PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 5, May 2009, Pages 1543–1549
S 0002-9939(08)09750-5
Article electronically published on November 12, 2008

INTERSECTION OF MODULAR POLYNOMIALS

JIE LING

(Communicated by Wen-Ching Winnie Li)

Abstract. In this paper, we consider the intersection of classic modular polynomials. The intersection number on affine space is given by the well-known Hurwitz class numbers. We give two different ways to compute the intersection number by two different compactifications of $\mathbb{A}^2$. This yields a new and more elementary formula for the intersection number. Consequently we get a class number relation. We also give a pure combinatorial proof of this class number relation.

1. Introduction

Let $j = j(\tau)$ be the elliptic modular function on the upper half-plane. For $m \geq 1$ let $\phi_m(j, j') \in \mathbb{Z}[j, j']$ be the classical *modular polynomials*, defined by

$$\phi_m(j, j') = \phi_m(j(\tau), j(\tau')) = \prod_{\det A = m,\, A \in SL_2(\mathbb{Z})\backslash M_2(\mathbb{Z})} (j(\tau) - j(A\tau')). \tag{1.1}$$

The product in (1.1) is taken over the finite set of equivalence classes of integral matrices A of determinant m under the action of $SL_2(\mathbb{Z})$ on the left. It's well-known that ϕ_m is an integral polynomial (see e.g. [2] or [3]). But in general, it's not irreducible; in fact we have the factorization

$$\phi_m = \prod_{n^2 | m} \psi_{m/n^2}, \tag{1.2}$$

where ψ_m is defined by the product in (1.1) taken over the equivalence classes of primitive matrices, i.e., those that don't factor through multiplication-by-n. The polynomials ψ_m are absolutely irreducible.

Kronecker and Hurwitz established a number of important properties of the modular polynomials ϕ_m. Since there are exactly $\sigma_1(m) = \sum_{d|m} d$ orbits for the left action of $SL_2(\mathbb{Z})$ on the integral matrices of determinant m, we have the degree formula

$$\deg \phi_m(j, \alpha) = \sigma_1(m)$$

for all $\alpha \in \mathbb{C}$. When m is not a square, the polynomial

$$f_m(j) = \phi_m(j, j)$$

Received by the editors June 18, 2008.
2000 *Mathematics Subject Classification.* Primary 11G18, 14G35.
Key words and phrases. Intersection number, modular polynomial.

is non-zero and has a simple degree formula

$$\deg f_m(j) = \sum_{ad=m} \max\{a, d\}. \tag{1.3}$$

Now, let's consider the affine space defined by $\mathbb{A}^2 = \operatorname{Spec} \mathbb{C}[j, j']$, and let T_m be the divisor defined by $\phi_m = 0$. Then, (1.3) can be interpreted as the intersection formula

$$(T_1 \cdot T_m)_{\mathbb{A}^2} = \sum_{ad=m} \max\{a, d\} \tag{1.4}$$

if m is not a square. Here the intersection is defined by

$$(T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} = \dim_{\mathbb{C}} \mathbb{C}[j, j']/(\phi_{m_1}, \phi_{m_2}).$$

More generally, Hurwitz showed that the divisors T_{m_1}, T_{m_2} intersect properly on $\mathbb{A}^2$ if and only if $m_1 m_2$ is not a square, and in this case he gave an explicit expression

$$(T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} = \sum_{t\in\mathbb{Z}\ t^2<4m_1m_2} \sum_{d|\gcd\{m_1,m_2,t\}} d \cdot H(\frac{4m_1m_2 - t^2}{d^2}). \tag{1.5}$$

Here $H(D)$ denotes the Hurwitz class number, the number of $SL_2(\mathbb{Z})$-equivalent classes of positive definite binary quadratic form over $\mathbb{Z}$ with determinant D, counting the forms equivalent to $ex^2 + ey^2$ and $ex^2 + exy + ey^2$ with multiplicities $1/2$ and $1/3$, respectively. The basic idea is that the intersection $T_{m_1} \cdot T_{m_2}$ is supported on pairs of CM Elliptic Curves, then counting the local intersection number over all these pairs. Combined with (1.4), when $m_1 = 1$, $m_2 = m$ is not a square, we have the class number relation

$$\sum_{t\in\mathbb{Z}\ t^2<4m} H(4m - t^2) = \sum_{ad=m} \max\{a, d\}. \tag{1.6}$$

In this paper, we give another expression for the intersection formula in (1.5), which should be considered as a generalization of (1.4).

