Curriculum Vitae
Yi OUYANG

University of Science and Technology of China
School of Mathematical Sciences
Hefei, Anhui 230026
People's Republic of China

Office: (86) 551-63600337
Email: yiouyang@ustc.edu.cn
http://staff.ustc.edu.cn/∼yiouyang
ORCID: https://orcid.org/0000-0002-0993-3689

当前研究兴趣/Current Research Interests

Number Theory and Arithmetic Geometry

- Fontaine theory of p-adic representations and (φ, Γ)-modules, and its connection to Iwasawa theory.
- Theory of elliptic curves and its application in cryptography.
- Class groups and class numbers of number fields and function fields.

教育情况/Education

Ph.D. in Mathematics, June 2000, University of Minnesota.
Thesis advisor: Prof. Greg William Anderson.
Thesis title: "The group cohomology of universal ordinary distribution
and its application"

M.S. in Mathematics, July 1995, Univ. of Sci. and Tech. of China(USTC), P. R. China.

B.S. in Mathematics, July 1993, USTC, P. R. China.

工作情况/Employment

- Professor, University of Science and Technology of China, 2007-
- Associate professor, Tsinghua University, December 2003-December 2006;
- Lecturer, Tsinghua University, July 2003-December 2003;
- Postdoctoral Fellow, University of Toronto, Advisor: Prof. V. Kumar Murty, July 2000- June 2003.

访问情况/Visiting Positions

- Visiting professor, Erasmus Mundus-ALGANT program, Padova-Leiden-Bordeaux, April–June, 2006, Padova-Paris XI, May-July 2007.
- Visitor, IHES, Bures-sur-Yvette, France, January –June, 2001, January-March 2006, July 2006, November-December 2008.
- Visiting professor, KAIST, Korea, January 2009.
- Visiting scholar, ICTP, Trieste, Italy, April-May 2006, August-September 2009.
- Visiting professor, Mainz, Germany, April-May 2010, January-March 2011.
- Visiting scholar, Purdue University, USA, July 2013-July 2014.
- Visiting professor, Morningside center in Matematics, CAS, Beijing, Summer, 2007-

荣誉/Honors

- 2012 年安徽省教学成果一等奖（排名第二）
- 2012 年中国科学技术大学教学成果特等奖，排名第二
- 2017 年中国科学院教学成果二等奖（排名第三）
- 2017 年宝钢优秀教师奖
- 2018 年安徽省教学名师
- 2020 年教育部基础学科拔尖学生培养计划优秀导师奖
- 2021 年教育部基础学科拔尖学生培养计划优秀管理人员奖
- 第十八届霍英东教育基金会高等院校教育教学奖二等奖

论文/Publications (in general alphabet order)

1. - and Fei Xu, *Riemann-Hurwitz formula in Basic* $\mathbf{Z}_S$*-extensions,* Acta Arith. **LXXXI**.1 (1997), 1–10.
2. *The group cohomology of universal ordinary distribution and its applications*, Thesis, University of Minnesota, 2000.
3. *The group cohomology of universal ordinary distribution*, J. Reine Angew. Math. **537**(2001), 1–32.
4. *The universal norm distribution and Sinnott's index formula*, Proc. Amer. Math. Soc. **130**(2002), No. **8**, 2203-2213.
5. Greg W. Anderson and -, *A note on the cyclotomic Euler systems and the double complex method*, Canad. J. Math. 55, No.4(2003), 673–692.
6. *On the universal norm distribution*, J. Ramanujan Math. Soc. 17, No. 4(2002), 287–311.
7. *The universal Kolyvagin recursion implies the Kolyvagin recursion*, Acta. Math. Sin. (Engl. Ser.) 23, No.7 (2007), 1163–1172.
8. *The Gross conjecture over rational function fields*, Sci. China Ser. A Math. **48**, No. 12 (2005), 1609–1617.
9. Kumar Murty and -, *The growth of Selmer ranks of an abelian variety with complex multiplication*, Pure Appl. Math. Q. 2, No. 2(2006), 539–555.
10. - and Hang Xue, *Class numbers of Cyclic* 2*-extensions and Gross conjecture over* $\mathbf{Q}$, Sci. China Math. Vol. 53, No. 9 (2010), 2447–2462.
11. Yiwen Ding and -, *A simple proof of Dieudonné-Manin classification Theorem*, Acta. Math. Sin. (Engl. Ser.) Vol. 28, No. 8 (2012), 1553–1558.
12. -, F. Xu, C. Xing and P. Zhang, *Number Theory and Related Area*, editor, Advanced Lecture in Mathematics, Vol. 27, Higher Education Press and International Press, 2013.
13. *Lectures on p-adic zeta functions and* (φ,Γ)*-modules*, in *Number Theory and Related Area*, pp. 85-147, 2013.

