Overview and Interconnections

Dinesh S. Thakur

In this workshop, we went through several topics, probably rapidly for those who saw them for the first time. So now, we will just take an overview of what was done, see how different topics were connected with each other, what the main tools were, and mention briefly a few more simple applications and techniques which we could not cover earlier for the lack of time.

Starting with our three motivating problems mentioned in the first lecture, we were led to the study of number fields, and in particular to quadratic, cyclotomic and Kummer extensions: Quadratic reciprocity found natural proofs coming from comparison of factorization laws in quadratic and cyclotomic extensions, regular polygons could be constructed by studying the relevant cyclotomic extensions as successive quadratic ones and Fermat equation could be handled (for regular primes) via study of cyclotomic and Kummer extensions.

Basic structure theorems of number theory (unique factorization of ideals, finiteness of class group, structure theorems for the unit group) were provided, in the lectures on Dedekind domains. We saw usefulness of the basic tools of localization and completions. We saw Kronecker's theorem on how the prime decomposition in an extension can (essentially) be decided by factoring a polynomial modulo that prime. We studied structures of $\mathbf{Q}_p$, $\mathbf{Q}_p^*$, $\mathbf{Z}_p$ etc., classified unramified and totally ramified extensions, studied the concepts of decomposition and inertia groups, Frobenius, discriminant, ramification, prime splitting, its reformulation in terms of Galois groups, using Frobenius conjugacy classes (elements in case of abelian extensions). The existence of nice decomposition laws for quadratic, cyclotomic and Kummer extensions was explained by unifying feature of having abelian Galois group in the class field theory lectures.

We know that $\mathbf{C}$ has no finite non-trivial extension, while $\mathbf{R}$ has $\mathbf{C}$ as its only non-trivial finite extension and $\mathbf{Q}_p$ has many finite extensions, but all with solvable Galois groups (we also saw in problem sessions that for odd p, there is no extension of $\mathbf{Q}_p$ with the Galois group $(\mathbf{Z}/p\mathbf{Z})^3$, as a corollary to local class field theory and structure theorem of $\mathbf{Q}_p^*$ (see also the proof of Lemma 14.8 in Washington using Kummer theory)) and only finitely many of a given degree, in contrast to the global case of $\mathbf{Q}$. As a simple corollary to the determination of the Galois group of $\mathbf{Q}(\zeta_n)$ and structure theorems for abelian groups and for $(\mathbf{Z}/n\mathbf{Z})^*$, we saw that all finite abelian groups occur

as Galois groups of cyclotomic extensions over $\mathbf{Q}$. The Kronecker-Weber theorem proved the converse. It is conjectured that every finite group occurs as a Galois group of an extension of $\mathbf{Q}$.

We saw that we have nice tools such as Hensel's lemma (finding a p-adic root by successive Newton approximation method) to solve equations in local fields and then looked at local-global principle example of Hasse-Minkowski theorem. The obstruction to local-global principle (the class group in the case of units and the Tate-Shafarevich group in the case of elliptic curves) is an important object of study.

We looked at zeta and L-functions encoding unique factorization in their simple sum and product descriptions. The special values and leading terms of these simply defined functions encode very interesting arithmetic information: Bernoulli numbers, class number formula that residue at $s = 1$ of $\zeta_K(s)$ is $2^{r_1}(2\pi)^{r_2}hR/w_K\sqrt{|d|}$. The idea of the proof was that the defining sum over ideals for the zeta decomposes into h equal ideal classes contributions, each computed by looking at the limiting sums as integrals and computing the resulting volumes, as in the Dedekind domains lectures.

The regulator R, which is a certain determinant of logarithms of the units is usually hard to compute. But for $\mathbf{Q}$ or an imaginary quadratic field, the rank zero unit group leads to a trivial regulator. Since the Riemann zeta function has a simple pole with residue 1 at $s = 1$, the factorization into L-functions simplifies the left side of the class number formula, e.g., in the case of quadratic fields it becomes $L(1, \chi)$, where χ corresponds to the field.