Theorem 1.1. *If $m = m_1 m_2$ is not a perfect square, we have the intersection formula*

$$(T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} = \sum_{a_1d_1=m_1} \sum_{a_2d_2=m_2} \max\{a_1d_2, a_2d_1\}. \tag{1.7}$$

Combined with (1.5), as a consequence, we get a class number relation:

Corollary 1.1. *If $m = m_1 m_2$ is not a perfect square, we have the class number relation*

(1.8)

$$\sum_{t\in\mathbb{Z}\ t^2<4m_1m_2} \sum_{d|\gcd\{m_1,m_2,t\}} d \cdot H(\frac{4m_1m_2 - t^2}{d^2}) = \sum_{a_1d_1=m_1} \sum_{a_2d_2=m_2} \max\{a_1d_2, a_2d_1\}.$$

The basic idea to prove Theorem 1.1 is to embed $\mathbb{A}^2$ into the projective space $\mathbb{P}^2$ or $\mathbb{P}^1 \times \mathbb{P}^1$ so that we have

$$(T_{m_1} \cdot T_{m_2})_{\mathbb{P}^1\times\mathbb{P}^1} = (T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} + (T_{m_1} \cdot T_{m_2})_\infty \tag{1.9}$$

and

$$(T_{m_1} \cdot T_{m_2})_{\mathbb{P}^2} = (T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} + (T_{m_1} \cdot T_{m_2})_\infty, \tag{1.10}$$

where ∞ denotes the appropriate complementary space of $\mathbb{A}^2$.

The intersection numbers on both projective spaces are given by the Bézout Theorem. To compute the intersection at infinity, first we observe that they only intersect at certain points and then we can compute the local intersection multiplicities explicitly. In the end, we get the same intersection formula (1.7) with either compactification. As a remark, we notice that Theorem 1.1 can also be derived from its special case (1.4) and the Hurwitz formula by some combinatorial argument. In the last section, we start with the intersection formula of the pair $(T_1 \cdot T_m)_{\mathbb{A}^2}$ to derive the formula (1.7) using a combinatorial approach.

2. Modular polynomials

Letting $m \in \mathbb{N}$, consider the elliptic curve $E = \mathbb{C}/\Gamma$ with $\Gamma = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{H}$. The following is well-known; see e.g. [3].

Proposition 2.1. *There are canonical bijections between the following sets:*

(1) *isomorphism classes of isogenies $\phi : E' \to E$ of degree m,*
(2) *subgroups $\Gamma_1 \subseteq \Gamma$ of index m,*
(3) *$SL_2(\mathbb{Z})\backslash\{M \in M_2(\mathbb{Z})|\ \det M = m\}$, and*
(4) *$\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) | ad = m, a \geq 1$ and $0 \leq b < d\}$.*

All of these sets have $\sigma_1(m) = \sum_{d|m} d$ elements.

Under these bijections we rewrite the modular polynomials as follows. For $j, j' \in \mathbb{C}$, choose elliptic curves E, E' with j-invariants j, j', respectively. Then

$$\phi_m(j, j') = \phi_m(j(E), j(E')) = \prod_{E'_1 \to E'} (j(E) - j(E'_1)), \tag{2.1}$$

where the product is taking over isomorphism classes of isogenies of degree m. For elliptic curves E, E', the condition $\phi_m(j(E), j(E')) = 0$ is equivalent to the existence of an isogeny $E \to E'$ of degree m. Similarly, we can define $\psi_m(j, j')$ as the product over all "primitive" isogenies that don't factor through multiplication-by-n for some $n > 1$. Then we have

$$\phi_m = \prod_{n^2|m} \psi_{m/n^2}. \tag{2.2}$$

It's obvious that $\phi_1(x, y) = \psi_1(x, y) = x - y$. We will frequently use $x = j, y = j'$. The following is also well-known and can be found in [3].

