MODULAR FORMS, ELLIPTIC CURVES AND THE ABC–CONJECTURE

Dorian Goldfeld*

Dedicated to Alan Baker on the occasion of his sixtieth birthday.

§1. The ABC–Conjecture.

The ABC–conjecture was first formulated by David Masser and Joseph Osterlé (see [**Ost**]) in 1985. Curiously, although this conjecture could have been formulated in the last century, its discovery was based on modern research in the theory of function fields and elliptic curves, which suggests that it is a statement about ramification in arithmetic algebraic geometry. The ABC–conjecture seems connected with many diverse and well known problems in number theory and always seems to lie on the boundary of what is known and what is unknown. We hope to elucidate the beautiful connections between elliptic curves, modular forms and the ABC–conjecture.

Conjecture (ABC). *Let A, B, C be non–zero, pairwise relatively prime, rational integers satisfying $A + B + C = 0$. Define*

$$N = \prod_{p|ABC} p$$

to be the squarefree part of ABC. Then for every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that

$$\max(|A|, |B|, |C|) < \kappa(\epsilon) N^{1+\epsilon}.$$

A weaker version of the ABC–conjecture (with the same notation as above) may be given as follows.

Conjecture (ABC) (weak). *For every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that*

$$|ABC|^{\frac{1}{3}} < \kappa(\epsilon) N^{1+\epsilon}.$$

Oesterlé, [**Ost**] showed that if we define

$$\kappa(\epsilon) = \inf_{\substack{A+B+C=0 \\ (A,B)=1}} \frac{\max(|A|, |B|, |C|)}{N^{1+\epsilon}}$$

* Supported in part by a grant from the NSF.
The author would like to thank Iris Anshel and Shu-Wu Zhang for many helpful conversations.

then

$$\lim_{\epsilon \to 0} \kappa(\epsilon) = \infty.$$

The best result in this direction, known to date, seems to be in the paper of Stewart and Tijdeman **[S–T]**. They prove that for any fixed positive δ there exist infinitely many solutions of

$$A + B + C = 0, \quad (A, B) = 1, \quad N = \prod_{p|ABC} p \ > \ 3$$

with

$$\max(|A|, |B|, |C|) > N \exp\left((4 - \delta)\frac{\sqrt{\log N}}{\log\log N}\right).$$

In 1996 Alan Baker **[B]** proposed a more precise version of the ABC–conjecture.

Conjecture (ABC). (Baker) *For every $\epsilon > 0$ there exists a constant $\kappa(\epsilon) > 0$ such that*

$$\max\left(|A|, |B|, |C|\right) < \kappa(\epsilon) \cdot \left(\epsilon^{-\omega} N\right)^{1+\epsilon},$$

where ω denotes the number of distinct prime factors of ABC.

This conjecture would give the best lower bounds one could hope for in the theory of linear forms in logarithms. In the same paper **[B]** Baker attributes to Granville the following intriguing conjecture.

Conjecture (ABC). (Granville) *Let $\Theta(N)$ denote the number of integers less than or equal to N that are composed only of prime factors of N. Then*

$$\max\left(|A|, |B|, |C|\right) << N\Theta(N).$$

At present the best known results in the direction of the ABC–conjecture are exponential in small powers of N and are obtained using machinery from Baker's theory of linear forms in logarithms. The first such result was obtained by Stewart and Tijdeman **[S–T]** in 1986.

Theorem 1. *Let A, B, C be positive integers satisfying $A + B = C$, $(A, B) = 1$, $C > 2$. Then there exists a constant $\kappa > 0$ (effectively computable) such that $C < e^{\kappa \cdot N^{15}}$.*

This was improved in 1990 by Stewart and Yu **[S–Y]** to

Theorem 2. *Let A, B, C be positive integers satisfying $A + B = C$, $(A, B) = 1$, $C > 2$. Then there exists a constant $\kappa > 0$ (effectively computable) such that*

$$C < e^{N^{\frac{2}{3} + \frac{\kappa}{\log\log N}}}.$$

The constant $\frac{2}{3}$ has recently been improved by Yu to $\frac{1}{3}$.

§2. Applications of the ABC–Conjecture.

In order to show the profound importance of the ABC–conjecture in number theory, we enumerate some remarkable consequences that would follow if the ABC–conjecture were proven.

Theorem 3. *Assume the ABC–conjecture. Fix $0 < \epsilon < 1$, and fix non–zero integers α, β, γ. Then the diophantine equation*

$$\alpha x^r + \beta y^s + \gamma z^t = 0.$$

has only finitely many solutions in integers x, y, z, r, s, t satisfying

$$xyz \neq 0, \quad (x,y) = (x,z) = (y,z) = 1, \qquad r,s,t > 0 \quad \text{and} \quad \frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1 - \epsilon.$$

Moreover, the number of such solutions can be effectively computed provided the constant $\kappa(\epsilon)$ in the ABC–conjecture is effective.

Proof: Let

$$A = \alpha x^r, \ B = \beta y^s, \ C = \gamma z^t.$$

Without loss of generality, we may assume that $|C|$ is the maximum of $|A|, |B|, |C|$. The ABC–conjecture ($|C| < \kappa(\epsilon) N^{1+\epsilon}$) then implies that

$$|\gamma z^t| < \kappa(\epsilon) \cdot |\alpha\beta\gamma xyz|^{1+\epsilon}. \tag{2.1}$$

Since $|A|, |B| \leq |C|$ it immediately follows that

$$|x| \leq \left|\frac{\gamma}{\alpha}\right|^{\frac{1}{r}} \cdot |z|^{\frac{t}{r}}, \qquad |y| \leq \left|\frac{\gamma}{\beta}\right|^{\frac{1}{s}} \cdot |z|^{\frac{t}{s}}.$$

Plugging these bounds into (2.1) and taking the t^{th} root of both sides, we obtain

$$|z| << \kappa(\epsilon) \left|z^{\frac{1}{r}+\frac{1}{s}+\frac{1}{t}}\right|^{1+\epsilon} << \kappa(\epsilon)|z|^{1-\epsilon^2}, \tag{2.2}$$

where the implied constants $<<$ can be effectively computed and depend at most on α, β, γ. The inequality (2.2) plainly implies that there can be at most finitely many integers z satisfying (2.2).

