# Mathematics W4043 Algebraic Number Theory
# Assignment # 10

Benjamin Church
*Worked With Matthew Lerner-Brecher*

December 20, 2017

6.22 Consider the equation $y^2 = x^3 - 2$. Reducing modulo 2, $y \equiv x \pmod 2$ so either both $x$ and $y$ are even or they are both odd. If $x$ and $y$ are both even then $4 \mid x^3 - y^2 = 2$ which is a contradiction. Thus, $x$ and $y$ are even. We can rewrite this equation as,

$$x^3 = y^2 + 2 = (y + i\sqrt{2})(y - i\sqrt{2})$$

Therefore, the element $y^2 + 2 = (y + i\sqrt{2})(y - i\sqrt{2})$ is a square in $\mathbb{Z}[i\sqrt{2}]$. Let $K = Q(\sqrt{-2})$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[i\sqrt{2}]$ because $-2 \not\equiv 1 \pmod 4$ .

I claim that $a = y + i\sqrt{2}$ and $b = y - i\sqrt{2}$ are coprime. If $d \mid y + i\sqrt{2}$ and $d \mid y - i\sqrt{2}$ then $d \mid 2i\sqrt{2}$. Therefore, $\mathrm{N}^K_{\mathbb{Q}}(d) \mid \mathrm{N}^K_{\mathbb{Q}}\left(2i\sqrt{2}\right) = 8$. Therefore either $d = \pm 1$ or $\mathrm{N}^K_{\mathbb{Q}}(d)$ is even. However, $d \mid y + i\sqrt{2}$ so $\mathrm{N}^K_{\mathbb{Q}}(d) \mid \mathrm{N}^K_{\mathbb{Q}}\left(y + i\sqrt{2}\right) = y^2 + 2$ which is odd if $y$ is odd. Therefore $d = 1$. However, $\mathbb{Z}[\sqrt{-2}]$ is a PID and therefore a UFD. Thus, if $(y+i\sqrt{2})(y-i\sqrt{2})$ is a cube then $y + i\sqrt{2}$ is a cube as well. Now suppose that,

$$y + i\sqrt{2} = (a + bi\sqrt{2})^3 = a^3 - 6ab^2 + (3a^2 - 2b^2)bi\sqrt{2}$$

with $a, b \in \mathbb{Z}$. Because $\sqrt{2}$ is irrational, the coeficients must themselves be equal. Therefore, $(3a^2 - 2b^2)b = 1$ thus $b = \pm 1$ and $3a^2 - 2b^2 = \pm 1$ so $3a^2 = 3$ or $3a^2 = 1$. Since the latter is impossible, we have $a = \pm 1$ and $b = \pm 1$. Thus, $y = a^3 - 6ab^2 = a(a^2 - 6b^2) = a(1 - 6) = -5a$ which takes on the values $\pm 5$ because $a = \pm 1$.

The corresponding values of $x$ are given by the norm of $a+bi\sqrt{2}$ because if $y+i\sqrt{2} = (a+bi\sqrt{2})^3$ then $\mathrm{N}^K_{\mathbb{Q}}\left(y + i\sqrt{2}\right) = y^2+2 = (\mathrm{N}^K_{\mathbb{Q}}\left(a + bi\sqrt{2}\right))^3 = x^3$. Thus, $x = \mathrm{N}^K_{\mathbb{Q}}\left(\pm 1 \pm i\sqrt{2}\right) = 1+2 = 3$. No other values of $x$ are possible because, if, using the known solution for $y$, $x^3 = y^2 + 2 = 25 + 2 = 27$ then $x = 3$. Therefore, the only solutions to $y^2 = x^3 - 2$ are $(x, y) = (3, \pm 5)$.

