BIOGRAPHICAL DATA
Dorian Goldfeld

Personal Data

U.S. Citizen,
Birthdate: January 21, 1947, Marburg, Germany
Married with two children.

Education

B.S. School of Engineering, Columbia University, New York 1967
Ph.D. Columbia University, New York 1969. Thesis advisor: P. X. Gallagher.

Professional Experience

1985 –	Professor	Columbia University
1983 – 85	Associate Professor	University of Texas, Austin
1982 – 83	Visiting Professor	Harvard University
1979 – 82	Associate Professor	M.I.T.
1976 – 79	Assistant Professor	M.I.T.
1974 – 76	Visiting Professor	Scuola Normale Superiore, Pisa, Italy
1973 – 74	Member	Institute for Advanced Study, Princeton
1972 – 73	Lecturer	Tel-Aviv University, Israel
1971 – 72	Post-Doc	Hebrew University, Jerusalem, Israel
1969 – 71	Miller Fellow	University of California, Berkeley

Awards and Honorary Societies

Sloan Fellow, 1977 – 79
Vaughn Prize, 1985
Cole Prize in Number Theory, 1987
Elected to the American Academy of Arts and Sciences, April 2009
Became an inaugural Fellow of the American Mathematical Society 2012

Recent Grants

Simons Collaboration Grant 317607: Trace Formulae, L-functions and Analytic Number Theory, 2014 - 2016.

NSA Grant H98230-15-1-0035: Trace Formulae, L-functions and Analytic Number Theory, 2015 - 2016.

NSA Grant H98230-16-1-0009: Trace Formulae, L-functions and Analytic Number Theory, 2016 - 2018.

Prior National Science Foundation grants

1403383: Analytic Number Theory and its Applications, 2014 - 2015.

1001036 Collaborative Research: Automorphic forms, representations and L-functions, 2010 - 2014.

0739400 RTG: Joint Columbia-CUNY-NYU Research Training Group in Number Theory, 2008 – 2015.

0652554 FRG: Collaborative Research: Combinatorial representation theory, multiple Dirichlet series and moments of L-functions, 2007 – 2010.

0354582 Collaborative Research: FRG: Applications of Multiple Dirichlet Series to Analytic Number Theory, 2004–2007.

0312270 Joint COLUMBIA-CUNY-NYU Number Theory Seminar, 2003–2007.

0098633 Analytic Number Theory on Groups, 2001–2004.

9800048 Analytic Number Theory on Groups, 1998–2001.

9505584 Mathematical Sciences: Analytic Number Theory on Groups, 1995–1998.

9200716 Mathematical Sciences: Analytic Number Theory on Groups, 1992–1995.

9003907 Mathematical Sciences: Analytic Number Theory on Elliptic Curves, 1990–1992.

8702169 Mathematical Sciences: Analytic Number Theory on Groups, 1987–1990.

8502787, 8641838, 8696093 Mathematical Sciences: Analytic Number Theory on GL(n), 1985–1987.

8303621 Mathematical Sciences: Automorphic Functions and Number Theory, 1983–1985.

8203624 Automorphic Functions and Elliptic Curves (Mathematical Sciences), 1982–1983.

Professional and Public Service

Organizer for the conferences:

Number Theory Related to Fermat's Last Theorem, M.I.T. (1982)

Number Theory, Trace Formulas and Discrete Groups, Oslo (1987)

Proceedings of the Special Year in Number Theory at Columbia University (1992)

Algebraic Dynamics, CUNY Graduate Center (2004)

Workshop on p-adic methods in automorphic forms, Columbia University (2005)

Bretton Woods Workshop on Multiple Dirichlet Series, Bretton Woods, NH (2005)

Ergodic theory and Diophantine problems, Courant Institute, NY (2006).

Analytic number theory and higher rank groups, Courant Institute, NY (2008)

Multiple Dirichlet Series and Applications to Automorphic Forms, ICMS, University of Edinburgh (2008).

Number Theory and Representation Theory, A conference in honor of the 60th birthday of Benedict Gross, Harvard University (2010).

Arithmetic Geometry and Arithmetic Dynamics Conference on the occasion of the 70th birthday of Lucien Szpiro, CUNY Graduate Center, NY (2012).

Automorphic Forms, Representations, and Combinatorics: A Conference in Honor of Daniel Bump, Stanford University (2012).

