Factoring and Lattice Reduction
DRAFT
March 16, 1995

Leonard M. Adleman
University of Southern California

Abstract

Factoring integers and finding the smallest vector in a lattice are central problems in algorithmic number theory. The complexity of both problems is poorly understood. Neither is known to be computable in polynomial time nor to be NP-hard. In this paper it is shown (under reasonable assumptions) that the factoring problem is random polynomial time reducible to the lattice problem. This result raises the possibility of using 'approximate' lattice reduction algorithms for factoring.

1 Introduction

We will consider two well known computational problems:

Factoring: On input $n \in Z_{>0}$, output primes $p_1, p_2, \ldots, p_k \in Z_{>0}$ and $e_1, e_2, \ldots, e_k \in Z_{>0}$ such that $n = \prod_{i=1}^{k} p_i^{e_i}$.

Lattice: On input $\mathbf{R}$-independent vectors $b_1, b_2, \ldots, b_n \in \mathbf{Q^n}$, output $v \in Zb_1 \oplus Zb_2 \oplus \ldots \oplus Zb_n$ with $||v||_2 = \min\{||x||_2 \mid x \in Zb_1 \oplus Zb_2 \oplus \ldots \oplus Zb_n \ \& \ x \neq 0\}$.

The complexity of both of these problems has long been open [**?**]. We will argue (under reasonable assumptions) that Factoring is random polynomial time reducible to Lattice. A similar result seems likely for the discrete logarithm problem.

Since it is widely assumed that factoring is not in P, this gives the first substantial evidence that Lattice is not in P.

These results suggest the possibility of using well known 'approximate' lattice reduction algorithms (e.g. [**?**]) to give new algorithms for factoring and discrete logarithms.

Schnorr [**?**] appears to be the first to publish on the relationship between factoring and finding small vectors in a lattice. Many of the techniques used here are already to be found in [**?**]. Schnorr provides an heuristic argument that factoring is reducible to finding small vectors in a lattice using the $|| \,||_1$ norm (rather than the $|| \,||_2$ norm considered here). It is worth noting that Lagarias has previously shown that for the $|| \,||_\infty$ and $|| \,||_1$ the lattice problem is NP-hard [**?**].

2 Arguments

The notion of 'smoothness' is central to many factoring algorithms.

Definition For all $n \in Z$, for all $B \in \mathbf{R}_{>0}$, n is B-smooth iff for all primes $p|n$ $p \leq B$.

For most factoring algorithms to date, B-smooth numbers are used where B is of the form:

$$e^{(\delta+o(1))(\ln(n)^\gamma \ln\ln(n)^{1-\gamma})}$$

where $\delta \in \mathbf{R}_{>0}$ and $\gamma = 1/2$ or $1/3$.

Here much smaller B will be used, for example $B = \ln^c(n)$ where c is a small positive number. The informal term 'supersmooth' will sometimes be used for such numbers.

Much is known about supersmooth numbers [**?**]. We thank Carl Pomerance [**?**] for providing the following basic theorem:

For all $c \in Z_{>1}$, for all sufficiently large positive integers n, the number of squarefree positive integers less than n which are $\ln^c(n)$-smooth exceeds $n^{(c-1)/c}$.

Let n be a positive integer (e.g. that we wish to factor). The arguments which follow will hold for all sufficiently large n. The basic idea is to use lattice reduction to find a linear combination of the logs of n and the 'supersmall' primes $p_1, p_2, ..., p_z$ which is very close to zero. Such a combination will, upon exponentiation, yield a product of the form:

$$n^r P/Q = \exp\sigma$$

Where P and Q are supersmooth and the absolute value of σ is very small. Since $\exp\sigma$ is approximately $1+\sigma$, we have:

$$n^r P = Q + Q\sigma'$$

for some small σ' and hence:

$$Q \equiv -Q\sigma' \bmod n \tag{1}$$

When σ' is sufficiently small, $-Q\sigma'$ will be supersmooth and (**??**) is a congruence of supersmooth numbers. Such 'supersmooth congruences' are used in standard ways to factor n.

The details become a bit untidy as a consequence of the need to use approximations to logs in actual computations.

Let M denote n^4 and $p_1, p_2, ..., p_z$ be the primes less than $\ln^{20}(2n^{1.25})$. If there exits an $i \in Z_{\geq 1}^{\leq z}$ such that $p_i | n$, then replace n with $n|p_i$. Define $z+1$ vectors in $\mathbf{R}^{z+1}$ as follows.

