Theoretical Analysis of Relations in PPMPQS

Introduction

The multiple polynomial quadratic sieve (MPQS) is one of the algorithms used for factoring large numbers. One of its variations makes use of relations with two large primes (PPMPQS). These two large primes usually have the same upper bound. Lenstra and Manasse[1] mentioned the idea to have two different bounds for these primes, and this variation is implemented in the computer algebra package Magma.

Analysis of relations

In order to improve our understanding of this method we made a theoretical analysis of the densities of the different types of relations occurring in PPMPQS with different bounds for the large primes. For complete, partial and partial-partial relations with the same bound for the two large primes this is already done by Lambert[2]. To give a theoretical estimate for the number of partial-partial relations with different bounds for the two large primes, we derived the following generalization of a result of Lambert. Here $\Psi(x, y_1, y_2, y_3)$ denotes the number of positive integers $\leq x$ with greatest prime factor $\leq y_1$, one but greatest prime factor $\leq y_2$ and all other prime factors $\leq y_3$, and ρ is the Dickman ρ function.

Theorem 1 *For* $0 < \alpha < \omega < \beta < 1/2$ *the limit* $\lim_{x\to\infty} \Psi(x, x^\beta, x^\omega, x^\alpha)/x$ *exists and equals*

$$\frac{1}{2}\int_\alpha^\omega \int_\alpha^\omega \rho\left(\frac{1-\lambda_1-\lambda_2}{\alpha}\right)\frac{\mathrm{d}\,\lambda_1}{\lambda_1}\frac{\mathrm{d}\,\lambda_2}{\lambda_2} + \int_\alpha^\omega \int_\omega^\beta \rho\left(\frac{1-\lambda_1-\lambda_2}{\alpha}\right)\frac{\mathrm{d}\,\lambda_1}{\lambda_1}\frac{\mathrm{d}\,\lambda_2}{\lambda_2} \quad .$$

Results

Counts of partial-partial relations (pp) after sieving with 100 096 polynomials, both experimentally and theoretically.

digits	y_2	y_1	pp (exp.)	pp (th.)	difference
80	24 979 712	24 979 712	93 556	85 607	−8.50%
80	12 489 854	49 959 435	123 775	113 774	−8.08%
91	30 000 690	30 000 690	6756	7200	6.57%
91	15 000 354	60 001 434	8973	9618	7.19%
101	48 223 067	48 223 067	1391	1477	6.18%
101	24 111 564	96 446 162	1863	1985	6.55%
110	149 570 695	149 570 695	557	544	−2.33%
110	74 785 318	299 141 028	737	721	−2.17%

Conclusion

Our experiments show good agreement with the theoretical analysis. The study shows that it is advantageous to choose different upper bounds for the large primes. More experiments are necessary to find the optimal choice of y_1 and y_2.

[1] Factoring with Two Large Primes, Math.Comp. 63 (1994) 785-798

[2] Computational aspects of discrete logarithms, Ph.D. thesis, University of Waterloo (1996)