18.785 Analytic Number Theory Problem Set #6

Holden Lee

3/16/11

Problem 1 *(Simultaneous eigenfunctions of Hecke operators, with no Euler product expansion)*

(A) Simultaneous eigenfunction

Lemma 1.1: Every double coset $\Gamma_0(N)\alpha\Gamma_0(N)$ with $\alpha \in G_0(N)$ is one of the double cosets

$$\Gamma_0(N)\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}\Gamma_0(N)$$

where $d_1, d_2 \in (\mathbb{Z}_N^\times)_{\geq 0}$ and $\frac{d_2}{d_1} \in \mathbb{N}$ is relatively prime to N.

Proof. There exists n relatively prime to N so that $n\alpha \in \mathrm{GL}_2(\mathbb{Z})$. By the elementary divisors theorem we can write

$$n\alpha = \gamma_1 D' \gamma_2 \text{ for some } \gamma_1, \gamma_2 \in \Gamma(1). \tag{1}$$

where $D' = \begin{bmatrix} d_1' & 0 \\ 0 & d_2' \end{bmatrix}$ with positive $d_2'|d_1'$. Let $d_i = \frac{d_i'}{n}$ and $D = \frac{1}{n}D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$. The determinant of the LHS in (1) is $n^2\det(\alpha) \in \mathbb{Z}_N^\times$ (since $\det(\alpha) \in \mathbb{Z}_N^\times$). The determinant of the RHS is $d_1'd_2'$. Since d_1', d_2' are integers, d_1' and d_2' must be in $\mathbb{Z}_N^\times$. Since n is relatively prime to N, d_1 and d_2 are also in $\mathbb{Z}_N^\times$.

Let $d = \frac{d_1}{d_2}$. Note $d = \frac{d_1'}{d_2'} \in \mathbb{N}$ and $d \in \mathbb{Z}_N^\times$, so is a whole number relatively prime to N. Now

$$\alpha = \gamma_1 D \gamma_2.$$

Let $\beta_2 = \begin{bmatrix} v & x \\ dy & z \end{bmatrix} \in \Gamma_0(d)$. Let

$$\beta_1 = (D\beta_2 D^{-1})^{-1}.$$

Then

$$\alpha = \gamma_1\beta_1 D\beta_2\gamma_2. \tag{2}$$

Note

$$D\beta_2D^{-1} = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}\begin{bmatrix} v & x \\ dy & z \end{bmatrix}\begin{bmatrix} \frac{1}{d_1} & 0 \\ 0 & \frac{1}{d_2} \end{bmatrix} = \begin{bmatrix} v & dx \\ y & z \end{bmatrix} \in \Gamma(1)$$

so $\beta_1 \in \Gamma(1)$.

Now we claim we can choose $\beta_2 \in \Gamma_0(d)$ so that $\beta_2\gamma_2 \in \Gamma_0(N)$. If $\gamma_2 = \left[\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right]$, then

$$\beta_2\gamma_2 = \begin{bmatrix} ws + xu & wt + xv \\ dys + zu & dy + tzv \end{bmatrix}.$$

We will use the following.

Lemma 1.2: Let A, B, C be integers such that $\gcd(A, B, C) = 1$. Then there exists $k \in \mathbb{Z}$ such that

$$\gcd(A, B + kC) = 1.$$

Proof. For every prime p dividing A, p does not divide both B and C, so there exists a residue r_p modulo p such that $B + r_pC \not\equiv p \pmod{p}$. Now choose k so that $k \equiv r_p \pmod{p}$ for every $p|A$. □

Let $y = -u$ and $z = ds + Nk$, $k \in \mathbb{Z}$. So $dy = -du$. Now $\gcd(-du, ds, N) = 1$ since $\gcd(u, s) = 1$ (else γ_2 would not be invertible) and $\gcd(N, d) = 1$. Hence by the lemma above we can find k so that $\gcd(dy, z) = 1$. Then by Bézout we can choose v, x to make β_2 have determinant 1, and hence be in $\Gamma_0(d)$. Note the bottom left entry of $\beta_2\gamma_2$ is Nku so $\beta_2\gamma_2 \in \Gamma_0(N)$.

