WYKŁADY Z TEORII LICZB

Wykład ten składa się z dwóch odrębnych minikursów (można w nich brać udział niezależnie).

Minikurs 1: prof. dr Gerhard Frey (Uniwersytet w Essen), **Modular Forms and Galois Representations: Arithmetic, Algorithms and Applications,** 12-16.09.2011 r.
Minikurs 2: prof. dr Cornelius Greither (Uniwersytet w Monachium), **Galois modules, Iwasawa theory and Leading Term conjectures,** 19-23.09.2011

Polscy doktoranci z poza Poznania (w pierwszej kolejności z SSDNM, ale także inni) mogą otrzymać wsparcie finansowe (na koszty podróży i zakwaterowania) – w tym celu należy wysłąć prośbę wraz z rzetelnym szacunkiem kosztów do p. Skrzypczak (epskrzyp@amu.edu.pl) do 1 lipca 2011.

Szczegółowe dane poniżej:

MINIKURS 1.

Temat: ***Modular Forms and Galois Representations: Arithmetic, Algorithms and Applications***

Wykładowca: **prof. dr Gerhard Frey** (Uniwersytet w Essen)

Wymiar godzin: **10 godz.**

Termin: **12 – 16.09. 2011**

Rozkład godzin:

poniedziałek	**10.00-11.30**
wtorek	**10.00-11.30**
środa	**10.00-11.30**
czwartek	**10.00-11.30**
piątek	**10.00-11.30**

Miejsce: **Wydział Matematyki i Informatyki UAM**

Poznań, ul. Umultowska 87

Biogram wykładowcy:

Gerhard Frey jest matematykiem niemieckim, który jest sławny ze swoich wyników uzyskanych w teorii liczb. Krzywe Freya (to znaczy krzywe eliptyczne przyporządkowane rozwiązaniom równań Fermata) stanowią centralne narzędzie w dowodzie Wielkiego Twierdzenia Femata uzyskanego przez Andrew Wilesa w 1994 roku.
Frey studiował matematykę i fizykę na uniwersytecie w Tübingen. Doktorat z matematyki uzyskał na uniwersytecie w Heidelbergu w 1970, a habilitację trzy lata później na tym samym uniwersytecie. W latach 1969-1973 pracował jako profesor asystent w Heidelbergu, następnie (już jako profesor) w Erlangen (1973-1975), Saarbrücken (1975-1990), oraz do 2009 na uniwersytecie w Duisburgu-Essen, gdzie kierował zorganizowanym przez siebie Instytutem Matematyki Eksperymentalnej.
Badania naukowe Gerharda Freya koncentrują się wokół zagadnień teorii liczb, geometrii arytmetycznej oraz ich zastosowań w teorii kodowania i kryptologii algebraicznej. Jest autorem ponad siedemdziesięciu prac opublikowanych, między innymi w Canadian Bulletin of

Mathematics, Journal für die reine Mathematik, Compositio Mathematicae i Journal of Number Theory. Był profesorem wizytującym w Ohio State University w Columbus, Harvard University, University of California at Berkeley, Mathematical Sciences Research Institute (MSRI) w Berkeley, w Institute for Advanced Studies w Hebrew University w Jerozolimie oraz w IMPA w Rio de Janeiro.

W 1985 roku Frey odkrył związek pomiędzy Wielkim Twierdzeniem Fermata (wtedy hipotezą Fermata) i hipotezą Shimury-Taniyamy-Weila z teorii krzywych eliptycznych, co wkrótce doprowadziło do dowodu przez Kennetha Ribeta twierdzenia, które mówi, że hipoteza STW pociąga WTF. Ten związek stanowił podstawę dla Andrew Wilesa w jego dowodzie Wielkiego Twierdzenia Fermata. Za swoją pracę na temat WTF Frey uzyskał w 1996 roku medal imienia Gaussa towarzystwa *Braunschweigische Wissenschaftliche Gesellschaft*. Od 1998 roku Frey jest członkiem Akademii Nauk w Getyndze.

