Toy Factoring by Newton's Method

Daniel R. L. Brown*

April 1, 2008

Abstract

A theoretical approach for integer factoring using complex analysis is to apply Newton's method on an analytic function whose zeros, within in a certain strip, correspond to factors of a given integer. A few successful toy experiments of factoring small numbers with this approach, implemented in a naïve manner that amounts to complexified trial division, show that, at least for small numbers, Newton's method finds the requisite zeros, at least some of time (factors of nearby numbers were also sometimes found). Nevertheless, some heuristic arguments predict that this approach will be infeasible for factoring numbers of the size currently used in cryptography.

1 Cosh Product Factorization

Let

$$\begin{aligned} f(z) &= \prod_{n=1}^{\infty} \left(2 - \cosh\left(\frac{z}{\pi n}\right)\right) \\ &= 1 - \frac{1}{6}\frac{z^2}{2!} + \frac{7}{180}\frac{z^4}{4!} - \frac{53}{7560}\frac{z^6}{6!} - \frac{13}{75600}\frac{z^8}{8!} + \frac{227}{598752}\frac{z^{10}}{10!} + \dots \end{aligned} \tag{1}$$

The product converges for all z, so $f(z)$ is an entire function. The scaling $\frac{1}{\pi}$ is chosen merely to make the power series expansion of $f(z)$ have rational coefficients. The set of zeros of the function $f(z)$ is

$$\{a\pi \log(2+\sqrt{3}) + 2\pi^2 abi : a, b \in \mathbb{Z}, a \neq 0\} \tag{2}$$

In theory, to try to factor a semiprime N (an RSA modulus), one can try to search for zeros on the line the $\mathbb{R} + 2\pi^2 Ni$, say, by Newton's method.

Experiments done using Maple, factored numbers such as $N = 299$ using the approximation to $f(z)$ of $\prod_{n=1}^{100}(2 - \cosh(\frac{z}{\pi n}))$. That is, Newton's method starting from complex numbers on the line $\mathbb{R} + 2\pi^2 Ni$ with real parts near $\log(2+\sqrt{3})\pi\sqrt{N}$ tended to converge towards a zero on the same line with real part near 13, a factor of 299. Convergence seemed to occur more quickly if the lower factors of the partial product were omitted. The purpose of these experiments was to predict whether Newton's method would reliable or chaotic when run on the infinite product with larger values of N. The success rate for a few other similar trials was good, but not perfect. In failed

*Certicom Research

cases, usually a number near to N was factored instead. Based on these toy experiments, we may conjecture Newton's may find the desired zeros, and then wonder what other hurdles there would be to face for larger values of N.

For Newton's method on $f(z)$ to be effiicient an efficient algorithm to compute $f(z)/f'(z)$ for $z \approx \sqrt{N}\log(2+\sqrt{3})\pi + 2N\pi^2 i$, to an accuracy of about 1, or relative error of about $1/N$ is needed.

One approach to evaluate $f(z)$ is to use a partial product, as was done in the toy experiment. The derivative, $f'(z)$, or more precisely logarithmic derivative, $f'(z)/f(z)$, could then be evaluated by a partial sum. However the upper limit of the index n must be at least as large as the factor we wish to find. This could be as high as $\sqrt{N}$, evaluation of $f'(z)/f(z)$ requires a sum of $\sqrt{N}$ terms. Therefore, the cost of this approach is fairly large factor times the cost of trial division, which is considerably slower than the fastest factoring algorithms.

Another approach is to use a partial sum of the power series expansion of $f(z)$. If we use, say, t terms of the expansion, thouhgh, then $f(z)$ is a polynomial of degree t, and as such has at most t zeros. The function $f(z)$ has infinitely many zeros, which are much denser where the real part is smaller in magniture. If the partial sum polynomial approximates $f(z)$ well, then we can expect most of its zeros to be fairly close to zeros of $f(z)$. However, we can also expect that the polynomial approximates $f(z)$ only in a circle of a given radius. But because $f(z)$ has so many zeros near the imaginary line, and the zeros we seek are quite far away, we may need to take a large value of t to approximate all the zeros with small real values. A large value of t would make this approach just as infeasible as the previous approach, or worse.