As an application, the familiar calculation

$$\frac{\pi}{4} = \tan^{-1}(1) = \int_0^1 \frac{dx}{1+x^2} = \int_0^1 (1 - x^2 + x^4 + \cdots)\, dx = 1 - \frac{1}{3} + \frac{1}{5} - \cdots$$

which calculates the L-function for the quadratic character corresponding to $\mathbf{Q}(i)$, implies that its class number is 1 by the class number formula. For $\mathbf{Q}(\sqrt{-5})$, the L-value is $1+1/3+1/7+1/9-1/11-\cdots$ which is approximately 1.4, whereas the right side of the formula is $h\pi/\sqrt{20}$, which is approximately $.7h$ giving $h = 2$, (since h has to be an integer), as we had verified by ideal manipulations using Minkowski bounds, in the problem sessions. Such approximate calculations also allow to calculate exactly ($2h$-th power of) the fundamental unit ϵ of the real quadratic field: More precisely the class number formula gives $\epsilon^{2h} = e^{\sqrt{d}L(1,\chi)}$ which can be calculated approximately, leading to the exact calculation of (trace) integer $A = \epsilon^{2h} + \epsilon^{-2h}$, so that ϵ^{2h} is a root of $x^2 - Ax + 1 = 0$.

It should be mentioned that using character sum manipulations, class number formula simplifies further.

Thus, for the imaginary quadratic fields of discriminant $d = -p$, where p is a prime, we have $h = R_p - N_p$ or $(R_p - N_p)/3$ according as $p \equiv 7$ or $p \equiv 3$ modulo 8, where R_p (respectively N_p) is the number of quadratic residues (respectively non-residues) modulo p within 1 to $(p-1)/2$. No simpler proof of even $R_p > N_p$ is known.

In the case of cyclotomic fields, comparing the class number formulas for K and K^+, we cancel out regulators and get a nice useful formula for the ratio h^-.

The class field theory, the powerful theorems of which we just stated and illustrated, sets up a useful correspondence between the class fields (i.e., the finite abelian extensions) and ideal groups. The simplest and yet powerful example is the Hilbert class field, that is the class field corresponding to the principal ideal group. By the basic properties of the correspondence, we see that it is the maximal abelian everywhere unramified extension, its Galois group is isomorphic to the class group (via the Frobenius map, and hence) exactly the principal primes split in it. Another important theorem about it is the principal ideal theorem, which says that every ideal in the ground field becomes principal in it (but of course it may have non-principal ideals). So we may try to get a tower of Hilbert class fields, and if it stops (i.e., if at some stage the Hilbert class field has class number one), then we get rid of the class number problem, as all the relevant ideals are now principal, at the expense of going to an extension. This sometimes works, but quite often the Hilbert class field tower is infinite. (We do not know a good 'if and only if' criterion).

If we are just interested in making every ideal principal in an extension, there are easier ways: Take I_i be ideal representatives of the ideal classes giving a basis for the class group of a number field F and let o_i be the order of the class corresponding to I_i. Let $I_i^{o_i} = (\alpha_i)$ and let β_i be an o_i-th root of α_i. Then $F(\{\beta_i\})$ is a degree h_F extension in which all ideals of F become principal. But in general this is not the Hilbert class field and we loose other interesting properties that the Hilbert class field has.