ICERM Semester Program on "Automorphic Forms, Combinatorial Representation Theory and Multiple Dirichlet Series," ICERM (Spring 2013).

Representation Theory, Automorphic Forms, and Complex Geometry, A conference in honor of the 70th birthday of Wilfried Schmid, Harvard University (2013).

Analytic Number Theory and its Applications, A conference in honor of Jeffrey Hoffstein, Perrotis College, Thessaloniki, Greece (2014).

Organizer:

Columbia University Number Theory Seminar, 1985 – 2003.
Joint Columbia-CUNY-NYU Number Theory Seminar, 2003 – present.

Editor: Acta Arithmetica, Ramanujan Journal

Students Mentored

Jeffrey Hoffstein, Class numbers of totally complex quadratic extensions of totally real fields, Ph.D. Dissertation, M.I.T. (1978).

M. Ram Murty, Artin's conjecture and non-abelian sieves, Ph.D. Dissertation, M.I.T. (1980).

Ilan Vardi, *On the spectrum of the metaplectic group*, Ph.D. Dissertation, M.I.T. 1982.

Eric G. Stade, *Whittaker functions and Poincaré series for* $\mathrm{GL}(3,\mathbb{R})$, Ph.D. Dissertation, Columbia University 1988.

Paul T. Lockhart, *Diophantine equations and the arithmetic of hyperelliptic curves* Ph.D. Dissertation, Columbia University 1990.

Gabriel Gerber, *Hecke operators for non-congruence subgroups of the modular group* Ph.D. Dissertation, Columbia University 1992.

Bin–Long Zhang, *Kloosterman zeta functions for* $GL(3,\mathbb{Z})$ Ph.D. Dissertation, Columbia University 1994.

Nikos Diamantis, *Special values of higher derivatives of L–functions* Ph.D. Dissertation, Columbia University 1997.

Cormac O'Sullivan, *Properties of Eisenstein series formed with modular symbols,* Ph.D. Dissertation, Columbia University 1998.

Arjune Budhram, *Trace of Hecke operators and the Petersson norm of weight two Hilbert modular forms,* Ph.D. Dissertation, Columbia University 1999.

Gautam Chinta, *On the analytic rank of elliptic curves over cyclotomic fields,* Ph.D. Dissertation, Columbia University 2000.

Ambrus Pal, *Drinfeld modular curves, Heegner points, and interpolation of special values,* Ph.D. Dissertation, Columbia University 2000.

Joe Hundley, *Siegel zeroes of Eisenstein series,* Columbia University 2002.

Qiao Zhang, *Integral mean values of L–functions,* Ph.D. Dissertation, Columbia University 2003.

Meera Thillainatesan, *A kernel for automorphic L-functions on* $GL(n,R)$*,* Ph.D. Dissertation, Columbia University 2004.

Alex Kontorovich, *The hyperbolic lattice point count in infinite volume with applications to sieves,* Ph.D. Dissertation, Columbia University 2007.

Borislav Mezhericher *Computational aspects of Maass forms for* $SL(3,\mathbb{Z})$, Ph.D. Dissertation, Columbia University 2008.

Min Lee, *Approximate converse theorem,* Ph.D. Dissertation, Columbia University 2011.

Qing Lu, *Bounds for spectral mean value of L-functions on the critical line,* Ph.D. Dissertation, Columbia University 2011.

Fan Zhou, *Sato-Tate Problem for GL(3),* Ph.D. Dissertation, Columbia University 2013.

Ian Whitehead, *Multiple Dirichlet Series for Affine Weyl Groups,* Ph.D. Dissertation, Columbia University 2014.

Anna Puskas, *Demazure-Lusztig Operators and Metaplectic Whittaker Functions on Covers of the General Linear Group,* Ph.D. Dissertation, Columbia University 2014.

Nava Balsam, *The Parity of Analytic Ranks among Quadratic Twists of Elliptic Curves over Number Fields,* Ph.D. Dissertation, Columbia University 2014.

Timothy Heath, *On a spectral bound for congruence subgroup families in* $SL_3(\mathbb{Z})$, Ph.D. Dissertation, Columbia University 2015.