6.23 (a) Suppose that $A\vec{c} = \vec{c}$. Then for each $i$,

$$\sum_{j=1}^{r} a_{ij} c_j = 0 \quad \text{thus} \quad a_{ii} c_i + \sum_{j \neq i} a_{ij} c_j = 0$$

Therefore,

$$|a_{ii}||c_i| = \left| \sum_{j \neq i} a_{ij} c_j \right| \leq \sum_{j \neq i} |a_{ij}||c_j|$$

using the hypothesis and assuming that $|c_i| \neq 0$,

$$\left(\sum_{j\neq i} |a_{ij}|\right) |c_i| < |a_{ii}||c_i|$$

Let $c_m$ be the coefficients with the maximum absolute value. Then, $|c_j| \leq |c_m|$ so,

$$\left(\sum_{j\neq i} |a_{ij}|\right) |c_i| < |a_{ii}||c_i| \leq \sum_{j\neq i} |a_{ij}||c_j| \leq \left(\sum_{j\neq i} |a_{ij}|\right) |c_m|$$

and thus, $|c_i| < |c_m|$ which cannot hold for every $i$ because then we can choose $i = m$ and $|c_m| < |c_m|$ is clearly false. Therefore, $c_m = 0$ which implies that $c_i = 0$ for each $i$ because the maximum absolute value of all these coefficients is zero. Thus, the null space of $A$ is trivial so $A$ is invertible because it is a square matrix.

(b) Introduce the embedding $\Phi : \mathcal{O}_K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ given by

$$\Phi(\alpha) = (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha))$$

where $\sigma_i$ runs over real embeddings and one of each conjugate pair of complex embeddings. Now for any positive real numbers $t_1, \cdots t_n \in \mathbb{R}$ with $n = r_1 + r_2$, consider the convex set,

$$B(t_1, \cdots, t_n) = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_i| \leq t_i\}$$

which has volume $V_B = 2^{r_1}\pi^{r_2} t_1 \cdots t_{r_1} \cdot t_{r_1+1}^2 \cdots t_{r_1+r_2}^2$. By Minkowski's theorem, we are guaranteed that $B(t_1, \dots, t_n)$ containes a lattice point if $V_B \geq 2^n V_L$ where $V_L$ is the volume of a lattice cell. For a fixed $i$, we can ensure the volume satisfies this criterion by choosing $\tilde{t}_i > 2^{n-r_1}\pi^{-r_2} V_L$ then $B(1, \dots, \tilde{t}_i, \dots, 1)$ contains a non-zero lattice point. Therefore, $\exists \alpha_1 \in \mathcal{O}_K$ such that $\Phi(\alpha_1) \in B(1, \dots, t_i, \dots, 1)$. Now, we define a sequence of convex sets with $t_j = \frac{|\alpha_k|_j}{4}$ and $t_i = (4^k)^{r_1+2r_2-1}\tilde{t}_i$ where $\alpha_k$ begins with $\alpha_1$ and then takes on the value of the last construced algebraic integer. Therefore, when $i \leq r_1$,

$$V_n = 2^{r_1}\pi^{r_2} t_1 \cdots t_{r_1} \cdot t_{r_1+1}^2 \cdots t_{r_1+r_2}^2 < 2^{r_1}\pi^{r_2} \frac{1}{(4^k)^{r_1+2r_2-1}} (t_i)_k = 2^{r_1}\pi^{r_2}\tilde{t}_i > 2^n V_L$$

since $t_j \leq \frac{1}{4^k}$ because each $\alpha_k$ is choosen with $|\alpha_k|_j$ less than the previous $t_j$. Likewise when $i > r_1$ then

$$V_n = 2^{r_1}\pi^{r_2} t_1 \cdots t_{r_1} \cdot t_{r_1+1}^2 \cdots t_{r_1+r_2}^2 \leq 2^{r_1}\pi^{r_2} \frac{1}{(4^k)^{r_1+2r_2-2}} (t_i)_k^2 = 2^{r_1}\pi^{r_2}(4^k)^{r_1+2r_2}\tilde{t}_i > 2^n V_L$$

therefore, $B_{k+1}$ contains a non-zero lattice point. Thus, take $\alpha_{k+1}$ such that $\Phi(\alpha_k) \in B_k$. Consider the ideals $(\alpha_k)$ which all have norm,

$$|\mathrm{N}_{\mathbb{Q}}^{K}(\alpha_k)| = \prod_{i=1}^{r_1+2r_2} |\sigma_i(\alpha_k)| < t_1 \cdots t_{r_1} \cdot t_{r_1+1}^2 \cdots t_{r_1+r_2}^2 < 2^n V_L$$

