n$ therefore, $\Gamma = \langle u_1, -1\rangle$.

(b) For $b \in \mathbb{Z}^+$ take $q^{\pm}(b) = db^2 \pm 1$ and let b_1 be the smallest b such that either $q^+(b_1)$ or $q^-(b_1)$ is a square. Let $u_1 = a - b\sqrt{d}$ then $a^2 - db^2 = \pm 1$ and hence $a^2 = db^2 \pm 1 = q^{\pm}(b)$ thus $b_1 \leq b$ because $q^{\pm}(b)$ is a square and b_1 is minimal. However, if $b_1 < b$ then $q^{\pm}(b_1) = a^2$ so $a^2 - db_1^2 = \pm 1$ so u_1 is not minimal thus, $b_1 = b$. Thus, $u_1 = a - b_1\sqrt{d}$ but $a_1 = \sqrt{q^{\pm}(b_1)} = \sqrt{db_1^2 \pm 1} = \sqrt{a^2}$ so $a_1 = a$ and therefore, $u_1 = a_1 - b_1\sqrt{d}$.

(c) Case $d = 6$:
$q^+(1) = 6 + 1 = 7$, $q^-(1) = 6 - 1 = 5$, $q^-(2) = 24 - 1 = 23$, $q^+(2) = 24 + 1 = 25$ thus the smallest square is for $b_1 = 2$ and $a_1 = \sqrt{25} = 5$ so $u_1 = 5 - 2\sqrt{6}$ then $\mathrm{N}_{\mathbb{Q}}^{K}(u_1) = +1$.

Case $d = 10$:
$q^+(1) = 10 + 1 = 11$, $q^-(1) = 10 - 1 = 9$ thus the smallest square is for $b_1 = 1$ and $a_1 = \sqrt{9} = 3$ so $u_1 = 3 - \sqrt{10}$ then $\mathrm{N}_{\mathbb{Q}}^{K}(u_1) = -1$.

Case $d = 14$:
$q^+(1) = 14 + 1 = 15$, $q^-(1) = 14 - 1 = 13$, $q^-(2) = 56 - 1 = 55$, $q^+(2) = 56 + 1 = 57$, $q^+(3) = 126 + 1 = 127$, $q^-(3) = 126 - 1 = 125$, $q^+(4) = 224 + 1 = 225$, $q^-(3) = 224 - 1 = 223$ thus the smallest square is for $b_1 = 4$ and $a_1 = \sqrt{225} = 15$ so $u_1 = 15 - 4\sqrt{14}$ then $\mathrm{N}_{\mathbb{Q}}^{K}(u_1) = +1$.

3. (a) $9 = 3 \cdot 3 = -(1 - \sqrt{10})(1 + \sqrt{10})$. We want to show that these factorizations are not related by units. In particular, that 3 and $1 + \sqrt{10}$ are not equivalnt. For the case $d = 10$ the group of units of $\mathbb{Z}[\sqrt{10}]$ is generated by -1 and $u_1 = 3 - \sqrt{10}$. We must show that

$$1 + \sqrt{10} \neq (-1)^k \cdot 3 \cdot u_1^n = (-1)^k \cdot 3 \cdot (3 - \sqrt{10})^n = \pm 3 \cdot (a_n + b_n\sqrt{10})$$

so but the coefficient of $\sqrt{10}$ is 1 and thus cannot be divisible by 3.

(b) By a similar method to problem 2d on Assignment # 3, we claim that

$$(3) = (3, 1 + \sqrt{10})(3, 1 - \sqrt{10}) = AB$$

by the previous problem, neither A nor B can be equivalent to (3) and thus AB is the prime factorization of (3). This must hold because if A or B were not prime they could be decomposed as a product of primes but in a quadratic ring of integers, any $p\mathcal{O}_K$ factors as at most two primes. Thus, A and B must be primes themselves.

(c) First, we compute the Minkowski bound. Since $d = 10 \equiv 2 \bmod 4$ we have $\Delta_K = 4d = 40$ and $\mathbb{Q}(\sqrt{10})$ is a real quadratic extension so $r_1 = 2$ and $r_2 = 0$. Thus,

$$c_1 = \left(\frac{4}{\pi}\right)^{r_2} \frac{2!}{2^2} \sqrt{\Delta_K} = \sqrt{10} \approx 3.16$$

