Astérisque
312, 2007, p. 1–7

2. MODULAR POLYNOMIALS

by

Gunther Vogel

Abstract. — We introduce the classical modular polynomials and calculate (modulo the determination of a certain sum of representation numbers) the intersection number of two divisors defined by modular polynomials (Hurwitz's theorem).

***Résumé* (Polynômes modulaires).** — On introduit les polynômes modulaires classiques et détermine (modulo le calcul d'une certaine somme de nombres de représentations) le nombre d'intersection de deux diviseurs définis par des polynômes modulaires (théorème de Hurwitz).

We introduce modular polynomials and prove some elementary properties. This is classical and well-known, see e.g. [**L**, §5]. In the second part, we compute the intersection numbers of the divisors defined by two modular polynomials in the 2-dimensional complex plane. This computation, due to Gross and Keating ([**GK**]), re-proves the class number relations of Kronecker (Corollary 2.2).

We only consider elliptic curves over $\mathbb{C}$.

1. Modular Polynomials

Let $m \in \mathbb{N}$. Consider the elliptic curve $E = \mathbb{C}/\Gamma$ with $\Gamma = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{H}$.

Theorem 1.1 **([L, §5.3,5.1]).** — *There are canonical bijections between the following sets:*

(i) *isomorphism classes of isogenies $f\colon E_1 \to E$ of degree m (as group schemes over E),*
(ii) *subgroups $\Gamma_1 \subseteq \Gamma$ of index m,*

2000 ***Mathematics Subject Classification.*** — 11F32, 11F03, 11G15.
Key words and phrases. — Modular polynomials, representation number of a quadratic form, class number relations.

(iii) $\mathrm{SL}_2(\mathbb{Z})\backslash\{A \in M_2(\mathbb{Z}) \mid \det A = m\}$, *and*
(iv) $\left\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \,\middle|\, ad = m,\ a \geq 1 \text{ and } 0 \leq b < d\right\}$.
All of these sets have $\sigma_1(m) = \sum_{d|m} d$ *elements.*

Proof
(i)→(ii): Set $\Gamma_1 := f_*\pi_1(E_1)$. (ii)→(i): Set $E_1 := \mathbb{C}/\Gamma_1$.
(ii)↔(iii): Choose a basis $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ \tau \end{smallmatrix}\right)$ of Γ_1 with $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$.
(iii)↔(iv): Left multiplication by matrices from $\mathrm{SL}_2(\mathbb{Z})$ corresponds to row operations. The matrices in (iv) are obviously inequivalent (the columns must be stabilized). □

Now consider pairs (j, j') of j-invariants of elliptic curves E, E' such that there is an isogeny $E \to E'$ of degree m. These pairs are described by the divisor of a certain polynomial φ_m:

For $j, j' \in \mathbb{C}$ choose elliptic curves E, E' having j-invariants j, j', respectively. Set

$$\varphi_m(j, j') = \varphi_m(j(E), j(E')) := \prod_{E_1' \to E'} (j(E) - j(E_1'));$$

the product is over isomorphism classes of isogenies $E_1' \to E'$ of degree m. φ_m does not depend on the choices made and is a polynomial of degree $\sigma_1(m)$ in j. For elliptic curves E, E', the condition $\varphi_m(j(E), j(E')) = 0$ is equivalent to the existence of an isogeny $E \to E'$ of degree m.

Define $\psi_m(j, j')$ by the same formula, but restrict the product to the isogenies which do not factor over some multiplication-by-n map, $n > 1$. In the above correspondence, these isogenies correspond to primitive matrices, i. e., matrices whose entries have no common divisor. We have

$$\varphi_m = \prod_{n^2|m} \psi_{m/n^2}.$$

Obviously, $\varphi_1(X, Y) = \psi_1(X, Y) = X - Y$. As we will see below, φ_m and ψ_m are polynomials; they are called *modular polynomials*.

