# DISCRETE LOGARITHMS AND FACTORING

Eric Bach[1]

Computer Science Division
University of California
Berkeley, CA 94720

## ABSTRACT

This note discusses the relationship between the two problems of the title. We present probabilistic polynomial-time reductions that show:

1) To factor $n$, it suffices to be able to compute discrete logarithms modulo $n$.

2) To compute a discrete logarithm modulo a prime power $p^e$, it suffices to know it mod $p$.

3) To compute a discrete logarithm modulo any $n$, it suffices to be able to factor and compute discrete logarithms modulo primes.

To summarize: solving the discrete logarithm problem for a composite modulus is exactly as hard as factoring and solving it modulo primes.

## 1. INTRODUCTION

The discrete logarithm problem is the following: given integers $a$ and $b$, relatively **prime to** $n$, we wish to solve

$$a^x \equiv b \pmod{n}.$$

In general, to find such an $x$ by known methods is quite slow; indeed, we could factor $n$ in an equal amount of time. Shanks in [8] presents an algorithm that will compute a discrete logarithm modulo $n$ in approximately $\sqrt{n}$ steps; this is about the time needed to factor $n$ by brute force. The fastest known method for discrete logarithms is that of Adelman [1]; it makes use of the Morrison-Brillhart factoring algorithm and has the same complexity : an expected running time that is $O(\exp(c \cdot \sqrt{\log n \log\log n}))$. These observations lead one to look for relationships between the two problems, and that is the subject of this paper.

To fix ideas, let us first consider the analogous problem of solving polynomial equations modulo $n$. The following things are known:

1) Solving polynomial congruences $f(x) \equiv 0 \pmod{n}$ is as hard as factoring $n$; this was proved for quadratic polynomials by Rabin in [7].

2) If one has a solution to $f(x) \equiv 0 \pmod{p}$ for a prime $p$, one can lift it to a solution modulo any power of $p$ in polynomial time; this follows from the proof of Hensel's lemma, see, e.g. [4].

---

[1]This research was sponsored by NSF Grant MCS 82-04506.

3) If we know the factorization of $n$, then we can take the solutions to $f(x)\equiv 0$ modulo $p$ for $p \mid n$ and produce a solution modulo $n$ in polynomial time by using the Chinese Remainder Theorem.

The analogous theorems are all true for exponential congruences $a^x \equiv b \pmod{n}$. More precisely, we prove:

a) If we can solve $a^x \equiv b$ modulo $n$ in polynomial time, then with high probability we can find a proper factor of $n$ in polynomial time. This reduction can be made deterministic if the Extended Riemann Hypothesis is true.

b) All of the difficulty in solving $a^x \equiv b$ modulo a prime power is in solving it modulo a prime; if a solution exists modulo $p^e$, we can get it in polynomial time from a solution modulo $p$.

c) If we can factor in polynomial time, then to quickly solve $a^x \equiv b$ modulo $n$, all we need are solutions modulo the prime divisors of $n$.

To summarize: solving the discrete logarithm problem for a composite modulus is exactly as hard as factoring and solving it modulo primes.

## 2. NOTATION AND BACKGROUND

In this paper "polynomial time" means time bounded by a polynomial in the number of bits needed to represent the input; in practical terms, this means that an algorithm that works modulo $n$ takes time bounded by a fixed power of $r \cdot \log n$, where $r$ is the number of input values.

$\mathbb{Z}$ is the integers, and $\mathbb{Z}_n$ is the ring of integers modulo $n$. The additive group of $\mathbb{Z}_n$ is written $\mathbb{Z}_n^+$, and its multiplicative group of units is written $\mathbb{Z}_n^*$. When $n$ is prime $\mathbb{Z}_n^*$ is a cyclic group; it is also cyclic if $n$ is a power of a prime greater than 2. The Euler $\phi$-function $\phi(n)$ is defined to be the number of elements in $\mathbb{Z}_n^*$.

If $n$ has the the prime factorization

$$n = p_1^{e_1} \cdots p_r^{e_r},$$

then the structure of $\mathbb{Z}_n$ is given by the Chinese Remainder Theorem:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}.$$

Both directions of this isomorphism are computable in polynomial time. To project $x$ onto the $i$th factor, we reduce $x$ modulo $p_i^{e_i}$. To go the other way, we use the following theorem: given any set of linear congruences

$$a_i \cdot x \equiv b_i \pmod{n_i}, i = 1, \ldots, k,$$

we can decide if they are consistent and if so, compute a solution, all in polynomial time.

