The modular degree, congruence number, and multiplicity one *

Amod Agashe
Florida State University

joint work with K. Ribet and W. Stein

October 4, 2007

*Slides and paper available at:
http://www.math.fsu.edu/~agashe/math.html

Elliptic curves

Let E be an elliptic curve over $\mathbf{Q}$, i.e., an equation of the form $y^2 = x^3 + ax + b$, where $a, b \in \mathbf{Q}$

Example: The graph of $y^2 = x^3 - x$ over $\mathbf{R}$:

If p is a prime, then we can "think of" the equation for E modulo p
Let $a_p(E) = 1 + p - \#$solutions to E mod p.

Modular curves and modular forms

Let $N =$ a positive integer.
$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : N \mid c \right\}$.
e.g., $\Gamma_0(1) = \mathrm{SL}_2(\mathbf{Z})$
$\mathcal{H} =$ complex upper half plane
$\Gamma_0(N)$ acts on $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ as $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$
$X_0(N) = \Gamma_0(N) \backslash (\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q}))$

A modular form on $\Gamma_0(N)$ is a holomorphic function $f : \mathcal{H} \to \mathbf{C}$ such that
$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), f(\gamma z) = (cz+d)^2 f(z)$
and f is holomorphic at the cusps.
In particular, $f(z+1) = f(z)$, so
$f(z) = \sum_{n>0} a_n(f) q^n$, where $q = e^{2\pi i z}$.
f is said to be a cuspform if $a_0(f) = 0$, i.e., f vanishes at the cusps.

Modular degree and congruence number

By work of Wiles and Breuil-Conrad-Diamond-Taylor, if E is an (optimal) elliptic curve, then there is an integer N (the conductor of E) such that
1) $\exists$ a surjective morphism of curves
$\phi_E : X_0(N) \rightarrow E$, and
2) $\exists$ a cuspform f_E on $\Gamma_0(N)$ with integer Fourier coefficients such that $a_n(E) = a_n(f_E)\ \forall n$.

The modular degree of $E = \deg(\phi_E)$.
The congruence number of E
= the largest integer r such that
$\exists$ a cuspform g on $\Gamma_0(N)$ "orthogonal" to f_E with $a_n(f_E) \equiv a_n(g) \bmod r\ \forall n$.

Both are important invariants:
Bounds on modular degree related to abc conjecture (Frey, Mai-Murty)
Congruence primes (the primes that divide the congruence number) figured in work of Ribet and Wiles on Fermat's last theorem.

Relations between modular degree and congruence number

Theorem (Ribet $\sim$ 1985): The modular degree divides the congruence number. If N is prime, then the two are equal.

Frey and Müller asked: are they always equal?

Answer (Stein $\sim$ 2000): NO. e.g., there is an elliptic curve E of conductor 54 with modular degree $= 2$ and congruence number $= 6$.

Theorem (A, Ribet, Stein): If a prime p divides the ratio of the congruence number to the modular degree, then $p^2 \mid N$.

In particular, if N is square-free, then the congruence primes divide the modular degree.

Note: In previous example, $3^2 \mid 54$.

Multiplicity one

$J_0(N) =$ Jacobian of $X_0(N)$; thus
$J_0(N)(\mathbf{C}) =$ degree zero divisors on $X_0(N)(\mathbf{C})$ modulo principal divisors
Hecke algebra $\mathbf{T}$ = subring of $\mathrm{End}(J_0(N))$ generated by the Hecke operators.

We say that a maximal ideal $\mathbf{m}$ of $\mathbf{T}$ satisifies *multiplicity one* if $\dim_{\mathbf{T}/\mathbf{m}} J_0(N)[\mathbf{m}] = 2$.

The notion of multiplicity one was initiated by Mazur and played an important role in Wiles' proof of Fermat's last theorem.

Proposition (A, Stein, Ribet): If E is an elliptic curve of conductor N, and p is a prime such that p divides the congruence number of E but not the modular degree of E, Then $\mathbf{m} = \mathrm{Ann}_{\mathbf{T}} E[p]$ does not satisfy multiplicity one.

So by the previous example, for $N = 54$, there is a maximal ideal of $\mathbf{T}$ with residue characteristic 3 which does not satisfy multiplicity one.