

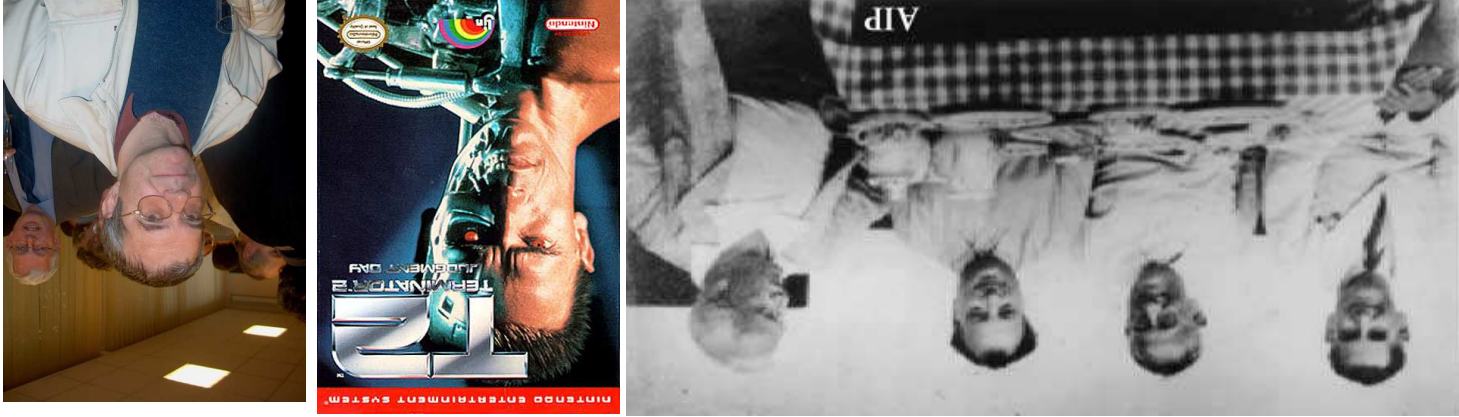
La méthode des graphes

Ifikhar Burhanuddin

burhanud@usc.edu

David Kohel, William Stein

MSRI August 11, 2006



LE PROJECT

Problem Check if the Stein Watkins database of Elliptic Curves of prime conductor (upto $> 10^8$) is **complete**.

Tools Supersingular j -invariants over \mathbb{F}_p , modular polynomials.

Theorem *There exists an isomorphism compatible with the action of Hecke operators, between $M_0^{Np} \otimes \mathbb{C}$ and the subspace $S_2(\Gamma_0(Np))$ generated by the newforms of level Np and old forms coming from the cusp forms of weight 2 and level $pd, d|N$.*

Method "Any sufficiently advanced technology is indistinguishable from magic". (A. C. Clarke's third law of prediction)

Q Given a of list of numbers (traces) and $N \dots$ is there an elliptic curve H over \mathbb{Q} with conductor N ?

MOG ALGORITHM

Given p, N , find all supersingular points on $X_0(N)(\mathbb{F}^{p^2})$ (where genus $X_0(N) = 0$)

- Find a SS j -invariant by first trying the \mathbb{F}^p -rational ones (these are class number 1 j -invariants). Otherwise find some D (small) such that $(\frac{D}{p}) \neq 1$, and use any root in \mathbb{F}^{p^2} of $H_D(X) \in \mathbb{Z}[X]$, where H_D is the **Hilbert Class polynomial**.

- If $N = 1$ use $\Phi_2^{(1)}(X, Y)$ (**Classical Modular Polynomial**) to solve for all SS j -invariants in \mathbb{F}^{p^2} . If $N > 1$, use $\Phi_2^{(N)}(X, Y)$ (**Dedekind Eta Modular Polynomial**).

We now have a basis for our SS module $\mathfrak{M} = \bigoplus_{i=1}^h \mathbb{Z}[x_{N,i}]$

$$\{x_{N,i}\} = SS(\mathbb{F}^{p^2}) \subset X_0(N)(\mathbb{F}^{p^2}) \cong \mathbb{P}_1(\mathbb{F}^{p^2})$$

- If $N > 1$ then use $\Psi_N(x_N, j)$ (**Canonical Dedekind Modular Polynomial**) to solve for x_N , i.e. let j run through SS j -invariants determined above and solve for all roots x_N .