$p$ will always denote a prime number. The Prime Number Theorem guarantees that there are enough of them: the $k$th one is asymptotic to $k \ln k$.

We define

$$\nu_p(x) = \max\{k : p^k \mid x\}.$$

$\nu_p(0)$ may be taken to be $+\infty$.

For real numbers $x$, $\lfloor x \rfloor$ denotes the largest integer $\leq x$, and $\log x$ means $\log_2(x)$.

## 3. HOW TO FACTOR BY COMPUTING DISCRETE LOGARITHMS

Assume that $n$ is an odd positive integer that is not a prime power (all of these conditions are checkable in random polynomial time); let its prime factorization be

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

Then

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^*.$$

Each direct factor is cyclic of order

$$\phi_i = (p_i - 1)\, p_i^{e_i - 1},$$

and so every element of this group has order dividing

$$\lambda = \operatorname{lcm}(\phi_1, \ldots, \phi_k).$$

The following theorem was proved (essentially) by Miller in [6] : assume that we can solve the congruence $a^x \equiv 1 \pmod{n}$ for some $x \neq 0$ in polynomial time (such an $x$ is called an *exponent* for $a$ ). Then if we select $a \in \mathbb{Z}_n^*$ at random, with probability $\geq 1/2$ we can use $a$ to find a proper factor of $n$ in polynomial time.

Here is how to do it : let

$$K = \{a \in \mathbb{Z}_n^* : a^{\lambda/2} \equiv \pm 1 \pmod{n}\}.$$

First, $K \neq \mathbb{Z}_n^*$, for we may as well assume that

$$\nu_2(p_1 - 1) \geq \nu_2(p_i - 1)$$

for all $i$, then let $a$ have order $\phi_1$ modulo $p_1^{e_1}$ and order $\phi_i/2$ modulo the other prime powers. We have now constructed one $a \notin K$, but by group theory we know more: if we select a random element of $\mathbb{Z}_n^*$, the odds are at least even that it is outside $K$.

If $a$ is such an element and $x$ is an exponent for it, then for some $k$, $0 < k < \log|x|$,

$$a^{x/2^k} \not\equiv \pm 1 \pmod{n}$$

but

$$(a^{x/2^k})^2 \equiv 1 \pmod{n}.$$

To see this, let $\alpha$ be the order of $a$ in $\mathbb{Z}_n^*$; we can write $\lambda = \alpha \cdot \beta_0$ and $x = \alpha \cdot \beta_1 \cdot 2^\nu$ for odd numbers $\beta_0$ and $\beta_1$. Then

$$a^{\lambda/2} \equiv a^{\beta_0 \lambda/2} \equiv a^{\alpha/2} \pmod{n},$$

and the result follows by taking $k = \nu + 1$.

It follows that

$$\gcd(n, (a^{x/2^k} + 1) \bmod n)$$

is a proper factor of $n$. Moreover, if $x$ is computed in polynomial time, it cannot be too large; we can therefore produce our factor quickly.

We now show how to find an exponent for $a$ by solving $a^x \equiv b \pmod{n}$; note that $b = 1$ will not help us as $x = 0$ is always a solution. We first need a prime $p \nmid \phi(n)$; we don't know $\phi(n)$ a priori, but we do know that it is less than $n$, and so among the first $\lfloor \log n \rfloor + 1$ primes there must be one that will work. Then such a $p$ is a unit mod $\phi$, and thus

$$(a^p)^y \equiv a \pmod{n}$$

has a solution $y$. If we put

$$x=py-1,$$

then $x\neq 0$, and $a^x\equiv 1$ as desired.

Two things should be noted. First, if the ERH is true, the above reduction can be made deterministic: we are factoring $n$ by finding an exponent for $a\notin K$, and the ERH implies that the least element outside $K$ is $O(\log n)^2$ ( see [2] ).

Second, Miller's argument works if we replace $\mathbb{Z}$ by the polynomial ring $k[X]$, for some finite field $k$. If $f\in k[X]$ has degree $r$ and $k$ has $q$ elements, then $\prod_{i=1}^{r}(q^i-1)$ is an exponent for any element in $(k[X]/(f))^*$. Thus, with almost no extra work, we also have a proof that polynomials over $k$ can be factored in random polynomial time ( see [3] ).

