Thm 2.2.1 Let $N \geq 2$.

(i) $\mathbb{C}(X_0(N)) = \mathbb{C}(j(z), j(Nz))$

(ii) Min^t monic poly of $j(Nz)$ over $\mathbb{C}(j)$ is in $\mathbb{Z}[j][Y] \subset \mathbb{C}(j)[Y]$ and is $\Phi_N(j, Y)$ for Φ_N symmetric

(iii) If $N = p$ is prime
$$\Phi_p(X, Y) = (Y^p - X)(Y - X^p) \bmod p$$

Proof (Cf. Milne's notes "MFMF" p90-92)

Clearly $j(Nz) \in \mathbb{C}(X_0(N))$, so $\mathbb{C}(j(z), j(Nz)) \subseteq \mathbb{C}(X_0(N))$.

Over $\mathbb{C}(j)$, RHS has degree $[PSL_2\mathbb{Z} : \overline{\Gamma_0(N)}]$
$= [SL_2\mathbb{Z} : \Gamma_0(N)] =: \mu$.

So if we can show $j(Nz)$ has degree μ over $\mathbb{C}(j)$, (i) follows.

Let $\gamma_1, \dots, \gamma_\mu$ be such that $SL_2\mathbb{Z} = \bigsqcup_{i=1}^{\mu} \Gamma_0(N)\gamma_i$. (wlog $\gamma_1 = 1$).

Consider the fcns $j(N\gamma_i z)$. All Galois conjugate to $j(Nz)$ over $\mathbb{C}(j)$ (via automorphism $z \mapsto \gamma_i z$ of $\mathbb{C}(\mathcal{H})$).

If we can show they're <u>distinct</u>, (i) follows by Galois theory.

So suppose $j(N\gamma_i z) = j(N\gamma_j z)$, $1 \leq i, j \leq \mu$, $\forall z \in \mathcal{H}$.

Then
$$j\Big(\underbrace{\begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \cdot \gamma_j \cdot \gamma_i^{-1} \cdot \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1}}_{A} \cdot z\Big) = j(z) \quad \forall z \in \mathcal{H}.$$

By a question from Sheet 1 this forces $\pm A \in PSL_2\mathbb{Z}$, so $\gamma_j \gamma_i^{-1} \in \Gamma_0(N) \Rightarrow i = j$. Pf (i) $\square$.

(ii) From (i), monic min^t poly of $j(Nz)$ is
$$\prod_{i=1}^{\mu} (Y - j(N\gamma_i z)).$$

Coeffs are <u>symmetric polys</u> in $\{j(N\gamma_i z)\}$ so all holomorphic on $\mathcal{H}$. Since they're also rat^l fcns in $j(z)$, must be <u>polynomials</u> in $j(z)$.

To control coeffs use q-exp's.

We know $j(z) = q^{-1} + 744 + \dots$
$\in q^{-1} + \mathbb{Z}[[q]]$.

Moreover, can choose the γ_i st $j(N\gamma_i z)$
$= j\left(\frac{az+b}{d}\right)$ some $a, b, d \in \mathbb{Z}$ st $ad = N$.

So $j(N\gamma_i z) \in \mathbb{Z}[\zeta_N]((q^{\frac{1}{N}}))$
$\zeta_N = e^{2\pi i/N}$.

So coeffs of $\Phi_N(j, Y)$ (as poly in Y) have q-exp's in $\mathbb{Z}[\zeta_N]((q^{\frac{1}{N}})) \cap \mathbb{C}((q))$
$= \mathbb{Z}[\zeta_N]((q))$

Claim: these coeffs are actually in $\mathbb{Z}[\zeta_N][j]$.

Let $P = \sum_{i=1}^{k} b_i j^i \in \mathbb{C}[j]$ have q-exp in $R((q))$ some $R \subseteq \mathbb{C}$ ring

Inspecting lowest term of q-exp^n, $b_n \in R$

Induction on degree $\Rightarrow$ all $b_i \in R$.

So $\Phi_N(X,Y) \in \mathbb{Z}[\zeta_N][X,Y]$.

Write $\Phi_N(X,Y) = \sum_{r,s} c_{rs} X^r Y^s$

Substitute in q-exp^{n}s of $j(z)$, $j(Nz)$ + equate coeffs. Get eq^{n}s for $\{c_{rs}\}$, linear with $\mathbb{Q}$-coeffs. Know $c_{rr} = \begin{cases} 1 & r=0 \\ 0 & r>0 \end{cases}$ + know there's a unique sol^n over $\mathbb{C}$.