For $1 \leq j \leq z$:

$V_j = < M\ln'(p_j), \overbrace{0, ..., 0}^{j-1}, \sqrt{}'\ln(p_j), \overbrace{0..., 0}^{z-j} >.$

Since in a polynomial time computation, ln cannot be computed to arbitrary precision, an 'approximate log' $\ln'$ is used which is obtained by 'rounding up' at the $\lceil 1.25\log_{10}(n)\rceil^{th}$ digit following the decimal point. Hence for all $a \in Z_{>0}$:

$$0 \leq \ln'(a) - \ln(a) \leq 5/n^{1.25}$$

Similarly, $\sqrt{}'\ln$ will be the 'approximate square root of the log' such that for all $a \in Z_{>0}$:

$$0 \leq (\sqrt{}'\ln(a))^2 - \ln(a) \leq 5/n^{1.25}$$

Hence a matrix with these vectors as rows has non zero entries only in the first column and along the diagonal.

Let:

$$V_0 =< M(\ln'(n)+\gamma), \overbrace{0, ..., 0}^{z} >$$

γ will act as a 'fudge factor' to compensate for the use of 'approximate logs' rather than true logs. γ will range over the values $a/10^{\lceil 1.25 \log_{10}(n) \rceil}$ where $a \in Z$ and $-16\ln(n) \leq a \leq 16\ln(n)$. Hence $-16\ln(a)/n^{1.25} \leq \gamma \leq 16\ln(a)/n^{1.25}$. γ will be described further in what follows.

It is clear that these vectors are independent over $\mathbf{R}$. Let the lattice they generate be denoted Λ.

In what follows we will use a number theoretic analysis to show that Λ has some small vectors which correspond to supersmooth congruences mod n. We will then show that the smallest vector in the Λ is just such a vector.

Consider all numbers of the form $Pn-1$ as $P = n^{1/4}+1, ..., 2n^{1/4}$. Then there are $n^{1/4}$ such numbers each greater than $n^{1.25}$ and less than $2n^{1.25}$. As is 'standard' in the analysis of factoring algorithms we will assume that these numbers have the same probability of being squarefree- supersmooth as a 'random' number less than $2n^{1.25}$. Hence at least one in $(2n^{1.25})^{1/20}$ of these numbers are squarefree-supersmooth with respect to $\ln^{20}(2n^{1.25})$. By the same assumption, at least one in $(2n^{1.25})^{1/20}$ of the P are squarefree-supersmooth. Now we will make another 'standard' assumption: that the probability that P is squarefree-supersmooth is independent of the probability that $Q = Pn-1$ is squarefree-supersmooth[1]. Hence we may assume the probability that P and Q will simultaneously be 'squarefree- supersmooth' is at least one in $(2n^{1.25})^{2/20} = 2^{1/10}n^{1/8}$. Hence there exist at least $n^{1/8}/2^{1/10}$ such pairs. Notice we must have $(P,Q) = 1$

Consider such a pair with $P = \prod_{i \in S} p_i$ and $Q = \prod_{i \in T} p_i$. Then $Pn - 1 = Q$ or equivalently $Pn/Q = 1 + 1/Q$. Now taking logs we have:

$$\ln n + \sum \ln(p_i) - \sum \ln(q_i) = \ln(1 + 1/Q)$$

Since $0 \leq \ln(1+1/Q) \leq 1/Q \leq 1/n^{1.25}$, and since there are at most $3\ln(n) - 1$ primes dividing PQ it follows that:

$$\ln' n + \sum \ln'(p_i) - \sum \ln'(q_i) + \gamma = 0$$

where $\gamma = a/10^{\lceil 1.25 \log_{10}(n) \rceil}$ for some $a \in Z$ with $-16\ln(n) \leq a \leq 16\ln(n)$.

[1] This cannot be strictly true since $(Q,P) = 1$. Nonetheless this is presumed to be 'essentially' true. A similar assumption is made in many factoring algorithms.

For the appropriate choice of γ in V_0, the vector $W = V_0 + \sum_{i \in S} V_i - \sum_{i \in T} V_i$ must have first coordinate equal to 0. Further by our selection of values along the diagonal, the length of W, $||W||_2$, will be near $\ln(PQ)$. In fact because of the use of 'approximate square root of the log' we have:

$$||W||_2 = \sum_{i \in S \cup T} (\sqrt{}' \ln p_i)^2 = \sum_{i \in S \cup T} \ln p_i + \beta$$

where $0 \leq \beta \leq 15 \ln(n)/n^{1.25}$.

