Old and New themes in Number Theory

R. Sujatha

TATA INSTITUTE OF FUNDAMENTAL RESEARCH

BOMBAY

INDIA

European Women in Mathematics

Cambridge

Sep 2–6 2007

Introduction

The human mind has long contemplated the problem of solving cubic equations

Introduction

The human mind has long contemplated the problem of solving cubic equations

- Babylonians (clay tablet from around 2000 BC; Berlin museum)

Introduction

The human mind has long contemplated the problem of solving cubic equations

- Babylonians (clay tablet from around 2000 BC; Berlin museum)
- Greeks, esp. Diophantus who was largely concerned with integral solutions

Introduction

The human mind has long contemplated the problem of solving cubic equations

- Babylonians (clay tablet from around 2000 BC; Berlin museum)
- Greeks, esp. Diophantus who was largely concerned with integral solutions


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis
Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM

A quatrain from Rubaiyat of Omar Khayyam, (translator: Edward Fitzgerald)

A quatrain from Rubaiyat of Omar Khayyam, (translator: Edward Fitzgerald)

"The Moving Finger writes: and, having writ,
Moves on: nor all thy Piety nor Wit
Shall lure it back to cancel half of it

Nor all thy Tears wash out a Word of it."

A quatrain from Rubaiyat of Omar Khayyam, (translator: Edward Fitzgerald)

"The Moving Finger writes: and, having writ,
Moves on: nor all thy Piety nor Wit
Shall lure it back to cancel half of it
Nor all thy Tears wash out a Word of it."

Rubaiyat

Khayyam

Omar Khayyam was also an astronomer and mathematician of repute, and is known for his geometric solution of cubic equations.

Omar Khayyam was also an astronomer and mathematician of repute, and is known for his geometric solution of cubic equations.

Around the 17th century, elliptic integrals arose in the study of arc lengths of an ellipse.

Omar Khayyam was also an astronomer and mathematician of repute, and is known for his geometric solution of cubic equations.

Around the 17th century, elliptic integrals arose in the study of arc lengths of an ellipse.

Associated to this closely was the study of elliptic functions

Omar Khayyam was also an astronomer and mathematician of repute, and is known for his geometric solution of cubic equations.

Around the 17th century, elliptic integrals arose in the study of arc lengths of an ellipse.

Associated to this closely was the study of elliptic functions

studied by Euler, Legendre, Abel, Jacobi...

Euler

Euler

Abel

Of particular interest and relevance here are equations of the form

$$E : y^2 = f(x),$$

where $f(x) \in \mathbb{Q}[x]$ is a cubic with distict roots;

- $\mathbb{Q}$: Field of rational numbers.

Of particular interest and relevance here are equations of the form

$$E : y^2 = f(x),$$

where $f(x) \in \mathbb{Q}[x]$ is a cubic with distict roots;

- $\mathbb{Q}$: Field of rational numbers.

Example: $y^2 = x^3 - x$

Of particular interest and relevance here are equations of the form

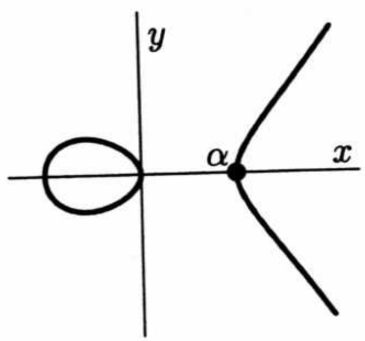
$$E : y^2 = f(x),$$

where $f(x) \in \mathbb{Q}[x]$ is a cubic with distict roots;

- $\mathbb{Q}$: Field of rational numbers.

Example: $y^2 = x^3 - x$

Viewed as a plane curve, its set of real points looks like



A Cubic Curve with Two Real Components

E is then an elliptic curve; these are curves of genus one.

E is then an elliptic curve; these are curves of genus one.

Its solution set $E(\mathbb{Q})$, consisting of pairs (x, y) with x, y in $\mathbb{Q}$, together with the point at ∞ has an abelian group structure. More generally true that the set of F-rational points, $E(F)$, is an abelian group for any field F.

E is then an elliptic curve; these are curves of genus one. Its solution set $E(\mathbb{Q})$, consisting of pairs (x, y) with x, y in $\mathbb{Q}$, together with the point at ∞ has an abelian group structure. More generally true that the set of F-rational points, $E(F)$, is an abelian group for any field F.

Problems related to elliptic curves were however studied in a different context from around the 10th century as we shall see below.

Mordell-Weil theorem

Theorem: For any finite field extension F of $\mathbb{Q}$, the group $E(F)$ is a finitely generated abelian group.

Mordell-Weil theorem

Theorem: For any finite field extension F of $\mathbb{Q}$, the group $E(F)$ is a finitely generated abelian group.

- In particular, $E(F) \simeq \mathbb{Z}^{g(E/F)} \oplus$ finite group

$g(E/F)$=rank of E/F, an arithmetic invariant.

Mordell-Weil theorem

Theorem: For any finite field extension F of $\mathbb{Q}$, the group $E(F)$ is a finitely generated abelian group.

• In particular, $E(F) \simeq \mathbb{Z}^{g(E/F)} \oplus$ finite group
$g(E/F)$=rank of E/F, an arithmetic invariant.

A deep conjecture due to Birch and Swinnerton-Dyer (BSD) predicts that $g(E/F)$ is equal to the order of a conjecturally analytic function $L(E/F, s)$ at $s = 1$.

Main topic today: Iwasawa theory; relatively modern (1960's).

Main topic today: Iwasawa theory; relatively modern (1960's).

