Explicit Construction of the Hilbert Class Fields of Imaginary Quadratic Fields with Class Numbers 7 and 11

*Erich Kaltofen**

University of Toronto
Department of Computer Science
Toronto, Ontario M5S1A4, Canada

and

*Noriko Yui**

University of Toronto
Department of Mathematics
Toronto, Ontario M5S1A1, Canada

Extended Abstract

In this note we summarize the progress made so far on using the Computer Algebra System MACSYMA [10] to explicitly calculate the defining equations of the Hilbert class fields of imaginary quadratic fields with prime class number. Our motivation for undertaking this investigation is to construct rational polynomials with a given finite Galois group. The groups we try to realize here are the dihedral groups D_p for primes p. These groups are non-abelian groups of order $2p$ and are generated by two elements

$$\sigma = (1\ 2\ 3 \cdots p) \text{ and } \tau = (1)(2\ \ p)(3\ \ p-1) \cdots (\frac{p+1}{2}\ \ \frac{p+3}{2})$$

with the relation $\tau\sigma\tau = \sigma^{-1}$, as subgroups of the permutation groups of degree p. These groups are solvable and thus can be realized as Galois groups. The problem is to construct, for a given prime p, an integer polynomial with Galois group D_p.

1. C. U. Jensen and N. Yui have found the following effective characterization for polynomials to have Galois group D_p.

Theorem (cf. Jensen and Yui [7, Theorem II.1.2]): Let $f(x)$ be a monic integral polynomial of degree p, where p is an odd prime. Assume that $p \equiv 1$ modulo 4 and that the Galois group of f is not the cyclic group of order p (*resp. assume that* $p \equiv 3$ *modulo* 4). Then necessary and sufficient conditions that the Galois group of f is D_p are:

* This research was partially supported by the National Science and Engineering Research Council of Canada under grant 3-643-126-90 (the first author) and under grant 3-661-114-30 (the second author).
First author's current address: Rensselaer Polytechnic Institute, Department Mathematical Sciences, Troy, New York, 12181.

(1) f is irreducible over the ring $\mathbf{Z}$ of integers.

(2) The discriminant of f is a perfect square (*resp. is not a perfect square*).

(3) The polynomial $g(x) = \prod_{1 \le i < j \le p}(x - \alpha_i - \alpha_j)$, α_i being the roots of f, which is of degree $p(p-1)/2$ and has all integral coefficients, decomposes into a product of $(p-1)/2$ distinct irreducible polynomials of degree p over $\mathbf{Z}$. □

Given an integral polynomial of degree p, it is quite easy to test whether conditions (1) – (3) are satisfied. Both the computation of the discriminant of f and that of the polynomial g can be accomplished by resultant calculations. The exclusion of the cyclic group of order p in the case that $p \equiv 1$ modulo 4 may be more involved but it is, for example, sufficient to establish that f does not have p real roots. For $p = 3$, 5, and 7 polynomials with Galois group D_p are known for at least a century (cf. Weber [12, Sec. 131]).

Unfortunately, extensive search for polynomials of degree 11 satisfying conditions (1) – (3) has not yet produced even one such polynomial. This is, to some extent, not surprising since the polynomial g will, for randomly chosen coefficients, almost always be irreducible due to the Hilbert irreducibility theorem. In order to construct such polynomials we therefore, at the moment, have to rely on the Hilbert class field theory. We shall briefly summarize the theoretic background of our computations.

2. We consider an imaginary quadratic number field $\mathbf{Q}(\sqrt{m})$ with discriminant d over the field $\mathbf{Q}$ of the rational numbers. Let $ax^2 + bxy + cy^2$, $a > 0$, $\mathrm{GCD}(a, b, c) = 1$, be a positive definite primitive quadratic form with discriminant $d = b^2 - 4ac$. The integral matrix $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ with determinant $\alpha\delta - \gamma\beta = 1$ transforms the quadratic form by replacing x by $\alpha x + \beta y$ and y by $\gamma x + \delta y$ into an equivalent one of the same discriminant d. The class number $h(d)$ of $\mathbf{Q}(\sqrt{m})$ is equal to the the number of such defined equivalence classes of positive definite primitive quadratic forms of discriminant d. A unique reduced form for each equivalence class can be selected with

$$-a < b \le a < c \quad \text{or} \quad 0 \le b \le a = c.$$

These conditions imply that $|b| \le \sqrt{|d|/3}$ and hence $h(d)$ is finite.

