Integer factoring and compositeness witnesses

Jacek Pomykała & Maciej Radziejewski

June 26, 2019

Integer factoring and compositeness witnesses

1. Objective: Factorization of a large integer n
   - Oracles
   - Techniques
   - How many hard numbers are there?
2. Compositeness witnesses
   - Fermat-Euclid
   - Miller-Rabin
   - Power difference
3. Results
   - Using the Φ oracle
   - Using the $\mathrm{Dec}\,\Phi$ oracle
   - Using iterated Φ oracle
4. Weaker oracles

Oracles

Φ	computes the value of $\phi(n)$ for any given n
$\mathrm{Dec}\,\Phi$	computes the prime factorization of $\phi(n)$
$\mathrm{Mul}\,\Phi$	computes some multiple $D = O(\exp((\log n)^{M'}))$ of $\phi(n)$
$\mathrm{Dec}\,\mathrm{Mul}\,\Phi$	computes the prime factorization of such a multiple

Techniques

- Factorization witnesses
  i.e. residues mod n wih special properties
  - We consider residues $b = 1, \ldots, B$,
    where $B \leq (\log n)^{O(1)}$ is a parameter.

- Exponent m of the group generated by $\{1, \ldots, B\}$
  - because $p \equiv 1 \pmod{m}$ for primes $p \mid n$

- Hensel-Berlekamp method
  - works if the exponent m is large enough

- Sieving out small prime factors $p \leq y$,
  where $y \leq (\log n)^{O(1)}$ is a parameter

- Reduction to square-free integers

Cf. Pomykała, Źrałek (2012), and Źrałek (2010).

How many hard numbers are there?

Main task:
Careful analysis how many numbers

$$n \leq x$$

are hard, i.e. unfactorable with a given method.

How many hard numbers are there? And why do we care?

If we only know that there are $o(x)$ such numbers, then they have density 0. However, it can mean many different things. E.g., there are

- $O(\frac{x}{\log x}) = o(x)$ primes $p \leq x$
- $O(\frac{x \log\log x}{\log x}) = o(x)$ integers of the form $n = pq \leq x$
- $O(\frac{x}{M \log\log x}) = o(x)$ integers $n \leq x$ without prime factors $p \leq (\log x)^M$
- $O(x^{1/2}) = o(x)$ squares $n \leq x$
- $O(x^{1/3}) = o(x)$ cubes $n \leq x$

How many hard numbers are there?

Given an algorithm $\mathcal{A}$ we call n

hard if $\mathcal{A}$ does not find the complete factorization of n

*-hard if $\mathcal{A}$ does not find any nontrivial divisor of n

We count factorizable integers. We put:

$F(x, \mathcal{A}, \mathcal{O}, t_{\mathcal{A}}, t_{\mathcal{O}})$ the number of $n \leq x$ that can be factored completely by $\mathcal{A}$ in time $t_{\mathcal{A}}$ with at most $t_{\mathcal{O}}$ queries to oracle O,

$F^*(x, \mathcal{A}, \mathcal{O}, t_{\mathcal{A}}, t_{\mathcal{O}})$ the number of $n \leq x$ that either are prime, or can be nontrivially factored by $\mathcal{A}$ in time $t_{\mathcal{A}}$ with at most $t_{\mathcal{O}}$ queries to oracle O.

Integer factoring and compositeness witnesses

Fermat-Euclid

Fermat-Euclid compositeness witness

A residue b such that

$$\gcd\left(b^{\frac{\operatorname{ord}_n b}{r}} - 1, n\right) \neq 1.$$

for some prime $r \mid \operatorname{ord}_n b$.

- Then r is called the **order** of the witness.
- If D is any multiple of $\operatorname{ord}_n b$, we can check $\gcd\left(b^{D/r^i} - 1, n\right)$ for $i = 1, 2, \ldots$
- We have a witness, unless $\operatorname{ord}_n b = \operatorname{ord}_p b$ for all $p \mid n$.
- Problem: how do we know wich r to try?

Miller-Rabin

Miller-Rabin compositeness witness

is just a Fermat-Euclid compositeness witness of order 2.

Lemma

Either there is a Miller-Rabin witness $b \leq B$ for n (square-free, without large prime divisors) or

- n is "B-exceptional", i.e. for some Dirichlet character mod n the least non-residue is greater than B, or
- n is determined by a pair of such exceptional integers

Power difference

Power difference compositeness witness

A residue b such that

$$1 < \gcd(b^u - b_0^{uj}, n) < n$$

for some prescribed b_0 and u.

- We can often find it if there are no Fermat-Euclid witnesses of a given order $r \geq 3$, but
- we need to check $j = 1, \ldots, r$.

