There is a natural action of $\mathbb{Z}/n\mathbb{Z}$ on $Y_1(n)$ via
$$
\phi : Y_1(n) \rightarrow Y_1(n), \quad (y; z) \mapsto (y; z^2 + y) = (y, \phi_y(z)).
$$
This action lifts to $X_1(n)$.

**Definition 4.11.** The curves $Y_0(n)$ and $X_0(n)$ are the quotients of $Y_1(n)$ and $X_1(n)$ via the action of $\phi$. As noted earlier, the quotient of a variety by a finite set of automorphisms always exists.

The points of $Y_0(n)$ classify isomorphism classes of pairs
$$
(\phi, O), \quad \text{where} \quad \begin{cases} 
\phi \text{ is a degree } 2 \text{ polynomial,} \\
O \text{ is an orbit of a point of formal period } n.
\end{cases}
$$
The isomorphism class of $(\phi, O)$ consists of all points $(\phi^f, f^{-1}(O))$ taken over all invertible affine maps $f = \alpha z + \beta$.

There are projections which, from the moduli viewpoint, are defined by
$$
Y_1(n) \rightarrow Y_0(n), \quad (\phi, \alpha) \mapsto (\phi, O_{\phi}(\alpha)).
$$

### 4.3. Irreducibility and genus formulas

The next result describes the geometry of the dynamical modular curves $Y_1(n)$, $X_1(n)$, and $X_0(n)$. It includes results of a number of authors. In particular, the smoothness of $Y_1(n)$ is due to Douady–Hubbard, and the irreducibility of $X_1(n)$ was proven using a variety of techniques by Bousch, Lau–Schleicher, and Morton. There is also a recent alternative proof of smoothness and irreducibility by Buff and Lei [24].

**Theorem 4.12.** (Bousch [21], Douady–Hubbard [35], Morton [83], Lau–Schleicher [63])

(a) The affine curve
$$
Y_1(n) : \Phi_n(y, z) = 0
$$
is nonsingular.

(b) The curves $X_0(n)$ and $X_1(n)$ are irreducible.

(c) The projection map
$$
X_1(n) \rightarrow \mathbb{P}^1, \quad (\phi_c(z), \alpha) \mapsto c,
$$
is Galois with maximal Galois group (which is a wreath product).

(d) Define
$$
\kappa(n) = \frac{1}{2} \sum_{k|n} \mu \left( \frac{n}{k} \right) 2^k.
$$
Then
$$
genus X_1(n) = 1 + \frac{n - 3}{2} \kappa(n) - \frac{1}{2} \sum_{m|n, m < n} m \kappa(m) \varphi \left( \frac{n}{m} \right).
$$
(There is a similar, but messier, formula for the genus of $X_0(n)$.)
**Proof Sketch.** We sketch Bousch’s proof of (a) and (b), following notes of Michelle Manes. We note that since there is a covering map $X_1(n) \to X_0(n)$, it suffices in (b) to prove that $X_1(n)$ is irreducible.

(a) Let $(z_0, c_0)$ be a point on the curve $Y_1(n)$. If
\[
\frac{\partial}{\partial z} \Phi_n(z, c_0) \bigg|_{z=z_0} \neq 0,
\]
then $(z_0, c_0)$ is a nonsingular point of $Y_1(n)$. So we are reduced to the case that
\[
\frac{\partial}{\partial z} \Phi_n(z, c_0) \bigg|_{z=z_0} = 0.
\]
This means that $z_0$ appears as (at least) a double root of $\Phi_n(z, c_0)$. It follows that the corresponding multiplier $\lambda_{\Phi_n}(z_0)$ equals 1 (cf. 2.31), so $c_0$ is a root of a hyperbolic component of the Mandelbrot set. But each hyperbolic component of the Mandelbrot set has a unique root (including multiplicity), since each such component is conformally isomorphic to the closed unit disk. Hence
\[
\frac{\partial}{\partial c} \Phi_n(z_0, c) \bigg|_{c=c_0} \neq 0,
\]
so $(z_0, c_0)$ is a nonsingular point of $Y_1(n)$.

(b) We will use two facts from classical complex dynamics.

(1) Let $c \in \mathbb{C}$ be a point that is not in the Mandelbrot set, i.e., such that
\[
\lim_{n \to \infty} \phi^n(0) = \infty.
\]
Then the Julia set $J(\phi_c)$ of $\phi_c$ is contained in two disjoint open sets, say $J(\phi_c) \subset \mathcal{U}_0 \cup \mathcal{U}_1$, and the dynamics of $\phi_c$ on its Julia set is conjugate to symbolic dynamics on two symbols via the itinerary map
\[
I : J(\phi_c) \to \{0, 1\}^\mathbb{N}, \quad z \mapsto (I_n(z))_{n \geq 0}.
\]
Here $I_n(z)$ is determined by the condition $\phi_c^n(z) \in \mathcal{U}_{I_n(z)}$

