Integer factoring using small algebraic dependencies

Nitin Saxena (IIT Kanpur, India)

(joint work with Manindra Agrawal and Shubham S. Srivastava)

2016, MFCS, Kraków

Contents

Integer factoring

- Integer factoring (IF) is the problem of finding a nontrivial factor of input number n.
  - Given as log n bits.
  - Ideally, we want polylog n time algorithm.
  - Brute-force takes at least $\sqrt{n}$ time.

- No good algorithms, even heuristics, are known.
  - RSA cryptosystem is based on it's ``hardness''.
  - Belief: It's not as hard as SAT, TSP, HamPath.
  - Because it's a more ``algebraically structured'' problem.

- Number field sieve (Lenstra, Lenstra, Manasse, Pollard, STOC'90, et al.):
  $\exp(2.\log^{1/3} n.\log\log^{2/3} n)$ time algorithm for IF.
  - Sets up $a^2 = b^2 \bmod n$ in $Q[x]/(f)$.
  - Factorizes *smooth numbers* in the number ring.

f represents n in some base.

Integer factoring – related qn.

- Primality is the question of testing whether input n is prime.
  - Test whether Z/n is a *field*.

- It has fast algorithms, based on the Frobenius map
  $\varphi: (Z/n)[x] \to (Z/n)[x]\ ;\ a(x) \mapsto a(x)^n$.

  Exponentiation
  - It's a (ring) homomorphism iff n is prime!
  - Criterion requires the x.

- With this starting point, there are numerous *randomized* $\mathrm{polylog}\ n$ time primality tests.
  - (Solovay, Strassen, 1977; Miller, Rabin, 1976; Agrawal, Biswas, 1998)

- (Agrawal, Kayal, Saxena, 2002) *derandomized* this approach to work in deterministic poly-time.

Contents

- Integer factoring
- Revisit AKS'02 test
- General questions
- Special case answers
- Conclusion

Revisit AKS'02 test

- Frobenius map φ on $(Z/n)[x]/(x^r-1)$; $a(x) \mapsto a(x)^n$.
- Consider $f_{a,n,r} := a(x)^n - a(x^n)$.
- If above is zero, for few linear $a(x)$, then:

  $$b(x)^m = b(x^m) \text{ in } (Z/p)[x]/(x^r-1)$$

  for *exponentially many* $b(x)$ & $m=n^i.p^j$ is deduced.
  - p is a prime dividing n .
- The above congruences, and finite field properties, are used to deduce: n is a power of p .
  - Latter is easy to test algorithmically.
- Arguments exploit the p-Frobenius and the exponentiation by n.

Contents

General questions- composite n

- Compute $f_{a,e,r} := a(x)^e - a(x^e)$ in $(Z/n)[x]/(x^r-1)$ for several a, e, r.
  - Guaranteed: Most are *nonzero* polynomials (AKS polynomials).
  - Could their coefficients factor n?
- Qn: *Design* a,e,r such that $f_{a,e,r}$ gives a zerodivisor ?
  - Case $r=n$: $(x+1)^n - (x^n+1)$ in $(Z/n)[x]/(x^n-1)$ has a zerodivisor.
- Collect nonzero ones in $S := \{ f_{a,e,r}$ in $(Z/n)[x]/(x^r-1) \mid$ small $a,e,r \}$.
- What ring operations on S could lead us to a zerodivisor in Z/n ?

General questions- composite n

- Compute $S_r := \{ f_{a,e,r}$ in $(Z/n)[x]/(x^r-1) \mid$ small $a,e \}$.
- One can consider the lattice L_r generated by:

  S_r and $\{ n, nx, nx^2, \ldots., nx^{r-1} \}$.
- Could the properties of L_r help in reaching a zerodivisor ?
- Eg. apply basis reduction algorithms (Lenstra,Lenstra,Lovász, 1982).
- We've done experiments but we've no good conjecture.

Contents

Special case answers

- Interesting case: RSA composites $n = p.q$, where $p<q$ are primes.
- Fermat method: If we know the difference $\alpha := q - p$, then we can factor in $\text{polylog } n$ time.
- Qn: What if we know a bivariate f such that $f(p,q)=0$?
  - Nondegenerate f . We don't want trivial ones, eg. $f = xy - n$.
  - Such f of degree d, sparsity γ exists with coefficients $\approx n^{d/\gamma}$.
- Using polynomial factoring methods we can find a root of $f(x,n/x)$ (Schönhage, 1984).
  - p is a root.
  - Takes time $d^6.\log^2 n$, assuming constant γ.

Special case answers

- Using *AKS-type* computations, we give an algorithm that is linear-time in d.
  - Proof is conditional on number theory conjectures.
  - It's simpler than integer polynomial factoring algorithms.

- *Proof by example*: Suppose we know that $q = \alpha + \beta p + \gamma p^2$.
  - Then, $n = \alpha p + \beta p^2 + \gamma p^3$.
  - We could guess $p \bmod r$, say t (or try *all* possibilities).

- Compute $\Pi := a(x)^n\, a(x^t)^{-\alpha}\, a(x^{t\text{^}2})^{-\beta}\, a(x^{t\text{^}3})^{-\gamma}$ in $(Z/n)[x]/(x^r-1)$.
  - $\Pi \bmod p$ is $a(x)^{n - \alpha.p - \beta.p\text{^}2 - \gamma.p\text{^}3} \equiv a(x)^0 \equiv 1$.
  - Say, $t \bmod r$ is q^e.
  - Then, $\Pi \bmod q$ is $a(x)^{n - \alpha.q\text{^}e - \beta.q\text{^}2e - \gamma.q\text{^}3e} \neq 1$.
  - Thus, $\Pi\text{-}1$ factors n. $\square$

With high probability for random $a(x),r$

Contents

- Integer factoring
- Revisit AKS'02 test
- General questions
- Special case answers
- Conclusion

At the end …

- We give a higher-degree generalization of Fermat method.
  - Heuristically, faster than known methods.
  - Exploits the *difference* in the two Frobenius maps.

- $(x+1)^n \bmod n$ contains zerodivisor. Could this be extracted efficiently?

- Lattice methods, ring operations etc. on exponentials $a(x)^e$ over extensions of Z/n ?

Thank you!