W 1998 roku Frey zaproponował atak na problem dyskretnego logarytmu oparty na własnościach formy dwuliniowej Weila w przypadku krzywych eliptycznych nad ciałem skończonym złożonego stopnia. Atak podany przez Freya spowodował, że wspomniane krzywe nie są już stosowane w kryptografii. Za swoje osiągnięcia w kryptografii i kryptologii krzywych eliptycznych w 2006 roku Gerhard Frey został uhonorowany nagrodą *Certicom ECC Vision Award.*

Opis wykładu:

Very often Diophantine problems can be stated in an elementary way but it is notoriously hard to solve them. The most famous example for this phenomenon was Fermat's Last Theorem. The situation becomes better whenever one finds a mathematical structure behind the problem, and in many cases this structure is delivered by the action of the Galois group on geometric objects like torsion points of elliptic curves or, more generally, abelian varieties. Then the arithmetic of Galois representations plays a dominant role. A key role in this game is occupied by Jacobian varieties of modular curves. These varieties are very well understood, and connections to modular forms allow deep theoretical and practical insights. It is the aim of the lectures to explain both theoretical and algorithmic aspects in this exciting part of arithmetic geometry. An additional bonus is that many of the results can be used to construct public key crypto systems and to discuss their security.

Contents

- Geometric Galois representations and the density theorem of Cebotarev, the Conjecture of Fontaine-Mazur, the isogeny theorem of Faltings and application to point counting on curves over finite fields
- Modular Varieties, modular forms and modular Galois representations, the congruence of Eichler-Shimura and modular forms of low weight As application: Merel's uniform boundedness theorem for torsion of elliptic curves
- Congruences between modular forms
- Serre's Conjecture for odd two-dimensional Galois representations over Q and consequences:
  Modularity of elliptic curves and GL(2)-abelian varieties, FLT, Artin's conjecture for odd two-dimensional representations
- Algorithmic Aspects: Computation of the space of forms of low weight by modular symbols, modular forms of weight 3/2 and families of twists of elliptic curves, congruences between modular forms

Literature and Background

In the lectures we shall explain all necessary notions. But it will be helpful to have a good knowledge of the basic structures in algebra and in (algebraic) number theory as well as in the basic theory of algebraic geometry, e.g. curves and their Jacobians.

A very short list of References: For elliptic curves and their arithmetic properties we recommend the two books of J. Silverman on “The Arithmetic of Elliptic Curves".

A classical monography on modular forms is G. Shimura:”Introduction to the Arithmetic Theory of Automorphic Functions", Princeton 1971.
Many aspects about the relations between modular representations and diophantine equations can be found by browsing through “Modular Forms and Fermat's Last Theorem", G. Cornell, J.H. Silverman, G. Stevens edts., Springer 1997.
Computational aspects are treated in W. Stein: ”Modular Forms: A computational Approach" (available via the web page of William).

MINIKURS 2.

Temat:	***Galois modules, Iwasawa theory and Leading Term conjectures***
Wykładowca:	**prof. dr Cornelius Greither** (Uniwersytet w Monachium)
Wymiar godzin:	**10 godz.**
Termin:	**19 - 23.09.2011 r.**
Rozkład godzin:	**poniedziałek 10.00 – 11.30**
	wtorek 10.00 – 11.30
	środa 10.00 – 11.30
	czwartek 10.00 – 11.30
	piątek 10.00 – 11.30
Miejsce:	**Wydział Matematyki i Informatyki UAM**
	Poznań, ul. Umultowska 87

Biogram wykładowcy:

Profesor Cornelius Greither jest wybitnym specjalistą algebraicznej teorii liczb, teorii modułów Galois i teorii Iwasawy. Jego najważniejsze wyniki dotyczą opisu struktury algebraicznej grup klas ideałów, p-adycznej interpolacji wartości specjalnych funkcji L oraz funkcji dzeta Dedekinda ciał liczbowych. Opublikował około sześćdziesiąt prac naukowych w tak prestiżowych czasopismach matematycznych jak: Inventiones mathematicae, Journal für die reine und angewandte Mathematik, Compositio Mathematica, Mathematische Zietschrift, Transactions of the AMS, Journal of Algebra, Acta Arithmetica i Journal of Number Theory. Jego rozprawa habilitacyjna została wydana w prestiżowej serii Lecture Notes in Mathematics wydawnictwa Springer.

Cornelius Greither doktoryzował się na podstawie pracy z algebry przemiennej na Uniwersytecie Ludwika Maksymiliana w Monachium w 1983 roku, a w 1988 habilitował się

na tej samej uczelni. Pracował na Uniwersytetach w Monachium, Karlsruhe, Ulm, na Uniwersytecie Lavala w Kanadzie i w Instytucie Maxa Plancka w Bonn. Od 1999 jest profesorem zwyczajnym na Uniwersytecie Bundeswehry w Monachium-Neubiberg. Wypromował sześciu doktorów matematyki. Jest edytorem czterech czasopism matematycznych o zasięgu międzynarodowym. Ponad 250 razy recenzował prace z matematyki dla Mathematical Reviews i dla Zentralblatt der Mathematik.