Iwasawa theory uses p-adic techniques to bring together the following three different strands of Mathematics with elliptic curves occurring as a common motif:

Main topic today: Iwasawa theory; relatively modern (1960's).

Iwasawa theory uses p-adic techniques to bring together the following three different strands of Mathematics with elliptic curves occurring as a common motif:

- (i) Age old arithmetic problems

Main topic today: Iwasawa theory; relatively modern (1960's).

Iwasawa theory uses p-adic techniques to bring together the following three different strands of Mathematics with elliptic curves occurring as a common motif:

- (i) Age old arithmetic problems
- (ii) special values of complex zeta and L-functions

Main topic today: Iwasawa theory; relatively modern (1960's).

Iwasawa theory uses p-adic techniques to bring together the following three different strands of Mathematics with elliptic curves occurring as a common motif:

- (i) Age old arithmetic problems
- (ii) special values of complex zeta and L-functions
- (iii) Algebraic questions concerned with study of modules

over Iwasawa algebras of compact p-adic Lie groups

The still largely conjectural connection between (i) and (ii) is one of the greatest mysteries of mathematics

The still largely conjectural connection between (i) and (ii) is one of the greatest mysteries of mathematics

Epitomised by the Birch and Swinnerton-Dyer (BSD) conjecture

The still largely conjectural connection between (i) and (ii) is one of the greatest mysteries of mathematics

Epitomised by the Birch and Swinnerton-Dyer (BSD) conjecture

But it goes back to work of Dirichlet (1830's), Kummer (1840's).

The still largely conjectural connection between (i) and (ii) is one of the greatest mysteries of mathematics

Epitomised by the Birch and Swinnerton-Dyer (BSD) conjecture

But it goes back to work of Dirichlet (1830's), Kummer (1840's).

Important milestone: Work of Andrew Wiles (mid 1990's) and others, leading to the proof of modularity of elliptic curves over $\mathbb{Q}$ and consequently a proof of Fermat's last theorem.

Connection between (ii) and (iii): loosely goes under the rubric of Main Conjectures

Connection between (ii) and (iii): loosely goes under the rubric of Main Conjectures

In the case of Cyclotomic fields, discovered by Iwasawa; all subsequent work grew out of this.

Connection between (ii) and (iii): loosely goes under the rubric of Main Conjectures

In the case of Cyclotomic fields, discovered by Iwasawa; all subsequent work grew out of this.

A general formulation of the Main Conjecture leads naturally to questions about noncommutative algebras, arising from compact p-adic Lie groups;

Connection between (ii) and (iii): loosely goes under the rubric of Main Conjectures

In the case of Cyclotomic fields, discovered by Iwasawa; all subsequent work grew out of this.

A general formulation of the Main Conjecture leads naturally to questions about noncommutative algebras, arising from compact p-adic Lie groups; first studied in the seminal paper of M.Lazard (1960's).

We shall discuss some aspects of these inter-relationships.

Connection between (ii) and (iii): loosely goes under the rubric of Main Conjectures

In the case of Cyclotomic fields, discovered by Iwasawa; all subsequent work grew out of this.

A general formulation of the Main Conjecture leads naturally to questions about noncommutative algebras, arising from compact p-adic Lie groups; first studied in the seminal paper of M.Lazard (1960's).

We shall discuss some aspects of these inter-relationships.

Arithmetic problems and L-functions

We shall illustrate the connection between (i) and (ii), related to exact formulae by examples, in their simplest form and in the historical order of their discovery.

Arithmetic problems and L-functions

We shall illustrate the connection between (i) and (ii), related to exact formulae by examples, in their simplest form and in the historical order of their discovery.

(a) Congruent Number Problem

Arithmetic problems and L-functions

We shall illustrate the connection between (i) and (ii), related to exact formulae by examples, in their simplest form and in the historical order of their discovery.

(a) Congruent Number Problem

- Over a 1000 years old;

Arithmetic problems and L-functions

We shall illustrate the connection between (i) and (ii), related to exact formulae by examples, in their simplest form and in the historical order of their discovery.

(a) Congruent Number Problem

• Over a 1000 years old; arguably the oldest major unsolved problem in mathematics

Arithmetic problems and L-functions

We shall illustrate the connection between (i) and (ii), related to exact formulae by examples, in their simplest form and in the historical order of their discovery.

(a) Congruent Number Problem

• Over a 1000 years old; arguably the oldest major unsolved problem in mathematics

Definition: An integer $N > 1$ is congruent if N is the area of a right angled triangle, all of whose sides have rational length.

Example: 5,6,7,13,14,15,21,22,23,29,30,31,34..... are congruent numbers

- 5 = Area of right angled triangle with sides (9/6,40/6,41/6)
- 6 = Area of right angled triangle with sides (3,4,5).

Example: 5,6,7,13,14,15,21,22,23,29,30,31,34..... are congruent numbers

- 5 = Area of right angled triangle with sides (9/6,40/6,41/6)
- 6 = Area of right angled triangle with sides (3,4,5).

- The proof that 1 is not congruent is due to Fermat and uses his beautiful *principle of infinite descent*

Example: 5,6,7,13,14,15,21,22,23,29,30,31,34..... are congruent numbers

- 5 = Area of right angled triangle with sides (9/6,40/6,41/6)
- 6 = Area of right angled triangle with sides (3,4,5).

- The proof that 1 is not congruent is due to Fermat and uses his beautiful *principle of infinite descent*

Despite overwhelming numerical evidence, the following conjecture is still open.

Example: 5,6,7,13,14,15,21,22,23,29,30,31,34..... are congruent numbers

• 5 = Area of right angled triangle with sides (9/6,40/6,41/6)

• 6 = Area of right angled triangle with sides (3,4,5).