Let $\gamma_1' = \gamma_1\beta_1$ and $\gamma_2' = \beta_2\gamma_2 = \left[\begin{smallmatrix} s' & t' \\ Nu' & v' \end{smallmatrix}\right]$. We have $\gamma_2' \in \Gamma_0(N)$. We show that this forces $\gamma_1' \in \Gamma_0(N)$. Let $\gamma_1' = \left[\begin{smallmatrix} s'' & t'' \\ u'' & v'' \end{smallmatrix}\right]$. Then modulo N, the lower-left entry of $\alpha = \gamma_1' D \gamma_2'$ is $s'u''d_1 + Nu'v''d_2$. Since $\alpha \in G_0(N)$, this must be divisible by N. Since N is relatively prime to d_1 and to s' (since N already divides the bottom-left entry of γ_2'), we conclude $N|u''$, and $\gamma_2' \in \Gamma_0(N)$. Thus (2) follows, as needed. □

Lemma 1.3: Suppose p is a prime not dividing N. Then

$$\Gamma_0(N)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_0(N) = \Gamma_0(N)\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\Gamma_0(N) = \Gamma_0(N)\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \sqcup \bigsqcup_{k=0}^{p-1}\Gamma_0(N)\begin{bmatrix} 1 & k \\ 0 & p \end{bmatrix}.$$

Proof. We first show that every element in the LHS is in the RHS. It suffices to show that every element $\left[\begin{smallmatrix} pa & pb \\ Nc & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right]$ is in (exactly) one of the cosets, i.e. $\left[\begin{smallmatrix} pa & pb \\ Nc & d \end{smallmatrix}\right] M^{-1} \in \Gamma_0(N)$ for exactly one of the coset representatives M listed above. We have

$$\begin{bmatrix} pa & pb \\ Nc & d \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & p \end{bmatrix}^{-1} = \begin{bmatrix} pa & -ak + b \\ Nc & \frac{-Nck + d}{p} \end{bmatrix} \tag{3}$$

$$\begin{bmatrix} pa & pb \\ Nc & d \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a & pb \\ \frac{Nc}{p} & d \end{bmatrix}. \tag{4}$$

The first is in $\Gamma_0(N)$ iff $Nck \equiv d \pmod{p}$. If $c \not\equiv 0 \pmod{p}$, since $p \nmid N$, there is exactly one value of k such that this holds. If $c \equiv 0 \pmod{p}$, then $d \not\equiv 0 \pmod{p}$; else the matrix would not be invertible in $\mathrm{GL}_2(\mathbb{Z}_N)$. Hence $Nck \not\equiv d \pmod{p}$ for any choice of k, so (3) does not have integral entries, but (4) does, and is in $\Gamma_0(N)$.

To show the RHS is included in the LHS, it suffices to show that all of the cases above are attainable. We can let $c = 1$ and vary d modulo p to get the first p cases. (Since we can vary d by multiples of p, we can choose d relatively prime to N.) The other entries can be chosen by Bézout's. That the last case is attainable is obvious, since we took $\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]$ as the double coset representative. □

$G_0(N)$ can be generated as follows.

$$G_0(N) = \left\langle \Gamma_0(N); \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}, p \text{ prime not dividing } N \right\rangle \tag{5}$$

Indeed, first note $\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]$ being in the group above implies $\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$ is in the group above, by the fact that they are in the same double coset (Lemma 1.3). By multiplying by matrices of this form or their inverse we can get to any double coset representative in Lemma 1.1. Since $\Gamma_0(N)$ is also in the group above, by Lemma 1.1 we get everything.

