RESEARCH STATEMENT

I am studying Arithmetic Algebraic Geometry and Number Theory.

Algebraic equations and their arithmetical properties have been an interest mankind since the times of Pythagoras and Diophantus, which were a milestone in their time. For many centuries such problems have fascinated both serious mathematicians (Fermat, Gauss, ...) and amateurs alike. However, developments in recent years have transformed the subject into one of the central areas of mathematical research, which has relations with, or applications to, virtually every mathematical field, as well as an impact to contemporary everyday life. The interaction of arithmetic and geometry have led to a complex and far-reaching web of conjectures proposing a deep explanation for the observed phenomena. At the same time, this interaction and the combination of the new, powerful methods have enabled the solution of some of these conjectures as well as of some long-standing ones (Fermat's Last Theorem). My study is focusing on two subjects namely, Galois Module Structure and Distribution of primes on certain products.

Galois Module Structure

The normal basis theorem implies that if N/K is a finite Galois extension of number fields with Galois group G, then N is a free $K[G]$-module of rank one. In particular, N is a free $\mathbb{Q}[G]$-module. Let $\mathcal{O}_N$ and $\mathcal{O}_K$ be the ring of integers of N and K respectively. Then we can ask for the analogous statement, namely, "Is $\mathcal{O}_N$ a free module over the group ring $\mathbb{Z}[G]$?" The first observation regarding this question belongs to E. Noether.

Theorem 1. *(E. Noether) Let N/K be a finite Galois extension of number fields with Galois group G. Then the ring of integers, $\mathcal{O}_N$ is a projective $\mathbb{Z}[G]$-module if and only if N/K is at most tamely ramified.*

When N/K is tamely ramified, the obstruction to $\mathcal{O}_N$ to be a stably free $\mathbb{Z}[G]$-module is the class $(\mathcal{O}_N)$ in the class group $Cl(\mathbb{Z}[G])$. Fröhlich's conjecture, proved by M.Taylor in [T], gives an interesting description for this class:

Theorem 2. *(M. Taylor) We have the following equality,*

$$(\mathcal{O}_N) = W_{N/K} \tag{1}$$

in $Cl(\mathbb{Z}[G])$. Here $W_{N/K}$ is the "root number class"; the class $W_{N/K}$ has order two and is given by the signs of the ϵ-constants in the functional equation of the Artin L-functions of symplectic representations of G.

The works of Chinburg and of Chinburg, Erez, Pappas and Taylor ([CEPT], [CPT]) generalize Fröhlich's conjecture by relating the ϵ-constants with the Galois modules attached to a group action on an arithmetic scheme. It turns out that one can consider more general equivariant projective Euler characteristics: Suppose that X is a scheme projective and flat over $\mathbb{Z}$ which supports a tame action of the finite group G. For any coherent sheaf $\mathcal{F}$ on X which supports a G-action that is compatible with the action of G on X one can define following Chinburg [C] the equivariant projective Euler characteristics $\chi(X, \mathcal{F}) \in Cl(\mathbb{Z}[G])$. The calculation of these Euler characteristic often connects to other fundamental problems in Number Theory. A recent method, developed by Chinburg, Pappas and Taylor in [CPT1], shows how to calculate the Euler characteristic of coherent sheaves on projective flat schemes over $\mathbb{Z}$ on which finite group acts. Unlike other techniques, this one does not neglect any torsion information if the base scheme has dimension less than 5. Also an illustration of the calculation is presented on an example. In particular, they determined the structure of the lattice of weight 2 cusp forms for $\Gamma_1(p)$ which have integral Fourier expansions as a module for the action of the finite group of diamond Hecke operators. This is done by calculating the equivariant Euler characteristic $\chi(X, \mathcal{O}_X)$ where X is a certain integral model of the modular curve $X_1(p)$.

My study can be thought of as a generalization of this example. I calculated the equivariant Euler characteristic of k-th power of the "twisted" canonical sheaf over an integral module of the modular curve $X_1(p)$ (here some twists are allowed along a fibral divisor at p for some technical reasons). I found a lower bound to the degree of the twist which guarantees that the first cohomology group vanishes. Consequently, the structure of the lattice of "twisted" cusp forms of weight $2k$ and Nebentypus character can be obtained as a module for the diamond Hecke operators. Here twist means that we allow the Fourier coefficients to have denominator a certain (bounded) power of a uniformizer over p .

Distribution of primes on certain products

Let us denote the product of the first n terms of an integer valued sequence a_k by A_n. The question of how the powers of the prime factors of this product are distributed as n grows appears in various guises in number theory. For example, if we take $a_k = k$, then we get $A_n = n!$. In this case, we can easily express the largest power of p dividing A_n for each prime $p = n$ in terms of p and n. On the other hand, one may ask many nontrivial questions concerning all of these powers simultaneously. For instance, let us examine whether or not A_n can be a square for $n = 2$. A proof of impossibility can be given using the famous Bertrands postulate.

In my study, by choosing the elements of the sequence a_k as the values of a polynomial at integers, we aim at answering similar questions as well as obtaining general results about the distribution of the powers. As a next step, taking $a_k = k^2 + d$ where d is a positive integer, we wish to show that A_n is not a square for sufficiently large values of n (depending on d), and explicitly list the values of n for which it is a square for many values of d. This question is solved by Cilleruelo [Ci] for $d = 1$: In this case, A_n is a square only for $n = 3$. For larger values of d there is no complete answer yet. In another paper, Ambederhan, Medina and Moll [AMM] take $a_k = k^p + 1$, and give a proof that for $p = 3$ prime and $n = 12$ the product A_n is not a square. However, it was shown via a counterexample by Gürel ve Kisisel [GK] that this proof is incorrect, and for $p = 3$ it was shown in the same paper that A_n is never a square by using another method. Let us remark that, in these proofs, tools like Bertrands postulate mentioned in the paragraph above could not be used, since even the infinitude of primes of the form $k^2 + 1$ is an open problem aging more than 200 years.

References

[AMM] Amdeberhan, T. , Medina, L. A. , Moll, V. H.: Arithmetical properties of a sequence arising from an arctangent sum, J. Number Theory 128 (2008), 18071846.

[C] T. Chinburg: Galois structure of de Rham cohomology of tame covers of schemes, Annals of Math., **139** (1994), 443–490. Corrigendum, Annals of Math., **140** (1994), 251.

[Ci] J. Cilleruelo: Squares in (12+1)(n2+1), J. Number Theory 128 (2008), 2488–2491.

[CEPT] T. Chinburg, B. Erez, G. Pappas, M. J. Taylor: ε-constants and the Galois structure of de Rham cohomology. Annals of Math. **146** (1997), 411-473.

[CPT] T. Chinburg, G. Pappas, M. J. Taylor: ε-constants and the Galois structure of de Rham cohomology 2. J. Reine Angew. Math. 519 (2000), 201-230.

[CPT1] T. Chinburg, G. Pappas, M. J. Taylor: Cubic Structures, Equivariant Euler Characteristics and Lattices of Modular Forms, submitted.

[T] M. J. Taylor: On Frochlich's conjecture for rings of integers of tame extensions. Inventiones Math., **63** (1981), 41–79.