(2) Again let $c$ be outside the Mandelbrot set, let $z, z' \in J(\phi_c)$ be distinct points of exact period $n$, and let $k = k(z, z')$ be the first index for which their itineraries differ. Then
\[
z - z' \sim \pm (2\sqrt{-c})^{1-k}.
\] (4.2)
In particular, we have
\[
\lim_{z,z' \in J(\phi_c) \setminus \Per^*_n(\phi_c) \atop z \neq z'} |z - z'| \cdot (2|c|^{1/2})^{k(z,z')-1} = 1.
\]
We will also need a special case of Zsigmondy’s theorem (this version is actually due to Bang).
Lemma 4.13 (Bang–Zsigmondy Theorem). For all \( n \geq 2 \) with \( n \neq 6 \) there is a prime \( p \) such that
\[
p | 2^n - 1 \quad \text{and} \quad p \nmid 2^d - 1 \quad \text{for all} \quad 1 \leq d < n.
\]
(For \( n = 6 \), we have \( 3^2 | 2^6 - 1 \) and \( 3^2 \nmid 2^d - 1 \) for \( d < 6 \).)

**Proof.** Exercise for the reader; or see [125].

We next show that it suffices to prove irreducibility over \( \mathbb{Z} \).

Lemma 4.14. If \( \Phi_n(z, c) \) is irreducible in \( \mathbb{Z}[z, c] \), then it is irreducible in \( \mathbb{C}[z, c] \).

**Proof.** For any given \( c_0 \in \mathbb{C} \), we can factor \( \Phi_n(z, c_0) \) over \( \mathbb{C} \). However, for \( c \) outside the Mandelbrot set, we can do this factorization in the ring of Laurent series using the variable \( \gamma = 1/\sqrt{-c} \). More precisely, we can (formally) factor
\[
\Phi_n(z, c) = (z - z_1)(z - z_2)\cdots(z - z_m)
\]
with
\[
z_i = a_{i, -1} + a_{i, 0} + a_{i, 1}\gamma + a_{i, 2}\gamma^2 + \cdots \in \gamma^{-1}\mathbb{Q}[\gamma].
\]
Suppose now that \( \Phi_n \) factors, say
\[
\Phi_n(z, c) = A(z, c)B(z, c) \quad \text{with} \quad A, B \in \mathbb{C}[z, c].
\]
Since \( \Phi_n(z, c) \) is monic in \( z \), we may assume the same for \( A(z, c) \) and \( B(z, c) \). Reordering the roots of \( \Phi_n \), we can write
\[
A(z, c) = (z - z_1)(z - z_2)\cdots(z - z_r) \in \gamma^{-1}\mathbb{Q}[\gamma][z],
\]
and similarly for \( B(z, c) \). Thus the coefficients of \( A \) and \( B \), as polynomials in \( z \), are in \( \mathbb{C}[c] \cap \gamma^{-1}\mathbb{Q}[\gamma] \), i.e., the coefficients are simultaneously:
- polynomials in \( c \) with complex coefficients,
- Laurent series in \( (-c)^{-1/2} \) with rational coefficients.

Hence \( A \) and \( B \) are in \( \mathbb{Q}[z, c] \). Thus \( \Phi_n(z, c) \) factors in \( \mathbb{Q}[z, c] \), and since the dynatomic polynomial \( \Phi_n(z, c) \) has integer coefficients, Gauss’s lemma tells us that it factors in \( \mathbb{Z}[z, c] \). \( \square \)

We now resume the proof of Theorem 4.12(b). From Lemma 4.14, it suffices to prove a contradiction from the assumption that \( \Phi_n(z, c) \) factors as
\[
\Phi_n(z, c) = A(z, c)B(z, c) \quad \text{with} \quad A, B \in \mathbb{Z}[z, c] \text{ monic in } z.
\]
From (a) we know that \( Y_1(n) \) is nonsingular, so the affine curves \( A(z, c) = 0 \) and \( B(z, c) = 0 \) have no intersection points in \( \mathbb{A}^2 \), since any such intersection point would necessarily be a singular point of \( Y_1(n) \). It follows that the polynomial
\[
\text{Resultant}_z(A(z, c), B(z, c)) \in \mathbb{C}[c]
\]
has no complex roots, so it must be constant. On the other hand, using the relation (4.2) from earlier, we see that

\[ \text{Resultant}_z(A(z, c), B(z, c)) \sim \pm (2\sqrt{-c})^t \]

for some integer \( t \), so the fact that the resultant is constant implies that \( t = 0 \), and hence that \( \text{Resultant}_z(A, B) = \pm 1 \).

We write

\[ C_D(z) = \prod_{k|D} (z^k - 1)^{\mu(D/k)} \]

for the \( D \)th cyclotomic polynomial. Then specializing the dynatomic polynomial \( \Phi_n(z, c) \) to \( c = 0 \), we obtain the factorization

\[ \Phi_n(z, 0) = \prod_{d|n} \left( z^{2^d} - z \right)^{\mu(n/d)} = \prod_{D \in \mathcal{D}} C_D(z), \]

where

\[ \mathcal{D} = \{ k : k \mid 2^n - 1 \} \setminus \bigcup_{d|n, d \neq n} \{ k : k \mid 2^d - 1 \}. \]

Using the putative nontrivial factorization \( \Phi_n(z, 0) = A(z, 0)B(z, 0) \), we can write \( \mathcal{D} \) as a disjoint union \( \mathcal{D} = \mathcal{A} \cup \mathcal{B} \) so that there are factorizations

\[ A(z, 0) = \prod_{D \in \mathcal{A}} C_D(z) \quad \text{and} \quad B(z, 0) = \prod_{D \in \mathcal{B}} C_D(z). \]

Further, since the cyclotomic polynomials are irreducible in \( \mathbb{Q}[z] \), these give the complete factorizations of \( A(z, 0) \) and \( B(z, 0) \) into irreducible factors.