Without loss of generality, we may now assume that $|A| \leq |B|$. It follows that

$$|x| \leq \left|\frac{\beta}{\alpha}\right|^{\frac{1}{r}} \cdot |y|^{\frac{s}{r}}. \tag{2.3}$$

Writing the ABC–conjecture in the form

$$|\beta y^s| < \kappa(\epsilon) \cdot |\alpha\beta\gamma xyz|^{1+\epsilon}, \tag{2.4}$$

and using the previously proved fact that $|z|$ lies in a finite set, it follows from (2.3) and (2.4) that

$$|y| << |y|^{(\frac{1}{r}+\frac{1}{s})\cdot(1+\epsilon)} << |y|^{1-\epsilon^2}.$$

Thus, y also lies in a finite set. Writing the ABC–conjecture in the form

$$|\beta x^r| < \kappa(\epsilon) \cdot |\alpha\beta\gamma xyz|^{1+\epsilon},$$

and noting that r must be ≥ 2, it immediately follows that

$$|x| << x^{\frac{1+\epsilon}{r}},$$

so that x also must lie in a finite set. Finally, we again use the ABC–conjecture to write

$$\max |\alpha x^r|, |\beta y^s|, |\gamma z^t| << 1$$

since x, y, z lie in a finite set. Thus, r, s, t also must lie in a finite set.

In 1988 Silverman **[S1]** proved the following theorem.

Theorem 4. *Assume the ABC–conjecture. Then there exist infinitely many primes p such that*

$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$

In 1991 Elkies **[E]** proved that the ABC–conjecture implies the Mordell conjecture (this was first proved by Faltings **[F]**) which states that every algebraic curve of genus ≥ 2 defined over $\mathbf{Q}$ has only finitely many rational points.

Another interesting application is due to Granville **[Gr]** 1998. He proved the following.

Theorem 5. *Let $f(x)$ be a polynomial with integer coefficients which is not divisible by the square of another polynomial. Then there exists a constant $c_f > 0$ such that*

$$\sum_{\substack{n \leq x \\ f(n) \text{ is squarefree}}} 1 \quad \sim \quad c_f x \qquad (x \to \infty).$$

The most recent application of ABC is due to Granville and Stark **[Gr-S]** (1999). They show that a very strong uniform ABC–conjecture for number fields implies there are no Siegel zeros for Dirichlet L–functions associated to imaginary quadratic fields $\mathbf{Q}(\sqrt{-d})$ where $-d < 0$, and d is squarefree with $-d \equiv 1(4)$ or $-d \equiv 8, 12(16)$.

Vojta (**[V]**, 1987) first showed how to formulate the ABC–conjecture for number fields. Let $K/\mathbf{Q}$ be a number field of degree n with discriminant D_K. For each prime ideal $\mathfrak{p}$ of K define a valuation $|\ |_{\mathfrak{p}}$ normalized so that $|\mathfrak{p}|_{\mathfrak{p}} = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{p})^{-\frac{1}{n}}$. For each embedding

$v : K \to \mathbf{C}$ define a valuation $|\ |_v$ by $|\alpha|_v = |\alpha^v|^{\frac{1}{n}}$, for $\alpha \in K$, and where $|\ |$ denotes the ordinary absolute value on $\mathbf{C}$. For $\alpha_1, \alpha_2, \ldots, \alpha_m \in K$ we define the height:

$$H(\alpha_1, \ldots, \alpha_m) = \prod_v \max\Big(|\alpha_1|_v, |\alpha_2|_v, \ldots, |\alpha_m|_v\Big),$$

where the product goes over all places v (prime ideals and embeddings). We also define the conductor:

$$N(\alpha_1, \ldots, \alpha_m) = \prod_{\mathfrak{p} \in I} |\mathfrak{p}|_{\mathfrak{p}}^{-1}$$

where I denotes the set of prime ideals $\mathfrak{p}$ such that $|\alpha_1|_{\mathfrak{p}}, \ldots, |\alpha_m|_{\mathfrak{p}}$ are not all equal. We can now state.

Uniform *ABC*–**Conjecture.** *Let $\alpha, \beta, \gamma \in K$ satisfy $\alpha + \beta + \gamma = 0$. Then for every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that*

$$H(\alpha, \beta, \gamma) \leq \kappa(\epsilon)\Big(D_K^{\frac{1}{n}} \cdot N(\alpha, \beta, \gamma)\Big)^{1+\epsilon}.$$

Assuming the uniform *ABC*–conjecture Stark and Granville obtained the following lower bound for the class number $h(-d)$ of $\mathbf{Q}(\sqrt{-d})$:

$$h(-d) \ \geq \ \Big(\frac{\pi}{3} + o(1)\Big)\frac{\sqrt{d}}{\log d} \sum_{\substack{(a,b,c) \in \mathbf{Z}^3 \\ -d = b^2 - 4ac \\ -a < b \leq a < c \ \text{ or } \ 0 \leq b \leq a = c}} \frac{1}{a} \qquad (d \to +\infty).$$

§3. Elliptic curves over Q (Global Minimal Models).

An elliptic curve over a field K is a projective non–singular algebraic curve of genus one defined over K, furnished with a K–rational point. Every such curve has a generalized Weierstrass equation or model of the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in K, (i = 1, 2, 3, 4, 6)$ with K–rational point (point at infinity) given in projective coordinates by $(0, 1, 0)$. It was first proved by Mordell **[Mo]** (for $K = \mathbf{Q}$) and generalized by Weil **[W]** to arbitrary K that the K–rational points on E (denoted $E(K)$) form a finitely generated abelian group (Mordell–Weil group). The rank of the Mordell–Weil group $E(K)$ is defined to be the number of generators of infinite order.

