Random Equivalence of Factorization and Computation of Orders

Douglas L. Long

Princeton University
Department of
Electrical Engineering and Computer Science
Princeton, New Jersey 08544

ABSTRACT

The computation of orders of elements of the group of units of the set of residues modulo n is shown to be equivalent to factoring n in the following sense. The computation of orders is polynomially reducible to factorization. Factorization is randomly polynomially reducible to computation of orders.

1. Introduction

The group of units of the set of residues modulo an integer n, Z_n^*, plays an important role in number theory and its applications to computer science, particularly in recent developments in cryptography. This note deals with the problem of computing the order of an element of this group, i.e. finding the smallest positive integer k such that

$$a^k \equiv 1 \bmod n.$$

We will denote the order of a by $ord(a)$. If the factorization problem is solved then it is easy to compute $ord(a)$ so computing $ord(a)$ is only as hard as factorization.

On the other hand, we would like to be able to show that factorization is only as hard as computing orders. Towards this end, we present a probabilistic reduction of the factorization of n to the computation of orders in the group Z_n^*.

The reduction is in two parts. The first part is a probabilistic method of computing a number m using order computation. The second part is a probabilistic version of an algorithm of Miller which uses m to factor n.

2. Notation and Some Number Theory

Let (e,f) denote the greatest common divisor of e and f. If d divides n we will write $d \mid n$. The group Z_n^* consists of those a $(1 \le a < n)$ such that $(a,n) = 1$. If $n = p_1^{e_1} \cdots p_k^{e_k}$ then the size of Z_n^* is $\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{e_i}) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}$. The function $\lambda(n) = lcm(p_1 - 1, \ldots, p_k - 1)$. $\left(\frac{a}{p}\right)$ is the Jacobi symbol of $a \bmod p$.

Using elementary number theory we can prove the following

Lemma. If $n = p_1^{e_1} \cdots p_k^{e_k}$ and $d \mid \varphi(n)$ then the number of elements of order d is

$\sum \varphi(d_1)\cdots\varphi(d_k)$

where the sum is over k-tuples $(d_1,\cdots,d_k)$ such that $d_i \mid \varphi(p_i^{e_i})$ and $d=lcm(d_1,d_2,\ldots,d_k)$.

3. Divisors of $ord(a)$

Since $ord(a)$ divides $\varphi(n)$ we can find factors of $\varphi(n)$ by picking a random $a\in[2,n-1]$. If $(a,n)\neq 1$ then we have found a factor of n, which in turn gives us information about factors of $\varphi(n)$. If $(a,n)=1$ we can compute $ord(a)$ to find a factor of $\varphi(n)$. The probability of finding a particular factor is the subject of the next theorem.

Theorem 1. Suppose $n=p_1^{e_1}\cdots p_k^{e_k}$, and q^m is the largest power of the prime q which divides p_1-1. Then the number of elements of Z_n^* of order divisible by q^m, which we will denote by $\#(q^m)$, is

$$\#(q^m) \geq \frac{q-1}{q}\varphi(n)$$

Proof. From the Lemma we get the following expression for $\#(q^m)$.

$$\#(q^m) = \sum \varphi(f_1)\cdots\varphi(f_k)$$

where the sum is over k-tuples $(f_1,\ldots,f_k)$ such that $f_i \mid \varphi(p_i^{e_i})$ and $q^m \mid lcm(f_1,\ldots,f_k)$.

We can obtain a lower bound on $\#(q^m)$ by considering only the contributions to this sum where $f_1 = dq^m p_1^k$ where $d \mid p_1-1$ and $0\leq k\leq e_1-1$. We can rewrite our expression for $\#(q^m)$ as

$$\#(q^m) \geq \sum_{d \mid \frac{p_1-1}{q^m}} \varphi(dq^m)\left\{\sum_{j=0}^{e_1-1}\varphi(p_1^j)\left[\sum_{f_i \mid \varphi(p_i^{e_i})}\varphi(f_2)\cdots\varphi(f_k)\right]\right\}$$

$$\geq \frac{\varphi(q^m)}{q^m}(p_1-1)p_1^{e_1-1}\prod_{i=2}^{k}\varphi(p_i^{e_i}) = \frac{q-1}{q}\varphi(n)$$

A similar theorem holds for prime divisors of n.

~~Theorem~~ Corollary 2. If the factorization of n is as given above and $e_1>1$ then

$$\#(p_1^{e_1-1}) \geq \frac{p_1-1}{p_1}\varphi(n)$$

Proof. Similar to Theorem 2.

