1 algebraic number theory

Quadratic congruences

$x^2 \equiv a \mod n$

Quadratic residues and non-residues

Fermat (1607-1665) knew for which odd primes p numbers $2,3,5$ are quadratic residues or non-residues mod p.

Euler (1707-1783) proved some partial cases

CTNT I

For a prime p and integer a prime to p

define $\left(\frac{a}{p}\right)$ to be equal to 1 if a is a square modulo p, and -1 otherwise.

Quadratic reciprocity law:

If p, q are odd primes then

$$\begin{aligned}\left(\frac{-1}{q}\right) &= (-1)^{\frac{q-1}{2}};\\ \left(\frac{2}{q}\right) &= (-1)^{\frac{q^2-1}{8}};\\ \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},\end{aligned}$$

Gauß (1777-1855), the ‘Golden Theorem’, 8 proofs of QRL, starting with one in his Disquisitiones Arithmeticae 1801

By now, QRL has more than 250 different proofs.

The genuine understanding of the quadratic reciprocity law came with class field theory and its reciprocity map.

Class field theory is the main achievement of algebraic number theory of the 20th century.

It has the largest number of applications.

Its full understanding was the outcome of efforts of many mathematicians:

Kronecker Hilbert Takagi Artin Chebotarev Hasse Chevalley Tate Weil Shafarevich Neukirch

2 zeta function

Euler invented many modern notations, $i, e, \pi, \Sigma, \ldots$

Euler Institute, Petersburg

CTNT I

In 1737 Euler, during his first Petersburg period, invented, for real $s > 1$, the first zeta function:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots$$

When $s \to 1$, the sum turns into the harmonic series which was known to Euler to diverge.

Euler also introduced the notation γ for $\log n + \gamma$, the partial sum of the harmonic series.

Euler product factorisation of the zeta function, relating addition with multiplication:

$$\zeta(s) = \frac{1}{1-2^{-s}} \frac{1}{1-3^{-s}} \frac{1}{1-5^{-s}} \frac{1}{1-7^{-s}} \cdots$$

One of easy consequences is another proof of the classical (more than 2000 years old) result about the infinity of prime numbers.

CTNT I

Euler worked with divergent series, applying the 'Euler equality':

$$\sum_{n\in\mathbb{Z}} a^n = 0 \quad \text{for} \quad a \neq 1.$$

If the left hand side makes sense, multiply by a, the LHS does not change, hence it is 0.

A modern justification comes from the theory of higher Haar measure on formal loop spaces, and there are some similarities with the Feynman path integral.

Euler computed $\zeta(-1)$, i.e. making sense of $1+2+3+4+5+\cdots$, obtaining the correct answer $\dfrac{-1}{12}$.

Euler knew the functional equation for the zeta function, relating $\zeta(s)$ and $\zeta(1-s)$.

So, knowing $\zeta(-1)$ also leads to the computation of

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}.$$

CTNT I

Riemann, as a side activity, did the obvious work of extending $\zeta(s)$ to a complex variable s,
using already existing complex analysis.

He proposed what is called the Riemann Hypothesis (RH), thinking about the properties of the operators associated to the heat equation.

The RH was among several hypotheses stated by him in his talk. All the rest were proved in the 19th century.

The statement of the RH, without the need to use complex analytic continuation:

$$\sum_{n\geqslant 1} \frac{(-1)^{n-1}}{n^s} \neq 0 \quad \text{for } s \in \mathbb{C}, \mathfrak{R}(s) \in (1/2,1).$$

Task: prove it, inventing completely new insights into zeta functions, e.g. coming from generalisations of class field theory.

CTNT I

The interaction of algebraic number theory and zeta functions has been very fruitful.

At the same time, part of analytic number theory became disjoint from algebraic number theory.

Analytic number theorists ‘accepted’, without checking, the proof of the Generalised Riemann Hypothesis by Deligne, the proof was very substantially based on Grothendieck’s arithmetic geometry.