However, by Dedekind prime factorization, there are only finitly many ideals with norm less than some bound so we must have infintly many $\alpha_k$ which generate the same ideal. Take $(\alpha_k) = (\alpha_l)$ with $k > l$ then $\alpha_k = u_i \alpha_l$ for $u \in \mathcal{O}_K^\times$. However, we can bound the absolute values of this unit, when $j \neq i$, $|u_i|_j = |\sigma_j(u_i)| = |\sigma_j(\frac{\alpha_k}{\alpha_l})| = \frac{|\sigma_j(\alpha_k)|}{|\sigma_j(\alpha_l)|} \leq \frac{1}{4}$ because at each state the absolute value is reduced by at least 1/4 and Minkowski's theorem ensures that none of the $\alpha_k$ are zero so none of the absolute values are zero. Also, because $|\mathrm{N}_{\mathbb{Q}}^{K}(u_i)| = |u_i|_1 \cdots |u_i|_{r_1} \cdot |u_i|^2_{r_1+1} \cdots |u_i|^2_{r_1+r_2} = 1$ then $|u_i|_i > 1$ since each other absolute value is less than 1. We have found a unit satisfying these criteria for each $i$.

(c) Consider the matrix of log-absolute values, i.e. $a_{ij} = \log |u_i|_j$ where $i$ and $j$ range from 1 to $r = r_1 + r_2 - 1$. Now, because $|\mathrm{N}_{\mathbb{Q}}^{K}(u_i)| = |u_i|_1 \cdots |u_i|^2_{r_1} \cdot |u_i|_{r_1+1} \cdots |u_i|^2_{r_1+r_2} = 1$ then $|u_i|_i > 1$ we have that,

$$\sum_{j=1}^{r+1} \log |u_i|_j = \log 1 = 0$$

and thus,

$$\sum_{j=1}^{r} a_{ij} = \sum_{j=1}^{r+1} \log |u_i|_j - \log |u_i|_{r+1} > 0$$

because $|u_i|_{r+1} \leq \frac{1}{4}$ so $-\log |u_i|_{r+1} > 0$. For $j \neq i$, the same condition applies i.e. $\log |u_i|_{r+1} < 0$ because $|u_i|_j \leq \frac{1}{4}$. Then,

$$|a_{ii}| = a_{ii} > -\sum_{j \neq i} a_{ij} = \sum_{j \neq i} |a_{ij}|$$

because $|u_i|_i > 1$ so $a_{ii} = \log |u_i|_i > 0$ and the other terms are negative. Thus, by part (a), $a_{ij}$ is an invertable matrix so its rows are independent. Therefore, the set of units $\{u_1, \cdots, u_r\}$ is independent because if $u_1^{e_1} \cdots u_r^{e_r} = 1$ then for any $j$,

$$\log |u_1^{e_1} \cdots u_r^{e_r}|_j = \sum_{i=1}^{r} e_i \log |u_i|_j = \sum_{i=1}^{r} e_i a_{ij} = \log |1|_j = 0 \implies e_i = 0$$

because the matrix has independent rows.

2. (a) Let $\mathbf{1}$ denote the function $\mathbf{1}(n) = 1$. Now consider the convolution,

$$(\mathbf{1} * \mathbf{1})(n) = \sum_{d|n} \mathbf{1}(d)\mathbf{1}(\tfrac{n}{d}) = \sum_{d|n} 1 = \left|\{d \in \mathbb{Z}^+ \mid d \mid n\}\right| = \tau(n)$$

(b) Let $f$ and $g$ be multiplicative functions, now consider the convolution of $f$ and $g$ applied to coprime $a, b$,

$$(f * g)(ab) = \sum_{d|ab} f(d)g(\tfrac{ab}{d})$$

If $d \mid ab$ then let $d' = \frac{d}{(d,a)}$ which is coprime with $a' = \frac{a}{(d,a)}$. Futhermore, $d' \mid a'b$ but $(d', a') = 1$ so $d' \mid b$. Thus, $d = d'(d, a)$ which is a divisor of $a$ times a divisor of $b$. Futhermore, I claim that if $a$ and $b$ are coprime then these products are distinct. This holds because if $e, f \mid a$ and $g, h \mid b$ and $eg = fh$ therefore $e \mid fh$ and $f \mid eg$. However,