We have seen, as an application of Minkowski's discriminant bounds, that the maximal unramified extension of $\mathbf{Q}$ is $\mathbf{Q}$ itself. Again it is not known when exactly the maximal unramified extension is finite or infinite. Infinite class field tower examples lead to infinitely many such examples. For example, any $\mathbf{Q}(\sqrt{d})$, with d being square free and product of 8 or more distinct primes, has infinite class field tower. As an application of Odlyzko discriminant bounds, we can see for example that the maximal unramified extension (and the Hilbert class field) of $\mathbf{Q}(\sqrt{-5})$ is $\mathbf{Q}(\sqrt{-5}, \sqrt{5})$. (Exercise: Verify this by calculating basis of algebraic integers, discriminants and using Odlyzko discriminant bounds. Without Odlyzko bounds or class field theory,

verify also that every ideal becomes principal (only one ideal needs to be checked) and with a little more work, verify that it is of class number one, in fact. Verify also that the recipe above need not give the Hilbert class field in this case. (See Washington 11.4 and exercise 11.2). In this case, we could verify existence (and determination) of the Hilbert class field without class field theory ideas. In general, it seems difficult.

Kummer congruences on zeta values at negative integers lead to p-adic interpolation of the zeta function. The Kummer congruences can be thought of as reflection of Fermat little theorem congruences on $n^{p^{k-1}(p-1)} \equiv 1$ modulo p^k, if we think that even after analytic continuation the zeta values retain formal formula $\zeta(-k) = \sum n^k$. The integration approach (for other approaches see Washington or the article 'Modular forms and related objects' by Harold Stark in CMS Conf. Proc., 7) to the interpolation that we saw justifies this intuition. In fact, before the concept of analytic continuation was clear, Euler used this idea to give heuristic calculation of $\zeta(1-k)$, for $k > 0$:

$$\zeta(1-k) = \sum n^{k-1} = (d/dt)^{k-1} \sum e^{nt}|_{t=0} = -B_k/k$$

with the last equality implied by the fact that the geometric sum $1/(1-e^t)-1$ is basically the generating function for the Bernoulli numbers (or rather $B_k/k!$ depending on how you normalize).

Iwasawa theory lectures explained, how analogies (see 7.4 and 13.6 of Washington or Iwasawa's original paper for more) between number fields and function fields motivate the Iwasawa theory, its main conjecture, conjecture about $\mu = 0$ in the class number growth formula. In this original analogy, since the constant field extension tower of a function field is obtained by adjoining roots of unity, we also look at such a tower over a number field. There are different kind of analogies and ideas back and forth between Iwasawa theory and Carlitz-Hayes-Drinfeld explicit cyclotomic theory over function fields leading to a quite active interesting area of research. (We refer to two surveys on these aspects: J. Algebra 81 (1983), 107-149 by David Goss and Contemporary Math. 174 (1994), 157-165, Ed. Jones J. and Childress N., by me).

It is usually hard to get information on class numbers. But, by his simple structure theorem Iwasawa was able to get precise growth estimate $e_n = \lambda n + \mu p^n + \nu$ for n large, for the largest power p^{e_n} dividing the class number at the n-th layer in any $\mathbf{Z}_p$-extension. Now $e_n = 0$ for the $\mathbf{Z}_p$-extension of $\mathbf{Q}$ (and for any base F which has only one prime above p and class number not divisible by p). But in fact, in the traditional function field analogy, the constant field p^n- extension tower is the analogue of the

cyclotomic tower, as it is also obtained by adjoining roots of unity. It is easy to calculate class number growth there (Washington 7.4), because of Weil's results on Frobenius eigenvalues. This led Iwasawa to conjecture by analogy that $\mu = 0$ for the cyclotomic $\mathbf{Z}_p$-extension for any number field base. Ferrero and Washington (and later Sinnott) proved this for abelian extensions of $\mathbf{Q}$. Another conjecture, which comes through this analogy, is that λ remains bounded, if we vary p (for cyclotomic $\mathbf{Z}_p$-extensions) over a fixed number field and known only for the base $\mathbf{Q}$, as λ is identically 0 then. Greenberg conjectures more generally that λ is identically 0 for cyclotomic $\mathbf{Z}_p$-extension over totally real number fields.