14. - and Shenxing Zhang, *On non-congruent numbers with* 1 *modulo* 4 *prime factors*, Sci. China Math., Vol. 57, No. 3(2014), 649–658.

15. - and Jinbang Yang, *On the cohomology of semi-stable p-adic Galois representations*, C. R. Math. Acad. Sci. Paris Vol. 352(2014), 557–561.

16. - and Zhe Zhang, *Hilbert genus fields of biquadratic fields*, Sci. China Math., Vol. 57, No. 10(2014), 2111–2122.

17. - and Zhe Zhang, *Hilbert genus fields of real biquadratic fields*, Ramanujan J. 37(2015) 345-363.

18. - and Shenxing Zhang, *On second* 2*-descent and non-congruent numbers*, Acta Arith. 170 (2015), 343-360. Errata, Acta Arith. 202 (2022), 203-203.

19. - and Jinbang Yang, *Newton Polygons of L functions of polynomials* $x^d + ax$, J. Number Theory 160(2016), 478-491.

20. - and Shenxing Zhang, *Birch's lemma over global function fields*, Proc. Amer. Math. Soc. 145(2017), 577-584.

21. - and Shenxing Zhang, *Newton polygons of L-functions of polynomials* $x^d + ax^{d-1}$ *with* $p \equiv -1 \bmod d$, Finite Fields Appl. 37(2016), 285-294.

22. - and Jinbang Yang, *On a conjecture of Wan about limiting Newton polygons*, Finite Fields Appl. 41(2016), 64-71. https://doi.org/ 10.1016/j.ffa.2016.05.003

23. Bei Wang, - and Honggang Hu, *Efficient Pairing Computation on Twisted Weierstrass Curves*, Chinese J. Electronics **27**(2018), 739-745.

24. Songsong Li and -, *Counting the solutions of* $\lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t} \equiv c \bmod n$, J. Number Theory **187**(2018), 41-65. https://doi.org/10.1016/j.jnt.2017.10.017

25. Yang Liu and -, *On binary quadratic forms modulo* n, Commun. Math. Stat. 7 (2019), no. 1, 61-67.

26. - and Xianhong Xie, *Linear complexity of generalized cyclotomic sequences of period* $2p^m$, Des. Codes Cryptogr. 87 (2019), no. 11, 2585-2596. https://doi.org/10.1007 /s10623-019-00638-5

27. - and Zheng Xu, *Loops of isogeny graphs of supersingular elliptic curves at* $j = 0$, Finite Fields Appl. 58 (2019), 174-176.

28. Songsong Li, - and Zheng Xu, *Neighborhood of the supersingular elliptic curve isogeny graph at* $j = 0$ *and* 1728, Finite Fields Appl. 61(2020), January 2020, 101600. https://doi.org /10.1016/j.ffa.2019.101600

29. Songsong Li, - and Zheng Xu, *Endomorphism rings of supersingular elliptic curves over* $\mathbb{F}_p$, Finite Fields Appl. 62(2020), February 2020, 101619.

30. Jianing Li, -, Yue Xu and Shenxing Zhang, *ℓ-Class groups of fields in Kummer towers*, Publ. Mat. 66 (2022), 235−267.

31. Jianing Li, - and Yue Xu, 阿贝尔 p 分歧扭子群和新 *Cohen-Lenstra* 猜想 (Abelian p-ramification groups and new Cohen-Lenstra heuristics), Sci Sin. Math. **51**(2021), No. 10, 1635-1654.

32. Bei Wang, -，Songsong Li and Honggang Hu: *A New Twofold Cornacchia-Type Algorithm and Its Applications*, Advances in Mathematics of Communications 2021, doi:10.3934/amc.2021026.

33. Bei Wang, Xianhong Xie, Songsong Li, Honggang Hu and -: *General* 4*-GLV Lattice Reduction Algorithms*, accepted for 2021 International Conference on Computational Intelligence and Security (CIS'2021), November 19-22，2021，Chengdu，China.

34. Bei Wang, Songsong Li, - and Honggang Hu. *Ready-Made Short Basis for GLV+GLS on High Degree Twisted Curves.* AIMS Mathematics, 2022, 7(1): 306-314. doi: 10.3934/math.2022021.

35. Jianing Li, - and Yue Xu, *On abelian* 2*-ramification torsion modules of quadratic fields*, Sci. China Math., 2022. doi: 10.1007/s11425-021-1946-0

36. Xianhong Xie, -, Honggang Hu and Ming Mao, *Construction of three classes of Strictly Optimal Frequency-Hopping Sequence Sets*, Advances in Mathematics of Communications 2022. doi: 10.3934/amc.2022024

37. -, Sen Wang and Xianhong Xie, *Almost balanced and uncorrelated quaternary sequence pairs of even length.* JUSTC, 2022, 52(3): 4.