Principal Conference Lectures

Journées Arithmétique de Caen (1976), *The conjecture of Birch and Swinnerton-Dyer and the class numbers of quadratic fields.*

Journées Arithmétique Marseilles (1978), *Analytic and arithmetic theory of Poincaré series.*

Number Theory Conference, Carbondale (1979), *Conjectures on elliptic curves over quadratic fields.*

Modern Trends in Number Theory Related to Fermat's Last Theorem, M.I.T. (1982) *On automorphic forms of half-integral weight with applications to elliptic curves.*

Séminaire de Théorie des Nombres de Bordeaux (1983) *Poincaré series for* $SL(3,\mathbb{Z})$.

Durham Symposium on Modular Forms, Durham, England (1984) *A Kronecker limit formula for cubic fields.*

The Selberg Trace Formula and Related Topics, Proc. AMS-IMS-SIAM Conf., Bowdoin College, Maine (1984) *Poincaré series and Kloosterman sums.*

Academia Sinica, Beijing, China (1985) *The class number problem of Gauss.*

Tokyo University, Tokyo, Japan (1985) *Theory of Kloosterman zeta functions.*

One Hour Address, Annual Meeting of the American Mathematical Society (1985) *Gauss' class number problem for imaginary quadratic fields.*

Forty Five Minute Address, International Congress of Mathematicians (1986) *Kloosterman zeta functions for* $GL(n,\mathbb{Z})$.

Number Theory, Trace Formulas and Discrete Groups, Oslo, Norway (1987) *Explicit formulae as trace formulae.*

First Canadian Number Theory Conference, Banff, Canada (1988) *Modular elliptic curves and diophantine problems.*

Number Theory and Geometry, Japan American Institute, Johns Hopkins University, Baltimore, Md. (1988) *Quasicharacters of congruence groups.*

Conference in Analytic Number Theory, Montreal, Canada (1989) *Parametrization of modular elliptic curves by Poincaré Series.*

Institut Henri Poincaré, Paris (1990), *Lecture Series on Modular Elliptic Curves.*

Algebraic Geometry, Oberwohlfach (1991) *Special Values of Derivatives of L-functions associated to Elliptic Curves.*

Special Year in Diophantine Problems, MSRI (1992) *Bounds for the Tate-Shafarevich Group.*

Fourth Canadian Number Theory Conference, Halifax, Nova Scotia (1993) *Special values of derivatives of L–functions.*

Special Year in Automorphic Forms, MSRI (1994) *Siegel zeros for higher rank groups.*

Amer. Inst. of Math., Symposium on the Riemann Hypothesis, Seattle, Washington (1996) *A Spectral Interpretation of Weil's Explicit Formula.*

International Conference in Honor of the 60th Birthday of Andrej Schinzel, Zakopane, Poland (1997) *The distribution of modular symbols.*

Number Theory and Diophantine Geometry at the Gateway to the Millenium, ETH, Zurich (1999) *Modular forms, elliptic curves, and the abc–conjecture.*

Chinese Academy of Sciences, Beijing, China (1999) *Four lectures on the abc–conjecture.*

Kyoto, Japan (2000), Conference on Automorphic forms, automorphic representations and automorphic L-functions over algebraic groups, *Grossencharakter L-functions of real quadratic fields twisted by modular symbols.*

Analytic Theory of Automorphic Forms and L–Functions, I.A.S. Princeton (2000), *Modular forms, elliptic curves, and the abc–conjecture.*

Math. Sciences Research Institute, Berkeley, CA (2001), *The Gauss class number problem.*

Inst. for Pure and Applied Math. UCLA, CA (2001) *A Linear Time Matrix Key Agreement Protocol.*

Kuwait Foundation Lecture at Cambridge University, U.K. (2002) *Multiple Dirichlet Series and Moments of Zeta and L-Functions.*

First KIAS-POSTECH International Workshop on Number Theory-Modular Forms, Seoul, Korea (2002), *Counting congruence subgroups.*

Newton Institute, Cambridge, U.K. (2004) workshop on Matrix Ensembles and L-Functions, *Multiple Dirichlet series, an historical survey.*

AMS/DMV Joint International Meeting, Mainz, Germany (2005), *Key agreement, the Algebraic Eraser^{TM}, and lightweight cryptography.*

Gauss–Dirichlet Conference, Göttingen, Germany (2005), *Moments of $GL(2)$ L-functions.*

CRM, Université de Montreal, Canada (2006), Workshop on L-Functions and Related Themes, *A simple proof of multiplicity one for GL(3, R).*

KIAS-POSTECH-SNU International Number Theory Workshop, Seoul, Korea (2006), *Multiple Dirichlet series associated to cusp forms on GL(n).*