Hence $||W||_2 = \ln(PQe^{\beta})$. For sufficiently large n, $1 \leq e^{\beta} \leq 2$ so:

$$\ln(n^{1.5}) \leq ||W||_2 \leq \ln(8n^{1.5})$$

We will next argue that for this choice of γ, the shortest vector in Λ must correspond to a supersmooth pair P,Q with $Pn - Q = s$ with s supersmooth. Let the shortest vector in Λ be $U = rV_0 + \sum_{i \in S} a_i V_i - \sum_{i \in T} b_i V_i$ where $S \cap T = \emptyset$, for all $i \in S$, $i \neq 0$ & $a_i \in Z_{>0}$, for all $i \in T$, $i \neq 0$ & $b_i \in Z_{>0}$, and wlog $r \in Z_{\geq 0}$. Let $P = \prod_{i \in S} p_i^{a_i}$ and $Q = \prod_{i \in T} p_i^{b_i}$. Notice that $S \cap T = \emptyset$ implies that $(P, Q) = 1$.

The first coordinate of U is $M(r \ln'(n) + r\gamma + \sum_{i \in S} a_i \ln'(p_i) - \sum_{i \in T} b_i \ln'(p_i))$. This must be 0 otherwise it is at least $n^4/10^{\lceil 1.25 \log_{10}(n) \rceil}$ and hence the vector W described above is shorter. Hence $r \ln'(n) + r\gamma + \sum_{i \in S} a_i \ln'(p_i) - \sum_{i \in T} b_i \ln'(p_i)) = 0$. Since $\ln'$ is obtained by rounding up, there exist non-negative real 'error terms' ρ, α, β such that:

$$[\rho + r \ln(n))] + [r\gamma] + [\alpha + \sum_{i \in S} a_i \ln(p_i)] - [\beta + \sum_{i \in T} b_i \ln(p_i))] = 0 \qquad (2)$$

where the following bounds can be easily obtained:

$$\rho \leq \frac{5}{n^{1.25}} r$$

$$-16 \ln(n)/n^{1.25} \leq \gamma \leq 16 \ln(n)/n^{1.25}$$

$$\alpha \leq \frac{5}{n^{1.25}} \sum_{i \in S} a_i$$

$$\beta \leq \frac{5}{n^{1.25}} \sum_{i \in S} b_i$$

In addition:

$$\ln(2) \sum_{i \in S} b_i \leq \ln(Q) \leq \ln(PQ) \leq ||U||_2 \leq ||W||_2 \leq \ln(8n^{1.5}) \tag{3}$$

It follows that:

$$\beta \leq \frac{5}{n^{1.25}} \frac{\ln(8n^{1.5})}{\ln(2)}$$

and hence when n is sufficiently large:

$$\beta \leq \frac{\ln(n^2)}{n^{1.25}} \tag{4}$$

A similar argument gives:

$$\alpha \leq \frac{\ln(n^2)}{n^{1.25}}$$

Exponentiating equation (**??**) gives:

$$e^{\rho} n^r e^{r\gamma} e^{\alpha} P = e^{\beta} Q$$

Assume that n is sufficiently large that $\rho, \alpha, \beta \leq 1$ and $|\gamma| \leq 1$. Then:

$$(n/e)^r \leq e^{\rho} n^r e^{r\gamma} e^{\alpha} P = e^{\beta} Q \leq eQ$$

By inequality (**??**) $Q \leq 8n^{1.25}$. It follows that for n sufficiently large $r < 2$.

However, $r \neq 0$ since otherwise:

$$e^{\alpha} P = e^{\beta} Q$$

Hence:

$$P \leq eQ \;\&\; Q \leq eP \tag{5}$$

Wlog assume that $P > Q$. Then:

$$P \leq Qe^{\beta} \leq Q(1 + \beta + \beta^2)$$

and so:

$$P - Q \leq Q(\beta + \beta^2)$$

But the left hand side is a positive integer so:

$$1 \leq Q(\beta + \beta^2)$$

Hence by (**??**) for n sufficiently large:

$$Q \geq \frac{n^{1.25}}{2\ln(n^2)}$$

Together with inequalities (**??**), this contradicts inequality (**??**) that $\ln(PQ) \leq \ln(8n^{1.25})$. Hence $r = 1$ and

$$e^{\rho} n e^{\gamma} e^{\alpha} P = e^{\beta} Q$$

Letting $\theta = \beta - \rho - \gamma - \alpha$:

$$nP = e^{\theta} Q$$

and for all sufficiently large n:

$$|\theta| \leq \frac{3\ln(n^2)}{n^{1.25}} \leq 1 \tag{6}$$

Assume $Q < Pn$, then:

$$nP = e^{\theta} Q \leq (1 + \theta + \theta^2)Q \leq (1 + \frac{3\ln(n^2)}{n^{1.25}})Q$$