Proposition 2.2. *The following are true:*

(1) *$\phi_m(x, y), \psi_m(x, y) \in \mathbb{Z}[x, y]$.*
(2) *$\psi_m(x, t)$ is irreducible over $\mathbb{C}(t)$.*
(3) *For $m > 1$, $\psi_m(x, y)$ is symmetric. When $m = 1$, $\phi_1(x, y) = \psi_1(x, y) = x - y$.*
(4) *One has*

$$\deg_x \phi_m(x, y) = \deg_y \phi_m(x, y) = \sigma_1(m),$$
$$\deg \phi_m(x, y) = \sum_{ad=m} \max\{a, d\}.$$

3. Intersection of modular polynomials

Let T_m denote the divisor or the curve defined by $\phi_m = 0$. We don't specify the space in which it lies; it might be $\mathbb{A}^2$, $\mathbb{P}^2$ or $\mathbb{P}^1 \times \mathbb{P}^1$. Hurwitz computed the intersection number of different divisors in the affine space $\mathbb{A}^2$; see [1].

Theorem 3.1 (Hurwitz)**.** *In the affine space $\mathbb{A}^2$, the curves T_{m_1}, T_{m_2} intersect properly if and only if the integer $m = m_1 m_2$ is not a perfect square. In this case the intersection $T_{m_1} \cdot T_{m_2}$ is supported on the zero-cycle of points (E, E') corresponding to pairs of elliptic curves with complex multiplication by orders whose discriminants $d(E), d(E') \geq -4m$. Moreover, the intersection number is given by*

$$(T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} = \sum_{t \in \mathbb{Z} \ t^2 < 4m_1 m_2} \sum_{d | \gcd\{m_1, m_2, t\}} d \cdot H(\frac{4m_1 m_2 - t^2}{d^2}).$$

For the rest of the paper, we always assume that $m = m_1 m_2$ is not a perfect square.

Let $\mathbb{P}^1 \times \mathbb{P}^1 = \text{Proj } \mathbb{C}[X : U; Y : V]$ be one compactification of $\mathbb{A}^2 = \text{Spec } \mathbb{C}[x, y]$, where $x = \frac{X}{U}, y = \frac{Y}{V}$. Now we consider T_m as a compactified curve in the space $\mathbb{P}^1 \times \mathbb{P}^1$. They intersect properly under the same condition. But, when they intersect. properly, they may intersect extra points which are not in $\mathbb{A}^2$. We can decompose $\mathbb{P}^1 \times \mathbb{P}^1$ into $\mathbb{A}^2 \cup \mathbb{A}^1 \times \{\infty\} \cup \{\infty\} \times \mathbb{A}^1 \cup \{(\infty, \infty)\}$. Thanks to Proposition 2.1(4), we can express the modular polynomial as

(3.1)

$$\phi_m(j(\tau), j(\tau')) = \prod_{\det A = m, A \in SL_2(\mathbb{Z}) \backslash M_2(\mathbb{Z})} (j(\tau) - j(A\tau')) = \prod_{a,b,d} (j(\tau) - j(\frac{a\tau' + b}{d})),$$

where the product is taking over the representatives in Proposition 2.1(4). Look at each branch $(j(\tau) - j(\frac{a\tau'+b}{d}))$. They don't intersect at any point on $\mathbb{A}^1 \times \{\infty\} \cup \{\infty\} \times \mathbb{A}^1$, the only possible intersection point outside $\mathbb{A}^2$ being (∞, ∞). So we have

$$(T_{m_1} \cdot T_{m_2})_{\mathbb{P}^1 \times \mathbb{P}^1} = (T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} + (T_{m_1} \cdot T_{m_2})_{(\infty, \infty)}. \tag{3.2}$$

To compute the intersection number on $\mathbb{P}^1 \times \mathbb{P}^1$ is rather easy by the Bézout Theorem and Proposition 2.2.