Following Tate's formulaire [**T1**], we define

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta, \end{aligned}$$

where Δ denotes the discriminant of E.

Let

$$E' : y'^2 + a_1'xy + a_3'y = x'^3 + a_2'x'^2 + a_4'x' + a_6'$$

be another elliptic curve defined over K. Then E, E' are isomorphic if and only if there is a coordinate change of the form

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t$$

with $r, s, t \in K$ and $u \in K^*$, which transforms E to E'. In this case we have

$$j' = j, \qquad \Delta' = u^{-12}\Delta.$$

For each rational prime number p, consider the local field $\mathbf{Q}_p$. Let v_p denote the p–adic valuation normalized so that $v_p(p) = 1$, $\mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid v_p(x) \geq 0\}$, denotes the ring of p–adic integers.

Fix a rational prime p. Among all isomorphic models of a given elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

defined over $\mathbf{Q}_p$, we can find one where all coefficients $a_i \in \mathbf{Z}_p$, and thus $v_p(\Delta) \geq 0$. This is easily seen by the coordinate change $x \to u^{-2}x$, $y \to u^{-3}y$ which sends each a_i to u^ia_i. Choosing u to be a high power of p does what we want. Since v_p is discrete, we can look for an equation with $v_p(\Delta)$ as small as possible.

Definition (Global Minimal Model). *Let E be an elliptic curve over $\mathbf{Q}$ with Weierstrass equation given by*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then E is defined to be minimal at p if

- $a_i \in \mathbf{Z}_p \;\; (i = 1, 2, 3, 4, 6)$
- $v_p(\Delta)$ *is minimal (among all isomorphic models over $\mathbf{Q}_p$).*

We define E to be a global minimal model if E is minimal at every prime p.

§4. Conjectures which are equivalent to ABC.

Let E be an elliptic curve defined over $\mathbf{Q}$ (global minimal model) with Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then associated to E we have two important invariants:

- Discriminant $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$,
- Conductor $N = \prod_p \Delta p^{f_p}$, where

$$f_p = \begin{cases} 0, & \text{if } E(\mathbf{F}_p) \text{ is nonsingular;} \\ 1, & \text{if } E(\mathbf{F}_p) \text{ has a nodal singularity;} \\ 2+\delta, & \text{if } E(\mathbf{F}_p) \text{ has a cuspidal singularity, with } \delta = 0 \text{ if } p \neq 2,3. \end{cases}$$

The recipe for the conductor was first shown by Ogg [**O**] in 1967. An algorithm to compute f_p in all cases was proposed by Tate in a letter to Cassels (see [**T1**]). An elliptic curve which never has bad reduction of cuspidal type is said to be semistable, and in this case N is always the squarefree part of Δ. This is the bridge between the theory of elliptic curves and the ABC–conjecture.

Conjecture. (Szpiro, 1981) *Let E be an elliptic curve over $\mathbf{Q}$ which is a global minimal model with discriminant Δ and conductor N. Then for every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that*

$$\Delta < \kappa(\epsilon)N^{6+\epsilon}.$$

We show that Szpiro's conjecture above is equivalent to the weak ABC–conjecture. Let A, B, C be coprime integers satisfying $A + B + C = 0$ and $ABC \neq 0$. Set $N = \prod_{p|ABC} p$. Consider the Frey–Hellegouarch curve

$$E_{A,B} : y^2 = x(x - A)(x + B).$$

A minimal model for $E_{A,B}$ has discriminant $(ABC)^2 \cdot 2^{-s}$ and conductor $N \cdot 2^{-t}$ for certain absolutely bounded integers s, t, (see Frey [**F1**]). Plugging this data into Szpiro's conjecture immediately shows the equivalence.

Another conjecture equivalent to a version of the ABC–conjecture is the degree conjecture. Let $\Gamma_0(N)$ denote the group of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z})$ with $c \equiv 0 \pmod N$, and set $X_0(N)$ to be the compactified Riemann surface realized as the quotient of the upper–half plane by $\Gamma_0(N)$. An elliptic curve E defined over $\mathbf{Q}$ is said to be modular if there exists a non–constant covering map

$$\phi : X_0(N) \to E,$$

normalized so that $\phi(i\infty) = 0$, the origin on E. It is now known (by work of Christophe Breuil, Brian Conrad, Fred Diamond, Richard Taylor, and Andrew Wiles) that every

elliptic curve over $\mathbf{Q}$ is modular. The degree conjecture concerns the growth in N of the topological degree of the map ϕ as $N \to \infty$.

Degree Conjecture. (Frey 1987) *For every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that* $\deg(\phi) < \kappa(\epsilon) N^{2+\epsilon}$.

Frey **[F2]** proved that some bound for the degree implies a weak version of the ABC–conjecture. It was shown by Mai–Murty **[M–M]** (1994) that the ABC–conjecture implies the degree conjecture for all Frey–Hellegouarch curves and by Murty **[M]** in 1996 that the degree conjecture implies the ABC–conjecture. These results use work of Wiles–Diamond **[Wi]**, **[D]** as well as work of Goldfeld–Hoffstein–Liemann–Lockhart **[G-H-L-L**] on the non–existence of Siegel zeros on $GL(3)$ which are symmetric square lifts from $GL(2)$.

The ABC conjecture is also intimately related to the size of the periods of the Frey–Hellegouarch curve

$$E_{A,B} : y^2 = x(x-A)(x+B).$$

Assume $-B < 0 < A$. This curve has two periods:

$$\Omega_1 = 2\int_{-B}^{0} \frac{dx}{\sqrt{x(x-A)(x+B)}}$$

and

$$\Omega_2 = 2\int_{A}^{\infty} \frac{dx}{\sqrt{x(x-A)(x+B)}}.$$

Period Conjecture. (Goldfeld 1988) *Let $E_{A,B} : y^2 = x(x-A)(x+B)$ be the Frey–Hellegouarch curve with $A, B \in \mathbf{Z}$, $(A,B) = 1$, and $-B < 0 < A$. Let N denote the conductor of $E_{A,B}$. Then for every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that*

$$\min\left(|\Omega_1|, |\Omega_2|\right) > \kappa(\epsilon) N^{-\frac{1}{2}-\epsilon}.$$

It was shown in **[G1]** that the period conjecture implies the weak ABC–conjecture.