Now let $SL_2(\mathbf{Z})$ be the modular group:

$$SL_2(\mathbf{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbf{Z},\ ad - bc = 1 \right\},$$

and let H denote the upper half complex plane:

$$H = \{z = x + iy \in \mathbf{C} \mid y > 0\},$$

where $\mathbf{C}$ is the field of complex numbers. $SL_2(\mathbf{Z})$ acts on H by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(z) = \frac{az + b}{cz + d}.$$

A ***fundamental domain*** F for $SL_2(\mathbf{Z})$ in H is defined to be a subset of H such that every orbit of $SL_2(\mathbf{Z})$ has one element in F, and two elements of F are in the same orbit if and only if they lie on the boundary of F. Then F is given by the set

$$F = \{ z = x + iy \in \mathbf{C} \mid |z| \geq 1,\ |x| \leq \frac{1}{2} \}.$$

We now introduce the *elliptic modular j-invariant*. For each complex number z with non-negative imaginary part, let $q = e^{2\pi i z}$ and let

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n, \quad \sigma_3(n) = \sum_{\substack{t \mid n \\ t>0}} t^3.$$

Furthermore, let

$$\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n) = q^{\frac{1}{24}} \left[1 + \sum_{n=1}^{\infty} (-1)^n (q^{\frac{n(3n-1)}{2}} + q^{\frac{n(3n+1)}{2}}) \right].$$

The j-invariant $j(z)$ is defined as

$$j(z) = \left[\frac{E_4(z)}{\eta(z)^8} \right]^3.$$

It is well-known that $j(z)$ satisfies the following properties:

(i) $j(i) = 1728$, $j((\pm 1 + i\sqrt{3})/2) = 0$,

(ii) $j(x + iy)$ and $j(-x + iy)$ are complex conjugates for any $\pm x + iy \in F$, and

(iii) $j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$.

3. The following theorem now shows how to construct an integral polynomial with dihedral Galois group of prime degree.

Theorem (cf. Deuring [2]): Let $\mathbf{Q}(\sqrt{m})$ be an imaginary quadratic field with discriminat d, and with class number $h(d) = p$, p an odd prime. For each reduced positive definite primitive quadratic form $a_k x^2 + b_k xy + c_k y^2$ of discriminant d, $1 \leq k \leq p$, let $\vartheta_k = (-b_k + \sqrt{d})/(2a_k)$ be the root of $a_k \vartheta^2 + b_k \vartheta + c_k = 0$ belonging to F. Furthermore, let the class equation H_d be defined as

$$H_d(x) = \prod_{k=1}^{p} (x - j(\vartheta_k))$$

Then $H_d(x)$ is an irreducible integral polynomial whose Galois group over $\mathbf{Q}$ is the dihedral group D_p. □

4. We constructed $H_d(x)$ for selected imaginary quadratic fields $\mathbf{Q}(\sqrt{m})$ with $-m$ a prime and $h(d) = 7$ or 11. First we wish to make some comments encountered during our calculations. In all cases we knew the class number in advance. Therefore it was quite easy to calculate the ϑ_k, $1 \leq k \leq p$. Indeed,

for $|b_k| \le a_k < c_k$, we get two roots $\vartheta_k = (\mp b_k + \sqrt{d})/(2a_k)$, and for $0 \le b_k \le a_k = c_k$, one root $\vartheta_k = (-b_k + \sqrt{d})/(2a_k)$, belonging to F. Using the above mentioned properties of j we only had to evaluate $j(\vartheta_k)$ for $(p+1)/2$ different values of ϑ_k. The evaluation of each $j(\vartheta_k)$ was done to high floating point precision. We experienced that the Taylor series of j evaluated at q converged extremely slowly. Therefore we evaluated the Taylor series of E_4 and η separately at q, then raised the value $\eta(q)$ to the eighth power, divided $E_4(q)$ by this result, and finally raised the quotient to the third power. This process yields $j(q)$ to high precision fairly quickly.