Lemma 3.1. *The intersection number on the space $\mathbb{P}^1 \times \mathbb{P}^1$ is given by*

$$(T_{m_1} \cdot T_{m_2})_{\mathbb{P}^1 \times \mathbb{P}^1} = 2\sigma_1(m_1)\sigma_1(m_2).$$

Proof. Consider the Picard group of $\mathbb{P}^1 \times \mathbb{P}^1$:

$$\text{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) = \text{Pic}(\mathbb{P}^1) \times \text{Pic}(\mathbb{P}^1) = \mathbb{Z} \times \mathbb{Z}.$$

More precisely, we can choose two generators H_1 and H_2 to be the divisors given by $U = 0$ and $V = 0$ respectively. We have the following well-defined bilinear pairing:

$$\begin{array}{ccc} \text{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) \times \text{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) & \longrightarrow & \mathbb{Z} \\ (D_1, D_2) & \mapsto & (D_1 \cdot D_2)_{\mathbb{P}^1 \times \mathbb{P}^1}. \end{array}$$

It is clear that $(H_1 \cdot H_2)_{\mathbb{P}^1 \times \mathbb{P}^1} = 1$ since $U \cdot V = \{(\infty, \infty)\}$. To compute the self-intersection number $(H_1 \cdot H_1)_{\mathbb{P}^1 \times \mathbb{P}^1}$, we notice that H_1 is equivalent to the divisors defined by $X = 0$, but these two parallel divisors have no intersection, so the self-intersection number is 0. For the same reason, $(H_2 \cdot H_2)_{\mathbb{P}^1 \times \mathbb{P}^1}$ is also 0.

Recall from Proposition 2.2(4) that the divisor T_m is linearly equivalent to $\sigma_1(m)H_1 + \sigma_1(m)H_2$, so the intersection number

$$\begin{aligned}(T_{m_1} \cdot T_{m_2})_{\mathbb{P}^1\times\mathbb{P}^1} &= ((\sigma_1(m_1)H_1 + \sigma_1(m_1)H_2) \cdot (\sigma_1(m_2)H_1 + \sigma_1(m_2)H_2))_{\mathbb{P}^1\times\mathbb{P}^1}\\ &= 0 + \sigma_1(m_1)\sigma_1(m_2) + \sigma_1(m_1)\sigma_1(m_2) + 0\\ &= 2\sigma_1(m_1)\sigma_1(m_2). \qquad \square\end{aligned}$$

To get a formula for the intersection on affine space, we still need to calculate the local intersection multiplicity at infinity. We have the following formula.

Lemma 3.2. *The local intersection of $T_{m_1} \cdot T_{m_2}$ at infinity is*

$$(T_{m_1} \cdot T_{m_2})_{(\infty,\infty)} = \sum_{a_1d_1=m_1}\sum_{a_2d_2=m_2} \min\{a_1d_2, a_2d_1\}.$$

Proof. At (∞,∞), we can use local parameters $s = 1/j, t = 1/j'$. By Proposition 2.1 both $\deg_x \phi_{m_i}$ and $\deg_y \phi_{m_i}$ are $\sigma_1(m_i)$ and we can write

$$\frac{\phi_{m_i}(j,j')}{j^{\sigma_1(m_i)}j'^{\sigma_1(m_i)}} = \widetilde{\phi}_{m_i}(s,t) \in \mathbb{C}[s,t].$$