Theorem 1.2 **([L, §5.2])**
(i) $\varphi_m, \psi_m \in \mathbb{Z}[X, Y]$.
(ii) $\psi_m(X, t)$ *is irreducible over* $\mathbb{C}(t)$.
(iii) *For* $m > 1$, *we have* $\psi_m(X, Y) = \psi_m(Y, X)$. *Consequently,* $\varphi_m(X, Y) = \pm\varphi_m(Y, X)$ *("−" precisely if* m *is a square).*

Proof
(i) First notice that the coefficients k_i of

$$\psi_m(X, j(\tau')) = \prod_{\mathrm{SL}_2(\mathbb{Z})\backslash\{A \in M_2(\mathbb{Z}) | \det A = m,\ A \text{ primitive}\}} (X - j(A\tau')) \in \mathcal{O}_{\mathbb{C}}[X]$$

are holomorphic in τ' and invariant under $\mathrm{SL}_2(\mathbb{Z})$. From the formula

$$(*) \qquad \psi_m(X, j(\tau')) = \prod_{a,b,d} \Big(X - j\Big(\frac{a\tau'+b}{d}\Big)\Big) = \prod_{a,b,d} \Big(X - \frac{1}{(q')^{a/d}\zeta_m^{ab}} - 744 - \dots\Big)$$

(a, b, d as in 1.1 (iv) and $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ primitive, $\zeta_m := \mathrm{e}^{2\pi\mathrm{i}/m}$) we see that the k_i are meromorphic at infinity. Since the q-expansion of the j-function has integral coefficients, we have

$$k_i \in \mathbb{Z}[\zeta_m][[q']]\Big[\frac{1}{q'}\Big].$$

Now there are polynomials $p_i \in \mathbb{Z}[\zeta_m, T]$ such that $k_i - p_i(j(q'))$ lies in $q'\mathbb{Z}[\zeta_m][[q']]$ and therefore, being a modular function, must vanish identically. Hence, $\psi_m \in \mathbb{Z}[\zeta_m][X, Y]$.

There are two operations of $(\mathbb{Z}/m\mathbb{Z})^\times$: first, on matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ as in 1.1 (iv) by

$$\sigma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} := \begin{pmatrix} a & \sigma b \\ 0 & d \end{pmatrix} \quad (\text{via } (\mathbb{Z}/d\mathbb{Z})^\times \text{ on } \{0, \dots, d-1\} \cong \mathbb{Z}/d\mathbb{Z}),$$

and the first product in $(*)$ is invariant under this operation. Second, $(\mathbb{Z}/m\mathbb{Z})^\times$ operates in a compatible way on $\mathbb{Z}[\zeta_m]$ by $\sigma\zeta_m = \zeta_m^\sigma$, and since the coefficients of φ_m are invariant under this operation, we find that $\psi_m \in \mathbb{Z}[X, Y]$.

(ii) By mapping $t \mapsto j$, the field of meromorphic functions on $\mathbb{H}$ becomes an extension field of $\mathbb{C}(t)$ carrying an operation of the group $\mathrm{SL}_2(\mathbb{Z})$. By the elementary divisors theorem, it permutes the zeroes of $\psi_m(X, t)$ transitively, hence $\psi_m(X, t)$ is irreducible over $\mathbb{C}(t)$.

(iii) The condition $\psi_m(j(E), j'(E)) = 0$ is equivalent to the existence of an isogeny $E \to E'$ of degree m which does not factor over a multiplication-by-n map for some $n > 1$. This last property is also true for its dual isogeny, hence $\psi_m(j(E'), j(E)) = 0$. For a fixed j_0', the irreducible polynomial $\psi_m(X, j_0')$ is therefore a divisor of $\psi_m(j_0', X)$, and conversely. It follows that $\psi_m(j, j') = \pm\psi_m(j', j)$. If the "$-$" sign is correct, $\psi_m(t, t)$ vanishes identically, so $\psi_m(X, t)$ has a zero in $\mathbb{C}(t)$, hence the degree of $\psi_m(X, t)$ must be 1. This is true precisely for $m = 1$. □