In each case there were two parameters to choose: The floating point precision and the order of the Taylor expansions. We decided to choose the same order for both E_4 and η. The constant coefficient of each polynomial turned out to be the one of largest size. Therefore we chose the floating point precision typically 20 digits more than the number of digits in that coefficient. In all cases we then could read off the correct corresponding integer from its approximation. It turns out that the constant coefficient $H_d(0)$ must be a perfect cube. Verifying this condition proved to be a valuable test to see whether the order of the Taylor approximation was high enough. If not, we incremented the order by 5 and tried again. A further confirmation for the correctness of all coefficients is to factor both $H_d(0)$ and the discriminant $\Delta(H_d)$ of H_d both of which surprisingly have only small prime factors. A full explanation for this phenomenon has been found only very recently by B. Gross and D. Zagier. With their permission, we state a version of their theorem best suited for our discussion.

Theorem (Gross and Zagier [3]): Let q be a prime. For a positive integer $n \in \mathbf{N}$ such that $(\frac{n}{q}) \neq +1$, define the function $F_q(n)$ by

$$F_q(n) = \begin{cases} l^{kr_1 \cdots r_t} & \text{if } n = l^{2k-1} l_1^{2n_1} \cdots l_s^{2n_s} q_1^{r_1-1} \cdots q_t^{r_t-1} \\ & \text{where } (\frac{l}{q}) = (\frac{l_i}{q}) = -1, (\frac{q_i}{q}) = +1 \\ & \text{with } k, r_i \ge 1 \text{ and } n_i \ge 0, \\ 1 & \text{if } n = l_1^{2k_1-1} l_2^{2k_2-1} \cdots l_s^{2k_s-1} t \\ & \text{where } (\frac{l_i}{q}) = -1 \text{ with } k_i \ge 1, s \ge 3 \\ & \text{and } t \in \mathbf{N}. \end{cases}$$

(a) Let $\mathbf{Q}(\sqrt{m})$, $m < 0$ and $-m$ a prime $\equiv 3 \pmod 4$, be an imaginary quadratic field of discriminant d and of class number $h(d) = h$, an odd prime. Let $Q_k(x,y) = a_k x^2 + b_k xy + c_k y^2$, $a_k > 1$, $b_k > 0$, $k = 1, 2, \ldots, (h-1)/2$ be the reduced positive definite primitive quadratic forms of discriminant d associated with $\mathbf{Q}(\sqrt{m})$. Let $H_d(x)$ be the class equation of $\mathbf{Q}(\sqrt{m})$. Then

$$\Delta(H_d) = I^2(-m)^{\frac{h-1}{2}} \quad \text{where } I = I_1 \cdots I_{\frac{h-1}{2}}$$

and

$$I_k = \prod_{n=1}^{-m-1} F_{-m}(-m-n)^{r_k(n)},$$

$$r_k(n) = \frac{1}{2}\#\{(x,y) \in \mathbf{Z}\times\mathbf{Z} \mid Q_k(x,y) = n\}.$$

In particular, the largest prime dividing $\Delta(H_d)$ does not exceed $-m$, and all its prime factors except $-m$ appear in even powers.

(b) Let z, $z' \in F$ be imaginary quadratic numbers belonging to two distinct imaginary quadratic fields $\mathbf{Q}(\sqrt{m})$ and $\mathbf{Q}(\sqrt{m'})$, respectively, where $-m$ and $-m'$ are primes $\equiv 3 \pmod 4$. Then

$$|Norm(j(z) - j(z'))| = \left(\prod_{\substack{0<x<\sqrt{mm'} \\ x \text{ odd}}} F_{-m'}\left(\frac{mm'-x^2}{4}\right) \right)^{\frac{w(m')}{2}},$$

where the *Norm* is taken over $\mathbf{Q}$ and $w(m')$ denotes the number of units in $\mathbf{Q}(\sqrt{m'})$.