PICKING A SS_j -INVARIANT

```
def supersingular_j(F):  
    prime = FF.characteristic()  
    if not (rings.Integer(prime).is_prime()):  
        raise ValueError, "%s is not a prime"%prime  
    if rings.kronecker(-1, prime) != 1:  
        j_invs = 1728  
        # (2^2 * 3)^3  
        if rings.kronecker(-2, prime) != 1:  
            j_invs = 8000  
            # (2^2 * 5)^3  
            if rings.kronecker(-3, prime) != 1:  
                j_invs = 0  
            # 0^3  
            if rings.kronecker(-7, prime) != 1:  
                j_invs = 16581375  
                # (3 * 5 * 17)^3  
            if rings.kronecker(-11, prime) != 1:  
                j_invs = -32768  
                # -(2^5)^3
```

```

elif rings.kronecker(-19, prime) == 1:
    j_invs = -884736 #-(2^5 * 3)^3
elif rings.kronecker(-43, prime) == 1:
    j_invs = -884736000 #-(2^6 * 3 * 5)^3
elif rings.kronecker(-67, prime) == 1:
    j_invs = -147197952000 #-(2^5 * 3 * 5 * 11)^3
elif rings.kronecker(-163, prime) == 1:
    j_invs = -262537412640768000 #-(2^6 * 3 * 5 * 23 * 29)^3
else:
    D = supersingular_D(prime)
    DBCF = HilbertClassPolynomialDatabase()
    hc_poly = rings.PolynomialRing(FF)(DBCF[D])
    root_hc_poly_list = list(hc_poly.roots())
    j_invs = root_hc_poly_list[0][0]
return FF(j_invs)

```

COMPUTE HECKE OPERATOR (BRANDT MATRIX)

Given $N, p, \{x_{N,i}\} = SS(\mathbb{F}^{p^2})$

- Computation of Hecke operators T_l for $l = 2, 3, 5, \dots$ need to construct the **graphs** of l -isogenies.

- Let l be fixed and use $\Phi_{(N)}^l(x_{N,i}, Y) = \prod_{j=1}^l (Y - x_{e_{N,i,j}})$ polynomial. For $i = 1, \dots, h$, solve for roots of

- Set $T_l = (e_{i,j}) \dots$ **Incidence matrix**.

- Note there are exactly $l + 1$ roots for each i , i.e. $\sum_{j=1}^{l+1} e_{ij} = l + 1$ ($l \neq p$ and $l \nmid N$). If $l \mid N$ then there are l roots.

SWDB

- Check if the Stein Watkins database of Elliptic Curves of prime conductor (upto $> 10^8$) is **complete**.

- In search of 1-dim eigenspaces. Commuting operators **preserve**

eigenspaces: Say $S(f) = a \cdot f$. Then

$$S(T(f)) = T(S(f)) = T(a \cdot f) = a \cdot T(f).$$

- **Sturm Bound**: to compute Hecke operators T_l on eigenspaces for $l \leq \frac{6}{d+1}$

OPTIMIZATIONS

- Dictionaries . . . **hashing**
 - Writing optimized **code** . . . polynomial ring arithmetic
 - T_2 .kernel() . . . **smaller** dimension eigenspaces . . . now do T_l .decomposition_of_subspace() for all $l > 2$ instead
- ps: Mat.copy()

FUTURE

- $X_0(Np)$, where **genus** $X_+^0(N) = 0$ (currently $N = 1$)
 - Leverage **Atkin-Lehner** involutions in enumerating 1-dim eigenspaces using.
 - **Stein-Watkins** database prime conductors up to 10^8
- ps: Limitations

RESULTS

- Code ran for > 19 hours **sans** crashing. About (first) 1000 primes levels of SWDB have been "verified".
- **SupersingularModule** part of sage repository

Thanks to Lassina Dembélé, Stephanie Jakus, David Kohel, William Stein, **MSRI** . . .