From the proof of (iii) we also see that $f_m(X) := \varphi_m(X, X)$ vanishes if and only if m is a square. If m is not a square, the degree of f_m can be read off the q-expansion in $(*)$: set $X = j(q')$, then because of $a \neq d$, the pole order of one factor is equal to $\max\{1, a/d\}$, hence the pole order of the entire product is

$$\deg f_m = \sum_{ad=m} d \max\{1, a/d\} = \sum_{ad=m} \max\{a, d\}.$$

One also sees that the leading coefficient of f_m is ± 1.

2. Intersections

We first need to fix some notation. A quadratic space (L, Q) over a ring R consists of a free R-module L of finite rank and a quadratic form Q on L. The associated bilinear form on L is defined by

$$(x, y) = Q(x + y) - Q(x) - Q(y).$$

The determinant of Q is the element of $R/(R^\times)^2$ given by the determinant of the matrix $((b_i, b_j))_{ij}$ for some basis $\{b_i\}$ of L. The diagonal of Q with respect to some fixed basis $\{b_i\}$ is defined to be the n-tuple $(Q(b_i))_i$ where n is the rank of L.

For a quadratic form F on R^m, we define the representation number $R_L(F)$ as the cardinality of the set

$$\begin{aligned}&\{(f_i) \in L^m \mid Q(x_1 f_1 + \cdots + x_m f_m) = F(x_1, \ldots, x_m) \text{ for all } x \in R^m\}\\ &= \{\text{isometries } (R^m, F) \to (L, Q)\}.\end{aligned}$$

For $R = \mathbb{Z}$ and positive definite Q, this set is finite. (For each $x = e_i$, $i = 1, \ldots, m$, there are only finitely many possible values of $x_1 f_1 + \cdots + x_m f_m = f_i$.)

For a positive integer D, let $H(D)$ be the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of positive definite binary quadratic forms over $\mathbb{Z}$ with determinant D (which is well-defined as an element of $\mathbb{Z}$), counting the forms equivalent to $ex_1^2 + ex_2^2$ and $ex_1^2 + ex_1x_2 + ex_2^2$ for some natural number e with multiplicities $1/2$ and $1/3$, respectively. If the positive integer m is not a square, we define

$$G(m) := \sum_{\substack{t \in \mathbb{Z} \\ t^2 \le 4m}} H(4m - t^2).$$

Define $T_m := V(\varphi_m) \subset \mathbb{A}^2_{\mathbb{C}}$.

Theorem 2.1 **([GK, 2.4])**. — *The curves T_{m_1} and T_{m_2} intersect properly if and only if $m = m_1 m_2$ is not a square. In this case, their intersection is supported on pairs (E, E') of elliptic curves with complex multiplication by orders whose discriminants satisfy $d(E), d(E') \ge -4m$. The intersection number is*

$$T_{m_1} \cdot T_{m_2} = \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4m}} \sum_{d \mid \gcd(m_1, m_2, t)} d \cdot H\Big(\frac{4m - t^2}{d^2}\Big) = \sum_{n \mid \gcd(m_1, m_2)} n \cdot G(m/n^2).$$

Proof. — If $m = m_1 m_2$ is a square, T_{m_1} and T_{m_2} contain $V(\psi_g)$, $g = \gcd(m_1, m_2)$, as a common component (note that m_1/g and m_2/g are coprime, hence squares themselves). Conversely, if T_{m_1} and T_{m_2} do not intersect properly, they must contain some $V(\psi_g)$ as a common component, but then $g = m_1/n_1^2 = m_2/n_2^2$, so $m = g^2 n_1^2 n_2^2$ is a square.