Now $\Delta(z)$ is a modular form for $\Gamma(1)$ and hence for $\Gamma_0(N)$. Letting $\gamma = \left[\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right]$,

$$\Delta(N\gamma z) = \Delta\left(\frac{Naz + Nb}{Ncz + d}\right) = \Delta\left(\frac{a(Nz) + Nb}{c(Nz) + d}\right) = \Delta(Nz),$$

so $\Delta(Nz)$ is a modular form for $\Gamma_0(N)$ as well.

To show $\Delta(z) + \Delta(Nz)$ is a simultaneous eigenfunction for the Hecke operators, by 5 it suffices to show that $\Delta(z) + \Delta(Nz)$ is an eigenfunction for the $T| \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Using the decomposition in Lemma 1.3,

$$T| \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} (\Delta(z)+\Delta(6z)) = p^5 \sum_{k=0}^{p-1} \Delta(z)| \begin{bmatrix} 1 & k \\ 0 & p \end{bmatrix} + \Delta(z)| \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} + \sum_{k=0}^{p-1} \Delta(6z)| \begin{bmatrix} 1 & k \\ 0 & p \end{bmatrix} + \Delta(6z)| \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}.$$

Let $\Delta(z) = (2\pi)^{12} \sum_{n=0}^{\infty} a_n e(nz)$. Then

$$\begin{aligned} \sum_{k=0}^{p-1} \Delta(z)| \begin{bmatrix} 1 & k \\ 0 & p \end{bmatrix} &= (2\pi)^{12} p^{-6} (pa_0 + pa_p e(z) + pa_{2p} e(2z) + \cdots) \\ \Delta(z)| \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} &= (2\pi)^{12} p^{6} (a_0 + a_1 e(pz) + a_2 e(2pz) + \cdots) \\ \sum_{k=0}^{p-1} \Delta(6z)| \begin{bmatrix} 1 & k \\ 0 & p \end{bmatrix} &= (2\pi)^{12} p^{-6} (pa_0 + pa_p e(6z) + pa_{2p} e(12z) + \cdots) \\ \Delta(6z)| \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} &= (2\pi)^{12} p^{6} (a_0 + a_1 e(6pz) + a_2 e(12pz) + \cdots) \end{aligned} \tag{6}$$

Note the first equation follows from the fact that

$$\begin{aligned} \sum_{k=0}^{p-1} \Delta(z)| \begin{bmatrix} 1 & k \\ 0 & p \end{bmatrix} &= p^{-6} \sum_{k=0}^{p-1} \Delta\left(\frac{z+k}{p}\right) \\ &= (2\pi)^{12} p^{-6} \sum_{k=0}^{p-1} \sum_{n=0}^{\infty} a_n e(nk/p) e(nz/p) \\ &= (2\pi)^{12} p^{-6} \sum_{n=0}^{\infty} \sum_{k=0}^{p-1} a_n e(nk/p) e(nz/p) \end{aligned}$$

The inner sum is 0 (sum of roots of unity) for $p \nmid n$ and p for $p \mid n$, giving (6). The third equation follows similarly. Matching coefficients gives that the coefficient of $e(nz)$ in $\Delta(z) + \Delta(6z)$ is

$$b_n = p^5(p^{-5}a_{pn} + p^6 a_{\frac{n}{p}} + p^{-5}a_{\frac{pn}{6}} + p^6 a_{\frac{n}{6p}}) \tag{7}$$

where for convenience we let $a_m = 0$ if m is an invalid index. But we know

$$\begin{aligned} a_{mn} &= a_m a_n, & m \perp n \\ a_{p^{n+1}} &= a_p a_{p^n} - p^{11} a_{p^{n-1}}. \end{aligned}$$

Hence

$$\begin{aligned} a_{np} &= a_p a_n - p^{11} a_{\frac{n}{p}} \\ a_p a_n &= a_{np} + p^{11} a_{\frac{n}{p}}. \end{aligned}$$

Together with (7), we get

$$b_n = a_p(a_n + a_{n/6})$$

showing that $T| \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right] (\Delta(z) + \Delta(6z)) = a_p(\Delta(z) + \Delta(6z))$, as needed.