Distinguished Lecture Series at Brown University (2007), *Multiple Dirichlet series.*

Euler International Mathematical Institute, St. Petersburg, Russia (2007), International Conference on Arithmetic Geometry in celebration of Euler's 300^{th} birthday, *From Euler products to multiple Dirichlet series.*

International Conference on the Occasion of the 60th Birthday of Samuel J. Patterson, Mathematisches Institut, Göttingen (2009), *Moments of L-functions.*

International Conference on Number Theory and Representation Theory Shandong University, Weihai, China (2009), *Fourier expansions of newforms on $GL(2, \mathbb{Q})$ at various cusps.*

BC-MIT Number Theory Seminar (2009) *Symmetry types of higher rank Rankin-Selberg L-functions*

University of Florida, Mathematics Department, Third Ramanujan Colloquium (2009), *Multiple Dirichlet Series*

First Joint Meeting, American Mathematical Society and Sociedad de Mathemática de Chile, Pucón, Chile (2010), *Fourier expansions of $GL(2)$ newforms at various cusps.*

Temple University Mathematics Colloquium, (Sept. 2011), *The Kuznetsov trace formula for GL(3)*

Escuela Latinoamericana de Geometra Algebraica y Aplicaciones, La Cumbre, Cordóba, Argentina (2011) *The Kuznetsov trace formula for $GL(n)$*

Paul Turan Memorial Conference, Budapest, Hungary (2011), *A converse theorem for Dirichlet series in two complex variables*

Conference on Modular Forms and Related Topics, Temple University (Nov. 2012), *An orthogonality relation for Fourier coefficients of Maass forms on $GL(n)$*

Special year in Number Theory, Chennai, India (2012), *Low lying zeros of $GL(3,\mathbb{R})$ L-functions*

International Colloquium on Automorphic Representations and L-Functions, Tata Institute of Fundamental Research, Mumbai, India (2012) *On the symmetry type of the family of adjoint L-functions on $GL(3)$*

Automorphic Forms and L-Functions, Darmstadt, Germany, (2013) *An orthogonality relation for Fourier coefficients of Maass forms on $GL(n)$*

University of Florida, Ramanujan 125 (2013), *Ramanujan Sums*

SCHOLAR - A Scientific Celebration Highlighting Open Lines of Arithmetic Research in honour of Professor M. Ram Murty's mathematical legacy on his 60th birthday (2013), *A converse theorem for double Dirichlet series*

NCTS Special Week in Arithmetic and Number Theory, Hsinchu, Taiwan, (July 2013), *Multiple Dirichlet Series*

ICCM (2013), Taipei, *The work of Yitang Zhang*

ICCM 2013, Taipei, Morningside lecture, *The relative trace formula for unipotent subgroups*

Pohang Mathematics Institute, (July 2013), *Large Prime Numbers : How close can they get?*

Princeton University Mathematics Colloquium (November 2013), *Multiple Dirichlet Series*

Tata Institute of Fundamental Research, Mumbai (January, 2014), *Four lectures on the Relative Trace Formula*

Second ERC Research Period on Diophantine Geometry, 2014, Cetraro, Italy, *The vertical Sato-Tate conjecture*

Number Theory in honor of Krishna Alladi's 60th birthday (March, 2016), University of Florida, Gainesville, *On an additive prime counting function of Alladi and Erdős*

Publications

Densities in arithmetic progressions, Proc. Amer. Math. Soc., **19** (1968), 1389–1392.

Artin's conjecture on the average, Mathematika, **15** (1968), 223–226.

(with D. Aulicino) *A new relation between primitive roots and permutations*, Amer. Math. Monthly, **76** (1969), 664–666.

On the number of primes p for which $p + a$ has a large prime factor, Mathematika, **16** (1969), 23–27.

A large sieve for a class of non–abelian L–functions, Israel Journal of Math., **14** (1973), 39–49.

A simple proof of Siegel's theorem, Proc. Nat. Acad. Sci. U.S.A., May (1974), 1055.

On Dirichlet series with identical beginnings, J. Number Theory, **7** (1975), 177–183.

A further improvement of the Brun–Titchmarsh theorem, J. London Math. Soc., **11** (1975), 434–444.

An asymptotic formula relating the Siegel zero and the class number of quadratic fields, Annali Scuola Nor. Sup. Pisa, Serie IV, Vol II (1975), 611–615.