One could try to compute a theoretical formula for coefficients of the power series expansion of $f'(z)/f(z)$, but one cannot that the power series converges for large values of z, because it has poles, since $f(z)$ has zeros. The poles implies that the power series has a small radius of convergence. Instead, one could try to compute the power series expansion of $f(z)/f'(z)$. It too would have poles if $f'(z)$ has any zeros, which some very crude experiments suggest it does. If $f'(z)$ has any zeros, then a power series expansion for $f(z)/f'(z)$, would not likely to be useful.

If $f(z)$ has a closed formula, then there is more possibility of computing $f(z)/f'(z)$ efficiently. More precisely, if $f(z)/f'(z)$ satisfies a functional equation, or if it is aysmptotic to a function $g(z)$ satisfying a functional equation, then perhaps the desired accuracy can be obtained. For example, a function of the form $g(z) = e^z h(1/z)$, where h has power series expansion, can be evaluated to sufficient relative accuracy fairly efficiently, even for a large z. The multiplicative properties the exponential factor e^z allow this to be done. Unforunately, we can see that $f(z)$ does not have such a form $g(z)$, since this would imply that $h(z)$ has infinitely zeros in arbitrarily small disks around the origin, which implies that h is identically zero.

The numerators and denominators of the coefficients of $f(z)$ do not match any entries the Online Encyclopedia of Integer Sequences. This suggests either that $f(z)$ has no closed formula, or if it does, that its power series expansion is not well known.

Despite all these heuristic arguments suggesting that neither $f(z)$ nor $f(z)/f'(z)$ can be evaluated efficiently, suppose hypothetically that the Newton iterations can be evaluated efficiently, and futhermore, that they converge to the desired zeros. It may still be the case,, however, that too many iterations are required. If the Newton iterations step by less than a unit, for example, then Newton's method would again be as slow as or slower than trial division. In antipication of this, one cansider some techniques that might reduce the number of iterations. Divide $f(z)$ by various functions to remove some of its zeros without adding any new zeros. By reducing the number of zeros, we may hope to increase the basins of attraction for the remaining zeros, and perhaps also

to increase the rate of convergence inside the basins (when far away from a zero, since sufficiently near a zero the convergence of Newton's method is quadratic).

To this end, dividing by a partial product $\prod_{n=1}^{M}(2-\cosh(z/\pi n))$ removes many zeros near the imaginary line. Toy experiments suggest that this actually does increase the speed of convergence. One could also find factor of numbers near to N, such as $N \pm 1$, locate the corresponding zeros of $f(z)$, then form a polynomial $p(z)$ with those zeros. Dividing $f(z)$ by this $p(z)$ may have the affect of decreasing the attraction of zeros on lines parallel to our search line $\mathbb{R} + 2\pi^2 Ni$. It may also be useful to divide out by functions that have zeros at all nonzero integral multiples of $(\pi \log(2+\sqrt{3}) + 2\pi^2 ib)$ for small b. (These functions may be obtained by scaling the sine function).

2 Weierstrass Sigma Factorization

Let Λ be a lattice in $\mathbb{C}$. The Weirstrass sigma function $\sigma_\Lambda(z)$ is an entire function with zeros precisely at the lattice points. The Weierstras sigma functions, and more importantly its logarithmic derivative, the Weierstrass zeta function, which is essentially what would be used in Newton's method on the sigma functions, obey functional equations that enable their efficient evaluation, even for large arguments. Therefore this choice of function solves the evaluation dilemma that we encountered in the infinite product of hyperbolic cosines.

Fix, for simiplicity, the lattice to be $\Lambda = \mathbb{Z} + \mathbb{Z}i$. To factor an integer N, we could try to find zeros of σ along the hyperbola $\{a + bi : a, b \in \mathbb{R}, ab = N\}$. However, one would expect there to be many such zeros, that is, lattice points near to this hyperbola. Newton's method would seem likely to go towards the nearest lattice point from the starting point. Newton's method has no reason to stay on or near these hyperbola, even if starts on the hyperbola. One could try to modify Newton's method to steer it back onto the hyperbola, but it seems very likely that the effect of any such modification would merely result in aimless wandering along the hyperbola, perhaps with a tendency to hang around lattice points are especially close the hyperbola. The true zeros on the hyperbola could be still be very far away.