4. Computation of a multiple of $\lambda'(n)$

We first demonstrate a method of finding a multiple, m, of $\lambda'(n)$. We do this simply by picking a random a and computing $m=ord(a)$. We can place the following lower bound on the probability that this m is satisfactory. If $q^k \mid p_i-1$ then by Theorem 1 the probability that $q^k \mid ord(a)$ is greater than $\frac{q-1}{q}$. Thus

$$Prob(\lambda'(n)\mid m) \geq \prod_{q \mid \lambda'(n)}\left(\frac{q-1}{q}\right)$$

A lower bound can be placed on this probability. Given $\varepsilon>0$ there exists $N(\varepsilon)$ such that

$$Prob(\lambda'(n)\,|\,m) \geq (1-\varepsilon)\frac{\exp(-\gamma)}{loglog\ n} \quad \text{for } \lambda'(n) \geq N(\varepsilon).$$

(γ is Euler's constant.) See [Ap], pg 298. By choosing at most $O(loglog\ n)$ random numbers the probability that we will have a multiple of $\lambda'(n)$ is greater than one-half. Thus we have a probabilistic reduction of the computation of a multiple of $\lambda'(n)$ to computation of orders over Z_n^*.

5. Factoring n with a multiple of $\lambda'(n)$

Next we present a probabilistic version of an algorithm due to Miller which, if a multiple of $\lambda'(n)$ is known, will find a non-trivial factor of n with probability greater than one-half. Miller's algorithm is deterministic and will run in polynomial time if the Extended Riemann Hypothesis is true. We can remove this dependency on the ERH by introducing a random search rather than a deterministic search. Define $\#_2(n) = \max\{K : 2^K | n\}$. Suppose m is a multiple of $\lambda'(n)$.

Algorithm A. Pick a random a from the range $[1 \ldots n]$. Do the following until a factor is found.

(a) If $(a,n)\neq 1$ then a factor is found.

(b) For each $1\leq i\leq \#_2(m)$.

If $((a^{m/2^i} \bmod n) - 1, n)\neq 1$ then a factor is found.

(c) No factor has been found. Stop.

Theorem 3. Algorithm A will produce a factor with probability greater than one-half.†

This theorem has the immediate corollary that factorization is randomly polynomially reducible to the problems of computing multiples of $\varphi(n)$, $\lambda(n)$, or $\lambda'(n)$. Since the computation of a multiple of $\lambda'(n)$ is randomly polynomially reducible to computing orders over Z_n^* we can conclude that factorization is randomly polynomially reducible to computing orders.

Proof. Miller [M] gave conditions on a that will let Algorithm A find a factor. They are summarized in the following

Lemma (Miller). Suppose n is composite. Then either (1) or (2) holds for n.

(1) There exists a $p\,|n$ such that for any common a such that $\left(\frac{a}{p}\right) = -1$ then either a or $(a^{\lambda'(n)/2} \bmod n) - 1$ has a nontrivial divisor with n.

(2) Suppose $p\,|n$ and $q\,|n$. If $\left(\frac{a}{pq}\right)=-1$ then either a or $(a^{\lambda'(n)/2} \bmod n)-1$ has a nontrivial divisor with n.

The following holds for all n.

(3) If $p\,|n, \lambda'(n)\,|m$ and $k = \#_2[m/\lambda'(n)]+1$ then $a^{\lambda'(n)/2}\equiv a^{m/2^k} \bmod p$.

If (1) holds for n then $\left(\frac{a}{p}\right) = -1$ for exactly one-half the a less than n where in Z_n where $(a,p)=1$. If $p\,|a$ then $(a,n)=p$. Thus for more than half the $a<n$ Algorithm A will

†I am grateful to P. Flajolet at IRIA in France for pointing out this randomized version of Miller's algorithm to K. Lieberherr here at Princeton who in turn passed it on to me. The proof I give here is my own.

find a factor of n.

If (2) holds for n we must determine the size of $S = \{a : (a,n)=1$ and $\left[\frac{a}{p}\right]=1$ for all $p \mid n\} \cup \{a \mid (a,n)=1$ and $\left[\frac{a}{p}\right]=-1$ for all $p \mid n\}$. If $a \notin S$ then a choice of this a will cause Algorithm A find a factor of n. S is a proper subgroup Z_n^*. Since S is a proper subgroup its order must divide $\varphi(n)$ meaning $|S| \leq \frac{1}{2}\varphi(n)$. Thus at least half of the $a < n$ will produce a factor of n by Algorithm A.

Acknowledgement

I would like to express my appreciation to Professor Karl Lieberherr for his assistance with the preparation of this note.

References

[Ad] Adleman, L. and Manders, K., "Reducibility, Randomness and Intractability," *Proc. 9th Annual ACM Symposium on Theory of Computing*, (1977), pp.151-163.

[Ap] Apostol, T., *Introduction to Analytic Number Theory*, Springer-Verlag, New York/Berlin (1976).

[Ir] Ireland, K. and Rosen, M., *Elements of Number Theory*, Bogden & Quigley, Tarrytown-on-Hudson, New York (1972).

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

[R] Rabin, M., "Probabilistic Algorithms," *Algorithms and Complexity*, J. F. Traub, ed., Academic Press, New York (1976), pp. 21-38.

$S_1 \cup S_2$

$S_0 = \{a : (a,n)=1 \ \& \ \left[\frac{a}{p}\right]=1 \ \forall p \mid n\}$

$S_1 = \{a : (a,n)=1 \ \& \ \left[\frac{a}{p}\right]=-1 \ \forall p \mid n\}$