We encountered two other important open problems: The *Leopoldt conjecture* on independence of units in the p-adic context says that p-adic regulator is non-zero or equivalently that there are exactly $r_2 + 1$ (unconditionally, the number is between $r_2 + 1$ and $r_1 + 2r_2$) independent $\mathbf{Z}_p$ extensions for any number field. The conjecture is known (Washington 5.32) for an abelian extension of $\mathbf{Q}$ (or of an imaginary quadratic field), as an application of p-adic transcendence theory. The *Kummer-Vandiver conjecture* states that p does not divide h^+, the class number of $\mathbf{Q}(\zeta_p)^+$.

It has many important *consequences*: Since it implies that all even components of A, the p-sylow subgroup of the class group of $\mathbf{Q}(\zeta_p)$ are zero, by the reflection theorem we proved, we get that the odd components are cyclic. Combining the annihilation information in Herbrand theorem with the p-adic class number formula, we then see that the i-th component is then isomorphic to $\mathbf{Z}_p/B_{1,w^{-i}}\mathbf{Z}_p$ for odd i between 3 and $p-2$. That the size of both the sides is the same is a hard (unconditional) theorem of Mazur-Wiles as a consequence of their proof of main conjecture of Iwasawa theory. (Another proof is due to ideas of Thaine, Kolyavagin and Rubin). The cyclicity is still unknown unconditionally. Note that even this size comparison proves the Ribet's converse to Herbrand that we saw. In fact, the Ribet's theorem was one of the starting points to Mazur-Wiles. Similarly, we see as implication of Vandiver that the odd part A^- of A is isomorphic to R^-/I^- as R-modules (again the index formula we saw, follows by comparing the sizes of two isomorphic objects), so that the Stickelberger ideal gives all the relations in A^-. Vandiver also implies this for the whole cyclotomic tower, it gives the full main conjecture as easy implication. Some important known quasi-isomorphisms in the theory become isomorphisms under Vandiver hypothesis. We refer to Washington 10.3 for more details.

Note that given even i, since p does not divide B_i for large enough p, Herbrand's theorem implies that $(p-i)$-th component of A vanishes, for large enough p. A similar consequence was explained using some ideas from K-theory, for odd i.

We saw how useful the Gauss and Jacobi sums are: Study of their factorization leads to Stickelberger theorem on ideal class annihilators for the cyclotomic fields. They can be used for power reciprocity proofs.

We saw reciprocity laws in various general contexts. Here is a nice application to the Fermat equation. We first state the *Artin-Hasse explicit reciprocity* law for p-th power residue symbol $(\alpha/\beta) \in \mu_p$:

With $\zeta = \zeta_p$, $\lambda = 1 - \zeta$ as usual, for $\alpha, \beta \in \mathbf{Z}[\zeta]$, $(\alpha, \beta) = 1$ and $\alpha \equiv 1$ modulo λ and $\beta \equiv 1$ modulo p, we have $(\beta/\alpha)(\alpha/\beta)^{-1} = \zeta^{tr(\eta)}$ where $\eta = (\beta - 1)(\alpha - 1)/(p\lambda)$. Here tr denotes the trace from $\mathbf{Q}(\zeta)$ to $\mathbf{Q}$. Note that for $p = 2$, we have $\lambda = 2$ and this reduces to the usual statement of quadratic reciprocity.

Application: If we have a first case solution to the p-th Fermat equation, i.e., $x^p + y^p = z^p$, $(x, y, z) = 1$ and xyz is not divisible by p, then $q^{p-1} \equiv 1$ modulo p^2 for any prime q dividing xyz. (The special case $q = 2$ is called *Wieferich criterion*. Only primes $p < 3 \times 10^9$ which satisfy $2^{p-1} \equiv 1$ modulo p^2 are 1093 and 3511. So the first case follows for the rest).