• The proof that 1 is not congruent is due to Fermat and uses his beautiful *principle of infinite descent*

Despite overwhelming numerical evidence, the following conjecture is still open.

Conjecture: Every integer $N > 1$ with $N \equiv 5, 6, 7 \mod 8$ is congruent.

Example: 5,6,7,13,14,15,21,22,23,29,30,31,34..... are congruent numbers

- 5 = Area of right angled triangle with sides (9/6,40/6,41/6)
- 6 = Area of right angled triangle with sides (3,4,5).

- The proof that 1 is not congruent is due to Fermat and uses his beautiful *principle of infinite descent*

Despite overwhelming numerical evidence, the following conjecture is still open.

Conjecture: Every integer $N > 1$ with $N \equiv 5, 6, 7 \bmod 8$ is congruent.

Surprisingly, this is really a problem about *elliptic curves*

• Congruent number problem for an integer $N > 1$ leads very naturally to studying elliptic curves of the form $E : y^2 = x^3 - N^2 x.$

• Congruent number problem for an integer $N > 1$ leads very naturally to studying elliptic curves of the form $E : y^2 = x^3 - N^2 x.$

Lemma: The integer N is congruent $\Leftrightarrow$ there is a point (x, y) on E with x, y rational and y non-zero.

Tate-Shafarevich group

CNP is the simplest example of the BSD conjecture, as we shall explain later.

Tate-Shafarevich group

CNP is the simplest example of the BSD conjecture, as we shall explain later.

There is a group that arises naturally in the study of elliptic curves over $\mathbb{Q}$, namely the Shafarevich-Tate group, denoted $Ш(E/\mathbb{Q})$, defined by

$$Ш(E/\mathbb{Q}) = Ker(H^1(\mathbb{Q}, E(\bar{\mathbb{Q}})) \to \prod_p H^1(\mathbb{Q}_p, E(\bar{\mathbb{Q}}_p))).$$

Tate-Shafarevich group

CNP is the simplest example of the BSD conjecture, as we shall explain later.

There is a group that arises naturally in the study of elliptic curves over $\mathbb{Q}$, namely the Shafarevich-Tate group, denoted $Ш(E/\mathbb{Q})$, defined by

$$Ш(E/\mathbb{Q}) = Ker(H^1(\mathbb{Q}, E(\bar{\mathbb{Q}})) \rightarrow \prod_p H^1(\mathbb{Q}_p, E(\bar{\mathbb{Q}}_p))).$$

• This group parametrizes some curves defined over $\mathbb{Q}$ that become isomorphic to the given elliptic curve E over extension fields of $\mathbb{Q}$

• The Tate-Shafarevich group is among the most mysterious groups occurring in mathematics!

• The Tate-Shafarevich group is among the most mysterious groups occurring in mathematics!

• Part of the BSD conjecture is that it is always finite, and the conjecture gives an exact formula for its order.

- The Tate-Shafarevich group is among the most mysterious groups occurring in mathematics!
- Part of the BSD conjecture is that it is always finite, and the conjecture gives an exact formula for its order.
- Numerically it is extremely difficult to calculate, but the BSD formula shows numerically that its order is remarkably small.

Iwasawa theory enables one to prove the following:

Iwasawa theory enables one to prove the following:

Theorem: Assume $N \equiv 5, 6, 7 \bmod 8$. If the p-primary torsion part $\text{Ш}\ E/\mathbb{Q}(p)$ is finite for some prime p, then N is congruent.

Iwasawa theory enables one to prove the following:

Theorem: Assume $N \equiv 5, 6, 7 \bmod 8$. If the p-primary torsion part $⧢\, E/\mathbb{Q}(p)$ is finite for some prime p, then N is congruent.

We now turn to the next example in cyclotomic fields, due to Kummer.

Cyclotomic fields

• p an odd prime number, $K = \mathbb{Q}(\mu_p)$, where μ_p is the group of p-th roots of unity viz. $\{x \in \mathbb{C} \mid x^p = 1\}$.

Cyclotomic fields

- p an odd prime number, $K = \mathbb{Q}(\mu_p)$, where μ_p is the group of p-th roots of unity viz. $\{x \in \mathbb{C} \mid x^p = 1\}$.
- $\zeta(s)$: Riemann zeta function defined as $\sum_{n \geq 1} 1/n^s$, where s is a complex variable.

Cyclotomic fields

- p an odd prime number, $K = \mathbb{Q}(\mu_p)$, where μ_p is the group of p-th roots of unity viz. $\{x \in \mathbb{C} \mid x^p = 1\}$.
- $\zeta(s)$: Riemann zeta function defined as $\sum_{n \geq 1} 1/n^s$, where s is a complex variable.
- $\zeta(-k) \in \mathbb{Q}$, $(k = 1, 3, 5, ...)$; $\zeta(-k) = -B_{k+1}/(k+1)$, where B_{k+1} is the $(k+1)$-th Bernoulli number.

Cyclotomic fields

- p an odd prime number, $K = \mathbb{Q}(\mu_p)$, where μ_p is the group of p-th roots of unity viz. $\{x \in \mathbb{C} \mid x^p = 1\}$.
- $\zeta(s)$: Riemann zeta function defined as $\sum_{n \geq 1} 1/n^s$, where s is a complex variable.
- $\zeta(-k) \in \mathbb{Q}$, $(k = 1, 3, 5, \ldots)$; $\zeta(-k) = -B_{k+1}/(k+1)$, where B_{k+1} is the $(k+1)$-th Bernoulli number.

The *class group* of K is an arithmetic invariant attached to K, defined as the group of fractional ideals of the ring of integers in K modulo the principal ideals.