Zeta function remains the main area of interaction between algebraic number theory and analytic number theory.

The Iwasawa-Tate theory studies the zeta function of algebraic number fields, as well as its twists,
called L-functions,
using harmonic analysis on associated adelic spaces and
self-duality of the additive topological locally compact group of adeles.

The topological self-duality of adeles and harmonic analysis imply proofs of several central results in algebraic number theory such as

- Dirichlet’s unit theorem,

- the finiteness of the class number,

CTNT I

- the analytic continuation and functional equation of the Dedekind zeta function.

The Iwasawa-Tate theory is a ***non-linear*** theory, similar to class field theory.

The Iwasawa-Tate theory was at the foundation of the Langlands correspondences which can be viewed as an attempt to extend class field theory using linear representations.

In the last 50 years three main generalisations of class field theory have been developed:

- Higher class field theory, using algebraic K-theory: abelian and non-linear

K. Kato, Sh. Saito, Bloch, Fesenko, Spieß, …

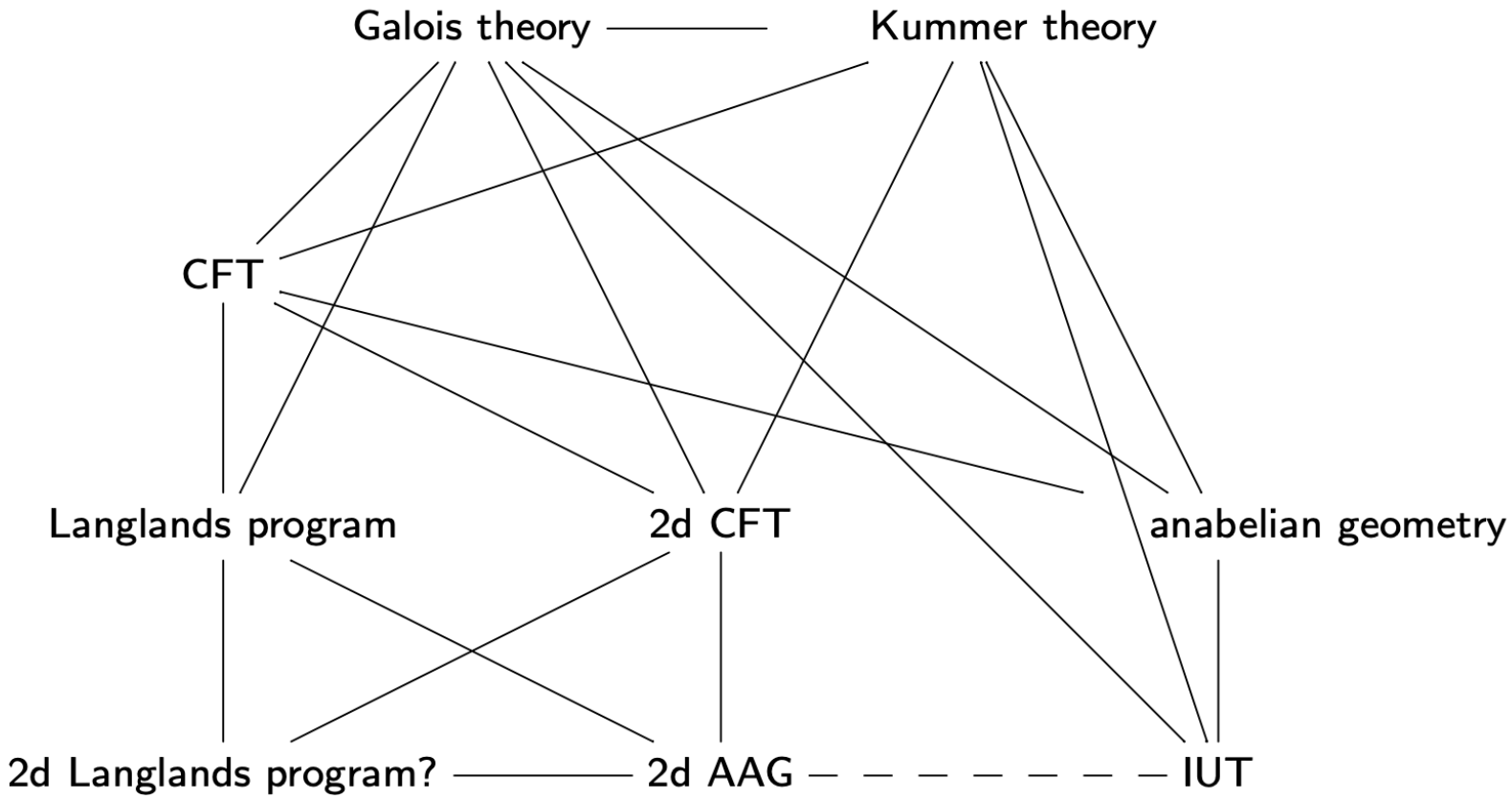
- Langlands program: non-abelian and linear modulo class field theory