(B) No Euler expansion
Write $\Delta(z)$ as before. Then

$$\Delta(6z) = (2\pi)^{12}(a_0 + a_1 e(6z) + a_2(12z) + \cdots).$$

Let $\Delta(z) + \Delta(6z) = (2\pi)^{12} \sum_{n=0}^{\infty} c_n e(6nz)$. Then since $\Delta(z)$ has coefficients of $e(2z)$ and $e(3z)$ equal to 0 while the coefficient of $e(6z)$ equal to $a_1 = 1$,

$$\begin{aligned} c_2 &= a_2 \\ c_3 &= a_3 \\ c_6 &= a_6 + 1 \\ c_6 &= c_2 c_3 + 1 \neq c_2 c_3. \end{aligned}$$

Since c_n is not multiplicative, $\Delta(z) + \Delta(6z)$ cannot have an Euler product expansion.

Problem 2 *(Modular equation)*

(A) $F(X,Y) = F(Y,X)$
Replacing z with $-\frac{1}{Nz}$ in

$$F(j(z), j(Nz)) = 0$$

gives

$$F\left(j\left(-\frac{1}{Nz}\right), j\left(-\frac{1}{z}\right)\right) = 0.$$

Note that j is invariant under $\gamma = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ which sends z to $-\frac{1}{z}$. Hence $j\left(-\frac{1}{Nz}\right) = j(Nz)$, $j\left(-\frac{1}{z}\right) = j(z)$, and we get

$$F(j(Nz), j(z)) = 0.$$

Since $F(X,Y)$ is irreducible in $\mathbb{C}[X,Y]$, so is $F(Y,X)$. Then $F(Y,j)$ is also the irreducible polynomial of Y over $\mathbb{C}(j)$, so replacing j with X, this says that $F(Y,X)|F(X,Y)$. The only way for this to happen is if $F(X,Y) = cF(Y,X)$. We have $F(X,Y) = cF(Y,X) = c^2F(X,Y)$, so $c = \pm 1$. If $c = -1$, then $F(X,Y) = -F(Y,X)$, and putting $X = Y$ gives $F(X,X) = 0$. This shows $X - Y|F(X,Y)$, which is impossible since $F(X,Y)$ is irreducible with degree $[\Gamma(1) : \Gamma_0(N)] > 1$. Thus $F(X,Y) = F(Y,X)$.

(B) $N = p \implies F(X,Y) \equiv X^{p+1} + Y^{p+1} - X^pY^p - XY \pmod p$

Lemma 2.1: Let $\gamma_1, \ldots, \gamma_{p+1}$ be coset representatives for $[\Gamma(1) : \Gamma_0(p)]$. Then

$$\{j(p\gamma_1 z), \ldots, j(p\gamma_{p+1}z)\} = \{j(pz)\} \cup \left\{ j\left(\frac{z+k}{p}\right) : 0 \le k < p \right\}.$$