(b):Kummer's criterion

Theorem: (Kummer) The prime p divides the class number of $K \Leftrightarrow p$ divides the numerator of at least one of $\zeta(-1), \zeta(-2), \cdots, \zeta(4-p)$.

(b):Kummer's criterion

Theorem: (Kummer) The prime p divides the class number of $K \Leftrightarrow p$ divides the numerator of at least one of $\zeta(-1), \zeta(-2), \cdots, \zeta(4-p)$.

Example: $\zeta(-11) = 691/32760$; hence the prime 691 divides the class number of $\mathbb{Q}(\mu_{691})$.

(b):Kummer's criterion

Theorem: (Kummer) The prime p divides the class number of $K \Leftrightarrow p$ divides the numerator of at least one of $\zeta(-1), \zeta(-2), \cdots, \zeta(4-p)$.

Example: $\zeta(-11) = 691/32760$; hence the prime 691 divides the class number of $\mathbb{Q}(\mu_{691})$.

• Kummer's criterion thus relates an arithmetic object namely the class group, to an analytic object, namely the special values of the Riemann zeta function.

(b):Kummer's criterion

Theorem: (Kummer) The prime p divides the class number of $K \Leftrightarrow p$ divides the numerator of at least one of $\zeta(-1), \zeta(-2), \cdots, \zeta(4-p)$.

Example: $\zeta(-11) = 691/32760$; hence the prime 691 divides the class number of $\mathbb{Q}(\mu_{691})$.

• Kummer's criterion thus relates an arithmetic object namely the class group, to an analytic object, namely the special values of the Riemann zeta function.

The class group has a superficial analogy with the Tate-Shafarevich group.

We now come to our final example.
(c): Elliptic curves and the BSD conjecture

We now come to our final example.

(c): Elliptic curves and the BSD conjecture

$E/\mathbb{Q}$ an elliptic curve; the Hasse-Weil L-function, $L(E,s)$ is a natural generalization of the Riemann zeta function

We now come to our final example.
(c): Elliptic curves and the BSD conjecture

$E/\mathbb{Q}$ an elliptic curve; the Hasse-Weil L-function, $L(E,s)$ is a natural generalization of the Riemann zeta function

• Defined using the integers $a_p := p + 1 - \#E(\mathbb{F}_p)$, the number of points of E over the finite fields $\mathbb{F}_p$, as p varies over the prime numbers.

We now come to our final example.
(c): Elliptic curves and the BSD conjecture

$E/\mathbb{Q}$ an elliptic curve; the Hasse-Weil L-function, $L(E,s)$ is a natural generalization of the Riemann zeta function

• Defined using the integers $a_p := p + 1 - \#E(\mathbb{F}_p)$, the number of points of E over the finite fields $\mathbb{F}_p$, as p varies over the prime numbers.

• Euler product expression
$L(E,s) = \prod_p (1 - a_p p^{-s} + (p^{1-2s}))^{-1}$, Re(s)> 3/2

• Dirichlet series expression $L(E,s) = \sum_{n=0}^{\infty} a_n/n^s$.

We now come to our final example.
(c): Elliptic curves and the BSD conjecture

$E/\mathbb{Q}$ an elliptic curve; the Hasse-Weil L-function, $L(E,s)$ is a natural generalization of the Riemann zeta function

• Defined using the integers $a_p := p+1-\#E(\mathbb{F}_p)$, the number of points of E over the finite fields $\mathbb{F}_p$, as p varies over the prime numbers.

• Euler product expression
$L(E,s) = \prod_p (1 - a_p p^{-s} + (p^{1-2s}))^{-1}$, Re(s)> 3/2

• Dirichlet series expression $L(E,s) = \sum_{n=0}^{\infty} a_n/n^s$.

A deep and important result is that $L(E,s)$ has an analytic continuation to the whole complex plane.

Birch and Swinnerton-Dyer conjecture

Conjecture: The rank $g(E/\mathbb{Q})$ = order of vanishing of $L(E, s)$ at $s = 1$.
In particular, $E(\mathbb{Q})$ is infinite $\Leftrightarrow$ $L(E, s)$ vanishes at $s = 1$.

Birch and Swinnerton-Dyer conjecture

Conjecture: The rank $g(E/\mathbb{Q})$ = order of vanishing of $L(E,s)$ at $s = 1$.
In particular, $E(\mathbb{Q})$ is infinite $\Leftrightarrow$ $L(E,s)$ vanishes at $s = 1$.

• BSD conjecture even gives an exact formula for the leading coefficient of $L(E,s)$ at $s = 1$.

Birch and Swinnerton-Dyer conjecture

Conjecture: The rank $g(E/\mathbb{Q})$ = order of vanishing of $L(E, s)$ at $s = 1$.
In particular, $E(\mathbb{Q})$ is infinite $\Leftrightarrow$ $L(E, s)$ vanishes at $s = 1$.

• BSD conjecture even gives an exact formula for the leading coefficient of $L(E, s)$ at $s = 1$.

• Extraordinary link between arithmetic objects and analytic objects.

Birch and Swinnerton-Dyer conjecture

Conjecture: The rank $g(E/\mathbb{Q})$ = order of vanishing of $L(E, s)$ at $s = 1$.
In particular, $E(\mathbb{Q})$ is infinite $\Leftrightarrow$ $L(E, s)$ vanishes at $s = 1$.

- BSD conjecture even gives an exact formula for the leading coefficient of $L(E, s)$ at $s = 1$.
- Extraordinary link between arithmetic objects and analytic objects.

For the CNP, with $N \equiv 5, 6, 7 \mod 8$, and for the curves $E : y^2 = x^3 - N^2 x,$ the theory of L-functions shows that $L(E, s)$ has an odd order zero at $s = 1$.