One could try to transform the complex plane with the hope to increase the distance of such distracting lattice points. To this end, consider the function $\psi(z) = \sigma(\sqrt{z})$. The set of zeros of ψ is:

$$\{(a^2 - b^2) + 2abi : a, b \in \mathbb{Z}\}. \tag{3}$$

So, to factor an RSA modules $N = pq$, we can search for nontrivial zeros of $f(z)$ along the line $\mathbb{R} + 2Ni$. The trivial zeros have $\{a, b\} \in \{\{1, N\}, \{-1, -N\}\}$, so the real part is $\pm(N^2 - 1)$. The nearest zeros off the target line have distance at least two.

Applications of Newton's method on the ψ, for small values, finds that it very quickly leaves the target horizontal lines, usually heading, instead, towards the origin. Again, one might be able artificially modify Newton's method is stay on or near the desired line, but there is no good reason that the resulting modification will find the zeros sought. Indeed, to a first order approximation, Newton's method on ψ simply mimics Newton's method on σ. One shouldn't expect the second order differences to improve things much.

3 Previous Work

Bentahar [Ben04] previously and independently attempted to apply Newton's method to integer factorization. One function he considered is

$$f(z) = \cos(\pi z) + \cos(\pi n/z) + 2, \tag{4}$$

where n is an odd integer. The real roots of f are precisely the integral factors of n.

4 Conclusion

Loosely speaking, the regularity of the zeros of the Weierstrass sigma make possible for it to have a functional equation that leads an efficient evaluation algorithm. On the other hand, the regularity of the zeros leads to a high density of zeros, which is problematic for our approach to factoring. Newton's method gets distracted by the presence of so many other nearby zeros that do not correspond to the factors of the number to be factored. Any trick of trying to make the zeros less dense seems to be approximately conjugation, which does not seem likely to resolve the problem.

The hyperbolic cosine product seemed to have the obstacle that the irregular location of its zero rules out any efficient evaluation method. Its zeros are much less dense, so perhaps Newton's method would indeed lead to a factoring algorithm, if only the evaluation could be done. If we were to consider other functions, we would somehow need to simultaneously obtain more regularity of the zeros and less density, while maintaining a correspondence between zeros and factors, but this seems quite unlikely.

This approach seems to be a dead end. The analysis here is purely informal, but probably only a little more thought is needed to show that this approach is doomed to fail.

References

[Ben04] Kamel Bentahar, *The Newton method: History, theory and applications*, Master's thesis, Imperial College, London, June 2004.

A Comments on the Cosh Product Power Series Expansion

The lower coefficients of the power series expansion of $f(z)$ were computed using some tools from the theory of symmetric functions. Computing the cofficient of z^n by this method requires require sums involving up to $\frac{1}{2}p(n)^2$ terms, where $p(n)$ the number of partitions. This is highly inefficient, asymptotically. The formula is

$$\sum_{\alpha,\beta\vdash n} \frac{M_{\alpha,\beta}}{(2\alpha+1)!(-2\beta)!} \tag{5}$$

where α and β are range over partitions of n, with $(2\alpha+1)!$ indicating the product $\prod_i (2\alpha_i + 1)!$, and $(-2\beta)!$ indicating[1] $\prod_i -(2\beta_i)!$. The integers $M_{\alpha,\beta}$ are the entries in the change of basis matrix $M(m,e)$ that expresses the mononomial symmetric function basis in terms of the elementary

[1] Awkward notation, sorry.

symmetric function basis (see I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., 1995).

As noted earlier, it would be interesting to see if $f(z)$ has a closed form, or at least satisfies some differential equation, or even a functional equation (such as an efficient doubling formula). To this end, one can try to find a pattern in the power series expansion. Let B_n be the Bernoulli numbers, and let $B_n = N_n/D_n$ in lowest terms. Let $E_n = \prod_{k=1}^{n} D_{2k}$. Let

$$f(z) = 1 + \sum_{n=1}^{\infty} \frac{F_n}{E_n} \frac{z^{2n}}{(2n)!}, \tag{6}$$

Numerical computations of F_n, using the Maple package SF of John Stembridege, which was done $1 \leqslant n \leqslant 15$, yield integers. We conjecture that this is always the case. Although F_9 is prime, for other n, the denominator E_n and F_n have common factors, so the fractions $\frac{F_n}{E_n}$ are not always in lowest terms.