The final conjecture we shall discuss (which is equivalent to ABC) is a conjecture on the size of the Shafarevich–Tate group Ш (see **[Sha]**, **[T2]**) of an elliptic curve defined over $\mathbf{Q}$. It was only recently (see **[R1]**, **[R2]**, **[Kol1]**, **[Kol2]**, **[Kol3]**) that Ш was proved finite for a single elliptic curve and this explains why the ABC conjecture is so intractable. We shall now define Ш from first principles.

Let X be a set. We say a group G acts on X with left set–action $\bullet$ if for all $g \in G,\ x \in X$, the binary operation $g \bullet x \in X$, and $\bullet$ satisfies (for all $g, g' \in G, x \in X$) the identities: $e \bullet x = x,\ (g \cdot g') \bullet x = g \bullet (g' \bullet x)$, where e is the identity in G and $\cdot$ denotes the group operation in G. If A is an abelian group with internal operation $+$, we say G acts on A with left–group action $\circ$ if $\circ$ is a left set–action which also satisfies $g \circ (a + a') = g \circ a + g \circ a'$ for all $g \in G$ and $a, a' \in A$.

Let A be an abelian group with internal operation $+$ and let G be another group which acts on A with left group–action $\circ$. We define $Z^1(G,A)$ to be the group of all functions (cocycles) $c : G \to A$ which satisfy the cocycle relation

$$c(g \cdot g') = c(g) + g \circ c(g'),$$

where $\cdot$ denotes the group operation in G. The subgroup $B^1(G,A)$ of coboundaries consists of all cocycles of the form $g \circ a - a$ with $a \in A$. We define the first cohomology group $H^1(G,A)$ to be the quotient group $H^1(G,A) = Z^1(G,A)/B^1(G,A)$.

Definition. *Fix an abelian group A and another group G acting on A with a left group–action $\circ$. A principal homogeneous action for $(G,A,\circ)$ is a left set–action $\bullet$ of G on A which satisfies the identity*

$$g \bullet a - g \bullet a' = g \circ a - g \circ a'$$

for all $g \in G$ and $a, a' \in A$.

We now define an equivalence relation on the set of principal homogeneous actions.

Definition. *Two principal homogeneous actions $\bullet, \bullet'$ for $(G,A,\circ)$ are said to be equivalent if*

$$g \bullet a - g \bullet' a = g \circ a_0 - a_0$$

for all $g \in G$, all $a \in A$, and some fixed $a_0 \in A$.

Let $WC(G,A)$ denote the set of equivalence classes of principal homogeneous actions for $(G,A,\circ)$. We will show that $WC(G,A)$ (Weil–Châtelet group) is in fact a group by demonstrating that there is a bijection (of sets) $\beta : WC(G,A) \to H^1(G,A)$. First, if $\bullet$ is a principal homogeneous action for $(G,A,\circ)$ then for some fixed $a_0 \in A$ we have that $c(g) := g \bullet a_0 - a_0 \in Z^1(G,A)$ because

$$\begin{aligned} c(g \cdot g') &= (g \cdot g') \bullet a_0 - a_0 = g \bullet (g' \bullet a_0) - a_0 = g \bullet (g' \bullet a_0) - g \bullet a_0 + g \bullet a_0 - a_0 \\ &= g \circ (g' \bullet a_0) - g \circ a_0 + c(g) = g \circ c(g') + c(g). \end{aligned}$$

Further, if we replace a_0 by $a_0 + a$ for any $a \in A$ then the cocycle changes to $c(g) + g \circ a - a$ which is equivalent to $c(g) \bmod B^1(G,A)$. Thus each principal homogeneous action $\bullet$ maps to a unique element of $H^1(G,A)$. One also easily checks that equivalent homogeneous actions map to the same element of $H^1(G,A)$. Finally, to show the surjectivity, let $c(g) \in Z^1(G,A)$. Define a left action $\bullet$ of G on A by $g \bullet a := c(g) + g \circ a$ for all $g \in G$ and $a \in A$. If we change $c(g)$ to the equivalent cocycle $c(g) + g \circ a_0 - a_0$ then this gives rise to a new action $\bullet'$ given by $b \bullet' a = c(g) + g \circ a_0 - a_0 + g \circ a$. Clearly $\bullet$ and $\bullet'$ are equivalent principal homogeneous actions.

Remark. *The identity element in the group $WC(G,A)$ is the equivalence class of all actions equivalent to $\circ$. A principal homogeneous action $\bullet$ is equivalent to $\circ$ if and only if G has a fixed point under the left set–action $\bullet$, i.e., if and only if there exists $a_0 \in A$ such that $g \bullet a_0 = a_0$ for all $g \in G$ (clearly true because $g \bullet a_0 - a_0$ is the zero cocycle).*

In order to explicitly realize principal homogeneous actions, it is often convenient to consider a set $X = \phi(A)$ where ϕ is a bijection. The bijection ϕ leads to a transitive right set–action of A on X (denoted X^A) and defined by $x^{a'} = \phi(a + a')$ for all $x = \phi(a) \in X$, and all $a' \in A$. In this situation, the existence of a principal homogeneous action $\bullet$ for $(G, A, \circ)$ gives rise to a left set–action $\bullet'$ of G on X defined by

$$g \bullet' x = \phi(g \bullet a)$$

for all $g \in G$, and $x = \phi(a) \in X$. One checks that $g \bullet' x^{a_1} = (g \bullet' x)^{g \circ a_1}$ for all $a_1 \in A$. Thus X has the properties of a principal homogeneous space (see [**Se**]), i.e., there is a right set–action of A on X and a left principal homogeneous action $\bullet$ of G on X.