So sol^n must be $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$-inv^t.

ie $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$.

For symmetry:

$$\Phi_N(j(z), j(Nz)) = 0 \quad \forall z \in \mathcal{H}$$

$$\Rightarrow \Phi_N\left(j\left(\frac{-1}{Nz}\right), j\left(\frac{-N}{Nz}\right)\right) = 0 \ \forall z \in \mathcal{H}$$

$$\Rightarrow \Phi_N(j(Nz), j(z)) = 0.$$

So $\Phi_N(Y,X)$ is a multiple of $\Phi_N(X,Y)$

$\Phi_N(Y,X) = c\,\Phi_N(X,Y) \Rightarrow c^2 = 1$.

Since $N \geq 2$, can't have $c=-1$ as this would force Φ_N to be a multiple of $X-Y$.

So $c=1$. This completes (ii).

For part (iii):

$\Phi_p(j(z), Y)$ has q-exp^n

$$(Y - j(pz))\left(\prod_{i=0}^{p-1}\left(Y - j\left(\frac{z+i}{p}\right)\right)\right)$$

Q-exp^{n}s of fns $j\left(\frac{z+i}{p}\right)$ all congruent mod unique prime $\mathfrak{p} \mid p$ of $\mathbb{Z}[\zeta_p]$ so mod $\mathfrak{p}$ red^n of $\Phi_p(j, Y)$ is

$$(Y - j(pz))\left(Y - j\left(\frac{z}{p}\right)\right)^p$$

$$\equiv (Y - j(z)^p)\left(Y^p - j\left(\frac{z}{p}\right)^p\right)$$

$$\equiv (Y - j(z)^p)(Y^p - j(z)) \mod \mathfrak{p}.$$

This forces some congruence for Φ_p as a polynomial.

$\square$

Remarks

(i) $Y_0(N)$ is not the curve in $\mathbb{A}^2$ defined by $\Phi_N(X,Y) = 0$.

It is birationally equiv^t to it but not generally isomorphic; $\{\Phi_N(X,Y) = 0\}$ is generally singular

(ii) Φ_N's have huge coeffs

$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488XY(X+Y) - 162000(X^2+Y^2) + 40,733,375\,XY + 8,768,000,000(X+Y) - 157,464,000,000,000$$

(iii) Note that mod p red^n of Φ_p defines a reducible curve — two copies of $\mathbb{P}^1$ intersecting

We define $X_0(N)_{\mathbb{Q}}$ as the unique smooth proj. curve $/\mathbb{Q}$ with function field $\mathbb{Q}(X,Y)/\Phi_N(X,Y)$.

<u>Theorem 2.2.2</u> There is a sheaf $\omega_{k\mathbb{Q}}$ on $X_0(N)_{\mathbb{Q}}$ whose base-ext^n to $\mathbb{C}$ is ω_k.

<u>Proof</u> As $-1 \in \Gamma_0(N)$, ω_k is only nonzero for $k \in 2\mathbb{Z}$.

We know $\omega_2 \cong \Omega^1_{X_0(N)_{\mathbb{C}}}(\text{cusps})$

and more generally we always have

$$\omega_{2k} \cong \left(\Omega^1_{X_0(N)_{\mathbb{C}}}\right)^{\otimes k}(D_k)$$

where D_k is a $\mathbb{Z}$-linear comb^n of the divisors (cusps), (ell. pts of order 2), (ell. pts of order 3).

<u>Claim</u>: These 3 divisors descend to $X_0(N)_{\mathbb{Q}}$.

<u>Proof</u> For (cusps) this is clear: the map $X_0(N)_{\mathbb{Q}} \to X_0(1)_{\mathbb{Q}}$ is def^n/$\mathbb{Q}$ (as $j \in \mathbb{Q}(j(z), j(Nz))$) cusps are exactly preimages of the $\mathbb{Q}$-pt $(\infty) \in X_0(1)$.