Poza matematyką profesor Greither aktywnie interesuje się muzyką i lingwistyką. Gra na fortepianie w tercecie Triphonia wykonującym utwory muzyki klasycznej i kameralnej. Potrafi komunikować się w ponad dziesięciu językach, w tym perfekcyjnie po angielsku i po francusku. Po zaledwie trzech kilkudniowych wizytach w naszym kraju opanował w zadowalającym stopniu język polski.

Opis wykładu:

The underlying theme of these lectures (and of much work in the past and present) is the connection between algebraic structures coming from number theory and geometry on the one side, and arithmetic data coming from zeta and *L*-functions on the other. A prototypical and classical example is the analytic class number formula. If *K* is a number field, then its class number (the order of the ideal class group of *K*) is given by $-w_K / R_K$ times the leading coefficient of the Dedekind zeta function $\zeta_K(s)$ at $s = 0$. Since Galois extensions *K/F* play such an enormous role in algebraic number theory, it is natural to regard actions of the Galois group *G* of *K/F* on all kind of objects, for example the class group cl_K. This class group together with the *G*-action is a much more interesting and subtle object than just the class number. For instance one can sometimes factor the class number into χ-class numbers, one for each irreducible character of *G*. Such a factorisation should also be reflected in a refined class number formula involving *L*-functions, again one function for each χ. This is indeed possible. In the proofs, Iwasawa theory play a decisive role. Its main idea is to consider not only one field *K* but a whole (infinite) tower of fields $K = K_0 \subset K_1 \subset K_2 \ldots$ Contrary to appearances, this sometimes has a simplifying effect. (This can be compared to analysis; real numbers are given by infinite series, but they are a most useful abstraction. Working with finite precision is often much more cumbersome from the theoretical point of view.)

This series of lectures will try to tell something about the techniques (local methods, Iwasawa theory, a little homological algebra) as well as the results. The philosophy sketched above extends to many other domains of contemporary mathematics; we only mention *K*-theory and the theory of elliptic curves.

Contents:

1. Quick review of Galois theory, examples

2. Some algebra: Free and projective modules. Exact sequences, some standard functors. Localisation (i.e. calculating with fractions over a commutative ring).
3. Completions: Projective limits. Rings and fields of *p*-adic numbers. Local-global principles in algebraic number theory. Completed groups rings (Iwasawa algebras).
4. Tame additive Galois module structure: Ramification. Noether's Theorem (given a Galois extension *N/K* of number fields, then the ring of integers O_N is $O_K[G]-$projective iff *N/K* is at most tamely ramified). Freeness (or otherwise) of O_N over $O_K[G]$ or $\mathbf{Z}[G]$.
5. Classical Iwasawa modules: Cyclotomic towers of number fields. Construction of *X* as the projective limit of certain class groups in the tower. Classification up to pseudo-isomorphism. Application to class groups: Iwasawa's invariants λ, μ, ν. The Main Conjecture in Iwasawa Theory.
6. Projective limits of units: Freeness results for projective limits of units. Special units (in particular cyclotomic units) and their limits. The Main Conjecture revisited.
7. Cohomology: Definition of group cohomology in low degrees (0 to 2), with many easy and explicit examples, taken from number theory. Projective resolutions. Some basics on Ext, canonical classes.
8. Leading term conjectures: Statement of one such conjecture (also called ETNC). A relatively easy example. Report on the status of the conjecture.

Prerequisites and references:

Some familiarity with algebra and basic number theory will be very useful. Two good sources on number theory in general and local theory (completions) in particular are the books "Algebraic number theory" by J. Neukirch and "Algebraic number fields" by G. Janusz. For preliminary reading on Iwasawa theory, probably the best book would be L. Washington's "Introduction to Cyclotomic Fields". A lot of information on *L*-functions, units and class number formulas can be found in the early chapters of J. Tate's book on Stark's conjectures (Birkhäuser). If anyone requires preliminary reading on Galois module theory, a first impression is probably easier to get from the article of Cassou-Noguès et al. in the Durham Proceedings (L.M.S. Lecture Notes 153, 1989) than from A. Fröhlich's big monograph (Springer 1983). There is no "compulsory" preliminary reading, and more references will be given during the course.