38. - and Jianfeng Xie, *The growth of Tate-Shafarevich groups in cyclic extensions*, Compositio Math. **158** (2022), 2014–2032.

预印本/Preprints (in general alphabet order)

1. Jean-Marc Fontaine and -, *Theory of p-adic Galois representations*, a book in preparation.

2. Xianhong Xie, - and Ming Mao, *Vectorial bent functions and Linear Codes from Quadratic Forms*, preprint, 2020.

3. Jianing Li, Songsong Li and -, *Factorization of Hilbert class polynomials over prime fields*, preprint, 2021.

4. Xianhong Xie and -, *On vectorial functions with maximal number of bent components*, preprint, 2022.

5. Sen Wang, - and Xianhong Xie, *New Classes of Optimal and Distance Optimal Two or Three-weight Codes*, preprint, 2022.

6. - and Jianfeng Xie, *Unboundedness of Tate-Shafarevich groups in fixed cyclic extensions*, preprint, 2022.

其他写作/Other Writings

1. The China Legacy of Jean-Marc Fontaine, la Gazette des Mathématiciens No. 162，Octobre 2019, 15-17.
2. 悼念雷诺教授, 2018. (In memory of Professor Michel Raynaud, 2018).
3. (冯克勤, 欧阳毅) 中法数论代数几何合作,《清华数学 90 年》，清华大学, 2017.
4. 仿佛来自虚空—亚历山大 • 格洛腾迪克的生平故事, 译自 Allyn Jackson 的著名文章 “Comme Appelé du Néant, As If Summoned from the Void: The Life of Alexandre Grothendieck, Part I, Notices AMS, Vol 51, No. 9; Part II, Notices AMS, Vol 51, No. 10”, 发表于《数学译林》.
5. 黎曼假设有关的数学巨匠和数学进展. 见《代数学 III：代数学进阶》数字课程网站 (http://abook.hep.com.cn/1251847).
6. 艾米 • 诺特小传. 同上.
7. 二次曲线和 p 进数. 同上.
8. Inverse limits and Galois theory. 同上.
9. Introduction to Iwasawa theory.
10. Galois and Kummer's influence in algebra and number theory, lecture notes.
11. (葛力明, 欧阳毅, 田野, 邢朝平, 徐飞) 冯克勤先生简介, SCIENTIA SINICA Mathematica, 2021. (https://doi.org/10.1007/SSM-2021-0171).

教学论文论著/Teaching Publications

1. 基于代数类课程教学改革的探索与实践,《大学数学》Vol. 34, No. 4, 2018 年 8 月。
2. (欧阳毅，申伊塃)《代数学 I: 代数学基础》，高等教育出版社, 2016 年 8 月.
3. (欧阳毅, 叶郁，陈洪佳)《代数学 II: 近世代数》，高等教育出版社, 2017 年 1 月.
4. 《代数学 III: 代数学进阶》，高等教育出版社, 2019 年 10 月.
5. Mathematical introduction to coding theory and cryptography, preprint, 2020.

学术报告/Presentations (since 2016)

- On a conjecture of Wan, New progress in Number theory in China and Korea 2016, Postech, Pohang, Korea, January 27, 2016.
- Birch's Lemma over global function fields, Xiamen Workshop in Arithmetic Geometry, Xiamen University, Xiamen, July 8 2016.
- Birch's Lemma over global function fields, The 3rd Sichuan-Chongqing Workshop on Number Theory, Changjiang Normal University, Chongqing, December 11, 2016.
- Counting the solutions of $\lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t} = c \mod n$, The 8th Conference on Finite Fields and Their Applications, Beijing, November 7, 2017.
- Masters and progress in mathematics associated to Riemann Hypothesis, 2018 Annual Meeting of Anhui Provencial Mathematical Society, Anhui Jianzhu University, Hefei, October 27, 2018.