$(e,h)=1$ so $e \mid f$ but $(f,g)=1$ so $f \mid e$. Thus, $e=f$ ad $g=h$. Therefore,

$$(f*g)(ab) = \sum_{d \mid ab} f(ab) g(\tfrac{ab}{d}) = \sum_{d_1 \mid a} \sum_{d_2 \mid b} f(d_1 d_2) g(\tfrac{ab}{d_1 d_2}) = \sum_{d_1 \mid a} \sum_{d_2 \mid b} f(d_1) f(d_2) g(\tfrac{a}{d_1}) g(\tfrac{b}{d_2})$$
$$= \left( \sum_{d_1 \mid a} f(d_1) g(\tfrac{a}{d_1}) \right) \cdot \left( \sum_{d_2 \mid b} f(d_2) g(\tfrac{b}{d_2}) \right) = (f*g)(a)(f*g)(b)$$

(c) Define $f(n) = n$ and $\mu(1) = 1$ and $\mu(p) = -1$ and $\mu(n) = 0$ iff $n$ contains a square. First, we consider the function $f * \mu$ applied to prime powers. Because $f$ and $\mu$ are multiplicative, $f * \mu$ is as well so the result will extend to all integers.

$$(f * \mu)(p^k) = \sum_{d \mid p^k} f(d) \mu(\tfrac{p^k}{d})$$

The only divisors of $p^k$ which are not sent to zero by $\mu$ are 1 and $p$ so we only need to sum over $d = p^k$ and $d = p^{k-1}$. Therefore,

$$(f * \mu)(p^k) = f(p^k) \mu(\tfrac{p^k}{p^k}) + f(p^{k-1}) \mu(\tfrac{p^k}{p^{k-1}}) = p^k \mu(1) + p^{k-1} \mu(p) = p^k - p^{k-1} = \phi(p^k)$$

Because both $f * \mu$ and $\phi$ are multiplicative and agree for prime powers, by unique factorization they agree on all integers. Therefore, $f * \mu = \phi$.

(d) Define the function $\Lambda(p^k) = \log p$ and $\Lambda(n) = 0$ if $n$ is not a prime power. Now, define,

$$D(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

We will apply the theorem proved in class to conclude that if $f(n) = O(n^\beta)$ then,

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

coverges for $\mathrm{Re}(s) > 1 + \beta$. Take any $\beta > 0$ then because for any $n \in \mathbb{Z}^+$, $|\log(n)| < n$ we have the inequality, $\log(n^\beta) < n^\beta$ so $\log(n) < \frac{1}{\beta} n^\beta$. Therefore,

$$|\Lambda(n)| \le |\log(n)| < \frac{1}{\beta} n^\beta$$

so $\Lambda(n) = O(n^\beta)$ and thus $D(s)$ converges for $\mathrm{Re}(s) > 1 + \beta$ for every $\beta > 0$. Take any $s$ with $\mathrm{Re}(s) > 1$ then choose $\beta = \frac{\mathrm{Re}(s)-1}{2} > 0$ then $\mathrm{Re}(s) > 1 + \beta = \frac{\mathrm{Re}(s)+1}{2}$ so $D(s)$ converges on the right half plane $\mathrm{Re}(s) > 1$.

Now in the right half plane $\mathrm{Re}(s) > 1$ on which $\zeta(s)$ is a holomorphic function, the function,

$$f(s) = -\frac{\mathrm{d}}{\mathrm{d}s} \log \zeta(s) = -\frac{\zeta'(s)}{\zeta(s)}$$

exists and is holomorphic. Using the Euler product,

$$f(s) = -\frac{\mathrm{d}}{\mathrm{d}s}\log\prod_p \frac{1}{1-p^{-s}} = \frac{\mathrm{d}}{\mathrm{d}s}\sum_p \log\left(1-p^{-s}\right) = \sum_p \frac{\mathrm{d}}{\mathrm{d}s}\log\left(1-p^{-s}\right) = \sum_p \frac{p^{-s}\log p}{1-p^{-s}}$$
$$= \sum_p p^{-s}\log p\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots\right) = \sum_p\sum_{k=1}^{\infty}\frac{\log p}{(p^k)^s} = \sum_p\sum_{k=1}^{\infty}\frac{\Lambda(p)}{(p^k)^s} = \sum_{n=1}^{\infty}\frac{\Lambda(p)}{n^s} = D(s)$$

where the sum can be extended from only prime powers to all positivie integers because $\Lambda(n) = 0$ for all $n$ which are not a prime power and the sums are all absolutly convergent so rearrangement poses no issue.