Proof: By assumption, $x + \zeta^i y = I_i^p$, for ideal I_i. So $\alpha := 1 - y\lambda/(x+y) \equiv 1$ (λ) is a p-th power of a fractional ideal I and hence $(\beta/\alpha) = (\beta/I)^p = 1$, for any β prime to α. In particular, put $\beta := q^{p-1} \equiv 1$ (p). Without loss of generality, $q|y$ and so $\alpha \equiv 1$ (q). Hence $(\alpha/q) = 1$, so that $(\alpha/\beta) = 1$ and by the reciprocity law, we get $(q^{p-1} - 1)tr((\alpha - 1)/\lambda)/p \equiv 0$ (p). But $tr((\alpha - 1)/\lambda) = -(p-1)y/(x+y) \not\equiv 0$ (p), proving the claim.

Urge for more and more general and refined reciprocity laws led to so-called *non-abelian class field theory and Langlands program*. We saw that in the abelian case, irreducible representations of the Galois groups lead to characters. In the next stage, we look at Galois group representations with values in $Gl_2(\mathbf{C})$ rather than $Gl_1(\mathbf{C}) = \mathbf{C}^*$ i.e., move from the commutative domains of numbers to the non-commutative domain of 2 by 2 matrices. It turns out that there are modular forms of weight one with q-expansion $\sum a_n q^n$ with a_p being the trace of Frobenius at p viewed as the corresponding matrix. So, for example, p splits in the corresponding extension, if $p = 2$. So the generalized congruence conditions for splitting in the class field theory get replaced by such conditions governed by modular forms. (The analogy is clearer in the adelic setting: The automorphic forms (closely related to modular forms) are then Gl_2 analogs of Gl_1 (Hecke) characters). The modular forms are still manageable interesting objects: They form a finite dimensional space.

As for the eventual proof of the Fermat's last theorem by Wiles, the techniques went way beyond the cyclotomic theory, but nonetheless there is *historical continuation of motivation and techniques* from the cyclotomic theory:

In Kummer's approach, as we saw, hypothetical non-trivial solution to the Fermat equation for the exponent p gave a Kummer extension of degree p of $\mathbf{Q}(\zeta_p)$ which was unramified everywhere and hence could not exist for the regular primes. In (Hellagouarch, Frey, Serre, Ribet and Taylor-) Wiles approach, the hypothetical non-trivial solution gives rise to an elliptic curve (with discriminant essentially a p-th power) whose p-torsion points give a field extension with Galois group inside $Gl_2(\mathbf{Z}/p\mathbf{Z})$, unramified outside 2 and p and only 'mildly' ramified at p etc.. (In fact, as we saw using the Tate curve, this ramification analysis boiled down to that for a Kummer extension of a cyclotomic one). We used class field theory to rule out the extension in the Kummer case, for regular primes. Now we use non-abelian class field theory (and modular forms mentioned above) to rule this extension, for all primes. The problem is that non-abelian class field theory is not well-developed yet (just as Kummer did not have class field theory at his disposal and had to take detours) to have an easy classification doing the job, so Wiles had to invent and use a lot of techniques to do the job. (In fact, the crucial non-abelian part of Langlands program that got used (due to Langlands and Tunnel) is still in 'solvable' domain, done using class field theory, but the point is that the correct framework of ideas it provides helps).

To continue listing inputs from cyclotomic theory ideas to the techniques and motivations, we first note that Eichler, Shimura, Deligne, Serre's works connecting Galois representations and modular forms, Ribet's proof of converse to Herbrand theorem are some of the starting points of the circle of ideas used eventually. Next, Hida (and Mazur) developed Iwasawa theory in this non-abelian context: Just as Iwasawa theory takes the advantage of structural simplicity once we pass to inverse limit over the tower, they studied the liftings of the representations in rings of matrices with entries in large p-adic rings where we can deform them and use geometric techniques. We looked at Kolyavagin's Euler system argument to control class groups, class number formulas, main conjecture etc. These have their counterparts in elliptic curves theory, which got used. (See Washington's article 'Number fields and elliptic curves' and 'Modular forms and Fermat's last theorem' volume for a good exposition of related ideas).

Dinesh Thakur
Department of Mathematics
University of Arizona
Tucson, AZ 85721
USA
e-mail: thakur@math.arizona.edu