## 4. LIFTING SOLUTIONS TO A PRIME-POWER MODULUS

In this section assume that we have $x_1$ such that $a^{x_1}\equiv b(\mathrm{mod}\ p)$ for $a,b\in\mathbb{Z}_p^*$; we show how to compute $x$ such that $a^x\equiv b(\mathrm{mod}\ p^e)$ (if one exists) in polynomial time. For now, assume that $p\geq 3$; the algorithm for $p=2$ is slightly different and the modifications will be indicated later.

First, since $\mathbb{Z}_{p^e}^*$ is cyclic, we know that

$$\mathbb{Z}_{p^e}^*\cong\mathbb{Z}_p^*\times\mathbb{Z}_{p^{e-1}}^+.$$

The projection onto $\mathbb{Z}_p^*$ is given by reduction mod $p$, and it will be shown later that the projection $\theta$ onto $\mathbb{Z}_{p^{e-1}}^+$ is polynomial-time computable. Assuming this latter fact, then, we compute $x_2$ such that

$$x_2\cdot\theta(a)\equiv\theta(b)(\mathrm{mod}\ p^{e-1});$$

we already know $x_1$ such that

$$a^{x_1}\equiv b(\mathrm{mod}\ p).$$

We then find an integer $x$ that satisfies

$$x\equiv x_1(\mathrm{mod}\ p-1),$$

$$x\equiv x_2(\mathrm{mod}\ p^{e-1});$$

then $a^x\equiv b(\mathrm{mod}\ p^e)$.

It remains to show how to compute $\theta$. We have the factorization

$$\mathbb{Z}_{p^e}^*\cong\mathbb{Z}_p^*\times U,$$

where

$$U=\{x\in\mathbb{Z}_{p^e}^*:x\equiv 1(\mathrm{mod}\ p)\}.$$

The projection $\pi$ onto $U$ is given by raising an element to the $p-1$th power, and so we are done if we have a polynomial-time computable isomorphism $\lambda:U\to\mathbb{Z}_{p^{e-1}}^+$, for then we set $\theta=\lambda\circ\pi$. If we define $\lambda$ by

$$\lambda(x)=[\frac{x^{p^{e-1}}-1}{p^e}]\ \mathrm{mod}\ p^{e-1},$$

then we can compute it in polynomial time by evaluating the numerator inside brackets modulo $p^{2e-1}$.

We now show that $\lambda$ has the right algebraic properties. First, if $a,b\in\mathbb{Z}$, $\nu_p(a-b)\geq 1$, and $k\geq 1$, then

$$\nu_p(a^{p^k}-b^{p^k})=\nu_p(a-b)+k \qquad (*)$$

by induction on $k$. In particular, then, $p^e \mid a^{p^{e-1}}$ when $a\equiv 1(\mathrm{mod}\ p)$, so that $\lambda$ makes sense for integer arguments. It is well-defined as a function on $U$, for if $a\equiv b(\mathrm{mod}\ p^e)$, then

$$\frac{a^{p^{e-1}}-1}{p^e}\equiv\frac{b^{p^{e-1}}-1}{p^e}\ (\mathrm{mod}\ p^{e-1})$$

by (*). Using the identity

$$xy-1=(x-1)+(y-1)+(x-1)(y-1)$$

we can prove that it is a homomorphism from $U$ into $\mathbb{Z}^+_{p^{e-1}}$. Finally, to prove that it is an isomorphism, choose $a\in\mathbb{Z}$ such that $\nu_p(a-1)=1$. Then by (*), $\nu_p(a^{p^{e-1}}-1)=e$, so that the integer

$$\frac{a^{p^{e-1}}-1}{p^e}$$

is invertible modulo $p^{e-1}$. This implies that $\lambda$ is onto, and must therefore be an isomorphism.