Iwasawa theory

- Provides a systematic technique to attack the BSD conjecture using p-adic methods.

Iwasawa theory

- Provides a systematic technique to attack the BSD conjecture using p-adic methods.
- First developed by Iwasawa in his study of class groups of cyclotomic extensions; fully explains the philosophy behind Kummer's criterion.

Iwasawa theory

- Provides a systematic technique to attack the BSD conjecture using p-adic methods.
- First developed by Iwasawa in his study of class groups of cyclotomic extensions; fully explains the philosophy behind Kummer's criterion.
- Basic Idea: To seek a simple connection between special values of L-functions and arithmetic over certain infinite Galois extensions F_∞ of $\mathbb{Q}$. This is precisely the content of the Main Conjecture.

Iwasawa theory

- Provides a systematic technique to attack the BSD conjecture using p-adic methods.
- First developed by Iwasawa in his study of class groups of cyclotomic extensions; fully explains the philosophy behind Kummer's criterion.
- Basic Idea: To seek a simple connection between special values of L-functions and arithmetic over certain infinite Galois extensions F_∞ of $\mathbb{Q}$. This is precisely the content of the Main Conjecture.

From this perspective, the BSD conjecture seems very natural; can see how points of infinite order over $\mathbb{Q}$ give rise to a zero of multiplicity $g(E/\mathbb{Q})$, of a p-adic analogue of $L(E, s)$.

Examples:

(i) $F_\infty = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n\geq 0} \mathbb{Q}(\mu_{p^n})$, obtained by adjoining all the p-power roots of unity.

Examples:

(i) $F_\infty = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n\geq 0} \mathbb{Q}(\mu_{p^n})$, obtained by adjoining all the p-power roots of unity.

(ii) $E/\mathbb{Q}$ an elliptic curve; $E_{p^n} = E_{p^n}(\bar{\mathbb{Q}})$ is the Galois extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the p^n-division points of E; $F_\infty = \bigcup_{n\geq 0} F(E_{p^n})$.

Examples:

(i) $F_\infty = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n\geq 0} \mathbb{Q}(\mu_{p^n})$, obtained by adjoining all the p-power roots of unity.

(ii) $E/\mathbb{Q}$ an elliptic curve; $E_{p^n} = E_{p^n}(\bar{\mathbb{Q}})$ is the Galois extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the p^n-division points of E; $F_\infty = \bigcup_{n\geq 0} F(E_{p^n})$.

- $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$; then G is a compact p-adic Lie group.

In the first example, $G = \mathbb{Z}_p^\times$, the units of the ring of p-adic integers, isomorphic to $\mathbb{Z}_p \times \mathbb{Z}/(p-1)$.

In the first example, $G = \mathbb{Z}_p^\times$, the units of the ring of p-adic integers, isomorphic to $\mathbb{Z}_p \times \mathbb{Z}/(p-1)$.

In (ii), there are two cases:

In the first example, $G = \mathbb{Z}_p^\times$, the units of the ring of p-adic integers, isomorphic to $\mathbb{Z}_p \times \mathbb{Z}/(p-1)$.

In (ii), there are two cases:

first if E has complex multiplication, then $G \supset (\mathbb{Z}_p \times \mathbb{Z}_p)$ of index 2.

If E does not have complex multiplication, then $G \simeq$ open subgp of $GL_2(\mathbb{Z}_p)$ (Serre).

In the first example, $G = \mathbb{Z}_p^\times$, the units of the ring of p-adic integers, isomorphic to $\mathbb{Z}_p \times \mathbb{Z}/(p-1)$.

In (ii), there are two cases:

first if E has complex multiplication, then $G \supset (\mathbb{Z}_p \times \mathbb{Z}_p)$ of index 2.

If E does not have complex multiplication, then $G \simeq$ open subgp of $GL_2(\mathbb{Z}_p)$ (Serre).

Iwasawa algebras

G a compact p-adic Lie group.

Iwasawa algebras

G a compact p-adic Lie group.

The Iwasawa algebra of G, denoted $\Lambda(G)$ is the *completed group algebra*

Iwasawa algebras

G a compact p-adic Lie group.

The Iwasawa algebra of G, denoted $\Lambda(G)$ is the *completed group algebra*

$$\Lambda(G) = \varprojlim \mathbb{Z}_p[G/G'].$$

Iwasawa algebras

G a compact p-adic Lie group.

The Iwasawa algebra of G, denoted $\Lambda(G)$ is the *completed group algebra*

$$\Lambda(G) = \lim_{\longleftarrow} \mathbb{Z}_p[G/G'].$$

Here G' runs over open normal subgroups of G and the inverse limit is taken with respect to the natural maps of the corresponding group rings.

Examples

(i) If $G \simeq \mathbb{Z}_p^\times$, then $\Lambda(G) \simeq (p-1)$ copies of $\mathbb{Z}_p[[T]]$.

Examples

(i) If $G \simeq \mathbb{Z}_p^\times$, then $\Lambda(G) \simeq (p-1)$ copies of $\mathbb{Z}_p[[T]]$.

(ii) $G \simeq \mathbb{Z}_p^d$, then $\Lambda(G) \simeq \mathbb{Z}_p[[T_1, \cdots, T_d]]$.
When G is commutative, study of modules over $\Lambda(G)$ is thus classical.

Examples

(i) If $G \simeq \mathbb{Z}_p^\times$, then $\Lambda(G) \simeq (p-1)$ copies of $\mathbb{Z}_p[[T]]$.

(ii) $G \simeq \mathbb{Z}_p^d$, then $\Lambda(G) \simeq \mathbb{Z}_p[[T_1, \cdots, T_d]]$.
When G is commutative, study of modules over $\Lambda(G)$ is thus classical.