(with A. Schinzel) *On Siegel's zero*, Annali Scuola Nor. Sup. Pisa, Serie IV, Vol II (1975), 571–583.

(with S. Chowla) *A remark on certain Hecke L–series which are non–negative on the real axis*, Acta Arith., XXX (1976), 1–3.

The class number of quadratic fields and the conjectures of Birch and Swinnerton–Dyer, Annali Scuola Nor. Sup. Pisa, Serie IV, Vol. III (1976), 623–663.

The conjectures of Birch and Swinnerton–Dyer and the class numbers of quadratic fields, Soc. Math. de France, Astérisque, **41–42** (1977), 219–227.

(with S. Chowla) *On the twisting of Epstein zeta functions into Hecke–Artin L–series of Kummer fields*, Number Theory Day, Lecture Notes in Math. **626**, Springer–Verlag (1977), 25–42.

An analogue of the class number problem, Appendix to the paper: Rational isogenies of prime degree by B. Mazur, Invent. Math., **44** (1978), 158–161.

Analytic and arithmetic theory of Poincaré series, Soc. Math. de France, Astérisque, **61** (1979), 95–107.

Conjectures on elliptic curves over quadratic fields, Number Theory, Carbondale 1979, Lecture Notes in Math. **751**, Springer–Verlag (1979), 108–119.

Mean values of L–functions associated to elliptic, Fermat and other curves at the centre of the critical strip, J. Number Theory, **3** II (1979), 305–320.

On convolutions of non–holomorphic Eisenstein series, Advances in Math., (3) **39** (1981), 240–256.

(with J. Hoffstein and S.J. Patterson) *On automorphic forms of half–integral weight with applications to elliptic curves*, Proceedings of Conference on Modern Trends in Number Theory Related to Fermat's Last Theorem, Progress in Math. **26**, Birkhäuser, Boston (1982), 153–194.

Sur les produits partiel euleriens attachés aux courbes elliptiques, Comptes. Rendus Acad. Sci. Paris, Ser. I Math., **294** (1982), 471–474.

(with C. Viola) *Some conjectures on elliptic curves over cyclotomic fields*, Trans. Amer. Math. Soc., (2) **276** (1983), 511–515.

(with P. Sarnak) *Sums of Kloosterman sums*, Invent. Math., Fasc. (2) **71** (1983), 243–250.

Poincaré series for $SL(3,\mathbb{Z})$, Séminaire de Théorie des Nombres de Bordeaux (1983–1984, exposé no. 17.

(with D. Bump) *A Kronecker limit formula for cubic fields*, Proc. Durham Symposium on Modular Forms (1984), 43–49.

(with J. Hoffstein) *Eisenstein series of 1/2–integral weight and the mean value of real Dirichlet L–series*, Invent. Math. **80** (1985), 185–208.

Gauss' class number problem for imaginary quadratic fields, Bulletin of the A.M.S., Vol. 13, Number 1 (1985), 23–37.

(with D. Bump and S. Friedberg) *Poincaré series and Kloosterman sums*, Contemporary Math. Vol 53, (1986), 39–49.

Kloosterman zeta functions for $GL(n,\mathbb{Z})$, Proc. Inter. Congress of Math., Berkeley, Calif. U.S.A. (1986), 417–424.

Analytic number theory on $GL(r,\mathbb{R})$, Analytic Number Theory and Diophantine Problems, Birkhauser, Boston (1987), 165–180.

(with D. Bump and S. Friedberg) *Poincaré series and Kloosterman sums for $SL(3,\mathbb{Z})$*, Acta Arith. **L** (1988), 32–89.

(with M. Anshel) *Applications of the Hardy–Ramanujan partition theory to linear diophantine problems*, J. Ramanujan Math. Soc., **3** (1), (1988), 97–110.

Explicit formulae as trace formulae, Number Theory, Trace Formulae and Discrete Groups (Editors, E. Bombieri, K.E. Aubert, D. Goldfeld), Oslo 1987, Academic Press, Boston, (1989), 281–288.

Modular elliptic curves and diophantine problems, Proc. of the First Canadian Number Theory Assoc., Banff, Canada 1988, de Gruyter, New York (1989), 156–175.

On quasicharacters of congruence groups, Algebraic Analysis, Geometry, and Number Theory, Proc. JAMI Inaugural Conf., Johns Hopkins Univ. Press (1989) (Edited by J–I Igusa), 99–113.

