Shor's Algorithm and Factoring: Don't Throw Away the Odd Orders

Anna M. Johnston
Juniper Networks
amj at juniper dot net

February 6, 2017

Abstract

Shor's algorithm factors an integer N in two steps. The quantum step computes the order of $a \bmod N$ where a is relatively prime to N. The classical step uses this order to factor N. Descriptions of the classical step require the order, s, to be even and that $a^{s/2} \not\equiv -1 \bmod N$. If s is odd or $a^{s/2} \equiv -1 \bmod N$, then the quantum step is repeated. This paper describes how each prime divisor of the order s, not just 2, can be used to factor N.

1 Sketch of Shor's Algorithm

Shor's[4] algorithm factors a composite integer N, which is not a non-trivial power, in two steps. The first step uses quantum computing to find the order of some integer a modulo N, where $\gcd(a, N) = 1$. In other words, this step finds the smallest positive integer s such that $a^s \equiv 1 \bmod N$.

The second step uses the order, s, and classical techniques to factor N. If s is odd or $a^{s/2} \equiv -1 \bmod N$, then the quantum step is repeated. Otherwise, let $b_2 \equiv a^{s/2} \bmod N$, and notice that b_2 has order 2 modulo N. In other words, $b_2^2 \equiv 1 \bmod N$ and

$$\left(b_2^2 - 1\right) \equiv \left(b_2 - 1\right)\left(b_2 + 1\right) \equiv 0 \bmod N.$$

A non-trivial factorization of N is

$$N = \gcd(\left(b_2 - 1\right), N) \gcd(\left(b_2 + 1\right), N).$$

2 How the Classical Step Works

The classical step can be understood in two ways:

1. Factorization of a simple quadratic: Since $(b_2)^2 - 1 \equiv 0 \bmod N$, we know that $(b_2+1)(b_2-1) \equiv 0 \bmod N$. b_2 is not 1 or -1, so neither is 0 mod N and their GCD's must completely factor N.

2. Da Yen (Sun Tsu's theorem/Chinese remainder theorem): Let N factor into two non-trivial, relatively prime integers $N = AB$. This is guaranteed by the fact that N is composite and not a non-trivial power.

   The da yen [1][2] states that $\mathbb{Z}/N\mathbb{Z}$ is isomorphic to $\mathbb{Z}/A\mathbb{Z} \times \mathbb{Z}/B\mathbb{Z}$. Integers modulo N can be represented as a pair of integers, one modulo A and one modulo B:

   $$v \bmod N \cong [v_A \bmod A, v_B \bmod B] \,.$$

   Operations modulo N are equivalent to operations $[\text{mod}A, \text{mod}B]$.

   For every prime p dividing N, $b_2 \equiv \pm 1 \bmod p$. It is fairly easy to show that for every p^k dividing N, if $b_2 \equiv 1 \bmod p$ then $b_2 \equiv 1 \bmod p^k$, and if $b_2 \equiv -1 \bmod p$ then $b_2 \equiv -1 \bmod p^k$. Let $N = AB$ where A is the product of all prime powers with $b_2 \equiv 1$ and B the product of all prime powers with $b_2 \equiv -1$. Then

   $$(b_2 - 1) \bmod N \cong [0 \bmod A, -2 \bmod B]$$
   $$(b_2 + 1) \bmod N \cong [2 \bmod A, 0 \bmod B]$$

   and $\gcd((b_2 - 1 \bmod N), N) = A$ and $\gcd((b_2 + 1 \bmod N), N) = B$.

3 Beyond Even Orders

Using the da yen, any prime factor of s (the order of $a \bmod N$), not just 2, can be used in a similar way to factor N. If r is a prime divisor of s, we can compute an element of order r: $b_r \equiv a^{s/r} \bmod N$. For any divisor of N, the order of b_r must be either r or 1 since r is prime. Just as was done for $r = 2$, N can be factored into the prime powers for which b_r have order 1 and the prime powers which have order r. If $N = AB$ where $b_r \equiv 1 \bmod A$ and $b_r \not\equiv 1 \bmod B$, then:

$$b_r - 1 \bmod N \cong [0 \bmod A, h - 1 \bmod B] \tag{1}$$

where $h \not\equiv 1 \bmod B$. Just as before,

$$\gcd((b_r - 1), N) = A. \tag{2}$$

Unlike the case when $r = 2$, taking the GCD of $(b_r + 1)$ and N will not yield a factor.

Instead of throwing out the order s if it is odd or if $a^{s/2} \equiv -1 \bmod N$, elements b_r for other prime divisors should be computed and used to factor (equation 2). This significantly reduces the probability that the very expensive quantum step of the algorithm will have to be repeated, thus significantly reducing the overall cost of the algorithm.