(iii) G open subgroup of $GL_n(\mathbb{Z}_p)$; $\Lambda(G)$ is more complicated; first investigated by Lazard.

Examples

(i) If $G \simeq \mathbb{Z}_p^\times$, then $\Lambda(G) \simeq (p-1)$ copies of $\mathbb{Z}_p[[T]]$.

(ii) $G \simeq \mathbb{Z}_p^d$, then $\Lambda(G) \simeq \mathbb{Z}_p[[T_1, \cdots, T_d]]$.
When G is commutative, study of modules over $\Lambda(G)$ is thus classical.

(iii) G open subgroup of $GL_n(\mathbb{Z}_p)$; $\Lambda(G)$ is more complicated; first investigated by Lazard.

Fact: If G has no elements of order p (eg. $p > n+1$ in (iii)), then $\Lambda(G)$ is a Noetherian, Auslander regular domain with finite global dimension.

Examples

(i) If $G \simeq \mathbb{Z}_p^\times$, then $\Lambda(G) \simeq (p-1)$ copies of $\mathbb{Z}_p[[T]]$.

(ii) $G \simeq \mathbb{Z}_p^d$, then $\Lambda(G) \simeq \mathbb{Z}_p[[T_1, \cdots, T_d]]$.
When G is commutative, study of modules over $\Lambda(G)$ is thus classical.

(iii) G open subgroup of $GL_n(\mathbb{Z}_p)$; $\Lambda(G)$ is more complicated; first investigated by Lazard.

Fact: If G has no elements of order p (eg. $p > n+1$ in (iii)), then $\Lambda(G)$ is a Noetherian, Auslander regular domain with finite global dimension.

This enables one to study modules over $\Lambda(G)$ quite generally using techniques from dimension theory and homological algebra.

Return to Arithmetic

Fundamental idea: Find a module over the Iwasawa algebra which simultaneously reflects both the arithmetic of E and the special values of the complex L-function attached to E.

Return to Arithmetic

Fundamental idea: Find a module over the Iwasawa algebra which simultaneously reflects both the arithmetic of E and the special values of the complex L-function attached to E.

Classical descent theory tells us what arithmetic module we should consider over our p-adic Lie extension F_∞; namely the compact Pontryagin dual $X_p(E/F_\infty)$ of the p- primary Selmer group of E over F_∞.

Return to Arithmetic

Fundamental idea: Find a module over the Iwasawa algebra which simultaneously reflects both the arithmetic of E and the special values of the complex L-function attached to E.

Classical descent theory tells us what arithmetic module we should consider over our p-adic Lie extension F_∞; namely the compact Pontryagin dual $X_p(E/F_\infty)$ of the p- primary Selmer group of E over F_∞.

This is a finitely generated module over the corresponding Iwasawa algebra $\Lambda(G)$, with $G = \mathrm{Gal}(F_\infty/F)$.

There is an exact sequence of $\Lambda(G)$-modules

$$0 \to \widehat{Ш\, E(F_\infty)}(p) \to X_p(E/F_\infty) \to \mathrm{Hom}(E(F_\infty) \otimes \mathbb{Z}_p, \mathbb{Z}_p) \to 0.$$

There is an exact sequence of $\Lambda(G)$-modules

$$0 \to Ш\, E\widehat{(F_\infty)}(p) \to X_p(E/F_\infty) \to \mathrm{Hom}(E(F_\infty) \otimes \mathbb{Z}_p, \mathbb{Z}_p) \to 0.$$

• $X_p(E/F_\infty)$ encodes information on $E(F)$ and the Tate Shafarevich group for all finite layers F in F_∞.

There is an exact sequence of $\Lambda(G)$-modules

$$0 \to ш\, E\widehat{(F_\infty)(p)} \to X_p(E/F_\infty) \to \mathrm{Hom}(E(F_\infty) \otimes \mathbb{Z}_p, \mathbb{Z}_p) \to 0.$$

• $X_p(E/F_\infty)$ encodes information on $E(F)$ and the Tate Shafarevich group for all finite layers F in F_∞.

• Its in no way obvious how to even formulate a precise conjecture relating this module to values of complex L-functions.

There is an exact sequence of $\Lambda(G)$-modules

$$0 \to \text{Ш}\, \widehat{E(F_\infty)}(p) \to X_p(E/F_\infty) \to \mathrm{Hom}(E(F_\infty) \otimes \mathbb{Z}_p, \mathbb{Z}_p) \to 0.$$

• $X_p(E/F_\infty)$ encodes information on $E(F)$ and the Tate Shafarevich group for all finite layers F in F_∞.

• Its in no way obvious how to even formulate a precise conjecture relating this module to values of complex L-functions.

This is exactly where the Main Conjecture intervenes.

Main Conjecture in Iwasawa theory

- Attach an algebraic and analytic invariant to $X_p(E/F_\infty)$.

Main Conjecture in Iwasawa theory

- Attach an algebraic and analytic invariant to $X_p(E/F_\infty)$.

The analytic invariant should p-adically interpolate values of the complex L-function twisted by Artin characters ρ of $G = \mathrm{Gal}(F_\infty/F)$.

Main Conjecture in Iwasawa theory

- Attach an algebraic and analytic invariant to $X_p(E/F_\infty)$.

The analytic invariant should p-adically interpolate values of the complex L-function twisted by Artin characters ρ of $G = \mathrm{Gal}(F_\infty/F)$.

More precisely, consider the function $\rho \mapsto L(E, \rho, 1) \in \mathbb{C}$.

Main Conjecture in Iwasawa theory

- Attach an algebraic and analytic invariant to $X_p(E/F_\infty)$.