To define the Shafarevich–Tate group Ш for an elliptic curve E defined over $\mathbf{Q}$ we first consider the Weil–Châtelet group $WC(G, E(\bar{\mathbf{Q}}))$ where $G = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ which acts on $E(\bar{\mathbf{Q}})$, the group of $\bar{\mathbf{Q}}$–rational points on E. Elements of $WC(G, E(\bar{\mathbf{Q}}))$ can be realized as curves of genus one, denoted X, defined over $\mathbf{Q}$ which are birationally equivalent to E over $\bar{\mathbf{Q}}$ together with an appropriate action $\bullet$. Note that a curve of genus one defined over $\mathbf{Q}$ may not have a point in $\mathbf{Q}$. Let $\phi : E \to X$ be such a birational equivalence. Then for any $g \in G$ the map

$$(g\phi)\phi^{-1} : E \to E$$

is of the type (see [**C2**])

$$a \to a + c(g)$$

with $a \in E(\bar{\mathbf{Q}})$, $c(g) \in Z^1(G, E(\bar{\mathbf{Q}}))$, and addition above denoting addition on the elliptic curve E. The right action of $E(\bar{\mathbf{Q}})$ on $X(\bar{\mathbf{Q}})$ is then given by translation (on the elliptic curve E): $x^{a'} = \phi(a + a')$ for $x = \phi(a) \in X(\bar{\mathbf{Q}})$, $a, a' \in E(\bar{\mathbf{Q}})$. The left action $\bullet$ of G on $X(\bar{\mathbf{Q}})$ is given by $g \bullet x = \phi(a + c(g))$ with $x = \phi(a) \in X(\mathbf{Q})$ which is induced from the cocycle $c(g)$ associated to the birational equivalence. The Tate–Shafarevich group Ш for E over $\mathbf{Q}$ is defined to be the subgroup of $WC(G, E(\bar{\mathbf{Q}}))$ associated to curves X as above which have a point in $\mathbf{R}$ and in every p–adic field $\mathbf{Q}_p$, or equivalently, the elements of $WC(G, E(\bar{\mathbf{Q}}))$ which have trivial images in $WC(G_p, E(\bar{\mathbf{Q}}_p)$ and $WC(G_\infty, E(\mathbf{C})$, where $G_p = \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ for all finite primes p, and $G_\infty = \mathrm{Gal}(\mathbf{C}/\mathbf{R})$. If X has a point in $\mathbf{Q}$ then by the remark above, the action $\bullet$ of G on X is in the identity class of principal homogeneous actions. Thus, Ш measures the obstruction to the Hasse principle (Hasse's principle states that if a curve has points in $\mathbf{R}$ and in every p-adic field $\mathbf{Q}_p$ then it has a point in $\mathbf{Q}$).

Definition. Mazur [**Ma2**] *defined the notion of a companion to an elliptic curve E as a curve X of genus one which is isomorphic to E over R and over Q_p for all primes p. The Shafarevich –Tate group* Ш *may then be defined as the set of isomorphism classes over* $\mathbf{Q}$ *of companions of E, each endowed (as above) with the structure of a principal homogeneous space.*

Conjecture I. (Bound for Ш) *Let E be an elliptic curve defined over* $\mathbf{Q}$ *of conductor N with Shafarevich–Tate group* Ш. *Then for every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that*

$$|Ш| < \kappa(\epsilon) N^{\frac{1}{2}+\epsilon} \qquad (N \to \infty).$$

One of the most remarkable conjectures in number theory is the Birch–Swinnerton–Dyer conjecture [**B-S-D**] which relates the rank of the Mordell–Weil group of an elliptic curve E and the Shafarevich–Tate group of E to the special value at $s = 1$ of the Hasse–Weil L–function associated to E (see [**S2**] for the definition of the Hasse–Weil L–function). It was shown in Goldfeld–Szpiro (1995) [**G-S**] that assuming the B–S–D (for rank 0 curves only), the above conjectured bound for Ш implies the following version of the ABC–conjecture:

$$|ABC|^{\frac{1}{3}} << N^{3+\epsilon}.$$

If one further assumes the generalized Riemann hypothesis (for the Rankin–Selberg zeta function associated to the weight $\frac{3}{2}$ cusp form coming from the Shintani–Shimura lift) then it was also shown in [**G-S**] that the above conjectured bound for Ш (for rank 0 curves only) implies the weak ABC–conjecture:

$$|ABC|^{\frac{1}{3}} << N^{1+\epsilon}.$$

Actually, similar implications can be obtained from the following weaker conjecture.

Conjecture II. (Average Bound for $Ш_q$) *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve of conductor N with $a, b \in \mathbf{Z}$. For a square–free integer q, define the twisted curve $E_q : y^2 = x^3 + q^2ax + q^3b$ with Mordell–Weil rank r_q and Shafarevich–Tate group $Ш_q$. Then there exists a constant $c > 0$ and for every $\epsilon > 0$ there exists a constant $\kappa(\epsilon) > 0$ such that*

$$\sum_{\substack{q < N^c \\ r_q = 0}} |Ш_q| \ < \ \kappa(\epsilon) N^{c+\frac{1}{2}+\epsilon} \qquad (N \to \infty).$$

We now sketch the proof that Conjecture II plus B-S-D implies a version of the ABC–conjecture. The B-S-D conjecture states that the Hasse–Weil L–function $L_E(s)$ of an elliptic curve E defined over $\mathbf{Q}$ has a zero of order $r =$ rank of the Mordell-Weil group of $E(\mathbf{Q})$ and that the Taylor series of $L_E(s)$ about $s = 1$ is given by

$$L_E(s) = \left(\frac{c_E \Omega_E \cdot |Ш_E| \cdot \mathrm{vol}(E(\mathbb{Q}))}{|E(\mathbb{Q})_{\mathrm{tor}}|^2} \right) \cdot (s-1)^r + O(s-1)^{r+1}.$$

Here Ω_E is either the real period or twice the real period of E (depending on whether or not $E(\mathbb{R})$ is connected), $|Ш_E|$ is the order of the Tate–Shafarevich group of $E/\mathbb{Q}$, $\mathrm{vol}(E(\mathbb{Q}))$ is the volume of the Mordell–Weil group for the Néron–Tate bilinear pairing, $|E(\mathbb{Q})_{\mathrm{tors}}|$ is the order of the torsion subgroup of $E/\mathbb{Q}$, and $c_E = \prod_p c_p$ where $c_p = 1$ unless E has bad reduction at E in which case c_p is the order $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ (Here $E_0(\mathbb{Q}_p)$ is the set of points reducing to non-singular points of $E(\mathbb{Z}/p\mathbb{Z})$.) (see [**S2**]).