Parametrization of modular elliptic curves by Poincaré series Automorphic Forms and Analytic Number Theory, Publ. CRM, Univ. de Montreal, Montreal, Canada (1990) (Edited by Ram Murty), 48–63.

(with M. Anshel) *Partitions, Egyptian fractions and free products of finite abelian groups,* Proc. AMS., Vol. 111, Number 4, (1991), 889–899.

(with J. Hoffstein) *On the number of Fourier coefficients that determine a modular form,* Contemporary Mathematics 143, A Tribute to Emil Grosswald: Number Theory and Related Analysis (1991) (Edited by M. Knopp, M. Sheingorn), 385–393.

On the computational complexity of modular symbols, Math. of Comp. Volume 58, Number 198 (1992), 807–814.

(with S. Friedberg) *Mellin transforms of Whittaker functions,* Bull. Soc. Math. Fr., 121 (1993), 91–107.

(with J. Hoffstein and D. Lieman) , In the appendix to the paper, Coefficients of Maass forms and the Siegel zero, Annals of Math. (1994)

A Spectral Interpretation of Weil's Explicit Formula, Explicit Formulas, Lecture Notes in Math. 1593, Springer Verlag (1994), 135–152 .

(with L. Szpiro) *Bounds for the order of the Tate–Shafarevich group*, Compositio Math. **97** (1995), 71–87.

Special values of the derivatives of L–functions Canadian Math. Soc., Conference Proceedings, Volume **15** (1995), 159–173.

(with D. Lieman) *Effective bounds on the size of the Tate–Shafarevich group* , Math. Research Letters, Vol. **3**, (1996), 309–318.

(with M. Anshel) *Zeta functions, one–way functions, and pseudorandom number generators*, Duke Math. J., Vol. 88, No. 2, (1997), 371–390.

(with I. Anshel and M. Anshel) *An algebraic method for public key cryptography,* Math. Research letters **6** (1999), 287–291.

The distribution of modular symbols, Number Theory in Progress, Proc. of the Intern. Conference in Honor of the 60th Birthday of Andrej Schinzel, Zakopane, Poland (1997), Volume **2**, Elementary and Analytic Number Theory, Walter de Gruyter, Berlin, NY, (1999), 849–865.

(with S. Zhang) *The holomorphic kernel of the Rankin–Selberg convolution,* Asian J. of Math., Special Issue for the 70th Birthday of Sir Michael Atiyah, Vol. **3** Number 4 (1999), 729–748.

Zeta functions formed with modular symbols, Proc. of Symposia in Pure Math., **66** (1999), 111–121.

(with P. Gunnells) *Eisenstein series twisted by modular symbols for the group SL(n), Math. Res. Lett. 7 (2000), 747–756.*

(with G. Chinta) *Grössencharakter L-functions of real quadratic fields twisted by modular symbols,* Automorphic forms, automorphic representations and automorphic L-functions over algebraic groups (Japanese) (Kyoto, 2000). Surikaisekikenky usho K oky uroku No. 1173 (2000), 200–216.

(with I. Anshel, M. Anshel, B. Fisher) *New key agreement protocols in braid group cryptography,* Topics in cryptology—CT-RSA 2001 (San Francisco, CA), 13–27, Lecture Notes in Comput. Sci., 2020, Springer, Berlin, 2001.

(with G. Chinta) *Grössencharakter L–functions twisted by modular symbols,* Invent. Math., 144 (2001), 435–449.

Modular forms, elliptic curves and the ABC–conjecture, A panorama of number theory, Cambridge University Press, (2002), 128–147.

(with C. O'Sullivan) *Estimating additive character sums for Fuchsian groups,* The Ramanujan Journal, Vol. 7 (2003), 241–267.

(with I. Anshel, M. Anshel) *Non–abelian key agreement protocols,* Discrete Applied Math. I30 (2003), 3–12.

(with A. Diaconu and J. Hoffstein) *Multiple Dirichlet series and moments of zeta and L–functions,* Compositio Math., Vol 139 (2003), 297–360.

The elementary proof of the prime number theorem: an historical perspective, Number Theory, New York Seminar 2003, edited by D. Chudnovsky, G. Chudnovsky, M.B. Nathanson, Springer Verlag (2003), 179–192.

The Gauss Class Number problem for Imaginary Quadratic Fields, Heegner points and Rankin L-series, edited by H. Darmon, S-W Zhang, Cambridge Univ. Press. (2004).