Weil, Taniyama, Shimura, Langlands, Jacquet, Arthur, Shahidi, Drinfeld, Lafforgue, …

- Anabelian geometry, using Grothendieck's arithmetic geometry: non-abelian and non-linear

Neukirch, Uchida, Ikeda, Pop, Nakamura, Tamagawa, Mochizuki, Hoshi, …

CTNT I


Galois theory
Kummer theory
CFT
Langlands program
2d CFT
anabelian geometry
2d Langlands program?
2d AAG
IUT

Japan is the only country whose researchers have contributed to each of the three generalisations of class field theory.

We would like to see Chinese names in the list of contributors to generalisations of class field theory.

The number of researchers working in higher class field theory and anabelian geometry is many times smaller than the number of people working in LP.

Almost all the main problems in higher class field theory and anabelian geometry have been solved.

This is quite different from the current situation in the Langlands program where the main problems over number fields have not been solved in the last 50 years.

In positive characteristic, due to the work of V. Drinfeld, L. Lafforgue and V. Lafforgue, using Grothendieck's arithmetic geometry, several fundamental problems in the Langlands program have been solved.

Anabelian geometry leads to the IUT theory of S. Mochizuki, which is a far reaching understanding of the relation between addition and multiplication on integers.

Applications of IUT include abc type inequalities.

CTNT I

Fermat's Last Theorem (FLT):

the Diophantine equation

$x^n + y^n = z^n$ for an integer $n > 2$ does not have positive integer solutions x, y, z.

Euler contributed to the case $n = 3$.

Gauß was not interested.

CTNT I

There are now 2 (and, maybe, soon 3) published proofs of FLT:

(1) 1995 proof of a stronger property of modularity of elliptic curves over rationals with semi-stable reduction (an exercise in the Langlands program), by Wiles and Taylor, using some explicit formulas in class field theory; this method cannot be extended to other Diophantine equations to most other number fields.

(2) 2022 proof of stronger property of effective abc inequality over rationals and imaginary quadratic fields, using anabelian geometry, local class field theory and the IUT theory of Mochizuki, by Mochizuki-Fesenko-Hoshi-Minamide-Porowski; this method is applicable to many Diophantine equations and extendable to other number fields.

Effective abc inequality:

for every two coprime (i.e. no common prime divisors) positive integer numbers a, b *and their sum* $c = a + b$,

the following inequality holds

$$\log(abc) < \max\{1.7 \cdot 10^{30}, 6 \log \mathrm{rad}(abc)\},$$

here the radical is the product of all prime divisors.

CTNT I

Using new lower bounds on solutions of the Fermat equation (Case II) by Mihailescu, applications of the abc inequality leads to the second proof of FLT.

These two proofs involve elliptic curves over number fields.

(3) a recent preprint claiming another proof of FLT, using cyclotomic fields, without using elliptic curves.

CTNT I

What about applications of the other generalisation of class field theory, higher class field theory?