For a pair of elliptic curves (E, E') corresponding to an intersection point of T_{m_1} and T_{m_2}, there are isogenies $f_1, f_2 \colon E \to E'$ of degrees m_1 and m_2, respectively. Then, $\alpha := {}^t f_2 f_1$ is an endomorphism of E of degree m. Since m is not a

square, E has complex multiplication, and $\mathbb{Z}+\mathbb{Z}\alpha$ is a sublattice of $\operatorname{End} E$. Hence, its discriminant $(\operatorname{Tr}\alpha)^2-4m<0$ is divisible by $d(E)$, so

$$d(E)\geq(\operatorname{Tr}\alpha)^2-4m\geq -4m.$$

Similarly, considering $\beta:=f_2{}^t f_1$, it follows that $d(E')\geq -4m$.

Next, we compute the local intersection number at some point $(j_0,j_0')\in\mathbb{C}^2$ corresponding to a pair of elliptic curves (E,E'). Set $u_E:=\frac{1}{2}\#\operatorname{Aut}E$, similarly for E'. Choose $\tau_0'\in\mathbb{H}$ such that $j(\tau_0')=j_0'$. Locally at τ_0', the map $j\colon\mathbb{H}\to\mathbb{C}$ is a branched covering of degree $u_{E'}$, so the local intersection number in the (j,j')-plane is the intersection number in the (j,τ')-plane divided by $u_{E'}$.

In the (j,τ')-plane, the φ_{m_i} decompose into factors of the form

$$j-j(A_i\tau')\qquad\text{where } A_i\in M_2(\mathbb{Z}),\ \det A_i=m_i.$$

Therefore, it suffices to compute the local intersection number of two such factors, both vanishing at (j_0,τ_0'). This number is the zero order of

$$(**)\qquad\qquad j(A_1\tau')-j(A_2\tau')$$

at $\tau'=\tau_0'$. Since $A_1\tau_0'$ and $A_2\tau_0'$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent, we may assume that $A_1\tau_0'=A_2\tau_0'=:\tau_0$ and $c_2=0$. Locally at τ_0,

$$j(\tau)=j(\tau_0)+s\cdot(\tau-\tau_0)^{u_E}+\text{higher order terms}$$

for some $s\neq 0$, hence $(**)$ is of the form

$$\begin{aligned}&s\Big(\frac{a_1\tau'+b_1}{c_1\tau'+d_1}-\frac{a_1\tau_0'+b_1}{c_1\tau_0'+d_1}\Big)^{u_E}-s\Big(\frac{a_2\tau'+b_2}{d_2}-\frac{a_2\tau_0'+b_2}{d_2}\Big)^{u_E}+\text{h. o. t.}\\ &=s\Big(\frac{\det A_1}{(c_1\tau_0'+d_1)^2}\cdot(\tau'-\tau_0')\Big)^{u_E}-s\Big(\frac{\det A_2}{d_2^2}\cdot(\tau'-\tau_0')\Big)^{u_E}+\text{h. o. t.}\end{aligned}$$

locally at τ_0'. We now claim that the two leading coefficients are different. (However, they have the same absolute value.) Otherwise, from

$$s\Big(\frac{\det A_1}{(c_1\tau_0'+d_1)^2}\Big)^{u_E}=s\Big(\frac{\det A_2}{d_2^2}\Big)^{u_E}$$

we get

$$\frac{c_1\tau_0'+d_1}{\sqrt{m_1}}=\omega\cdot\frac{d_2}{\sqrt{m_2}}$$

for some $2u_E$-th root of unity ω, implying

$$(***)\qquad\qquad c_1\tau_0'+d_1=\omega\cdot\frac{\sqrt{m_1m_2}}{a_2}.$$

The left-hand side is imaginary-quadratic, so by our assumption that $m=m_1m_2$ is not a square it follows that $\omega=\pm\mathrm{i}$ and $u_E=2$. But in this case, τ_0' corresponds to an elliptic curve isogenous to $E\cong\mathbb{C}/\langle 1,\mathrm{i}\rangle$, hence $\tau_0'\in\mathbb{Q}(\mathrm{i})$, contradicting $(***)$. Hence, the zero order of $(**)$ at τ_0' equals u_E.