In particular, taking $z = \frac{1+\sqrt{m}}{2}$ and $z' = \frac{1+\sqrt{-3}}{2}$, we have

$$|H_d(0)| = |Norm(j(\tfrac{1+\sqrt{m}}{2}))| = \left(\prod_{\substack{0<x<\sqrt{-3m} \\ x \text{ odd}}} F_{-3}\left(\frac{-3m-x^2}{4}\right) \right)^3$$

and therefore, the largest prime dividing $H_d(0)$ does not exceed $-m$. □

The table below summarizes the cases we considered.

m	$h(d)$	Order of Taylor exp.	Floating point precision	CPU time (VAX 780)
−71	7	25	50	123 sec.
−151	7	25	70	177 sec.
−223	7	25	70	164 sec.
−251	7	25	70	187 sec.
−463	7	25	100	219 sec.
−167	11	25	100	340 sec.
−271	11	30	100	431 sec.
−659	11	40	120	663 sec.

We shall illustrate our construction by two examples: $\mathbf{Q}(\sqrt{-251})$ and $\mathbf{Q}(\sqrt{-659})$. The remaining polynomials can be found in the full paper [8]. In each case we list quadratic form representatives as well as the polynomials H_d thus obtained. We factored out powers of primes ≤ 1000 dividing the coefficients. We also present the factored discriminant $\Delta(H_d)$.

$\mathbf{Q}(\sqrt{-251})$

Reduced quad. form	ϑ
$x^2 + xy + 63y^2$	$\frac{-1+\sqrt{-251}}{2}$
$3x^2 \pm xy + 21y^2$	$\frac{\mp 1+\sqrt{-251}}{6}$
$7x^2 \pm xy + 9y^2$	$\frac{\mp 1+\sqrt{-251}}{14}$
$5x^2 \pm xy + 13y^2$	$\frac{\mp 3+\sqrt{-251}}{10}$

$H_{-251}(x)$	
	x^7
$+ 2^{17}\cdot 29\cdot 1086122234032811$	x^6
$- 2^{30}\cdot 3^4\cdot 7\cdot 13\cdot 8364869403342457$	x^5
$+ 2^{49}\cdot 3^2\cdot 23\cdot 9113559120635943109$	x^4
$+ 2^{60}\cdot 5\cdot 1381976650295197345607$	x^3
$+ 2^{77}\cdot 11^3\cdot 2066916598433853809$	x^2
$- 2^{90}\cdot 11^6\cdot 817072976407817$	x^1
$+ (2^{36}\cdot 11^3\cdot 29\cdot 47)^3$	

The discriminant is:

$$\Delta(H_{-251}) = -2^{664}11^{42}19^{24}29^{14}37^{10}43^{8}47^{8}53^{8}59^{6}61^{6}71^{6}107^{2}$$
$$\times 127^{2}139^{2}151^{2}167^{4}191^{4}199^{2}223^{2}239^{2}251^{3}.$$

$\mathbf{Q}(\sqrt{-659})$

Reduced quad. form	ϑ
$x^2 + xy + 165y^2$	$\frac{-1+\sqrt{-659}}{2}$
$3x^2 \pm xy + 55y^2$	$\frac{\mp 1+\sqrt{-659}}{6}$
$5x^2 \pm xy + 33y^2$	$\frac{\mp 1+\sqrt{-659}}{10}$
$11x^2 \pm xy + 15y^2$	$\frac{\mp 1+\sqrt{-659}}{22}$
$9x^2 \pm 5xy + 19y^2$	$\frac{\mp 5+\sqrt{-659}}{18}$
$13x^2 \pm 11xy + 15y^2$	$\frac{\mp 11+\sqrt{-659}}{26}$

