RESEARCH STATEMENTS

JIANING LI

In my post-doctor years, I work in the area of algebraic number theory. Much of my work is on ideal class groups and Selmer groups and my work has the nature of explicit computation.

Works on class groups in Kummer and radical extensions:

- This item describes a joint work [1] with Yi Ouyang, Yue Xu and Shenxing Zhang. Let ℓ and p be prime numbers and $K_{n,m} = \mathbb{Q}(p^{\frac{1}{\ell^n}}, \zeta_{2\ell^m})$. When $\ell = 2$, we determine the structure of the 2-class group of $K_{n,m}$ for all $(n,m) \in \mathbb{Z}^2_{\geq 0}$ in the case $p \equiv 3, 5 \bmod 8$, and for $(n,m) = (n,0)$, $(n,1)$ or $(1,m)$ in the case $p \equiv 7 \bmod 16$, generalizing the results of Parry about the 2-divisibility of the class number of $K_{2,0}$. We also obtain results about the ℓ-class group of $K_{n,m}$ when ℓ is odd and in particular $\ell = 3$.
- Moreover, in a recent joint work with John Coates and Yongxiong Li [2], we further determine, for any $m \geq 1$, the 2-class group of $K_{2,m}$ with $\ell = 2$ when $p \equiv 7 \bmod 16$ by using a different method.
- In a joint work [3] with Yue Xu, we prove that 4 divides the class number of $K_{2,0} = \mathbb{Q}(\sqrt[4]{p})$ when $p \equiv 15 \bmod 16$ (previously it is known that 2 divides the class number). We also construct the 4-Hilbert class field of $K_{2,0}$ and find an explicit conjectural relation between the 2-class numbers of $K_{2,0}$ and $\mathbb{Q}(\sqrt{-2p})$ when $p \equiv 15 \bmod 16$.
- Very recently, Shenxing Zhang and I in [4] determine the 3-class group of $K_{1,0} = \mathbb{Q}(\sqrt[3]{p})$ and $K_{1,1} = \mathbb{Q}(\sqrt[3]{p}, \zeta_3)$ for $p \equiv 4, 7 \bmod 9$ with $\left(\frac{3}{p}\right)_3 = 1$. This result confirms a conjecture of Barrucand-Cohn made in 1980 and proves the last remaining case of a conjecture of Lemmermeyer on 3-class groups of $K_{1,1}$ (with $\ell = 3$).

Works on Iwasawa theory with base field $\mathbb{Q}(\sqrt{-q})$ where $q \equiv 7 \bmod 8$ is a prime

- Let $K = \mathbb{Q}(\sqrt{-q})$. Let $F = \mathbb{Q}(\sqrt[4]{-q})$. Write $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. Assume $\mathfrak{p}$ is unramified in F. In [5], I prove certain results on the $\mathfrak{p}$-adic logarithms of the fundamental unit (i.e. the $\mathfrak{p}$-adic regulator $R_\mathfrak{p}$) of the field $\mathbb{Q}(\sqrt[4]{-q})$, where $q \equiv 7 \bmod 8$ is a prime (indeed for $q \equiv 3 \bmod 4$). When $q \equiv 15 \bmod 16$, this result confirms a speculation of Coates-Li. In an unpulished print, I further proved a finer result on $R_\mathfrak{p}$ which confirms a statement suggested by numerical data calculated by Zhibin Liang when $q \equiv 15 \bmod 16$.
- For any algebraic extension R of K, let $M(R)$ be the maximal abelian 2-extension of R which is unramified outside the primes above $\mathfrak{p}$. Write $X(R) = \mathrm{Gal}(M(R)/R)$. Let K_∞ be the unique $\mathbb{Z}_2$-extension of K which is unramified outside $\mathfrak{p}$. Write $R_\infty = RK_\infty$. Let $J = K(\sqrt[4]{-q}, \sqrt{-1})$, $F = K(\sqrt[4]{-q})$, $F' = K(\sqrt{-\sqrt{-q}})$ and $D = K(\sqrt{-1})$, so that J/K is a bi-quadratic extension with the nontrivial intermediate fields F, F' and D.

  In a joint work [2] with John Coates and Yongxiong Li, we explicit compute $X(J), X(J_\infty)$, $X(F), X(F_\infty), X(F'), X(F'_\infty), X(D_\infty), X(D)$ when $q \equiv 7 \bmod 16$. We also prove some non-vanishing results for these modules when $q \equiv 15 \bmod 16$. We further obtain results on Iwasawa theory of a family of Gross curves.

  Let A be the $\mathbb{Q}$-curve defined over $H := \mathbb{Q}(j(\mathcal{O}_K))$ with complex multiplication by $\mathcal{O}_K$, minimal discriminant $(-q^3)$. Let $B/K = \mathrm{Res}_{H/K}A$ be the h-dimensional abelian variety. Our results combining with the celebrated work of Gross-Zagier and Kolyvagin and the analytic results of Miller-Yang, imply that, for all primes $q \equiv 7 \bmod 16$, one has $B(D) \otimes_\mathbb{Z} \mathbb{Q} \cong B(D_\infty) \otimes_\mathbb{Z} \mathbb{Q} \cong B(J_\infty) \otimes_\mathbb{Z} \mathbb{Q}$ are all $\mathbb{Q}$-vector spaces of dimension $2h$, and also $Ш(B/D_\infty)(\mathfrak{P}) = Ш(B/J_\infty)(\mathfrak{P}) = 0$. Here $\mathfrak{P}$ is the prime of $End_K(B)$ above $\mathfrak{p}$ such that it is in the kernel of the map $End(B) \to \mathcal{O}_K/2\mathcal{O}_K$ which is induced by the action of $End_K(B)$ on $B(K)_{\mathrm{tors}} = \mathcal{O}_K/2\mathcal{O}_K$.