4 A Probabilistic Problem

A problem arose when $r = 2$ and $a^{s/2} \equiv -1 \bmod N$. In this case the A portion of the factorization was trivial: $A = 1$ and $B = N$. The same problem can happen for other prime divisors r of s. However if r does not divide N, the probability of this problem occurring goes to zero as r goes to infinity. In other words, larger prime divisors of s have probability near 1 of generating a factor of N.

An element of order r exists modulo N if and only if r divides $\lambda(N)$[1]. Assume that r does not divide N and that $b_r \equiv a^{s/r} \bmod N$ is an element of order r. Then:

- r divides $(p - 1)$ for at least one prime divisor of N.
- If r does not divide $(q - 1)$ for some prime factor q of N, then there are no elements in $\mathbb{Z}/q^t\mathbb{Z}$, for any $q^t \,|N$, which have order r. This implies that the order of $b_r \bmod q^t$ is one, and that $b_r \equiv 1 \bmod q^t$.

Failure to factor using an element of order r (including the case where $r = 2$), b_r, implies that there does not exist a non-trivial factor A of N such that $b_r \equiv 1 \bmod A$. This implies

[1] Recall that Euler's totient function of a prime power is $\phi(p^e) = (p-1)\,p^{e-1}$ and the reduced totient function is $\lambda(N) = LCM\big(\{\phi(p_j^{e_j})\}\big) = LCM\Big(\Big\{(p_j - 1)p_j^{e_j - 1}\Big\}\Big)$, where p_j are all prime divisors of N and $p_j^{e_j} \,\|N$.

that for every prime q dividing N, r divides $(q-1)$. If $r=2$ and N is odd, then r will divide $(q-1)$ for every factor q of N. But when $r>2$, the probability of r dividing $(q-1)$ is $\frac{1}{r}$. The probability of failure goes to zero as the the size of r and/or the number of distinct prime divisors of N increases.

Factorization will succeed using an element of order s only if there exists a prime factor r of s such that b_r is a *factorable r-th root of unity* modulo N.

Definition 4.1 (Factorable r-th root of Unity)**:** A factorable r-th root of unity is an element b_r mod N of prime order r such that

1. $N = AB$ with $\gcd(A, B) = 1$;

2. $b_r \equiv 1 \bmod A$ and $b_r \not\equiv 1 \bmod B$.

5 Probability of Factorable Order for RSA Moduli

For simplicity, this probability lemma applies only to RSA moduli of the form $N = pq$ where p, q are distinct primes.

Lemma 5.1 (Probability of factorable r-th root of Unity)**:** Let $N = pq$, b_r be a non-trivial r-th root of unity mod N with p, q, r prime integers and $p, q > 2$. Then the probability that b_r is a factorable r-th root of unity is:

$$pr(b_r \text{ is factorable}) = \begin{cases} \frac{2}{3} & r = 2 \\ \frac{r^2}{\left(r^2 + \frac{(r-1)}{2}\right)} & r > 2 \end{cases}$$

Proof. Since the order of b_r is r and $N = pq$ with p, q, r prime, we know that r divides $(p-1)$ and/or $(q-1)$.

- The probability that r divides both $(p-1)$ and $(q-1)$, given that $r > 2$ (it will divide both if $r = 2$) and it divides at least one of them, is

$$\begin{aligned} pr\Big((r\,|p-1)\bigcap(r\,|q-1)\,\Big|(r\,|p-1)\bigcup(r\,|q-1)\Big) &= \frac{\left(\frac{1}{r^2}\right)}{\left(\frac{2r-1}{r^2}\right)} \\ &= \frac{1}{2r-1} \end{aligned}$$

- If r divides both $(p-1)$ and $(q-1)$, the probability that b_r is a factorable root of unity is $pr(b_r\text{factorable}\,|(r\,|(p-1)\,)\bigcap(r\,|(q-1)\,)\,)=\frac{2}{r+1}$:
  - the number of $b_r \in \mathbb{Z}/N\mathbb{Z}$ where b_r has order r, $h_p \equiv 1$, $h_q \not\equiv 1$ is $(r-1)$;
  - the number of $b_r \in \mathbb{Z}/N\mathbb{Z}$ where b_r has order r, $h_p \not\equiv 1$, $h_q \equiv 1$ is $(r-1)$;
  - the number of $b_r \in \mathbb{Z}/N\mathbb{Z}$ where b_r has order r is (r^2-1);
  - $pr(b_r\text{factorable}\,|(r\,|(p-1)\,)\bigcap(r\,|(q-1)\,)\,)=\frac{2(r-1)}{r^2-1}=\frac{2}{r+1}$
- If r does not divide both $(p-1)$ and $(q-1)$, then it is a factorable r-th root of unity. The only orders $(b_r \bmod p)$ and $(b_r \bmod q)$ can have is r or 1 since the order of b_r is r and r is prime. If r does not divide $(p-1)$ then there is no element of order r in $\mathbb{F}_p$, and $b_r \equiv 1 \bmod p$. $b_r \not\equiv 1 \bmod q$, otherwise $b_r \equiv 1$, and b_r must be factorable. The same argument holds if r does not divide $(q-1)$.