It is known that $c_E \geq 1$,

$$|E(\mathbb{Q})_{\mathrm{tors}}|^2 \ \leq \ 256 \qquad \text{(Mazur 1977 [\textbf{Ma1}])},$$

and that $\mathrm{vol}(E(\mathbb{Q})) = 1$ if $r = 0$. So in the rank $r = 0$ situation, a lower bound for $L_E(1)$ together with an upper bound for the order of $Ш_E$ would imply a lower bound for the period Ω_E. If the lower bound for the period were strong enough to give the period conjecture we would get a version of ABC. It is enough to do this for one twisted curve E_q since the period changes by $q^{-\frac{1}{2}}$. Now, by a theorem of Waldspurger (see **[Wa], [Koh]**) one can find enough twists ($q < N^c$ with $c >> 1$) of E with Mordell–Weil rank zero where $L_{E_q}(1) >> 1$, to do what we want. In the case $0 < c << 1$ it is necessary to use the generalized Riemann hypothesis.

Conjecture I can be proved for CM elliptic curves with $j \neq 0, 1728$ (we actually get better bounds). This was first done in Goldfeld–Lieman (1996) **[G-L]** (see Theorem 6 below). For CM elliptic curves E defined over $\mathbf{Q}$ we expect.

Conjecture. *Let E be a CM elliptic curve defined over $\mathbf{Q}$ with Shafarevich–Tate group $Ш_E$. Then*

$$\begin{aligned} |Ш_E| &<< N^{\frac{1}{4}+\epsilon}, \qquad (\textit{if } j \neq 0, 1728) \\ |Ш_E| &<< N^{\frac{5}{12}+\epsilon}, \qquad (\textit{if } j = 0) \\ |Ш_E| &<< N^{\frac{3}{8}+\epsilon}, \qquad (\textit{if } j = 1728). \end{aligned}$$

The constant $<<$ depends only on ϵ and is effectively computable.

Theorem 6. (Goldfeld–Lieman) *Let E be a CM elliptic curve defined over $\mathbf{Q}$ with Mordell–Weil rank 0 and Shafarevich–Tate group $Ш_E$. Then*

$$\begin{aligned} |Ш_E| &<< N^{\frac{59}{120}+\epsilon}, \qquad (\textit{if } j \neq 0, 1728) \\ |Ш_E| &<< N^{\frac{37}{60}+\epsilon}, \qquad (\textit{if } j = 0) \\ |Ш_E| &<< N^{\frac{79}{120}+\epsilon}, \qquad (\textit{if } j = 1728). \end{aligned}$$

The constant $<<$ depends only on ϵ and is effectively computable.

This result uses the deep work of K. Rubin **[R1]** (where the B-S-D conjecture is proved for CM elliptic curves over $\mathbf{Q}$ of Mordell–Weil rank 0), together with the upper bounds for special values of L–functions obtained by Duke–Friedlander–Iwaniec **[D–F–I]**.

§5. Large Shafarevich–Tate groups.

Cassels **[C1]** in 1964 showed that the Tate–Shafarevich group of an elliptic curve over $\mathbf{Q}$ can be arbitrarily large. Cassels method actually shows that there exist a fixed constant $c > 0$ and infinitely many integers N for which there exist an elliptic curve of conductor N, defined over $\mathbf{Q}$, with

$$|Ш| >> N^{\frac{c}{\log\log N}},$$

This result was obtained by a different method by Kramer **[Kr]** in 1983. Assuming the Birch–Swinnerton–Dyer conjecture, Mai–Murty **[M–M]** showed in 1994 that there are infinitely many elliptic curves, defined over $\mathbf{Q}$ for which

$$|Ш| >> N^{\frac{1}{4}-\epsilon}.$$

This was improved by De Weger in 1996 **[We]** who showed that

$$|Ш| >> N^{\frac{1}{2}-\epsilon}$$

infinitely often, under the assumption of both the generalized Riemann hypothesis and the Birch–Swinnerton–Dyer conjecture.

The connection between the ABC–conjecture and the growth of Ш allows one to construct elliptic curves with large Shafarevich–Tate groups from bad ABC examples. B. De Weger (1997) **[We]** has found 11 examples of curves with $|Ш| > \sqrt{N}$. Cremona (1993) **[Cr]** (by other methods) had also found several such curves.

The best known example of a Frey–Hellegouarch curve with large Ш is

$$y^2 = x(x - 643641)(x + 2)$$

coming from the ABC example, $A = 3^{10} \cdot 109,\ B = 2,\ C = 23^5,$ due to Reyssat with $N = 15042$. In this case:

$$\frac{|Ш|}{\sqrt{N}} = 0.7358...$$

§6. Modular Symbols.

Let $f(z) = \sum_{n=1}^{\infty} a(n)e^{2\pi inz}$ be a holomorphic Hecke newform of weight two for $\Gamma_0(N)$ normalized so that $a(1) = 1$. For $\gamma \in \Gamma_0(N)$ we define the modular symbol

$$< \gamma, f >= -2\pi i \int_{\tau}^{\gamma\tau} f(z)\, dz$$

which is independent of $\tau \in \mathfrak{h} \cup \mathbf{Q} \cup \{i\infty\}$. Shimura (1973) **[Sh]** showed that the modular symbol is a homomorphism of $\Gamma_0(N)$ into the period lattice associated with $J_0(N)$. More specifically, if the coefficients $a(n)$ all lie in $\mathbf{Q}$ then the homomorphism is into the period lattice of an elliptic curve, i.e.,

$$< \gamma, f >= m_1\Omega_q + m_2\Omega_2$$

where $m_1, m_2 \in \mathbf{Z}$ and $E = \mathbf{C}/\mathbf{Z}[, \Omega_1, \Omega_2]$. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, define the height of γ, denoted $H(\gamma)$ to be the maximum of $|a|, |b|, |c|, |d|$.