The analytic invariant should p-adically interpolate values of the complex L-function twisted by Artin characters ρ of $G = \mathrm{Gal}(F_\infty/F)$.

More precisely, consider the function $\rho \mapsto L(E, \rho, 1) \in \mathbb{C}$.

To view this association p-adically, have to divide the L-value by the "standard period" Ω_ρ; then get values in $\bar{\mathbb{Q}}$ and can hence view them in $\bar{\mathbb{Q}}_p$.

Main Conjecture in Iwasawa theory

• Attach an algebraic and analytic invariant to $X_p(E/F_\infty)$.

The analytic invariant should p-adically interpolate values of the complex L-function twisted by Artin characters ρ of $G = \mathrm{Gal}(F_\infty/F)$.

More precisely, consider the function $\rho \mapsto L(E, \rho, 1) \in \mathbb{C}$.

To view this association p-adically, have to divide the L-value by the "standard period" Ω_ρ; then get values in $\bar{\mathbb{Q}}$ and can hence view them in $\bar{\mathbb{Q}}_p$.

• The statement of the Main Conjecture is that these two invariants are equal.

• In the classical (abelian) examples (i) and (ii), these invariants are elements of $\Lambda(G)$.

• In the classical (abelian) examples (i) and (ii), these invariants are elements of $\Lambda(G)$.

• Associating the algebraic invariant in this case made easy due the existence of a structure theorem for finitely generated modules over commutative Iwasawa algebras.

• In the classical (abelian) examples (i) and (ii), these invariants are elements of $\Lambda(G)$.

• Associating the algebraic invariant in this case made easy due the existence of a structure theorem for finitely generated modules over commutative Iwasawa algebras.

• Any progress towards the Main conjecture in these cases (due to Coates-Wiles, Mazur-Wiles, Yager, Rubin, Kolyvagin, Kato, Skinner-Urban...) has had striking consequences for the BSD conjecture.

• In the classical (abelian) examples (i) and (ii), these invariants are elements of $\Lambda(G)$.

• Associating the algebraic invariant in this case made easy due the existence of a structure theorem for finitely generated modules over commutative Iwasawa algebras.

• Any progress towards the Main conjecture in these cases (due to Coates-Wiles, Mazur-Wiles, Yager, Rubin, Kolyvagin, Kato, Skinner-Urban...) has had striking consequences for the BSD conjecture.

$E(\mathbb{Q})$ infinite $\Rightarrow\ L(E,1) = 0.$
Assuming $Ш\,(E/\mathbb{Q})$ finite, $L(E,1) = 0 \Rightarrow E(\mathbb{Q})$ infinite.

Noncommutative case

- When G is noncommutative, $\Lambda(G)$ is noncommutative and severe complications arise in finding suitable algebraic invariants.

Noncommutative case

- When G is noncommutative, $\Lambda(G)$ is noncommutative and severe complications arise in finding suitable algebraic invariants.

- In joint work with Coates and Schneider, we prove an analogue of the structure theorem for modules over certain noncommutative Iwasawa algebras.

Noncommutative case

- When G is noncommutative, $\Lambda(G)$ is noncommutative and severe complications arise in finding suitable algebraic invariants.
- In joint work with Coates and Schneider, we prove an analogue of the structure theorem for modules over certain noncommutative Iwasawa algebras.
- Later fromulated a precise Main conjecture for the non-commutative case in joint work with Coates, Fukaya, Kato and Venjakob.

- A novelty in the noncommutative case is the use of algebraic K-theory; the algebraic and analytic invariants are elements of $K_1(R)$, where R is a noncommutative localisation of $\Lambda(G)$.

• A novelty in the noncommutative case is the use of algebraic K-theory; the algebraic and analytic invariants are elements of $K_1(R)$, where R is a noncommutative localisation of $\Lambda(G)$.

• Existence of an interesting Ore set makes such a localisation possible.

• A novelty in the noncommutative case is the use of algebraic K-theory; the algebraic and analytic invariants are elements of $K_1(R)$, where R is a noncommutative localisation of $\Lambda(G)$.

• Existence of an interesting Ore set makes such a localisation possible.

The noncommutative theory has a richer structure because of the existence of infinite families of self-dual irreducible Artin characters of G.

Applications and Examples

We illustrate these ideas with a simple noncommutative example;

Applications and Examples

We illustrate these ideas with a simple noncommutative example;

Uses recent joint work with Coates, Fukaya, Kato and has connections with joint work of T.Dokchitser and V. Dokchitser and that of Rohrlich on root numbers.

Let m be any integer > 1, always assumed p-power free.

Applications and Examples

We illustrate these ideas with a simple noncommutative example;

Uses recent joint work with Coates, Fukaya, Kato and has connections with joint work of T.Dokchitser and V. Dokchitser and that of Rohrlich on root numbers.

Let m be any integer > 1, always assumed p-power free.

Define

$$L_n = \mathbb{Q}(m^{1/p^n}), \; K_n = \mathbb{Q}(\mu_{p^n}), \; F_n = \mathbb{Q}(\mu_{p^n}, m^{1/p^n}),$$

$$F_\infty = \bigcup_{n \geq 0} F_n, \; G = \mathrm{Gal}(F_\infty/\mathbb{Q}).$$

Applications and Examples

We illustrate these ideas with a simple noncommutative example;

Uses recent joint work with Coates, Fukaya, Kato and has connections with joint work of T.Dokchitser and V. Dokchitser and that of Rohrlich on root numbers.

Let m be any integer > 1, always assumed p-power free.