$H_{-659}(x)$	
	x^{11}
$+ 2^{16}\cdot 11\cdot 14690154361125471419369330393 9$	x^{10}
$- 2^{31}\cdot 3^2\cdot 11\cdot 2356759517255791643768337607942768 51$	x^9
$+ 2^{46}\cdot 5\cdot 317\cdot 21253848824657244505372416849107899401473 3$	x^8
$- 2^{63}\cdot 433\cdot 677\cdot 14353896100789371720505020073678467001951 1$	x^7
$+ 2^{76}\cdot 7\cdot 458887012699765312295245955780620954239045856720 9$	x^6
$- 2^{91}\cdot 7\cdot 17\cdot 29\cdot 98510921202045068953860432795284740311821945 3$	x^5
$+ 2^{106}\cdot 17593263285454621669441419150144873354823923157 67$	x^4
$- 2^{120}\cdot 131\cdot 37505635773680520025236619876555341470269359 23$	x^3
$+ 2^{138}\cdot 3^2\cdot 23\cdot 409\cdot 27449498248914850869171135436577205414197$	x^2
$- 2^{162}\cdot 3\cdot 41^6\cdot 227\cdot 281\cdot 22635434377436275328117 71$	x^1
$+ (2^{60}\cdot 29\cdot 41^2\cdot 47\cdot 71\cdot 101\cdot 113)^3$	

The discriminant is:

$$\Delta(H_{-659}) = -2^{1746}7^{222}29^{42}31^{36}41^{26}43^{28}47^{26}53^{20}67^{14}71^{18}83^{10}97^{6}101^{10}$$
$$\times 103^{10}113^{8}131^{12}137^{4}151^{6}191^{6}193^{4}197^{4}199^{4}223^{2}227^{4}263^{6}$$
$$\times 359^{6}367^{2}383^{4}419^{4}431^{4}439^{4}467^{2}479^{6}503^{4}599^{4}607^{2}647^{2}659^{5}.$$

Using a different modular function, the class equations with much smaller coefficients have been constructed by M. Hanna [5] for the imaginary quadratic fields $\mathbf{Q}(\sqrt{-167})$ and $\mathbf{Q}(\sqrt{-191})$ (class number 13) and by G. N. Watson [11] for the fields $\mathbf{Q}(\sqrt{-383})$ (class number 17) and $\mathbf{Q}(\sqrt{-311})$ (class number 19). The given polynomials are actually the h degree integral factors of $x^h H_d((x-16)^3/x)$, where h is the class number and H_d the equation corresponding to the modular function used. We can also carry out this transformation on our class equations resulting in polynomials with much smaller coefficients. Following we give Hanna's polynomial for $\mathbf{Q}(\sqrt{-167})$ which has also passed the test for having Galois group D_{11} described at the beginning of this paper:

$$x^{11}+x^{10}+5x^9+4x^8+10x^7+6x^6+11x^5+7x^4+9x^3+4x^2+2x-1.$$

Appendix

The Explicit Form of the Modular Equation of Prime Order

Let $j(z)$ be the elliptic modular invariant. It is a classical result going back to Kronecker (see, e.g. Weber [12, Sec. 69]) that *if* $z = x + iy \in \mathbf{C}$ *belongs to an imaginary quadratic field with* $y > 0$, *then* $j(z)$ *is an algebraic integer.* This was proven by showing that $j(z)$ satisfies an algebraic equation with integral coefficients, called the *modular equation* (of order n for some $n > 1$).

However, the explicit form of the modular equation has not been known, except for few cases (cf. Fricke [3, II.4]).†

In this appendix, we shall discuss how to determine explicitly the modular equations of order p where $p = 5$ and 7. For a prime p, let

$$A = \left\{ \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & i \\ 0 & p \end{bmatrix} \text{ with } 0 \le i < p \right\}.$$

For $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in A$ and for $z = x + iy \in \mathbf{C}$, $y > 0$, we write $j \cdot \alpha$ for

$$(j \cdot \alpha)(z) = j(\alpha(z)) = j\left(\frac{az+b}{cz+d}\right),$$

and form the polynomial

$$\Phi_p(x) = \prod_{\alpha \in A} (x - j \cdot \alpha) = \prod_{\alpha \in A} (x - j(\alpha(z))).$$

