Factoring with Hints

Francesco Sica

Nazarbayev University

MathCifris
Online – 10 dicembre 2020

Motivation

- Understanding factorisation and especially why the Number Field Sieve is the best current factoring approach.
- Understand if one can use a more “natural ” approach with the Riemann ζ function.

The Fermat-Kraitchik Idea

Suppose we can find x, y integers with $x^2 \equiv y^2 \pmod{N}$ and $x \not\equiv \pm y \pmod{N}$. Then $1 < \gcd(x - y, N) < N$ and this can be computed quickly, giving rise to a nontrivial factor of N.

The Fermat-Kraitchik Idea

Suppose we can find x, y integers with $x^2 \equiv y^2 \pmod{N}$ and $x \not\equiv \pm y \pmod{N}$. Then $1 < \gcd(x - y, N) < N$ and this can be computed quickly, giving rise to a nontrivial factor of N.
To find x and y, the most successful technique uses smooth numbers (divisible by "small" primes only). It is due to Morrison & Brillhart.
This idea is at the heart of the most successful factoring methods (probabilistic like QS and NFS or deterministic like SQUFOF).

Running Times

ECM, QS, NFS all have subexponential running times.

- QS: $\exp\big(c_1(\log N)^{1/2}(\log\log N)^{1/2}\big)$
- ECM: $\exp\big(c_2(\log p)^{1/2}(\log\log p)^{1/2}\big)$, (where p is smallest prime dividing N)
- NFS: $\exp\big(c_3(\log N)^{1/3}(\log\log N)^{2/3}\big)$

Deterministic factoring algorithms are exponential with class group methods running in $O(N^{1/5+\epsilon})$ under General Riemann Hypothesis.

Current Work

We present a new approach:

- It does not use the Morrison-Brillhart paradigm.

Current Work

We present a new approach:

- It does not use the Morrison-Brillhart paradigm.
- It is deterministic in finding factors of N, but uses factorisations of other integers close to N, which may be easier to factor (e.g. using probabilistic methods).

Current Work

We present a new approach:

- It does not use the Morrison-Brillhart paradigm.
- It is deterministic in finding factors of N, but uses factorisations of other integers close to N, which may be easier to factor (e.g. using probabilistic methods).
- Works in $O(N^{1/3+\epsilon})$ bit operations, knowing $O(N^{1/3+\epsilon})$ factorisations.

Approaching Multiplicative Functions

Let $\sigma(n)$ be the Euler phi function. Suppose that N factors as $N = pq$, so that $\sigma(N) = N + p + \frac{N}{p} + 1 = f(p)$.
Then using Newton's method, an approximation to $\sigma(N)$ will yield an approximation to p, which is enough to recover it. For technical reasons, we work instead with

$$\sigma_{1/2}(N) = \sum_{d|N} d^{1/2} = 1 + \sqrt{N} + \sqrt{p} + \frac{\sqrt{N}}{\sqrt{p}}$$

Using Generating Functions

Riemann zeta function is

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \quad \Re s > 1$$

and therefore

$$\zeta(s)\zeta(s-1/2) = \sum_{n \geq 1} \frac{\sigma_{1/2}(n)}{n^s} \quad \Re s > 3/2$$

Isolating $\sigma_{1/2}(N)$

We have for integer $\nu \geq 2$

$$\frac{(\nu-1)!}{2\pi i}\int_{3-i\infty}^{3+i\infty}\frac{\zeta(s)\zeta(s-1/2)x^s}{s(s+1)\cdots(s+\nu-1)}\,ds=\sum_{n\leq x}\sigma_{1/2}(n)\left(1-\frac{n}{x}\right)^{\nu-1}$$

We call $F_\nu(x)$ the right-hand side, and

$$P_\nu(x)=x^{\nu-1}F_\nu(x)=\sum_{n\leq x}\sigma_{1/2}(n)\,(x-n)^{\nu-1}$$

The Functional Equation

The Riemann zeta function is an meromorphic function with a single pole at 1 with residue 1 satisfying the functional equation (given here in asymmetric form)

$$\zeta(s) = \frac{(2\pi)^s}{\pi}\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)\zeta(1-s)$$