For ell. pts need to be a bit careful:

$$\left\{\begin{matrix}\text{all pts of} \\ X_0(N) \\ \text{of order 2}\end{matrix}\right\} = \left\{\begin{matrix}\text{preimages of } i \in X_0(1) \\ \text{where proj}^n \text{ map } X_0(N) \to X_0(1) \\ \text{is unramified}\end{matrix}\right\}$$

ramification degree is <u>Galois inv^t</u> so done.

$$\left[\begin{matrix} j(i) = 1728 \\ j(\rho) = 0 \end{matrix} \Rightarrow i, \rho \in X_0(1)(\mathbb{Q})\right]$$

So we can define

$$\omega_{2k,\mathbb{Q}} = \left(\Omega^1_{X_0(N)_{\mathbb{Q}}}\right)^{\otimes k}(D_k).$$

<u>Corollary 2.2.3</u>

For any $k \geq 2$ even, any $N \geq 1$, the spaces $S_k(\Gamma_0(N))$ and $M_k(\Gamma_0(N))$ have bases consisting of forms with q-exp^{n}s in $\mathbb{Q}[[q]]$.

<u>Proof</u> We give argument for M_k. (S_k similar)

$$M_k(\Gamma_0(N)) = H^0(X_0(N)_{\mathbb{C}}, \omega_k)$$
$$= \mathbb{C} \otimes_{\mathbb{Q}} H^0(X_0(N)_{\mathbb{Q}}, \omega_{k\mathbb{Q}}).$$

<u>Claim</u> Image of $H^0(-_{\mathbb{Q}}, -_{\mathbb{Q}})$ is fns w. q-exp^{n}s in $(2\pi i)^{k/2}\mathbb{Q}[[q]]$

<u>Proof</u> Any <u>meromorphic</u> section of ω_k is in $\mathbb{Q}(j(z), j(Nz)) \cdot (dj)^{\otimes k/2}$.

$dj = j'(z)\,dz$ say $j(z) = J(q)$

$J'(q)\,2\pi i q\,dz$

So any mero. section of ω_k lands in $(2\pi i)^{k/2} \cdot \mathbb{Q}((q))$.

Chapter 3: Modular Curves as Moduli Spaces.

§3.1 Lattices & Level Structures

<u>Recall</u> If Λ is a lattice in $\mathbb{C}$ (a discrete subgp $\cong \mathbb{Z}^2$), Λ is homothetic to a lattice of form

$$\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\cdot\tau, \quad \tau \in \mathcal{H},$$

and τ is uniquely determined modulo $PSL_2\mathbb{Z}$.

$$Y(SL_2\mathbb{Z}) = \{\text{homothety classes of lattices}\}$$
$$= \{\text{iso. classes of elliptic curves}/\mathbb{C}\}.$$

<u>Exercise</u>

(i) For any $N \geq 2$ $\exists$ bijection

$$Y_0(N) \cong \left\{ \begin{array}{l} \text{pairs } (\Lambda, C),\ \Lambda \text{ lattice,} \\ C \text{ cyclic subgp of } \mathbb{C}/\Lambda \text{ of order } N, \\ \text{where } (\Lambda, C) \cong (\Lambda', C') \text{ if} \\ \exists \text{ isomorphism } \mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda', \\ \text{sending } C \text{ to } C' \end{array} \right\}$$

$$[\tau] \longmapsto \left(\mathbb{Z}+\mathbb{Z}\tau,\ \tfrac{1}{N}\mathbb{Z}\right)$$

(ii) $$Y_1(N) = \left\{ \begin{array}{l} \text{pairs } (\Lambda, P),\ P \text{ of exact order } N, \\ \text{modulo equiv rel}^n \\ (\Lambda, P) \sim (\Lambda', P') \text{ if } \exists\ \mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda' \\ \text{sending } P \text{ to } P'. \end{array} \right\}$$

Note that in (ii), (Λ, P) is always equ^t to $(\Lambda, -P)$.

In (i) have lots more exceptional cases coming from ell. pts.

Natural question: if $x \in Y_0(N)$ is a $\mathbb{Q}$-pt, does (E, C), $E = \mathbb{C}/\Lambda$, descend to $\mathbb{Q}$?

This is the right sort of question to ask to understand modular curves / number fields.

(This actual question is vacuous for $N \gg 0$ but we don't know that yet.)

---

§3.2 Moduli spaces and representable functors.

Have categories <u>Rings</u> (comm. + unital)
<u>R-Alg</u>, R ring
<u>Set</u>

(don't worry about foundational issues)

"Most sets that come up naturally in alg. geom are functors <u>Ring</u> $\to$ <u>Set</u>."
(or <u>R-Alg</u> $\to$ <u>Set</u>).

Eg
1. Points of varieties / schemes.
2. Classes of varieties or structures on varieties.

A lot of the fun of algebraic geometry arises from ~~the~~ fact that instances of ② are often ① in disguise.

These are <u>moduli spaces</u>.