Now consider the (s,t)-plane, where $(0,0)$ corresponds to the maximal ideal $M = (s,t) \subseteq \mathbb{C}[s,t]$, and consider the completion of the localization $\mathbb{C}[s,t]_M$ at M which is the formal power series ring $\mathbb{C}[[s,t]]$. So, by definition the local intersection multiplicity is given by

$$(T_{m_1} \cdot T_{m_2})_{(\infty,\infty)} = (\widetilde{\phi}_{m_1} \cdot \widetilde{\phi}_{m_2})_{(0,0)} = \dim_{\mathbb{C}} \mathbb{C}[[s,t]]/(\widetilde{\phi}_{m_1}, \widetilde{\phi}_{m_2}).$$

Recall that the classical q-expansion of the modular function is

$$j(\tau) = q^{-1} + 744 + 196884q + \dots,$$

where $q = e^{2\pi i\tau}$. So we have

$$\begin{aligned}s &= \frac{1}{j} = q - 744q^2 - 750420q^3 + \dots,\\ t &= \frac{1}{j'} = q' - 744q'^2 - 750420q'^3 + \dots\end{aligned}$$

and

$$\mathbb{C}[[s,t]] = \mathbb{C}[[q,q']].$$

Recall equation (3.1). We have

$$\widetilde{\phi}_{m_i}(s,t) = \frac{\phi_{m_i}(j,j')}{j^{\sigma_1(m_i)}j'^{\sigma_1(m_i)}} = \prod_{a,b,d}\Big(\frac{1}{j'^{a/d}} - \frac{j(\frac{a\tau'+b}{d})}{j'^{a/d}}\frac{1}{j}\Big).$$

Now consider the extension $\mathbb{C}[[q,r]]$ of $\mathbb{C}[[q,q']]$, where

$$r^l = \frac{1}{j'} = q' - 744q'^2 - 750420q'^3 + \dots, \qquad l = \operatorname{lcm}(m_1,m_2).$$

The advantage to working with $\mathbb{C}[[q,r]]$ is that each factor $(\frac{1}{j'^{a/d}} - \frac{j(\frac{a\tau'+b}{d})}{j'^{a/d}}\frac{1}{j})$ is inside $\mathbb{C}[[q,r]]$. Both $j(\frac{a\tau'+b}{d})$ and $j'^{a/d}$ have leading term $r^{la/d}$, so $\frac{j(\frac{a\tau'+b}{d})}{j'^{a/d}}$ is invertible in $\mathbb{C}[[q,r]]$. The extension is totally ramified of degree l. For simplicity, we can consider the intersection in $\mathbb{C}[[q,q']]$ with fractional multiplicity. Now we consider the branch intersection

$$\left(\frac{1}{j'^{a_1/d_1}} - \frac{j(\frac{a_1\tau'+b_1}{d_1})}{j'^{a_1/d_1}}\frac{1}{j}, \frac{1}{j'^{a_2/d_2}} - \frac{j(\frac{a_2\tau'+b_2}{d_2})}{j'^{a_2/d_2}}\frac{1}{j}\right)_{(\infty,\infty)},$$

where $a_i d_i = m_i, 0 \leq b_i \leq d_i - 1, for\ i = 1,2$. Since $\frac{j(\frac{a_i\tau'+b_i}{d_i})}{j'^{a_i/d_i}}$ are invertible, and $a_1/d_1 \neq a_2/d_2$ (m is not a perfect square), the branch intersection is $\min\{a_1/d_1, a_2/d_2\}$. Summing over the product we get

$$(T_{m_1} \cdot T_{m_2})_{(\infty,\infty)} = \sum_{a_1,b_1,d_1}\sum_{a_2,b_2,d_2} \min\{\frac{a_1}{d_1}, \frac{a_2}{d_2}\} = \sum_{a_1d_1=m_1}\sum_{a_2d_2=m_2} \min\{a_1d_2, a_2d_1\}.$$