Proof. There are indeed $p+1$ coset representatives because $\mu = N\prod_{\text{prime } q|N}\left(1 + \frac{1}{q}\right) = p+1$ in this case. Given $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, we have $p\gamma z = \left[\begin{smallmatrix} pa & pb \\ c & d \end{smallmatrix}\right] z$. For any $\gamma' \in \Gamma(1)$, we have $j(\gamma' p\gamma z) = j(p\gamma z)$ since j is invariant under $\Gamma(1)$. By Lemma 6.3.1 we can multiply $\left[\begin{smallmatrix} pa & pb \\ c & d \end{smallmatrix}\right]$ on the left by some matrix in $\Gamma(1)$ to get some $\left[\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right]$ with $a'd' = \det\left[\begin{smallmatrix} pa & pb \\ c & d \end{smallmatrix}\right] = p$ and $0 \le b' < d'$. The $p+1$ possible matrices are $\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 & k \\ 0 & p \end{smallmatrix}\right]$ for $0 \le k < p$. We claim that all these are in fact attained. Let M be one of these matrices. Then by the Elementary Divisors Theorem there exist $A, B \in \Gamma(1)$ such that $AMB = \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]$. But then $M = A^{-1}NB$, so $j(Mz) = j(A^{-1}NBz)$, and we could have picked B as a coset representative (the choice doesn't matter anyways). The lemma follows upon noting that $\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right] z = pz$ and $\left[\begin{smallmatrix} 1 & k \\ 0 & p \end{smallmatrix}\right] z = \frac{z+k}{p}$. □

Let ζ_p be a pth root of unity. We have that $1 - \zeta_p|p$: indeed

$$p = x^{p-1} + \cdots + 1|_{x=1} = (1-\zeta_p)\cdots(1-\zeta^{p-1}).$$

When we expand $j\left(\frac{z+k}{p}\right)$, its coefficients are roots of unity times the coefficients of $j(z)$. However, roots are unity are congruent to 1 modulo $\mathfrak{p}$, since $\zeta_p^k - 1 = (\zeta_p - 1)(\zeta_p^{k-1} + \cdots + 1)$. Then

$$\begin{aligned} F(j(z), Y) &= \prod_{i=1}^{p+1}(Y - j(\gamma_i pz)) \\ &= (Y - j(pz))\prod_{k=1}^{p}\left(Y - j\left(\frac{z+k}{p}\right)\right) \\ &\equiv (Y - j(pz))\left(Y - j\left(\frac{z}{p}\right)\right)^p \pmod{1-\zeta_p} \\ &\equiv (Y - j(z)^p)(Y^p - j(z)) \pmod{1-\zeta_p}, \end{aligned}$$

the last equation following because raising the j function to the pth power is the same, modulo p, as raising each term to the pth power, and the coefficients (which are integers) are not affected modulo p, while the exponents are multiplied by p. Replacing $j(z)$ by X we get

$$F(X,Y) \equiv (Y - X^p)(Y^p - X) \equiv X^{p+1} + Y^{p+1} - X^pY^p - XY \pmod{1-\zeta_p}.$$

However, $\langle 1-\zeta_p\rangle \cap \mathbb{Z} = \langle p\rangle$ (it contains $\langle p\rangle$, and $\langle p\rangle$ is maximal in $\mathbb{Z}$), and we know $F(X,Y)$ has integer coefficients, so congruence holds modulo p.

Problem 3 *(Rank of Jacobian Matrix)*

The problem follows from the more general theorem.

Theorem 3.1: Let C be an affine algebraic variety in $\mathbb{A}^n(\overline{k})$ corresponding to the ideal generated by $\phi_1, \dots, \phi_m$, and let P be a point on C. Then

$$n = \dim_{\overline{k}}(\mathfrak{m}_P/\mathfrak{m}_P^2) + \operatorname{rank}[D_j\phi_i(P)].$$

Proof. Let $\mathfrak{a}_P$ denote the maximal ideal of $\overline{k}[x_1, \dots, x_n]$ corresponding to P, i.e. if $P = (a_1, \dots, a_n)$ then $\mathfrak{a}_p = \langle x_1 - a_1, \dots, x_n - a_n\rangle$. Let $\mathcal{O}_P$ denote the local ring at P, i.e. $(\overline{k}[C])_{\langle x_1-a_1,\dots,x_n-a_n\rangle}$. Let $\mathfrak{m}_P$ denote the maximal ideal of $\mathcal{O}_P$.