It deals with two and higher dimensional objects, e.g. proper regular models of elliptic curves over number fields.

Using higher adelic analysis and geometry (2d AAG) and higher Iwasawa-Tate theory, it produces a new method to understand and prove the Birch - Swinnerton-Dyer - Tate conjecture about elliptic curves over number fields.

It also naturally produces a weaker version of the Langlands correspondence, this time between zeta functions of certain arithmetic schemes and mean-periodic functions.

It also produces a new approach to the Generalised Riemann Hypothesis for the zeta function of elliptic surfaces over number fields.

CTNT I

How about applications of modern number theory to the real world?

Aspects of LP and string theory.

For recent analogies between some aspects/ideas of anabelian geometry and IUT and of quantum computing see

Interdisciplinary applications of modern arithmetic geometry

https://ivanfesenko.org/wp-content/uploads/tk22.pdf

CTNT I

From which level to start this course? - please answer in a new online form

1
Modules over rings. Finitely generated modules, free modules.
Polylinear maps.
Tensor product of modules.
The dual module and its properties.

2
Three definitions of a Noetherian module.
First properties of Noetherian modules.
Hilbert Theorem about the polynomial ring over a Noetherian ring.

3
Divisibility and ideals.
PID are UFD. Rings with division algorithm are PID.
Polynomial rings over UFD. Gauss Lemma. Polynomial rings over UFD are UFD.

4
Submodules of free modules over PIDs.
The main theorem about finitely generated modules over PID.

5
Spectrum and m-spectrum of a ring. Geometric interpretation.
Multiplicative subset of a ring. Ring of fractions.
Localisation with respect to a prime ideal. Geometric interpretation.
Ideals of the ring of fractions.
Spectrum of localisation.

CTNT I

6
Algebraic elements.
Algebraic extensions and finite extensions.
Algebraic closure.
Field homomorphisms, relation with roots subsitution.
Main results of Galois theory.
Finite fields.

7
Integrality over rings, properties.
The integral closure.
Norms, traces.
Discriminant.
Dedekind rings. Ideals of Dedeking rings.
Factorization in the product of prime ideals in Dedekind rings.
The index of an ideal of a Dedekind ring.
Splitting of prime ideals in field extensions.
Ideal class group.
Finiteness of the ideal classes group. Minkowski's Theorem.

8
p-adic numbers.
Ostrowski's theorem about norms on rational numbers $\mathbb{Q}$ and all completions of $\mathbb{Q}$.

CTNT I

9
Discrete valuation fields - basic definitions.
Completion with respect to a discrete valuation.
Examples of complete discrete valuation fields.
The units filtration and the quotient filtration.
Raising to pth power when the residue field of characteristic p.
Infinite product representation.
Principal units as a $\mathbb{Z}_p$-module.

10
Extensions of complete fields.
Henselian property.
Its corollaries.
The numbers e and f.
Uniqueness of extension of discrete valuation from a complete field.
Types of ramified extensions.
Maximal unramified extension.
Maximal tamely ramified extension.
Ramification groups.
The norm map on the quotient filtration on the group of units for cyclic extensions of prime degree.

11
Structure of complete discrete valuation fields.
Solvability of Galois groups.
Frobenius map minus identity acting on the group of units of the max unratified extension.
The Neukirch map.
The Hazewinkel homomorphism.
The reciprocity map.
The norm groups.
Main theorems of local class field theory.
Existence theorem in local class field theory.
The Hilbert symbol and explicit formulas.
Other approaches to local class field theory.
Class field theory of complete discrete valuation fields with perfect residue field of positive characteristic.

12
Neukirch's general class field theory mechanism.
Applications of it to global fields and global class field theory.
Existence theorem in global class field theory.
Two types of class field theory: general and special.
Special class field theory: cyclotomic class field theory.
Special class field theory: complex multiplication class field theory.

CTNT I

This file will be made available from

https://ivanfesenko.org/wp-content/uploads/l1.pdf