Dixon's method of random squares

Tanja Lange

Eindhoven University of Technology

10 September 2020

Factorization using equivalence of squares

Target: odd integer n, want to factor it.

1. Fix a factor base $\mathcal{F}$ of small primes. Let $f = |\mathcal{F}|$.
2. Repeat the following until $f + 4$ relations are collected.
   - 2.1 Pick random integer a.
   - 2.2 Compute $b \equiv a^2 \bmod n$ with $b \in [0, n-1]$.
   - 2.3 Check whether b factors over the factor base, i.e. whether

$$b = \prod_{i=1}^{f} pi^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, store relation $(a, [e_1, e_2, \ldots, e_f])$
3. Put the exponents-part of the relations in a matrix, compute a non-zero vector in the kernel of the matrix modulo 2.
   If the matrix has no non-trivial vector, go back to collecting more relations.
4. Put A the product of all a involved in the kernel vector (non-zero entries).
   Compute the product of all prime powers involved in the kernel vector. All exponents are even, put B the square root.
   Compute $\gcd(A - B, n)$.