Works on distribution of $\mathcal{T}_2$-groups of quadratic fields

For a number field F, we let $\mathcal{T}_p(F)$ denote the $\mathbb{Z}_p$-torsion subgroup of the Galois group of the maximal abelian pro-p extension of F unramified outside p over F. In a joint work [6] with Yi Ouyang and Yue Xu, we study the distribution of $\mathcal{T}_2(F) := \mathcal{T}_2(m)$ where $F := \mathbb{Q}(\sqrt{m})$ is a quadratic field. We prove the 4-rank formula of $\mathcal{T}_2(-m)$ for $m > 0$ (i.e. F is imaginary) in terms of the rank of certain Rédei matrix, by exploring the connections of the $\mathcal{T}_2$-group to the ideal class group $\mathrm{Cl}_2(F)$ and the tame kernels of $\mathbb{Q}(\sqrt{m})$. We obtain the density of imaginary quadratic fields whose $\mathcal{T}_2$-groups have 4-rank r for any integer $r \geq 0$. We propose distribution conjectures on $6\mathcal{T}_p(F)$ when F varies over real or imaginary quadratic fields for any prime p, in the spirit of Cohen-Lenstra heuristics. We also derive explicit results for $\mathcal{T}_2(\pm l)$ where l is an odd prime and propose conjectures on the distributions of $\mathcal{T}_2(\pm l)$ when l varies. In the case $F = \mathbb{Q}(\sqrt{l})$, appealing to Coates' order formula, this reveals a speculation of Shanks-Sime-Washington on the distributions of the zeros of 2-adic L-functions and also reveals the distributions of the fundamental units.

An idelic-proof of Chevalley's ambiguous class number formula and its generalization by Gras. In much of my work, the Chevalley's formula and its generalization by Gras play a role. In a joint work [7] with Chia-Fu Yu, we give an idelic proof of this formula for global fields, in the most general form. We also give an adelic proof of the ambiguous formula for the class group of divisors of degree 0 in the function field case, which extends a result of Rosen.

In my doctor years, I made the following contribution in the **area of cryptography**. In a joint work [8] with my advisor Yingpu Deng, we obtain new nonexistence results of generalized bent functions (GBF) from $(\mathbb{Z}/q\mathbb{Z})^n$ to $\mathbb{Z}/q\mathbb{Z}$. (We recall that GBF are important functions in coding theory and cryptography, which have maximum non-linearity and are employed to resist linear crypto-analysis and correlation-attack.) Our result, in the first time, provides the non-existence result of an infinite family of of GBF such that there exist cyclotomic integers in $\mathbb{Z}[\zeta_q]$ with absolute values $q^{\frac{n}{2}}$. Previously, Keqin Feng proved the non-existence results by showing there are no such cyclotomic integers; Dingyi Pei and Yupeng Jiang proved the non-existence result in the case $(n, q) = (1, 2 * 7)$ and $(n, q) = (3, 2 * 23)$ respectively, noting that in this two cases, there are cyclotomic integers with the prescribed absolute values. In a later work [9] joint with Chang Lv, we proved further new non-existence results of GBF by using Stickerberger's theorem.

I am now interested in

(1) Iwasawa theory, especially topics (including explicit examples and algorithms) surrounding Greenberg's pesudo-null conjecture and Weber's class number problem.
(2) Compute the torsion subgroup of the $\mathbb{Q}$-rational points of the Jacobian varieties $J_0(N)$ of modular curves when N is composite, for example, the recent work of Yuan Ren.
(3) Compute the modular degrees of the Gross curves.

References

[1] Jianing Li, Yi Ouyang, Yue Xu, and Shenxing Zhang. *ℓ-class groups of fields in Kummer towers*, *to appear in* Publ. Mat., 2020, arXiv:1905.04966.
[2] John Coates, Jianing Li, and Yongxiong Li. *Classical Iwasawa theory and infinite descent on a family of abelian varieties*, arXiv:2008.10310.
[3] Jianing Li and Yue Xu. *On Class Numbers of Pure Quartic fields*, Ramanujan Journal (2020). `https:doi.org/10.1007/s11139-020-00253-2`.
[4] Jianing Li and Shenxing Zhang. *The* 3*-class group of* $\mathbf{Q}(\sqrt[3]{p})$, pdf.
[5] Jianing Li. *On the 2-adic logarithm of units of certain totally imaginary quartic fields*, *to appear in* Asian J. Math., 2020, arXiv:2005.09926.
[6] Jianing Li, Yi Ouyang, and Yue Xu. *On abelian 2-ramification torsion modules of quadratic fields* , arXiv:2009.13262.
[7] Jianing Li and Chia-Fu Yu. *The Chevalley-Gras formula over global fields*, *to appear in* Journal de Théorie des Nombres de Bordeaux. arXiv:2001.11413.
[8] Jianing Li and Yingpu Deng. *Nonexistence of two classes of generalized bent functions*, Designs, Codes and Cryptography, **85**, no. 1, 471-482, (2017).
[9] Chang Lv and Jianing Li. *On the Non-Existence of Certain Classes of Generalized Bent Functions*, IEEE Transactions on Information Theory, **63**, no. 1, pp. 738-746, (2017).

CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, PR China

E-mail address: `lijn@ustc.edu.cn`