Modular Symbol Conjecture. (Goldfeld 1988) *Let* $< \gamma, f >= m_1\Omega_1 + m_2\Omega_2$ *as above. Then* m_1, m_2 *have at most a polynomial growth in* $H(\gamma)$.

It is not hard to show that there exists $\kappa > 0$ such that $< \gamma, f >$ is larger than $N^{-\epsilon}$ for some γ with height $H(\gamma) << N^{\kappa}$. The above conjecture then implies a lower bound for the periods which can be used (via the period conjecture) to prove a version of the ABC–conjecture. Alternatively, the special value $L_E(1)$ (at the B-S-D point) can be expressed as a linear combination of modular symbols which also provides a bridge to the growth of Ш.

In order to study the growth properties of modular symbols, we have introduced a new type of Eisenstein series E^* twisted by modular symbols, which is defined as follows:

$$E^*(z,s) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} < \gamma, f > \mathrm{Im}(\gamma z)^s.$$

Now E^* is not an automorphic form, but it satisfies (for all $\gamma \in \Gamma_0(N)$) the following automorphic relation

$$E^*(\gamma z, s) = E^*(z,s) - < \gamma, f > E(z,s)$$

where

$$E(z,s) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} \mathrm{Im}(\gamma z)^s$$

is the classical Eisenstein series. We have shown [**G2**] that $E^*(z,s)$ has a meromorphic continuation to the entire complex s–plane with only one simple pole at $s = 1$ with residue given by

$$\frac{3}{\pi N} \prod_{p|N} \left(1 + \frac{1}{p}\right)^{-1} F(z)$$

where

$$F(z) = 2\pi i \int_z^{i\infty} f(w)\, dw.$$

As a consequence, it follows (see [**G3**]) that for fixed M, N and $x \to \infty$ that

$$\sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} < \gamma, f > e^{-\frac{c^2 M + d^2}{x}} \sim \frac{3}{\pi N} \prod_{p|N} \frac{F(iM)}{M} x. \tag{6.1}$$

This result was recently improved by O'Sullivan [**O'S**] who explicitly evaluated the error term as a function of M, N and found exponential decay in M. An intriguing possibility is to choose M so that $F(iM)$ is precisely the real period of the associated elliptic curve. The problem is that there is a lot of cancellation in the modular symbols so that the asymptotic relation (6.1) gives no information in the direction of the modular symbols conjecture. It would be of great interest to try to construct other such series which have positive coefficients and have a simple pole at $s = 1$ with residue given by the period of an elliptic curve. If the period were too small, such series would have to have a Siegel zero.

§7. REFERENCES.

[**B**] BAKER, A., *Logarithmic forms and the abc–conjecture,* Number Theory (Eger, 1996) de Gruyter, Berlin (1998), 37–44.

[**B-S-D**] BIRCH, B., SWINNERTON–DYER, H.P.F., *Notes on elliptic curves (I) and (II),* J. reine angew. Math. **212** (1963), 7–25 and **218** (1965), 79–108.

[**C1**] CASSELS, J.W.S., *Arithmetic on curves of genus I (VI). The Tate–Safarevic group can be arbitrarily large,* J. reine. angew. Math. **214/215** (1964), 65–70.

[**C2**] CASSELS, J.W.S., *Lectures on elliptic curves,* London Math. Soc. Stud. Texts, vol. 24, Cambridge Univ. Press, London and New York, (1991).

[**Cr**] CREMONA, J.E., *The analytic order of* Ш *for modular elliptic curves,* J. Th. Nombres Bordeaux **5** (1993), 179–184.

[**D**] DIAMOND, F., *On deformation rings and Hecke rings,* Ann. of Math. (2) **144** (1996), 137–166.

[**D–F–I**] DUKE W., FRIEDLANDER, J., IWANIEC, H., *Bounds for automorphic L-functions. II,* Invent. math. **115** (1994), 219–239.

[**E**] ELKIES, N.D., *ABC implies Mordell,* Intern, Math. Res. Notices 7 (1991), 99–109, in: Duke Math. Journ. 64 (1991).

[**F**] FALTINGS, G., *Arakelov's theorem for abelian varieties,* Invent. Math., **73** (1983), 337–347.

[**F1**] FREY, G., *Links between stable elliptic curves and certain diophantine equations,* Annales Universiatis Saraviensis, Vol 1, No. 1 (1986), 1–39.

[**F2**] FREY, G., *Links between elliptic curves and solutions of A-B=C,* Journal of the Indian Math. Soc. **51** (1987), 117–145.

[**G1**] GOLDFELD, D., *Modular elliptic curves and Diophantine problems,* in: Number Theory (edited by R. Mollin) Walter de Gruyter, Berlin, New York (1990), 157–175.

[**G2**] GOLDFELD, D., *Zeta functions formed with modular symbols,* Proc. of the Symposia in Pure Math., Vol 66, 1, Automorphic Forms, Automorphic Representations, and Arithmetic (1999), 111–122.

[**G3**] GOLDFELD, D., *The distribution of modular symbols,* in: Number Theory in Progress, Vol 2, Elementary and Analytic Number Theory (Edited by K. Györy, H. Iwaniec, J. Urbanowicz) Walter de Gruyter, Berlin, New York (1999), 849–866.

[**G–S**] GOLDFELD, D., LIEMAN, D., *Effective bounds on the size of the Tate–Shafarevich group,* Math. Research Letters, Vol. **3**, (1996), 309–318.