Power difference

Lemma

Given $r \geq 3$, either there is a Fermat-Euclid witness $b \leq B$ for n (square-free, without large prime divisors) or

- there is a power difference witness
- n is "B-exceptional", i.e. for some Dirichlet character mod n the least non-residue is greater than B, or

Integer factoring and compositeness witnesses

Using the Φ oracle

Theorem

We have, for arbitrary fixed $M \geq 4$, $\mathcal{A} = (\mathcal{A}_0(\mathcal{A}_1), B, y)$, and appropriate choices of B and y:

$$F\left(x, \mathcal{A}, \Phi, t_{\mathcal{A}}, t_{\Phi}\right) \geq x - O_M\left(x(\log x)^{-6.5M}\right)$$

and

$$F^*\left(x, \mathcal{A}, \Phi, t_{\mathcal{A}}, t_{\Phi}\right) \geq x - O_M\left(x^{1.34/M}\right),$$

where $t_{\Phi} = 1$ and $t_{\mathcal{A}} = O((\log x)^{M+5})$.

Using the Φ oracle

In other words:

- the set of *-hard numbers is very thin,
- the bound for hard numbers is much worse.

Reason:

- poor bounds for the smallest *-hard number,
- related to the Vinogradov least-non-residue problem,
- solved under Extended Riemann Hypothesis,
- top results keep getting improved.

Using the $\mathrm{Dec}\,\Phi$ oracle

Using the $\mathrm{Dec}\,\Phi$ oracle we can compute the orders of all $b = 1, \ldots, B$ mod n, and thus:

- use Fermat-Euclid witnesses of all orders
- compute the exponent m and use techniques based on it

Using the $\mathrm{Dec}\,\Phi$ oracle

Theorem

We have, for arbitrary fixed $M \geq 2$, $\mathcal{A} = (\mathcal{A}_0(\mathcal{A}_3), B, y)$, and appropriate choices of B and y:

$$F\left(x, \mathcal{A}, \mathrm{Dec}\,\Phi, t_{\mathcal{A}}, t_{\mathrm{Dec}\,\Phi}\right) \geq x - O_M\left(x \exp\left(-\frac{M^3(\log\log x)^3}{9(\log(M+2)+\log\log\log x)^2}\right)\right)$$

and

$$F^*\left(x, \mathcal{A}, \mathrm{Dec}\,\Phi, t_{\mathcal{A}}, t_{\mathrm{Dec}\,\Phi}\right) \geq x - O_M\left(x^{1/M}\right),$$

where $t_{\mathrm{Dec}\,\Phi} = 1$ and $t_{\mathcal{A}} = O((\log x)^{M+5})$.

Using the $\mathrm{Dec}\,\Phi$ oracle

Theorem

We have, for arbitrary fixed $M \geq 2$, $\mathcal{A} = (\mathcal{A}_0(\mathcal{A}_3), B, y)$, and appropriate choices of B and y:

$$F\left(x, \mathcal{A}, \mathrm{Dec}\,\Phi, t_{\mathcal{A}}, t_{\mathrm{Dec}\,\Phi}\right) \geq x$$
$$- O_M\left(x \exp\left(-\frac{M^3(\log\log x)^3}{9(\log(M+2) + \log\log\log x)^2}\right)\right)$$
$$> x - O\left(x/(\log x)^c\right) \qquad \text{for any fixed } c$$

and

$$F^*\left(x, \mathcal{A}, \mathrm{Dec}\,\Phi, t_{\mathcal{A}}, t_{\mathrm{Dec}\,\Phi}\right) \geq x - O_M\left(x^{1/M}\right),$$

where $t_{\mathrm{Dec}\,\Phi} = 1$ and $t_{\mathcal{A}} = O((\log x)^{M+5})$.

Using iterated Φ oracle

Idea:

- If you try to factorize n and need the decomposition of $\phi(n)$,
  - compute $\phi(\phi(n))$,
    - compute $\phi(\phi(\phi(n)))$,
      ...
    - and factorize $\phi(\phi(n))$,
  - and factorize $\phi(n)$.
- Then you can factorize n.

Using iterated Φ oracle

It is not as easy as iterating the algorithm $\mathcal{A}_0(\mathcal{A}_3)$, but we do have:

Theorem

For arbitrary fixed $M \geq 4$, $\mathcal{A} = (\mathcal{A}_4, B, y)$, and appropriate choices of B and y:

$$F\left(x, \mathcal{A}, \Phi, t_{\mathcal{A}}, t_{\Phi}\right) \geq x - O_M\left(x \exp\left(-\frac{M^3(\log\log x)^3}{9(\log(M+2) + \log\log\log x)^2}\right)\right)$$

and

$$F^*\left(x, \mathcal{A}, \Phi, t_{\mathcal{A}}, t_{\Phi}\right) \geq x - O_M\left(x^{1.34/M}\right),$$

where $t_{\Phi} \ll \log x$ and $t_{\mathcal{A}} = O((\log x)^{M+5})$.

Integer factoring and compositeness witnesses

Reduction to square-free integers

Reduction to square-free integers:

- shown by S. Landau (1988), with $O(\log^3 n)$ calls to Φ,
- we do it with 0 extra calls to Φ, reusing the initial value,
- we cannot do it if we replace Φ by $\operatorname{Mul}\Phi$.

Nevertheless we can do it for square-free integers.

Theorem

All except $O_M\left(x^{1/M}\right)$ integers of the form $n = pq \le x$ can be factored using algorithm $\mathcal{A}_1$ in time $t_{\mathcal{A}} = O\left((\log x)^{M+M'+5}\right)$ with one query to the oracle $\operatorname{Mul}\Phi$.