Shor's Algorithm Base Range Reduction: Symmetry of Successful Bases

[Preprint]

Muhammad Saad Bhatti
Department of Electrical Engineering
NED University of Engineering and Technology, Karachi
Email: bhatti150201@gmail.com

Abstract

Shor's algorithm factors large integers in polynomial time by reducing the problem to finding the order of a randomly chosen base modulo N. The algorithm succeeds when the chosen base a has an even order and avoids a trivial root of -1. In this paper, we prove a symmetry property: if a is a successful base for Shor's algorithm, then so is $N - a$. This symmetry implies that successful bases always occur in pairs, allowing us to restrict the search range of bases to less than $N/2$ without loss of generality.

1 Introduction

The discovery of Shor's algorithm revolutionized computational number theory and cryptography by showing that large integers can be factored efficiently on a quantum computer. The core step of the algorithm is the order-finding subroutine, where one chooses an integer a with $1 < a < N$ and $\gcd(a, N) = 1$, then determines the order $r = \mathrm{ord}_N(a)$.

The algorithm succeeds if r is even and $a^{r/2} \not\equiv -1 \pmod{N}$. These conditions ensure that nontrivial factors of N can be extracted via the greatest common divisor (gcd). In practice, the algorithm succeeds with high probability, but the precise structure of the successful bases is of mathematical interest.

In this paper, we prove that successful bases always occur in pairs of the form a and $N - a$. This symmetry property, though often overlooked, has implications for both the analysis and implementation of Shor's algorithm.

2 Preliminaries

Definition 1 (Order modulo N)**.** *For $a \in \mathbb{Z}$ with $\gcd(a, N) = 1$, the order of a modulo N, denoted $\mathrm{ord}_N(a)$, is the smallest positive integer r such that $a^r \equiv 1 \pmod{N}$.*

Definition 2 (Successful base)**.** *A base a with $1 < a < N$ and $\gcd(a, N) = 1$ is called a* successful base *for Shor's algorithm if:*

1. *$r = \mathrm{ord}_N(a)$ is even, and*
2. *$a^{r/2} \not\equiv -1 \pmod{N}$.*

3 Main Result

We now state and prove the central theorem of this paper.

Theorem 1 (Symmetry of Successful Bases)**.** *If a is a successful base for Shor's algorithm, then $N - a$ is also a successful base. Moreover,* $\mathrm{ord}_N(N-a) = \mathrm{ord}_N(a)$.

Proof. Let $r = \mathrm{ord}_N(a)$. Since r is even, we compute:

$$(N-a)^r \equiv (-a)^r = (-1)^r a^r \equiv a^r \equiv 1 \pmod{N}.$$

Thus $\mathrm{ord}_N(N-a)$, say s, divides r.

Suppose $s < r$. If s is even, then $a^s \equiv 1$, contradicting minimality of r. If s is odd, then $(-a)^s \equiv 1$ implies $a^s \equiv -1$. Squaring gives $a^{2s} \equiv 1$, so r divides $2s$. Since $s < r$ and s odd, we must have $2s = r$. But then $a^{r/2} \equiv -1$, contradicting the success condition. Hence $s = r$.

Finally, check the second success condition:

$$(N-a)^{r/2} \equiv (-a)^{r/2} = (-1)^{r/2} a^{r/2}.$$

If $r/2$ is even, this equals $a^{r/2} \not\equiv -1$. If $r/2$ is odd, it equals $-a^{r/2}$. If this were -1, then $a^{r/2} \equiv 1$, contradicting minimality of r. Thus $(N-a)^{r/2} \not\equiv -1$ in all cases.

Therefore, $N - a$ is also a successful base with the same order r. □

4 Consequences

The theorem shows that successful bases are always paired as $\{a, N-a\}$. As a result, the distribution of successful bases is symmetric about $N/2$. This means that the search for successful bases can be restricted to the range $1 < a < N/2$, effectively halving the domain without changing the probability of success.

5 Conclusion

We proved that if a is a successful base for Shor's algorithm, then so is $N - a$, and both share the same order. This symmetry doubles our understanding of the structure of successful bases and confirms that success probabilities remain unchanged if one samples bases only from half the range.

Future work may extend this symmetry analysis to explore other structural patterns in the distribution of bases, shedding light on the deeper algebraic features underlying Shor's algorithm.

6 Discussion

To the best of our knowledge, this symmetry property has not been explicitly stated in the existing literature on Shor's algorithm. While the underlying group-theoretic facts are standard, a structured search of `arXiv`, Google Scholar, and related databases using queries such as "Shor base symmetry," "$N - a$ order," and "restricting base range in Shor's algorithm" did not reveal prior work presenting this corollary in the context of quantum factoring. We therefore offer this note as a clarification of an implicit but useful observation, highlighting its direct consequence of halving the range of bases that must be considered.