Let θ denote the map $\overline{k}(C) \to \overline{k}^n$ defined by

$$\theta(f) = \left(\frac{\partial f}{\partial x_1}(P), \dots, \frac{\partial f}{\partial x_n}(P)\right).$$

Since any element of $\mathfrak{a}_P$ has P as root with multiplicity at least 1, any element of $\mathfrak{a}_P^2$ has P as root with multiplicity at least 2, so $\theta(\mathfrak{a}_P^2) = 0$ and θ induces a map $\theta' : \mathfrak{a}_P/\mathfrak{a}_P^2 \to \overline{k}^n$. We claim this is an isomorphism of vector spaces. This is clear when we translate P to the origin: In this case, $\mathfrak{a}_P$ is the space of all polynomials without constant term, $\mathfrak{a}_P^2$ is the space of all polynomials without constant or linear term, and the basis $\{x_1, \dots, x_n\}$ for $\mathfrak{a}_P/\mathfrak{a}_P^2$ gets sent to the standard basis $\{e_1, \dots, e_n\}$ for $\overline{k}^n$. Thus

$$\dim_{\overline{k}} \mathfrak{a}_P/\mathfrak{a}_P^2 = n. \tag{8}$$

Next, let $I = \langle \phi_1, \dots, \phi_m\rangle$. Since the ith row of $[D_j\phi_i(P)]$ is the the image of ϕ_i under k,

$$\operatorname{rank}[D_j\phi_i(P)] = \dim_{\overline{k}} \theta(I) = \dim_{\overline{k}}(\theta'((I + \mathfrak{a}_P^2)/\mathfrak{a}_P^2)) = \dim_{\overline{k}}((I + \mathfrak{a}_P^2)/\mathfrak{a}_P^2). \tag{9}$$

The last statement follows since θ' is an isomorphism.

Now note

$$\begin{aligned}
\mathfrak{m}_P &= (\mathfrak{a}_P/I)_P = \mathfrak{a}_P/I_P \\
\mathfrak{m}_P^2 &= ((\mathfrak{a}_P^2 + I)/I)_P = (\mathfrak{a}_P^2 + I_P)/I_P \\
\mathfrak{m}_P/\mathfrak{m}_P^2 &= \mathfrak{a}_P/(\mathfrak{a}_P^2 + I).
\end{aligned}$$

Hence

$$\dim_{\overline{k}} \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim_{\overline{k}} \mathfrak{a}_P/(\mathfrak{a}_P^2 + I). \tag{10}$$

Putting together (8), (9), and (10) gives

$$\begin{aligned} n = \dim_{\overline{k}}(\mathfrak{a}_P/\mathfrak{a}_P^2) &= \dim_{\overline{k}}(\mathfrak{a}_P/(\mathfrak{a}_P^2 + I)) + \dim((\mathfrak{a}_P^2 + I)/\mathfrak{a}_P^2) \\ &= \dim_{\overline{k}}(\mathfrak{m}_P/\mathfrak{m}_P^2) + \operatorname{rank}[D_j\phi_i(P)]. \end{aligned}$$

□

Since $\dim_{\overline{k}} \mathfrak{m}_P/\mathfrak{m}_P^2 \geq \dim \overline{k}[C]_P = \dim \overline{k}[C]$ (the last equality since we're localizing at a maximal ideal), and for curves we have $\dim \overline{k}(C) = 1$, we get

$$\operatorname{rank}[D_j\phi_i(P)] = n - \dim_{\overline{k}}(\mathfrak{m}_P/\mathfrak{m}_P^2) \leq n - 1$$

as needed.

(Alternatively, assuming by way of contradiction that $\operatorname{rank}[D_j\phi_i(P)] = n$, the theorem gives $\mathfrak{m}_P/\mathfrak{m}_P^2 = 0$. But by Nakayama's Lemma, this implies $\mathfrak{m}_P = 0$. Since this is true for every point P, the only maximal ideal of $\overline{k}[C]$ is 0, and $\overline{k}(C) = \overline{k}$, contradiction.)