The modular number, the congruence number, and multiplicity one *

Amod Agashe
Florida State University

January 11, 2010

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

Modular curves and modular forms

Let $N =$ a positive integer (the level).
$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : N \mid c \right\}$.
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 of weight 2 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. The space of cuspforms with coefficients in a ring R will be denoted $S_2(R)$.

Modular/congruence degree/number

$$
\begin{array}{rcl}
J & = & J_0(N) = \text{Jacobian of } X_0(N), \\
\mathbf{T} & = & \text{Hecke algebra}, \\
f & = & \text{a newform of weight 2 on } \Gamma_0(N), \\
I_f & = & \mathrm{Ann}_{\mathbf{T}} f, \text{ an ideal of } \mathbf{T}, \\
A_f & = & J_0(N)/I_f J_0(N); \text{ it is an elliptic curve} \\
 & & \text{if all } a_n(f) \text{ are integers.} \\
A & = & A_f^{\vee} = \text{the dual of } A_f. \\
B & = & I_f J \text{ ; so } A + B = J \text{ and } A \cap B \text{ is finite.}
\end{array}
$$

The *modular exponent/number* = the exponent/order of $A \cap B$. If A is an elliptic curve, then the modular exponent is the modular degree, and the modular number is its square.

The *congruence exponent/number* = the exponent/order of

$$\frac{S_2(\mathbf{Z})}{S_2(\mathbf{Z})[I_f] + S_2(\mathbf{Z})[I_f]^{\perp}}.$$

If A is an elliptic curve, then the congruence number is the largest integer r such that there exists a cuspform $g \in S_2(\mathbf{Z})$ orthogonal to f and congruent to f modulo r.

Multiplicity one

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

Notion initiated by Mazur; played an important role in Wiles's proof of Fermat's last theorem (among other places).

Fact: Let p be an odd prime and $\mathbf{m}$ be a maximal ideal of $\mathbf{T}$ with residue characteristic p such that $\rho_{\mathbf{m}}$ is irreducible. Assume that either $p \nmid N$ or $p || N$ and $I_f \subseteq \mathbf{m}$ for some newform f. Then $\mathbf{m}$ satisfies multiplicity one.

Mazur-Ribet: Examples of failure of multiplicity one if p^3 divides the level.

Kilford: Multiplicity one fails for a maximal ideal over 2 at levels 431, 503, and 2089.

Modular exponent, congruence exponent, and multiplicity one

Theorem 1 (A, Ribet, Stein): The modular exponent divides the congruence exponent and the ratio is only divisible by primes whose squares divide N.

Theorem 2 (A, Ribet, Stein): Let p be a prime such that every maximal ideal of residue characteristic p satisfies multiplicity one. Then the modular exponent equals the congruence exponent locally at p.

Example 1 (Stein): There is an elliptic curve E of conductor 54 with modular degree = 2 and congruence number = 6; hence multiplicity one fails for some maximal ideal at level 54.

Modular number, congruence number, and multiplicity one

By Theorem 1, if A_f is an elliptic curve, then the modular number divides the square of the congruence number. Is it true for all A_f?
Example 2 (Stein): There is a newform on $\Gamma_0(431)$ for which the answer is no (fails at 2).

Theorem 3: Let p be a prime such that every maximal ideal of residue characteristic p satisfies multiplicity one. Then the modular number is the square of the congruence number locally at p.

In Example 2 above, Theorem 3 shows that multiplicity one fails for some maximal ideal at level 431 – this could not be detected by Theorem 2 (in view of Theorem 1: 431 is prime); but was known by work of Kilford (different method).

If an elliptic curve has congruence number bigger than its modular degree, then multiplicity one fails (e.g., earlier Example 1).

Proof 1 of Theorem 3

Lemma 1 (Emerton): Let I be a saturated ideal of $\mathbf{T}$ and let $J[I]^0$ denote the abelian subvariety of J that is the connected component of $J[I]$. Then the quotient $J[I]/J[I]^0$ is supported at maximal ideals of $\mathbf{T}$ that do not satisfy multiplicity one.

Let $I_A = \text{Ann}A$ and $I_B = \text{Ann}B$. Then $A \subseteq J[I_A]$ and $B \subseteq J[I_B]$ are equalities locally at maximal ideals that satisfy multliplicity one.

Prop 1: The cokernel of the injection $A \cap B \to J[I_A + I_B]$ is supported at maximal ideals of $\mathbf{T}$ that contain $I_A + I_B$ and do not satisfy multiplicity one.

Fact: $|\frac{\mathbf{T}}{I_A+I_B}| =$ the congruence number.

Lemma 2 (Ribet): Let I be an ideal of $\mathbf{T}$ of finite index. Suppose that every maximal ideal $\mathbf{m}$ of $\mathbf{T}$ that contains I satisfies multiplicity one. Then $J[I]$ has order $|\mathbf{T}/I|^2$.

Que: Is $J[I]$ free of rank two over $\mathbf{T}/I$?

Proof 2 of Theorem 3

(due to M. Dimitrov and anonymous referee)

$$\begin{aligned} A \cap B &\cong \frac{H_1(J, \mathbf{Z})}{H_1(A, \mathbf{Z}) + H_1(B, \mathbf{Z})} \\ &= \frac{H_1(J, \mathbf{Z})}{H_1(J, \mathbf{Z})[I_A] + H_1(J, \mathbf{Z})[I_B]}. \end{aligned}$$

Suppose $\mathbf{m}$ satisfies multiplicity one.

Then by Mazur,
$H_1(J, \mathbf{Z}) \otimes_{\mathbf{T}} \mathbf{T}_{\mathbf{m}}$ is free of rank two over $\mathbf{T}_{\mathbf{m}}$.
So "locally at $\mathbf{m}$",
$A \cap B \cong$ two copies of $\frac{\mathbf{T}}{\mathbf{T}[I_A]+\mathbf{T}[I_B]} = \frac{\mathbf{T}}{I_B+I_A}$.

Prop 2: "Locally at $\mathbf{m}$", $A \cap B$ is free of rank two over $\frac{\mathbf{T}}{I_A+I_B}$.

Taking orders, Theorem 3 follows.

Moreover, combining with Prop 1, we get
Prop 4: "Locally at $\mathbf{m}$", $J[I_A + I_B]$ is free of rank two over $\frac{\mathbf{T}}{I_A+I_B}$.