(with A. Lubotzky, N. Nikolov, and L. Pyber) *Counting primes, groups, and manifolds,* Proc. Nat. Acad. Scis. U.S.A., Vol 101, no. 37 (2004), 13428–13430.

D. Goldfeld, A. Lubotzky, L. Pyber, *Counting congruence subgroups,* Acta Math., **193** (1), (2004), 73-104

(with I. Anshel, M. Anshel, and B. Fisher) *A group theoretic approach to public-key cryptography,* Unusual applications of number theory, 17–23, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 64, Amer. Math. Soc., Providence, RI, (2004).

(with A. Diaconu) *Second moments of GL_2 automorphic L–functions,* Analytic Number Theory, Proc. of the Gauss-Dirichlet Conference, Göttingen 2005, Clay Math. Proc., AMS,. 77–105.

(with X. Li) *Voronoi formulas on $GL(n)$*, International Mathematics Research Notices, vol. 2006, Article ID 86295, 25 pages, (2006).

(with I. Anshel and M. Anshel) *A linear time matrix key agreement protocol over small finite fields,* Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 3-4, 195–203.

(with M. Thillainatesan) *Rank lowering linear maps and multiple Dirichlet series associated to $GL(n, R)$*, Pure and Applied Math Quarterly, Vol. 2, No. 2 (Special Issue: In honor of John H. Coates, Part 2 of 2) (2006), 601-615.

(with I. Anshel, M. Anshel, S. Lemieux) *Key agreement, the Algebraic Eraser^{TM}, and Lightweight Cryptography,* In Contemporary Mathematics Vol. 418, Algebraic Methods in Cryptography, Amer. Math. Soc., Providence R.I. (2006).

Historical reminiscences on the Gauss class number problem, Colloquium De Giorgi 2006, 29–35, Colloquia, 1, Ed. Norm., Pisa, (2006).

(with A. Diaconu) *Second moments of GL_2 L–functions over an imaginary quadratic number field*, In: Multiple Dirichlet Series, Automorphic Forms, and Analytic Number Theory, Proc. of the Bretton Woods Workshop on multiple Dirichlet series 2005, Proc. Symp. Pure Math., **75**, AMS, Providence R.I. (2006).

Rank lowering operators on $GL(n, \mathbb{R})$, International Journal of Number Theory, Vol. 3; Number 3 (2007), 365–376.

(with I. Anshel, M. Anshel) *Actions, commutator identities, and the Algebraic Eraser,* Aspects of infinite groups, 18, Algebra Discrete Math., 1, World Sci. Publ., Hackensack, NJ, (2008).

(with X. Li) *The Voronoi formula for $GL(n, \mathbb{R})$*, International Mathematics Research Notices, vol. 2008, article ID rnm144, 39 pages (2008).

(with N. Diamantis) *A converse theorem for double Dirichlet series,* American Journal of Mathematics, 133(4), 913–938 (2011).

(with A. Diaconu and P. Garrett) *Moments of L-functions for $GL_r \times GL_{r-1}$,* In: Contributions in Analytic and Algebraic Number Theory, Festschrift for S.J. Patterson, (V. Blomer and P. Mihailescu editors), Springer Proceedings in Mathematics, 197–228, (2011).

(with A. Kontorovich and E. Stade) *On the Kontorovich-Lebedev transform,* , Commentarii mathematici Universitatis Sancti Pauli, Vol 60 (2011).

(with A. Diaconu and P. Garrett) *Natural Boundaries and Integral Moments of L-functions,* In: Multiple Dirichlet Series, L-functions and Automorphic Forms, Progress in Mathematics, Volume 300,, Bump, Daniel; Friedberg, Solomon; Goldfeld, Dorian (Eds.), 147–172, Birkhäuser, Basel, (2012).

(with A. Kontorovich) *On the determination of the Plancherel measure for Lebedev-Whittaker transforms on $GL(n)$*, to appear in Acta Arithmetica,); Acta Arithmetica 155 (2012), 15-26.

Goldfeld, D.; Kontorovich A.; *On the Lebedev-Whittaker transform for GL(3),* Acta Arith 155, (2012) 15-26. (Schinzel volume) arXiv:1102.5086

(with P. Gunnells) *Defeating the KalkaTeicherTsaban linear algebra attack on the Algebraic Eraser,* http://arxiv.org/abs/1202.0598 (2012).