We can view $\Phi_p(x)$ as a polynomial in two variables x and j over $\mathbf{Z}$,

$$\Phi_p(x) = \Phi_p(x, j) \in \mathbf{Z}[x, j],$$

and we call it the *modular polynomial of order p*. The importance of this polynomial is that there exists a prime p such that $\Phi_p(j(z), j(z)) = 0$. Since the leading coefficient of $\Phi_p(x, x)$ is $-x^{2p}$ $j(z)$ must be an algebraic integer. The equation $\Phi_p(x, j) = 0$ is called the *modular equation of order p*.

The modular equations of order p can be very difficult to determine explicitly as the cases $p = 2$ and 3 already suggest (cf. [3]). We shall make use of the following result.

Theorem (Yui [13]): Let $j^*(z) = j(pz)$ with $z = x + iy$, $y > 0$. Then

$$0 = \Phi_p(j^*, j) = (j^{*p} - j)(j^* - j^p) - p \sum_{m=1}^{p} \sum_{n=0}^{m-1} d_{m,n} (j^{*m} j^n + j^{*n} j^m)$$

$$- p \sum_{m=0}^{p-1} d_{m,m} j^{*m} j^m,$$

where $d_{m,n}$ and $d_{m,m}$ are integers. □

The coefficients $d_{m,n}$ and $d_{m,m}$ can be determined by noting that $j^*(q) = j(q^p)$ and then comparing the coefficients of the q-expansions of the identity in the above theorem. In order to obtain an equation for $d_{0,0}$ one must expand the this equation from q^{-p^2-p} through q^0. Therefore one needs the q-expansion of j to the order $p^2 + p - 1$. Using this algorithm we could successfully determine Φ_5 and Φ_7. We present the explicit form of Φ_7, again primes ≤ 1000 factored out of the coefficients. Φ_5 is given in the full paper [8].

† It was brought to our attention after we had completed our computations that W. Berwick [1] already determined Φ_5 and O. Herrmann [6] Φ_7. Their results coincide with ours but it appears to us that our methods are much more efficient.