Define

$$L_n = \mathbb{Q}(m^{1/p^n}), \; K_n = \mathbb{Q}(\mu_{p^n}), \; F_n = \mathbb{Q}(\mu_{p^n}, m^{1/p^n}),$$

$$F_\infty = \bigcup_{n \geq 0} F_n, \; G = \mathrm{Gal}(F_\infty/\mathbb{Q}).$$

G is noncommutative, isomorphic to the semidirect product of $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p$. The extensions L_n are not Galois while F_n are nonabelian Galois extensions.

G is noncommutative, isomorphic to the semidirect product of $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p$. The extensions L_n are not Galois while F_n are nonabelian Galois extensions.

Consider the representations

$\rho_n = \mathrm{Ind}_{F_n/K_n}^{F_n/\mathbb{Q}} \kappa_n,$ where κ_n is a character of Gal(F_n/K_n) of exact order p^n.

G is noncommutative, isomorphic to the semidirect product of $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p$. The extensions L_n are not Galois while F_n are nonabelian Galois extensions.

Consider the representations

$\rho_n = \mathrm{Ind}_{F_n/K_n}^{F_n/\mathbb{Q}} \kappa_n,$ where κ_n is a character of Gal(F_n/K_n) of exact order p^n. These are self-dual irreducible; every irreducible self-dual Artin representation of G of dimension >1 is of this form.

G is noncommutative, isomorphic to the semidirect product of $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p$. The extensions L_n are not Galois while F_n are nonabelian Galois extensions.

Consider the representations

$\rho_n = \mathrm{Ind}_{F_n/K_n}^{F_n/\mathbb{Q}} \kappa_n,$ where κ_n is a character of Gal(F_n/K_n) of exact order p^n. These are self-dual irreducible; every irreducible self-dual Artin representation of G of dimension >1 is of this form.

Also known that for an elliptic curve E defined over $\mathbb{Q}$, the twisted complex L-functions $L(E, \rho_n, s)$ are entire; this uses deep results from Automorphic theory.

Numerical Example: Consider the first elliptic curve occurring in nature:
$E/\mathbb{Q} = y^2 + y = x^3 - x^2$, conductor=11.

Numerical Example: Consider the first elliptic curve occurring in nature:
$E/\mathbb{Q} = y^2 + y = x^3 - x^2$, conductor=11.

The modularity of this curve was discovered in the 19th century by Fricke-Klein.
Corresponding cusp form of weight 2 for $\Gamma_0(11)$ is

$$f(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^2 \prod_{n=1}^{\infty} (1 - q^{11n})^2, \ q = e^{2\pi i \tau}.$$

Numerical Example: Consider the first elliptic curve occurring in nature:
$E/\mathbb{Q} = y^2 + y = x^3 - x^2$, conductor=11.

The modularity of this curve was discovered in the 19th century by Fricke-Klein.
Corresponding cusp form of weight 2 for $\Gamma_0(11)$ is

$$f(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^2 \prod_{n=1}^{\infty} (1 - q^{11n})^2, \; q = e^{2\pi i \tau}.$$

This is very similar to other modular forms studied by Ramanujan who had different arithmetic questions in mind.

We illustrate the previous theory for E by taking $p = 7$.
Recall that $L_n = \mathbb{Q}(m^{1/p^n})$.

We illustrate the previous theory for E by taking $p = 7$. Recall that $L_n = \mathbb{Q}(m^{1/p^n})$.

Theorem: For every $m > 1$, we have

$$g(E/L_n) \geq n, \ \ (n = 1, 2, 3 \cdots)$$

provided $Ш(E/L_n)(7)$ is finite.

We illustrate the previous theory for E by taking $p = 7$. Recall that $L_n = \mathbb{Q}(m^{1/p^n})$.

Theorem: For every $m > 1$, we have

$$g(E/L_n) \geq n, \ (n = 1, 2, 3 \cdots)$$

provided Ш $(E/L_n)(7)$ is finite.

Even for $n = 1$, numerically very difficult to find points of infinite order in $E(L_1)$.

We illustrate the previous theory for E by taking $p = 7$. Recall that $L_n = \mathbb{Q}(m^{1/p^n})$.

Theorem: For every $m > 1$, we have

$$g(E/L_n) \geq n, \ \ (n = 1, 2, 3 \cdots)$$

provided $Ш(E/L_n)(7)$ is finite.

Even for $n = 1$, numerically very difficult to find points of infinite order in $E(L_1)$.

Surprisingly, Iwasawa theory even gives sometimes an upper bound for the ranks.

Theorem: Assume m is any 7-power free integer with prime factors in the set $\{2, 3, 7\}$. Then for all $n = 1, 2, 3, \cdots$, we have

$$g(E/L_n) \leq n$$

with equality if and only if $Ш(E/L_n)(7)$ is finite.

Theorem: Assume m is any 7-power free integer with prime factors in the set $\{2, 3, 7\}$. Then for all $n = 1, 2, 3, \cdots$, we have

$$g(E/L_n) \leq n$$

with equality if and only if $Ш(E/L_n)(7)$ is finite.

In fact, if BSD holds in the above case, then $L(E, \rho_n, s)$ has a zero of order 1 at $s = 1$ for all $n \geq 1$.

Theorem: Assume m is any 7-power free integer with prime factors in the set $\{2, 3, 7\}$. Then for all $n = 1, 2, 3, \cdots$, we have

$$g(E/L_n) \leq n$$

with equality if and only if $Ш(E/L_n)(7)$ is finite.

In fact, if BSD holds in the above case, then $L(E, \rho_n, s)$ has a zero of order 1 at $s = 1$ for all $n \geq 1$.

This example is a special case of a more general theoretical result on $X_p(E/F_\infty)$; uses the philosophy of the noncommutative main conjecture.