Hence:

$$nP - Q \leq \frac{3\ln(n^2)}{n^{1.25}} Q \tag{7}$$

But $nP - Q$ is a positive integer, so:

$$1 \leq \frac{3\ln(n^2)}{n^{1.25}} Q$$

And therefore:

$$\frac{n^{1.25}}{3\ln(n^2)} \leq Q$$

But since $Q < Pn$:

$$\frac{n^{0.25}}{3\ln(n^2)}) \leq P$$

But since by inequality (**??**) $\ln(PQ) \leq \ln(8n^{1.5})$, it follows that:

$$Q \leq 24\ln(n^2) n^{1.25}$$

So by inequality (**??**):

$$nP - Q \leq \frac{3\ln(n^2)}{n^{1.25}} Q \leq 72\ln^2(n^2)$$

So there exists a positive integer $s = nP - Q$ such that $s \leq 72\ln^2(n^2)$. When n is sufficiently large, $s \leq \ln^{20}(2n^{1.25})$; hence s is supersmooth yielding the supersmooth congruence:

$$Q \equiv -s \bmod n$$

When $Pn < Q$ (by assumption on n, $(Pn, Q) = 1$ and hence $Pn \neq Q$) a similar argument (switching the roles of Pn and Q) yields the same result.

Thus by trying all possible γ, a 'supersmooth congruence' will be obtained.

It will be necessary to obtain many different supersmooth congruences. This will be accomplished by selecting random pairs of indices $1 \leq i \leq j \leq z$ and replacing V_0 by $V_0 + V_i + V_j$ and rerunning the algorithm above. Since there were at least $n^{1/8}/2^{1/10}$ squarefree-supersmooth pairs P, Q meeting the conditions described above, it is reasonable to assume that with high probability there exists some such pair with $p_i p_j | P$ (it seems possible that this assumption may be replaceable by a rigorous argument). It will then follow as above, that upon rerunning the algorithm such a P will be found. When $\ln^{20}(n^{1.25})$ random choices of i, j are tried, they are likely to yield distinct 'supersmooth congruences'. Finally we will make the 'standard' assumption that with high probability, after collecting $\ln^{20}(n^{1.25})$ such supersmooth congruences, linear algebra will yield a non trivial congruence of squares and hence a non-trivial factor of n. The complete factorization of n is then obtained by iteration.

3 Discussion

This result raises the possibility of using 'approximate' lattice reduction algorithms (e.g. L^3 [**?**]) to factor numbers. Whether 'lattice factorization' will be useful is unclear. L^3 does not always find the shortest vector in a lattice. In fact the best theoretical analysis suggest that sometimes the shortest vector it can produce will be longer that the true shortest by an 'exponential (in the dimension of the space)' multiplicative factor. For lattice factorization to be useful, it seems likely that either a more refined approach will be necessary or L^3 (or another algorithm) must in reality produce smaller vectors than the current analysis suggests.

Among the open problems which remain are the following. Is the lattice problem random polynomial time equivalent to factoring? Is the lattice problem in NP$\cap$ Co-NP? Is the lattice problem NP-complete. How 'good' an 'approximate' lattice reduction algorithm would be required to yield a factoring algorithm better than the best currently known. See [**?**] for additional information and references on factoring, lattice and other open problems of a number theoretic nature.

4 Acknowledgment

Schnorr long ago argued that an efficient method for finding smooth numbers above a given bound could improve factorization times. Odlyzko, recently revisited and refined Schnorr's results. It was interest in this approach which lead the author to begin considering lattices on logs. The author is grateful to Professor Ming-Deh Huang and Jonathan DeMarrais for their contributions to this paper.

5 Reference

References

[AM] Adleman L and McCurley K. ”Open problems in number-theoretic complexity II”, Proceedings of the 1994 Algorithmic Number Theory Symposium”, Ed. Adleman L and Huang M-D. Lecture Notes in Computer Science, Springer-Verlag 877 (1994).

[La] Lagarias J. ”The computational complexity of simultaneous diophantine approximation problems”, *SIAM Journal of Computing* 14:196-209 (1985).

[LLL] Lenstra A, Lenstra H and Lovász” L. ”Factoring polynomials with rational coefficients”, *Mathematische Annalen*261:515-534 (1982).

[No] Norton K.K. ”Numbers with small prime factors and the least kth power non-residue”, Mem. Amer. Math. Soc. 106 (1971).

[Po] Pomerance C. personal communication. (1995).

[Sc] Schnorr C. P. ”Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation”, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science* 13:172-181 (1993).