Goldfeld, D.; Kontorovich A.; *On the $GL(3)$ Kuznetsov Formula with applications to Symmetry Types of families of L-functions,* In Automorphic Representations and L-Functions, (ed. D. Prasad et al) Tata Institute, (2013), 263–310. arXiv:1203.6667

Goldfeld, D.; Hundley, J.; Lee, M.; *Fourier expansions of GL(2) newforms at various cusps*, Ramanujan Journal, online publication, Feb. (2013).

(with N. Diamantis) *A converse theorem for double Dirichlet series and Shintani zeta functions,* J. Math. Soc. Japan, 66(2) (2014), 449–477.

(with J. Sengupta) *First moments of Fourier coefficients of GL(n) cusp forms*, Journal of Number Theory, Journal of Number Theory (2016) pp. 435–443.

(with I. Anshel, D. Atkins, P. Gunnells) *Defeating the Ben-Zvi, Blackburn, and Tsaban Attack on the Algebraic Eraser,* http://arxiv.org/abs/1601.04780 (2016).

(with I. Anshel, D. Atkins, P. Gunnells) *A Class of Hash Functions Based on the Algebraic EraserTM,* preprint, Groups Complexity Cryptology, ISSN 1869-6104, April, (2016).

(with D. Atkins) *Addressing the Algebraic Eraser Diffie–Hellman Over-the-Air Protocol,* http://eprint.iacr.org/2016/205 (2016).

To Appear

(with I. Anshel) *The Artin-Feistel symmetric cipher*

(with Xiaoqing Li) *A standard zero free region for Rankin-Selberg L-functions*

An additive prime divisor function of Alladi and Erdős

Books

Higher Mathematics from an Elementary Point of View (Rademacher) Birkhäuser, Boston, 1982 (Edited by D. Goldfeld).

(with K.E. Aubert and E. Bombieri) Number Theory, Trace Formulas and Discrete Groups, Academic Press, Boston (1989).

(with I. Anshel) Calculus, A Computer Algebra Approach, International Press Inc., Boston (1995).

(with L. Gerritzen, M. Kreutzer, G. Rosenberger, V. Shpilrain) Algebraic Methods in Cryptography, Contemporary Mathematics, Vol. 418, Amer. Math. Soc. (2006).

(with S. Friedberg, D. Bump, J. Hoffstein) Multiple Dirichlet Series, Automorphic Forms, and Analytic Number Theory, Proc. of the Bretton Woods Workshop on multiple Dirichlet series 2005, Proc. Symp. Pure Math., Vol 75, Amer. Math. Soc. (2006).

Automorphic forms and L-functions for the group $GL(n, \mathbb{R})$, Cambridge Studies in Advanced Mathematics, Vol. 99 (2006), Cambridge University Press.
Paperback edition published November 2015.

(with Joe Hundley) Automorphic representations and L-functions for the general linear group, volumes 1, 2. Cambridge Studies in Advanced Mathematics, Volumes 129, 130 (2011), Cambridge University Press.

Collected works of Hervé Jacquet, American mathematical Society, Providence Rhode Island, (2011).

(with J. Jorgenson, D. Ramakrishnan, K. Ribet, J. Tate) Number Theory, Analysis and Geometry: In Memory of Serge Lang, Springer (2012).

Multiple Dirichlet Series, L-functions and Automorphic Forms, Progress in Mathematics, Volume 300, Bump, Daniel; Friedberg, Solomon; Goldfeld, Dorian (Eds.), Birkhäuser, Basel, (2012).

Patents

(with M. Anshel, I. Gertner, B. Klebansky) *Multistream Encryption System for Secure Communication* International Patent Number WO 95/10148 and amended version published by the US Patent Office in 1995, US Patent Number 05440640

(with M. Anshel) *A Multi–Purpose High Speed Cryptographically Secure Sequence Generator Based on One–Way Zeta Functions* 1996 US Patent, 5,577,124.

(with I. Anshel and M. Anshel) *Method and apparatus for cryptographically secure algebraic key establishment protocols based on monoids* , 2002 U.S. Patent 6,493,449.

(with I. Anshel and M. Anshel) *Method and apparatus for establishing a key agreement protocol,* 2010 U.S. Patent 7,649,999

(with I. Anshel) *Cryptographic hash function,* 2015 U.S. Patent 8,972,715

Founder:

SecureRF Corporation, 175 Post Road West, Westport, CT 06880.
http://www.securerf.com