$$
\begin{aligned}
\Phi_7(j^*, j) = 0 = \\
& j^{*8} + \cdot 2^3 \cdot 3 \cdot 7 \cdot 31 \cdot (j^6 \cdot j^{*7} + j^7 \cdot j^{*6}) \\
& - 13553 \cdot 2^2 \cdot 3^3 \cdot 7 \cdot (j^5 \cdot j^{*7} + j^7 \cdot j^{*5}) \\
& + 2^5 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 43 \cdot 509 \cdot (j^4 \cdot j^{*7} + j^7 \cdot j^{*4}) \\
& - 1067425727 \cdot 2 \cdot 3 \cdot 7^2 \cdot 13 \cdot (j^3 \cdot j^{*7} + j^7 \cdot j^{*3}) \\
& + 263733037 \cdot 2^4 \cdot 3^4 \cdot 7^2 \cdot 43 \cdot (j^2 \cdot j^{*7} + j^7 \cdot j^{*2}) \\
& - 6866816589877 \cdot 2^3 \cdot 7^2 \cdot 13 \cdot (j \cdot j^{*7} + j^7 \cdot j^*) \\
& + 26891 \cdot 2^{16} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 31 \cdot (j^{*7} + j^7) - j^7 \cdot j^{*7} \\
& + 32268467570786329 \cdot 2^4 \cdot 7^3 \cdot (j^5 \cdot j^{*6} + j^6 \cdot j^{*5}) \\
& + 3793318421100253701707 \cdot 2^3 \cdot 3 \cdot 7^2 \cdot (j^4 \cdot j^{*6} + j^6 \cdot j^{*4}) \\
& + 378554512130011411 \cdot 2^4 \cdot 3^5 \cdot 5 \cdot 7^2 \cdot 197 \cdot 227 \cdot (j^3 \cdot j^{*6} + j^6 \cdot j^{*3}) \\
& + 187987466668181444486823667 \cdot 2^2 \cdot 7^2 \cdot 29 \cdot (j^2 \cdot j^{*6} + j^6 \cdot j^{*2}) \\
& + 10020909155496489683 \cdot 2^{17} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 59 \cdot (j \cdot j^{*6} + j^6 \cdot j^*) \\
& + 1323331291097 \cdot 2^{30} \cdot 3^{10} \cdot 5^6 \cdot 7 \cdot 397 \cdot (j^{*6} + j^6) \\
& + 8389943 \cdot 3^2 \cdot 7^2 \cdot 13 \cdot 67 \cdot 97 \cdot j^6 \cdot j^{*6} \\
& + 35641291134170661786390 13 \cdot 2^5 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 113 \\
& \cdot (j^4 \cdot j^{*5} + j^5 \cdot j^{*4}) \\
& - 230011559218289608131917268811367 8807 \cdot 2^3 \cdot 7^2 \\
& \cdot (j^3 \cdot j^{*5} + j^5 \cdot j^{*3}) \\
& + 178299075699438778621099394269 \cdot 2^{19} \cdot 3^9 \cdot 5^3 \cdot 7^2 \\
& \cdot (j^2 \cdot j^{*5} + j^5 \cdot j^{*2}) \\
& - 34925787722711812538264201 \cdot 2^{33} \cdot 3^{11} \cdot 5^6 \cdot 7^2 \cdot (j \cdot j^{*5} + j^5 \cdot j^*) \\
& + 181122097371406153 \cdot 2^{47} \cdot 3^{16} \cdot 5^9 \cdot 7^2 \cdot 13 \cdot 31 \cdot (j^{*5} + j^5) \\
& - 10374612889856513538191507 \cdot 2^2 \cdot 3^2 \cdot 7^2 \cdot j^5 \cdot j^{*5} \\
& + 3893394856539704079067727101 \cdot 2^{16} \cdot 3^7 \cdot 5^4 \cdot 7^2 \cdot 37 \cdot 43 \cdot 661 \\
& \cdot (j^3 \cdot j^{*4} + j^4 \cdot j^{*3}) \\
& + 623497402974265297820492952 79 \cdot 2^{31} \cdot 3^{11} \cdot 5^6 \cdot 7^2 \cdot 17 \\
& \cdot (j^2 \cdot j^{*4} + j^4 \cdot j^{*2}) \\
& + 489378588475111548205 21 \cdot 2^{46} \cdot 3^{17} \cdot 5^9 \cdot 7^2 \cdot 13 \cdot (j \cdot j^{*4} + j^4 \cdot j^*) \\
& + 1323331291097 \cdot 2^{60} \cdot 3^{19} \cdot 5^{12} \cdot 7^2 \cdot 17^3 \cdot 397 \cdot (j^{*4} + j^4) \\
& + 912019631831096138476499139089037899 \cdot 2 \cdot 5 \cdot 7^2 \cdot 197 \cdot j^4 \cdot j^{*4} \\
& + 609518324373969241528663 \cdot 2^{46} \cdot 3^{16} \cdot 5^9 \cdot 7^2 \cdot 409 \cdot (j^2 \cdot j^{*3} + j^3 \cdot j^{*2})
\end{aligned}
$$