□

First proof of Theorem 1.1. Combining Lemmas 3.1, 3.2 with (3.2), we have

$$\begin{aligned}(T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} &= (T_{m_1} \cdot T_{m_2})_{\mathbb{P}^1\times\mathbb{P}^1} - (T_{m_1} \cdot T_{m_2})_{(\infty,\infty)}\\ &= 2\sigma_1(m_1)\sigma_1(m_2) - \sum_{a_1d_1=m_1}\sum_{a_2d_2=m_2} \min\{a_1d_2, a_2d_1\}\\ &= \sum_{a_1d_1=m_1}\sum_{a_2d_2=m_2} \max\{a_1d_2, a_2d_1\}.\end{aligned}$$

Taking $m_1 = 1, m_2 = m$ gives (1.4). □

Remark 3.3. We can consider another compactification of $\mathbb{A}^2$: $\mathbb{P}^2 = \text{Proj}\ \mathbb{C}[X:Y:Z]$, which can also be used to prove Theorem 1.1. The computation is quite similar to the case of $\mathbb{P}^1 \times \mathbb{P}^1$, so we just omit it.

4. A combinatorial approach

In this section, we use Theorem 3.1 and (1.4) (which is a special case of Theorem 1.1) to derive Theorem 1.1 by a combinatorial approach. Assume $m = m_1m_2$ is not a perfect square. Then one has by Theorem 3.1 and (1.4)

$$\begin{aligned}(T_{m_1} \cdot T_{m_2})_{\mathbb{A}^2} &= \sum_{t\in\mathbb{Z}\ t^2<4m_1m_2}\sum_{c|\gcd\{m_1,m_2,t\}} c \cdot H(\frac{4m_1m_2 - t^2}{c^2})\\ &= \sum_{c|\gcd\{m_1,m_2\}} c \sum_{t\in\mathbb{Z}\ t^2<\frac{4m_1m_2}{c^2}} H(\frac{4m_1m_2 - t^2}{c^2})\\ &= \sum_{c|\gcd\{m_1,m_2\}} c \sum_{a'd'=\frac{m_1m_2}{c^2}} \max\{a', d'\}\\ &= \sum_{c|\gcd\{m_1,m_2\}}\sum_{a'd'=\frac{m_1m_2}{c^2}} \max\{ca', cd'\}.\end{aligned}$$

Now, all we have to do is check

$$\sum_{a_1d_1=m_1}\sum_{a_2d_2=m_2} \max\{a_1d_2, a_2d_1\} = \sum_{c|\gcd\{m_1,m_2\}}\sum_{a'd'=\frac{m_1m_2}{c^2}} \max\{ca', cd'\}. \tag{4.1}$$

On both sides, (a_1d_2, a_2d_1) and (ca', cd') are decompositions of m. For any decomposition $m = st$, and let's count how often $(a_1d_2, a_2d_1) = (s,t)$ and how often $(ca', cd') = (s, t)$, let's denote them by $\lambda_{left}(s, t)$ and $\lambda_{right}(s, t)$, respectively. A simple calculation shows that

$$\lambda_{left}(s, t) = \lambda_{right}(s, t) = \sigma_0(\gcd\{m_1, m_2, s, t\}), \tag{4.2}$$

where $\sigma_0(m)$ denotes the number of divisors of m. So (4.1) holds, which proves Theorem 1.1 again.

Acknowledgment

The author thanks Tonghai Yang for his encouragement, helpful discussions, careful reading of this paper and helpful suggestions which made the exposition of this paper much better.

References

1. Gross, Benedict H.; Keating, Kevin, *On the intersection of modular correspondences*, Inventiones Mathematicae **112** (1993), 225-245. MR1213101 (94h:11046)
2. Lang, Serge, *Elliptic Functions*, Addison-Wesley, Reading, MA, 1973. MR0409362 (53:13117)
3. Vogel, Gunther, *Modular polynomials*, Astérisque No. 312, 2007. MR2340366 (2008h:11041)

Department of Mathematics, University of Wisconsin-Madison, Madison, Wisconsin 53705

E-mail address: ling@math.wisc.edu