Therefore

$$pr(b_r \text{ is factorable}) = \begin{cases} 0+\frac{2}{2+1} & r=2 \\ \frac{(2r-2)}{(2r-1)}\cdot 1+\left(\frac{1}{(2r-1)}\right)\left(\frac{2}{(r+1)}\right) & r>2 \end{cases}$$
$$= \begin{cases} \frac{2}{3} & r=2 \\ \frac{r^2}{\left(r^2+\frac{(r-1)}{2}\right)} & r>2 \end{cases}$$

□

5.1 Comment for Sophie Germain Primes or Unfactorable Orders

If the RSA modulus was generated with Sophie Germain primes and $N = pq$, $p = 2p_1 + 1$, $q = 2q_1 + 1$ where p_1, q_1 are both prime. For these moduli, most elements have order divisible by both p_1 and q_1. If the order returned one of the large primes, say p_1, then you know $p = 2p_1 + 1$ and can factor. If the order returned is $s = p_1 q_1$, then $p_1 + q_1 = \frac{N-4s-1}{2}$ and you can factor:

$$q_1 \in \left\{ \frac{\frac{N-4s-1}{2} \pm \left(\frac{(N-4s-1)^2}{4} - 4s\right)^{1/2}}{2} \right\}$$

What if N is not the product of two Sophie-Germain primes but returned order s is a large composite with no small prime factors? In this case, we still have that s is a large factor of the reduced totient function $\lambda(N)$. Alternate classical methods can use this information to factor. For example, Pollard's $(p-1)$ algorithm [3] can be run using this knowledge to insure the large prime factor does not divide the order of the element used. The resulting element is guaranteed to have a smaller order, significantly improving the run time of the algorithm.

6 Examples

The following small examples show how to factor if the quantum step of Shor's algorithm returns an odd order or a previously unusable even order. The first example assumes the quantum step returned an even order for which b_2 fails to factor. The second example uses the more common base of 2, but the quantum step returns an odd order.

6.1 Factor $N = 3304283$

Assume the quantum step of the algorithm returned the order of 751228 as $78 = 2 \cdot 3 \cdot 13$. This order is even, however $751228^{78/2} \equiv -1 \bmod N$.

Three primes (2, 3, 13) divide the factorization the order: $78 = 2 \cdot 3 \cdot 13$. This gives three possible factorable roots of unity. While b_2 fails to factor, b_3 and b_{13} return factors of N.

r	b_r	$\gcd(b_r - 1, N)$
2	$751228^{39} \equiv 3304282 \equiv -1$	1
3	$751228^{26} \equiv 1590268$	1847
13	$751228^{6} \equiv 1511706$	1789

6.2 Factor $N = 152942113$

Assume the quantum step of the algorithm returned the order of 2 as $4247705 = 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 59$. Five primes (5, 7, 11, 17, 59) divide the order. This gives five possible factorable roots of unity.

r	b_r	$\gcd(b_r - 1, N)$
5	$2^{849541} \equiv 84438464$	12343
7	$2^{606815} \equiv 3702901$	12343
11	$2^{386155} \equiv 121345064$	12391
17	$2^{249865} \equiv 93564442$	12391
59	$2^{71995} \equiv 124763045$	12343

7 Conclusion

This paper described an extension of the classical step of Shor's algorithm. Previous recommendations have been to re-run the costly quantum step of the algorithm if it returned an odd order or an unusable even order.

This paper explains how to use any odd prime divisor of the order in the classical step, minimizing the need to repeat the quantum step. Not only is there no need to throw out odd orders returned by the quantum step, but a single returned order, depending on its factorization, allows multiple attempts at factoring N.

References

[1] Thomas W. Hungerford, *Algebra*, ch. III, pp. 131–133, Springer-Verlag, 175 Fifth Avenue, New York, New York 10010, U.S.A., 1974.

[2] Ulrich Libbrecht, *Chinese mathematics in the thirteenth century*, 1 ed., ch. 15, pp. 271–274, Dover, 31 East 2nd Street, Mineola, NY 11501, 2005.

[3] J.M. Pollard, *Theorems on factorization and primality testing*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 76(3), 1974, pp. 521–528.

[4] Peter W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, Journal on Computing **26** (1997), no. 5, 484–1509.