

DANIEL M. GORDON
PUBLICATION LIST

1. Minimal permutation sets for decoding the binary Golay codes, *IEEE Transactions on Information Theory*, Volume IT-28 (1982), pp. 541–543.
2. (with D. Grenier and A. Terras) Hecke operators and the fundamental domain for $SL(3, \mathbb{Z})$, *Mathematics of Computation*, Volume 48 (1987), pp. 159–178.
3. Perfect multiple error-correcting arithmetic codes, *Mathematics of Computation*, Volume 49 (1987), pp. 621–633.
4. Pseudoprimes on elliptic curves, *Proceedings of the 1987 Laval University International Number Theory Conference*, Walter de Gruyter, West Germany, pp. 290–305.
5. On the number of elliptic pseudoprimes, *Mathematics of Computation*, Volume 52 (1989), pp. 231–245.
6. Parallel sorting on Cayley graphs, *Algorithmica*, Vol. 6 (1991), pp. 554–564.
7. Percolation in high dimensions, *Journal of the London Math. Soc.*, (2) 44 (1991), pp. 373–384.
8. (with Carl Pomerance) The distribution of Lucas and elliptic pseudoprimes, *Mathematics of Computation*, *Mathematics of Computation*, **57** (1991) pp. 825–838.
9. Discrete logarithms in $GF(p)$ using the number field sieve, *SIAM J. Discrete Math.*, **6** (1993), pp. 124–138.
10. (with David Grant) Computing the Mordell-Weil rank of curves of genus 2, *Transactions of the American Math. Soc.*, **337** (1993), pp. 807–824.
11. (with Frank Harary and Robert Robinson) Degree games for graphs, *Discrete Mathematics*, **128** (1994), pp. 151–163.
12. Equidistant arithmetic codes and character sums, *Journal of Number Theory*, **46** (1994), pp. 323–333.
13. (with E.F. Brickell, K.S. McCurley and D.B. Wilson) Fast exponentiation with precomputation *Proceedings of Eurocrypt 92*, Springer-Verlag, (1993), pp. 200–207.
14. Designing and detecting trapdoors for discrete log cryptosystems, *Advances in Cryptology—Crypto '92*, Springer-Verlag, (1993), pp. 66–75.
15. (with K.S. McCurley) Massively parallel computation of discrete logarithms, *Advances in Cryptology—Crypto '92*, Springer-Verlag, (1993), pp. 312–323.

16. The Prime Power Conjecture is true for $n < 2,000,000$, *Electronic Journal of Mathematics*, **1** (1994), Paper R6.
17. (with Oren Patashnik, John Petro and Herb Taylor) $C(12,6,3)=15$, *Ars Combinatorica*, **40** (1995), pp. 161–177.
18. (with Greg Kuperberg and Oren Patashnik) New constructions for covering designs, *Journal of Combinatorial Designs*, **3** (1995), pp. 269–284.
19. (with Greg Kuperberg, Oren Patashnik and Joel Spencer) Asymptotically optimal covering designs, *Journal of Combinatorial Theory A*, **75** (1996), pp. 270–280.
20. (with Brienne E. Brown) On sequences without geometric progressions, *Mathematics of Computation*, **65** (1996), pp. 1749–1754.
21. A survey of fast exponentiation algorithms, *Journal of Algorithms*, **27** (1998), pp. 129–146.
22. (with Gene Rodemich) Dense admissible sets, *Proceedings of ANTS III*, LNCS 1423 (1998), pp. 216–225.
23. Some restrictions on orders of abelian planar difference sets, *Journal of Combinatorial Mathematics and Combinatorial Computing*, **29** (1999), pp. 241–246.
24. (with David Cantor) Factoring polynomials over p-adic fields, *Proceedings of ANTS IV*, Springer-Verlag, (2000), pp. 185–208.
25. (with Warwick Delauney) A remark on Plotkin’s bound, *IEEE Transactions on Information Theory*, **47** (2001), pp. 352–355.
26. (with Warwick Delauney) A Comment on the Hadamard Conjecture, *JCT A*, **95** (2001), pp. 180–184.
27. (with Len Baumert) On the existence of cyclic difference sets with small parameters, *High Primes and Misdemeanours: lectures in honour of the 60th birthday of H. C. Williams*, to appear.