The Functional Equation

The Riemann zeta function is an meromorphic function with a single pole at 1 with residue 1 satisfying the functional equation (given here in asymmetric form)

$$\zeta(s) = \frac{(2\pi)^s}{\pi}\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)\zeta(1-s)$$

Also, the gamma function satisfies the following duplication equation

$$\Gamma(s)\Gamma\left(s+\frac{1}{2}\right) = \sqrt{\pi}\,2^{1-2s}\Gamma(2s)$$

New Identities

Moving the line of integration to the left and using the functional equation and the Legendre duplication formula shows

$$F_\nu(x) = \rho + \frac{(\nu-1)!}{2\pi i} \int_{(-1/4)} \zeta(s)\zeta(s-1/2)\, \frac{x^s}{s(s+1)\cdots(s+\nu-1)}\, ds$$

$$\doteq \frac{(-1)^\nu 2^{\nu-1/2} e^{-i\pi/4}(\nu-1)!}{(4\pi i)^\nu x^{\nu/2-1}} \sum_{n\geq 1} \sigma_{-1/2}(n) \frac{e^{-4\pi i\sqrt{xn}}}{n^{\nu/2}}$$

$$+ \frac{2^{\nu-1/2} e^{i\pi/4}(\nu-1)!}{(4\pi i)^\nu x^{\nu/2-1}} \sum_{n\geq 1} \sigma_{-1/2}(n) \frac{e^{4\pi i\sqrt{xn}}}{n^{\nu/2}}$$

where ρ is some easily expressible residue and $\doteq$ means that other (nonwritten) terms are easily calculated or are of lesser order

Factoring with Hints

After multiplying the previous equation by $x^{\nu-1}$, we obtain

$$P_\nu(x) = \sum_{n\leq x} \sigma_{1/2}(n)\,(x-n)^{\nu-1}$$

$$\doteq x^{\nu/2}\frac{2^{\nu-1/2}e^{i\pi/4}(\nu-1)!}{(4\pi i)^\nu}\sum_{n\geq 1}\sigma_{-1/2}(n)\frac{e^{4\pi i\sqrt{xn}}}{n^{\nu/2}} + \cdots$$

We then use finite differences and partial sums to obtain a nontrivial approximation of $\sigma_{1/2}(N)$.

Finite Differences

Let $h > 0$ and define $\nabla_h P_\nu(x) (= \nabla_h^1 P_\nu(x)) = P_\nu(x) - P_\nu(x-h)$ and $\nabla_h^{k+1} P_\nu(x) = \nabla_h \nabla_h^k P_\nu(x)$ for $k \geq 1$.

1. If P is a polynomial of degree d then $\nabla_h^{d+1} P = 0$.
2. $$\nabla_h^k P_\nu(x) = \sum_{i=0}^{k} \binom{k}{i} P_\nu(x - ih)$$

Letting $x = N + N^{1/3}$ and $h = N^{1/3}$ we see that $\nabla_h^\nu P_\nu(x)$ can be expressed as $\sigma_{1/2}(N) N^{(\nu-1)/3} +$ terms involving only $\sigma_{1/2}(n)$ for $x - \nu N^{1/3} \leq n \leq x$.

Calculation of the Singular Series

We now calculate

$$\sum_{n\geq 1}\sigma_{-1/2}(n)\frac{e^{4\pi i\sqrt{xn}}}{n^{\nu/2}}=\sum_{n_1n_2\leq X}\frac{e^{4\pi i\sqrt{xn_1n_2}}}{n_1^{\nu/2}n_2^{(\nu+1)/2}}+O\left(\frac{1}{X^{\nu/2-1}}\right)$$

within $N^{-\nu/6}$ by letting $X\approx N^{1/3}$. Since there are $O(N^{1/3}\log N)$ points (n_1,n_2) under the hyperbola in the right-hand sum we can do that in $O(N^{1/3+\epsilon})$ bit operations.

Conclusion

- New approach to factoring
- Advantage is that it transforms the arithmetic problem of factoring N into an analytic one, where there are many possible optimisations
- Work in progress

THANK YOU! ☺