Therefore, every ideal class contains an ideal with norm less than or equal to 3. We look at the ideals which factor (2) and (3) because these must include an element in each ideal class except for the unit norm ideal which coresponds to the class of principal ideals. These ideals are A, B, and C where $C^2 = (2)$ (which we know is ramified because $10 \equiv 2 \bmod 4$). We have shown that $\mathbb{Z}[\sqrt{10}]$ is not a UFD and therefore certainally not a PID so the class number is at least two. There are only four possible minimal ideals and also four possible groups with orders $2, 3, 4$ which are, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. However, the products of generators of A are

$$3 \cdot (1 + \sqrt{10}), 3 \cdot 3 = -(1 - \sqrt{10})(1 + \sqrt{10}), (1 + \sqrt{10})^2$$

each of which is divisible by $1 + \sqrt{10}$ so $A^2 \subset (1 + \sqrt{10})$ but

$$-(1 + \sqrt{10})^2 + 3(1 + \sqrt{10}) + 3 \cdot 3 = -1 - 2\sqrt{10} - 10 + 3 + 3\sqrt{10} + 9 = 1 + \sqrt{10}$$

so $(1 + \sqrt{10}) \subset A^2$ and thus $A^2 = (1 + \sqrt{10})$. However, an indentical argument shows that $B^2 = (1 - \sqrt{10})$. Therefore, since all principal ideals are in the identity ideal class, the orders of A, B, and C must be 2. Thus, the class group cannot be $\mathbb{Z}/3\mathbb{Z}$ (else two elements would have order 3) or $\mathbb{Z}/4\mathbb{Z}$ (else only one element would have order 2 and if these elements are not distinct we don't have enough elements anyway). However, A^2 and AB are both principal so A and B must be equivalent because inverses are unique. Therefore, we have at most 3 ideal classes which makes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ impossible. Therefore, the ideal class group is $\mathbb{Z}/2\mathbb{Z}$ so the class number is 2.

4. Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r + 1\}$ be all the prime ideals of a Dedekind domain R. Now consider the ideal

$$I = \mathfrak{p}_i^2 + \prod_{j \neq i}^{n} \mathfrak{p}_j$$

then both $\mathfrak{p}_i^2 \subset I$ and $\prod\limits_{j \neq i}^{n} \mathfrak{p}_j \subset I$ so $\mathfrak{p}_i^2 = IJ$ and $\prod\limits_{j \neq i}^{n} \mathfrak{p}_j = IJ'$ which implies that these ideals share prime factors. This is a contradiction unless $I = R$. Thus, by the Chinese remainder theorem, the projection

$$\pi : R \to R/\mathfrak{p}_i^2 \times \prod_{j \neq i}^{n} R/\mathfrak{p}_j$$

is a surjection. Therefore, $\exists x \in R$ s.t. $\pi(x) = ([z], [1], [1], \cdots, [1])$ where I have choosen $z \in \mathfrak{p}_i \backslash \mathfrak{p}_i^2$. This is always possible because $\mathfrak{p}_i = \mathfrak{p}_i^2$ would contradict the uniqueness of prime factorization. Now, $x \in \mathfrak{p}_i$ because $x - z \in \mathfrak{p}_i^2 \subset \mathfrak{p}_i$ and $z \in \mathfrak{p}_i^2$. Furthermore, $x \notin \mathfrak{p}_i^2$ because

$x - z \in \mathfrak{p}_i^2$ but $z \notin \mathfrak{p}_i^2$. Also, if $x \in \mathfrak{p}_j$ then because $x - 1 \in \mathfrak{p}_j$ we have that $1 \in \mathfrak{p}_j$ which contradicts its primality. Thus, $x \in \mathfrak{p}_i$ but $x \notin \mathfrak{p}_i^2$ and $x \notin \mathfrak{p}_j$ for $i \neq j$. Thus, $(x) \subset \mathfrak{p}_i$ so $(x) = \mathfrak{p}_i J$ but then $x \in J$ so J cannot have any factors of $\mathfrak{p}_j$ for $i \neq j$ else $I \subset \mathfrak{p}_j$ so then $x \in \mathfrak{p}_j$. Thus, $(x) = \mathfrak{p}_i \mathfrak{p}_i^k$ but $x \notin \mathfrak{p}_i^2$ so $\mathfrak{p}_i \mathfrak{p}_i^k \supsetneq \mathfrak{p}_i^2$ so $k = 0$. Thus, $(x) = \mathfrak{p}_i$ so every prime ideal is principal. Now any ideal I can be written as,

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{\mathrm{ord}_{\mathfrak{p}_i}(I)} = \prod_{i=1}^{n} (x_i)^{\mathrm{ord}_{\mathfrak{p}_i}(I)} = \left(\prod_{i=1}^{n} x_i^{\mathrm{ord}_{\mathfrak{p}_i}(I)} \right)$$

so every ideal is principal.