This gives a factorization of the resultant

\[ 1 = |\text{Resultant}_z(A(z, 0), B(z, 0))| = \prod_{(k, \ell) \in \mathcal{A} \times \mathcal{B}} \text{Resultant}_z(C_k(z), C_\ell(z)). \]

The cyclotomic resultants are integers, so we find that

\[ |\text{Resultant}_z(C_k(z), C_\ell(z))| = 1 \quad \text{for all } (k, \ell) \in \mathcal{A} \times \mathcal{B}. \] (4.3)

We now put various graph structures on \( \mathcal{D} \) by specifying the pairs of points that are connected by an edge. For example, the graph structure \( \mathcal{D} \times \mathcal{D} \) is the complete graph on \( \mathcal{D} \) in which every vertex (point of \( \mathcal{D} \)) is connected to every other vertex.

Consider first the graph on \( \mathcal{D} \) whose edges are given by the pairs

\[ \mathcal{G}_1 = \{ (k, \ell) \in \mathcal{G} : |\text{Resultant}_z(C_k(z), C_\ell(z))| > 1 \}. \]

(By abuse of terminology, we will call \( \mathcal{G}_1 \) a graph.) It follows from (4.3) that in \( \mathcal{G}_1 \), there are no edges connecting a point in \( \mathcal{A} \) to a point in \( \mathcal{B} \), so the graph \( \mathcal{G}_1 \) is disconnected.

But then the graph

\[ \mathcal{G}_2 = \{ (k, \ell) \in \mathcal{G} : k \neq \ell, k \mid \ell, |\text{Resultant}_z(C_k(z), C_\ell(z))| > 1 \}. \]
4.3. IRREDUCIBILITY AND GENUS FORMULAS 73

is also disconnected, since the edges in $G_2$ are a subset of the edges in $G_1$. We now observe that if $k \neq \ell$ and $k \mid \ell$, then

$$\text{Resultant}_z(C_k(z), C_\ell(z)) > 1 \iff \ell/k \text{ is a prime power.}$$

Hence the graph

$$G_3 = \{(k, \ell) \in G : k \neq \ell, \ k \mid \ell, \ \ell/k \text{ is a prime power}\}$$

is also disconnected, since $G_3 \subset G_2$.

The final part of the proof is to obtain a contradiction by showing that $G_3$ is connected. Let $N = 2^n - 1$, and factor $N$ as

$$N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

After possibly relabeling the primes, Lemma 4.13 tells us that $p_1^{e_1} \mid 2^d - 1$ for all $d \mid n$ with $d < n$.

Hence if $E$ is any divisor of $N$ with $\text{ord}_{p_1}(E) = e_1$, then the definition of $D$ implies that $E \in D$.

We now show that an arbitrary element $D \in D$ is connected to the point $N \in D$ in the graph $G_3$, which will show that $G_3$ is connected. We factor $D$ as

$$D = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r},$$

with $0 \leq f_i \leq e_i$. For each $0 \leq j \leq r$, let

$$D_j = p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j} p_{j+1}^{f_{j+1}} \cdots p_r^{f_r},$$

where by convention we set $D_0 = N$. For $j \geq 1$ we have $\text{ord}_{p_1}(D_j) = e_j$, so our earlier discussion implies that $D_j \in D$, and of course $D_0 = D \in D$ by assumption. Further, we have

$$\frac{D_{j+1}}{D_j} = p_j^{e_j - f_j},$$

so either $D_{j+1} = D_j$, or $D_{j+1}/D_j$ is a prime power. Letting $j_1 < j_2 < \cdots < j_t$ be the values of $j$ satisfying $D_{j+1} \neq D_j$, we see that

$$(D_{j_u}, D_{j_{u+1}}) \in G_3 \text{ for all } 1 \leq u < t,$$

and that the list of pairs

$$(D_{j_1}, D_{j_2}), (D_{j_2}, D_{j_3}), \ldots, (D_{j_{t-1}}, D_{j_t}) \in G_3$$

gives a path connecting $D$ to $N$. This proves that $G_3$ is connected, contradicting our earlier proof that $G_3$ is disconnected. Hence $\Phi_n(z, c)$ is irreducible, which completes the proof of Theorem 4.12.

The genera of $X_0(n)$ and $X_1(n)$ grow quite rapidly, as indicated in the following table.

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>genus $X_0(n)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>14</td>
<td>34</td>
<td>124</td>
</tr>
<tr>
<td>genus $X_1(n)$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>