Briefly, here are the modifications necessary for $p=2$. Assume that $e\geq 3$, then

$$\mathbb{Z}^*_{2^e}\cong S\times U,$$

where $S=\{\pm 1\}$ and $U=\{x:x\equiv 1(\mathrm{mod}\ 4)\}$. The projections onto $S$ and $U$ send $x$ to $\pm 1$ and $\pm x$, respectively, taking the $+$ sign when $x\equiv 1(\mathrm{mod}\ 4)$. $U$ is isomorphic to $\mathbb{Z}^+_{2^{e-2}}$ via

$$\lambda(x)=[\frac{x^{2^{e-1}}-1}{2^{e+1}}]\ \mathrm{mod}\ p^{e-2}.$$

This algorithm was presented in algebraic terms, but the intution behind it comes from analysis (see [4]). Say that integers $x$ and $y$ are "close" if they are identical modulo a power of $p$; the higher the power, the closer they are. Then we are seeking an approximation

$$a^x\sim b$$

If we had the right logarithm function $\lambda$, then we would expect that an approximation to

$$\frac{\lambda(a)}{\lambda(b)}$$

should be the required $x$. Amazingly enough, this "$p$-adic numerical analysis" works; by approximating the $p$-adic logarithm defined in [5], we get a fast algorithm.

## 5. GETTING A REGIONAL SOLUTION FROM LOCAL ONES

In this section we assume that all needed prime factorizations are available. Let the prime factorization of $n$ be

$$n=p_1^{e_1}\cdots p_r^{e_r},$$

and let $a,b\in\mathbb{Z}^*_n$. We want to take the "local" solutions $x_i$ to

$$a^{x_i}\equiv b(\mathrm{mod}\ p_i)$$

and produce the "regional" solution $x$ to

$$a^x\equiv b(\mathrm{mod}\ n).$$

By the results of the last section, we may assume that

$$a^{x_i} \equiv b \pmod{p_i^{e_i}},$$

and so we select $x$ to be congruent to $x_i$ modulo the order of $a$ in $\mathbb{Z}^*_{p_i^{e_i}}$, for $i=1, \ldots, r$.

The only thing left is to show how to compute the order of $a$ modulo a prime-power divisor $P$ of $n$. This is

$$\prod_{\substack{q \mid \phi(P) \\ q \text{ prime}}} q^{\nu_q(\text{order}(a))},$$

and

$$\nu_q(\text{order}(a)) = \min\{k : a^{\phi(P)/q^k} \equiv 1 \pmod{P}\}.$$

## 6. FINAL REMARKS

We have proved that the factorization of $n$ is necessary for solving discrete logarithm problems modulo $n$; one might ask also whether the factorization of $p-1$ is necessary for solving discrete logarithm problems modulo $p$. Conversely, one can ask for a fast algorithm for prime-modulus problems, assuming all needed factorizations. Both of these questions remain unanswered.

A traditional number-theoretic analogy is that "number fields" (e.g. $\mathbb{Q}$) are similar to "function fields" ( e.g. $\mathbb{Z}_p(X)$ ); the results of the first section indicate that we would do well to investigate this correspondence from the algorithmic point of view.

## 7. ACKNOWLEDGEMENTS

Manuel Blum got me interested in number theory, and in this problem in particular. Many people from the Berkeley TGIF seminar discussed these ideas with me: Po Tong read an earlier version of this paper, and Faith Fich, Shafi Goldwasser, Silvio Micali, Joan Plumstead, Jeff Shallit, Umesh and Vijay Vazirani, and Tim Winkler listened to many inchoate explanations of these results. To all of you, thanks!

## 8. REFERENCES

[1] Leonard Adelman, A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography, *Proceedings of the 1980 IEEE Symposium on Foundations of Computer Science,* pp. 55-60 (1980).

[2] Eric Bach, Fast Algorithms under the Extended Riemann Hypothesis: a Concrete Estimate, *Proceedings of the 14th Annual ACM Symposium on Theory of Computing,* pp. 290-295 (1982).

[3] David Cantor and Hans Zassenhaus, Factoring Polynomials over Finite Fields, *Mathematics of Computation 36,* pp. 587-592 (1981).

[4] Neal Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions,* New York: Springer (1977).

[5] Heinrich-Wolfgang Leopoldt, Zur Approximation des p-adischen Logarithmus, *Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg 25,* pp. 77-81 (1961).

[6] Gary Miller, Riemann's Hypothesis and Tests for Primality, *Journal of Computer and System Sciences 13,* pp. 300-317 (1976).

[7] Michael Rabin, *Digitalized Signatures and Public-Key Functions as Intractable as Factorization,* MIT Laboratory for Computer Science Report TR-212 (1979).

[8] Daniel Shanks, Class Number, a Theory of Factorization, and Genera, *Proceedings of the 1969 AMS Number Theory Institute,* pp. 415-440 (1969).