$$-88980809456419\cdot 2^{61}\cdot 3^{19}\cdot 5^{12}\cdot 7^2\cdot 17^3\cdot 19\cdot 487\cdot (j\cdot j^{*3}+j^3\cdot j^*)$$
$$+26891\cdot 2^{76}\cdot 3^{25}\cdot 5^{15}\cdot 7^3\cdot 17^6\cdot 31\cdot (j^{*3}+j^3)$$
$$-5559535565766995052158900399173 1\cdot 2^{31}\cdot 3^{10}\cdot 5^6\cdot 7^2\cdot j^3\cdot j^{*3}$$
$$-22541\cdot 2^{76}\cdot 3^{25}\cdot 5^{15}\cdot 7^2\cdot 17^7\cdot 947\cdot (j\cdot j^{*2}+j^2\cdot j^*)$$
$$+2^{90}\cdot 3^{27}\cdot 5^{18}\cdot 7^3\cdot 17^9\cdot (j^{*2}+j^2)$$
$$-98755869850221841\cdot 2^{61}\cdot 3^{20}\cdot 5^{12}\cdot 7^2\cdot 17^3\cdot j^2\cdot j^{*2}$$
$$+2^{91}\cdot 3^{27}\cdot 5^{18}\cdot 11\cdot 13\cdot 17^9\cdot j\cdot j^*+j^8.$$

The computation of Φ_5 took 982 seconds and the one of Φ_7 4091 seconds CPU time on a VAX 780. During the computation of Φ_{11} we ran out of virtual storage after approximately 7 hours of CPU time. We have recently developed a modified version of the above algorithm for computing Φ_p which is much less space consuming and which has already successfully computed the explicit form of Φ_{11} [9].

The modular polynomial $\Phi_p(x, x)$ factors into the product of powers of some class equations (cf. Weber [12, Sec. 116]). For $p = 7$, the factorization is the following.

$$\Phi_7(x,x) = -x^2\,(x-3^3\cdot 5^3\cdot 17^3)\,(x-2^4\cdot 3^3\cdot 5^3)^2$$
$$\times (x+3^3\cdot 5^3)\,(x+2^{15}\cdot 3^3)^2\,(x+2^{15}\cdot 3\cdot 5^3)^2$$
$$\times (x^2-2^7\cdot 3^3\cdot 1399x+2^{12}\cdot 3^6\cdot 17^3)^2.$$

Acknowledgement

We wish to thank the Department of Mathematics at Kent State University for allowing us to use their research VAX 780 for carrying out our computations. In particular, we are indebted to Professor Paul Wang for his advice on the usage of MACSYMA. We also wish to thank all colleagues who commented on an earlier version of this paper. Especially, we thank Professor Don Zagier for explaining us his joint results with Professor Benedict Gross. We also thank Professor David Chudnovsky and Professor Gregory Chudnovsky for bringing the work of M. Hanna and G. N. Watson to our attention.

References

[1] W. E. H. Berwick, "An invariant modular equation of the fifth order," *Quarterly J. Math.*, 47, 1916, pp. 94-103.

[2] M. Deuring, "Die Klassenkörper der komplexen Multiplikation," *Enzyklopädie Math. Wiss.* v. 12 (Book 10, part II), Teubner, Stuttgart, 1958.

[3] R. Fricke, *Lehrbuch der Algebra, Bd.* 3, Braunschweig, 1928.

[4] B. Gross and D. Zagier, in preparation.

[5] M. Hanna, "The modular equations," *Proc. London Math. Soc.*, 28, 1928, pp. 46-52.

[6] O. Herrmann, "Uber die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$," *J. Reine Angew. Math.* 274/275, 1974, pp. 187-195.

[7] C. U. Jensen and N. Yui, "Polynomials with D_p as Galois group," *J. Number Theory* v. 15, 1982, pp. 347-375.

[8] E. Kaltofen and N. Yui, "Explicit construction of the Hilbert class fields of imaginary quadratic fields with class numbers 7 and 11," *Math. Comp.*, submitted.

[9] E. Kaltofen and N. Yui, "On the Modular Equation of Order 11," manuscript 1984.

[10]MACSYMA, Reference Manual, v. 1 and 2, the Mathlab Group, Laboratory for Computer Science, MIT 1983.

[11]G. N. Watson, "Singular Moduli (4)," *Acta Arith.*, 1, 1935, pp. 284-323.

[12]H. Weber, *Lehrbuch der Algebra, Bd.* 3, Braunschweig, 1908.

[13]N. Yui, "Explicit form of the modular equation," *J. Reine Angew. Math.*, 299/300, 1978, pp. 185-200.