[**G–S**] GOLDFELD, D., SZPIRO, L., *Bounds for the order of the Tate-Shafarevich group,* Compositio Math. **97** (1995), 71–87.

[**Gr**] GRANVILLE, A., *ABC means we can count squarefrees,* International Mathematical Research Notices 19 (1998), 991–1009.

[**Gr-S**] GRANVILLE, A., STARK, H.M., *ABC implies no Siegel zeros for L–functions of characters with negative discriminant,* to appear.

[**G-H-L-L**] HOFFSTEIN, J., LOCKHART, P., *Coefficients of Maass forms and the Siegel zero,* Ann. of Math. (2) **140** (1994), 161–181. With an appendix by: GOLDFELD, D., HOFFSTEIN, J., LIEMAN, D., *An effective zero free region.*

[**Koh**] KOHNEN, W., *Fourier coefficients of modular forms of half-integral weight,* Math. Ann. **271** (1985), 237-268.

[**Kol1**] KOLYVAGIN, V.A., *Finiteness of $E(\mathbb{Q})$ and $Ш(\mathbb{Q})$ for a subclass of Weil curves,* Izv. Akad. Nauk USSR Ser. Mat. **52** (1988), 522–540; English transl., Math USSR-Izv. **32** (1989), 523–543.

[**Kol2**] KOLYVAGIN, V.A., *On the Mordell–Weil group and the Shafarevich–Tate group of elliptic curves,* Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), 1154–1180.

[**Kol3**] KOLYVAGIN, V.A., *Euler systems,* The Grothendieck Festschrift, vol. II (A collection of articles written in honor of the 60th birthday of Alexander Grothendieck), Birkhäuser, Basel, (1991), 435–483.

[**Kr**] KRAMER, K., *A family of semistable elliptic curves with large Tate–Shafarevich groups,* Proc. Amer. Math. Soc., **89** (1983), 379–386.

[**Ma1**] MAZUR, B., *Modular elliptic curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

[**Ma2**] MAZUR, B., *On the passage from local to global in number theory,* Bull. A.M.S., Vol. 29, No. 1, (1993), 14–50.

[**M**] MURTY, R., *Bounds for congruence primes,* Proc. of the Symposia in Pure Math., Vol 66, 1, Automorphic Forms, Automorphic Representations, and Arithmetic (1999), 177–192.

[**M–M**] MAI, L., MURTY, R., *A note on quadratic twists of an elliptic curve,* CRM Proceedings and Lecture Notes, **4** (1994), 121–124.

[**Mo**] MORDELL, L.J., *On the rational solutions of the indeterminate equations of the third and fourth degrees,* Proc. Cambridge Philos. Soc., **21** (1922), 179–192.

[**O**] OGG, A.P., *Elliptic curves and wild ramification,* Amer. J. Math. **89** (1967), 1–21.

[**Ost**] OSTERLÉ, J., *Nouvelles approches du Théorème de Fermat,* Sem. Bourbaki, n^o 694 (1987-88), 694-01 - 694-21.

[**O'S**] O'SULLIVAN, C., *Properties of Eisenstein series formed with modular symbols,* to appear.

[**R1**] RUBIN, K., *Tate-Shafarevich groups and L−functions of elliptic curves with complex multiplication,* Invent. math. **89** (1987), 527–559.

[**R2**] RUBIN, K., *The work of Kolyvagin on the arithmetic of elliptic curves,* Arithmetic of Complex Manifolds, Lecture Notes in Math. **1399**, Springer Verlag, New York (1989), 128–136.

[**Se**] SERRE, J.P., *Galois Cohomology,* Springer–Verlag, Berlin, Heidelberg (1997).

[**Sha**] SHAFAREVICH, I.R., *On birational equivalence of elliptic curves,* Dokl. Akad. Nauk SSSR 114_2 (1957), 267–270. Reprinted in: Collected Mathematical Papers, Springer Verlag, Berlin, Heidelberg (1989), 192–196.

[**Sh**] SHIMURA, G., *On the factors of the jacobian variety of a modular function field,* J. Math. Soc. Japan **25** (1973), 523-544.

[**S1**] SILVERMAN, J.H., Wieferich's criterion and the *abc*–conjecture, J. Number Theory, 30 (1988), 226–237.

[**S2**] SILVERMAN, J.H., *The Arithmetic of Elliptic Curves,* Springer-Verlag GTM 106 (1986).

[**S–T**] STEWART, C.L., TIJDEMAN, R., *On the Oesterlé-Masser Conjecture*, Monatsh. Math. 102 (1986) 251-257.

[**S–Y**] STEWART, C.L., YU, K.R., *On the abc–conjecture,* Math. Ann. 291 (1991), no. 2, 225–230.

[**T1**] TATE, J., *Algorithm for determining the Type of a Singular Fiber in an Elliptic Pencil,* in: Modular Functions of One Variable IV, Lecture Notes in Math. **476** (1975), 33–52.

[**T2**] TATE, J., *WC–groups over* $\mathfrak{p}$*–adic fields,* Séminaire Bourbaki, Exp. 156 (1957).

[**V**] VOJTA, P., *Diophantine Approximations and Value Distribution Theory,* Lecture Notes in Math. **1239** (1987).

[**Wa**] WALDSPURGER, J-L., *Sur les coefficients de Fourier des formes modulaires de poides demi-entier,* J. Math. Pures Appl. **60** (1981), 375-484.

[**W**] WEIL, A., *Sur un théorème de Mordell,* Bull. Sci. Math., **54** (1930), 182–191. Reprinted in: Oeuvres Scientifiques, Collected Papers, vol.1, Springer Verlag, New York (1980), 11-45.

[**We**] DE WEGER, B., $A + B + C$ *and big Sha's,* Math. Inst. University of Leiden, The Netherlands, Report no. W96–11 (1996).

[**Wi**] WILES, A., *Modular elliptic curves and Fermat's last theorem,* Ann. of Math. **141** (1995), 443–551.

Columbia University Department of Mathematics, New York, NY 10027
E-mail address: goldfeld@columbia.edu