- Linear complexity of generalized cyclotomic sequences of period $2p^m$, Workshop in Number Theory and its Applications, National Uuniversity of Defense Science and Technology, Changsha, November 30, 2018.
- 2-class groups in dyadic Kummer towers, Program on Galois Structures in Number Theory, Number Theory and Related Topics, Harbin Institute of Technology, Harbin, August 12, 2019.
- 数学专业线性代数教学的一点体会. 安徽省数学会 2019 年学术年会, 铜陵学院, 铜陵, 2019 年 11 月 16 日.
- Neighborhoods of $\mathbb{F}_p$-vertices in Supersingular isogeny graphs. AMSS, CAS, Beijing, December 19, 2019.
- Neighborhoods of $\mathbb{F}_p$-vertices in Supersingular isogeny graphs. The 6th South-West Number Theory Workshop, Chongqing, December 14, 2019.
- Neighborhoods of $\mathbb{F}_p$-vertices in Supersingular isogeny graphs. Capital Normal University, Beijing, December 20, 2019.
- ℓ-class groups in dyadic Kummer towers. Northwest University (China), Xi'an, January 2, 2020.
- Neighborhoods of $\mathbb{F}_p$-vertices in Supersingular isogeny graphs. Xidian University, Xi'an, January 3, 2020.
- New Cohen-Lenstra Heuristics for quadratic fields. Number Theory in Cloud, Xi'an Jiaotong University, Xi'an, May 9, 2020.
- The life of Galois and Kummer and their influences in algebra and number theory, Online Short Course, Southeast Mathematical Center, Xiamen University, August 9-August 14, 2020.
- Constructing sequences, vectorial bent functions and optimal linear codes. Finite fields and Their applications Workshop Online, Sichuan University, Chengdu, August 29, 2020.
- On abelian p-ramification torsion modules of quadratic fields. Workshop in Number Theory and Its Applications, National Defense University of Science and Technology, Changsha, October 24, 2020.
- On abelian p-ramification torsion modules of quadratic fields. Workshop in Number Theory and Its Applications. Hefei University of Technology, Hefei, November 7, 2020.
- 黎曼假设有关的数学巨匠和数学进展. 上海交通大学, 上海, 2020 年 11 月 15 日.
- On abelian p-ramification torsion modules of quadratic fields. Workshop in Number Theory and Automorphic Representations, Soochow University, Suzhou, November 21, 2020.
- On abelian p-ramification torsion modules of quadratic fields. Online Conference in Number Theory and its Applications. Sichuan University, Chengdu, November 23, 2020.

- The life of Galois and Kummer and their influences in algebra and number theory, Short Course, Shandong University, April 2021.
- On abelian p-ramification torsion modules of quadratic fields. Southeast University, Nanjing, May 5, 2021.
- Factorization of Hilbert class polynomials over prime fields. Minnan Normal University, October 8, 2021. (online)
- The growth of Tate-Shafarevich groups in $\mathbb{Z}/p\mathbb{Z}$-extensions. Xi’an Workshop in Number Theory and Its Applications, Northwest University, October 16, 2021.
- The growth of Tate-Shafarevich groups in $\mathbb{Z}/p\mathbb{Z}$-extensions. 山东大学珠峰讲坛, 山东大学, October 26, 2021. (online)
- The growth of Tate-Shafarevich groups in $\mathbb{Z}/p\mathbb{Z}$-extensions. Tongji University, November 19, 2021. (online)
- 从根与系数的关系谈起. 南方科技大学, 2021 年 12 月 10 日.

学术会议组织/Conferences Organized

1. (with Keqin Feng, Lei Fu, Jean-Marc Fontaine and Luc Illusie etc.) International conference and summer school on arithmetic geometry and automorphic forms, Tsinghua University and Chern Institute of Mathematics, Beijing and Tianjin, August 2005.
2. (with Fei Xu, Chaoping Xing and Pu Zhang) Number Theory and Related Area, a conference in honor of Professor Keqin Feng, USTC, Hefei and Huangshan, June 7-12 2011.
3. (with Mao Sheng and Kang Zuo) Algebraic and Arithmetic Geometry Conference, USTC, August 23-27, 2013.
4. (with David Harari, Peng Shan and Fei Xu) The 2nd Sino-French Conference in Arithmetic Geometry, Tsinghua Sanya International Math. Forum, Yau Mathematical Sciences Center, Sanya, November 7-11, 2016.
5. Summer School on Mathematical foundation of coding and cryptography, USTC, Hefei, July 17-30, 2016.
6. Summer School on Mathematical foundation of coding and cryptography, USTC, Hefei, July 2-17, 2017.
7. (with 田野等) 第八届全国数论会议, 江苏省常州市金坛区华罗庚中学, 2021 年 6 月 25 日-30 日.

教学情况/Teaching (since 2017)

- 线性代数 B1, 2017 年春
- 代数学, 2017 年秋
- 编码密码的数学基础, 2018 年春
- 算术代数几何选件, 2018 年秋

- 线性代数 A1, 2019 年春
- 线性代数 A2, 2019 年秋
- 编码密码学的数学理论, 2020 年春
- 数学分析 B1, 2020 年秋
- 近世代数, 2021 年春
- 线性代数 B2, 2021 年秋