IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 13, Issue I Ver. VI (Jan. - Feb. 2017), PP 37-41
www.iosrjournals.org

Algorithm Design and Implementation for a Mathematical Model of Factoring Integers

Jianhui LI
Department of Computer Science, Guangdong Neusoft Institue,
Foshan City, Guangdong Province, PRC, 528200

Abstract: *Based on an approximate formula of factoring an odd composite number, the article deduces a distribution for factors in big odd composite number and designs an algorithm to pick up the factors. Mathematical deduction is presented in detail and numerical experiment is made on some big numbers. Experiment shows that the algorithm is as efficient as the Pullard's Rho algorithm for conventional numbers.*

Keywords: *Integer factorization, Algorithm design, numerical experiments*
MSC 2000: 11A51,010108

I. Introduction

Factorization of integers has been an unsolved problem ever since the ancient time. Form the old trial approach and the Fermat approach to modern approach of number field sieve, human being have tried colorful efforts to solve the problem, as summarized in article [1]. Nevertheless, a better resolution has been appealed from both mathematicians and researchers of information security. Consequently, study of the problem never ceased. Recent years, literatures on the problem can frequently be seen in several occasions. In article [2], Jongsoo Park and Mathology Sys tried to do factorization using multiplication table; in article [3], W Aldrin, Wanambisi Shem Aywa, Cleophas Maende and Geoffrey Muchiri Muketha raised a mathematical model, namely a formula, to approximate factors of a composite number. In article [4] and [5], WANG built sieves of odd composite numbers and obtain approaches to factorize large numbers via factorization of small numbers. Articles [6] and [7] put a new approach to analyze odd numbers by binary tree and obtained new criterions for prime numbers and factorization of odd numbers. It can see that, article [3] did not give an algorithm or a detail procedure to realize the mathematical model though it presented a few special samples to demonstrate the correctness of the formula. Meanwhile, an algorithm called sequential searching algorithm in article [7] is a little slower than the Pollard's rho algorithm. Therefore, it is worth to have a try to an algorithm that can make the idea in article [3] realizable in a relative speed. This article mainly combines the mathematical model in article [3] with the sequential algorithm in article [7]. An algorithm is designed and relative tests are made. Experiments show that, the combined algorithm is as efficient as the Pullard's Rho algorithm.

II. Preliminaries

2.1 Symbols and Notations

This article continues using the symbols and notations that are given in article [7] unless specially commented.

2.2 Lemmas

Lemma 1 (see in [3]). *Let $m = pq$ be a large composite integer of decimal digit length $l \geq 5$ and difference $|p-q| = d \geq 0$; then the prime factors p and q are approximately $p = \sqrt{m+(\frac{d}{2})^2} - \frac{d}{2}$ and $q = \sqrt{m+(\frac{d}{2})^2} + \frac{d}{2}$.*

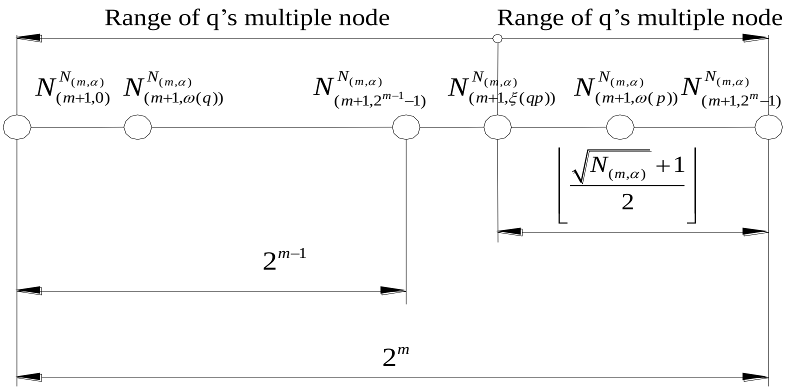
Lemma 2(see in [7]). *Let $N_{(m,\alpha)} = pq$ be an odd composite number such that $2^{m+1}+1 \leq N_{(m,\alpha)} \leq 2^{m+2}-1$ and $m > 2$, where p and q are odd coprimed numbers that fit $3 \leq p < q$; let symbols $N_{(m+1,0)}^{N_{(m,\alpha)}}$ and $N_{(m+1,2^m-1)}^{N_{(m,\alpha)}}$ be respectively the leftmost and the rightmost nodes on level m+1 in the left branch of $T_{N_{(m,\alpha)}}$; let $N_{(m+1,\omega(q))}^{N_{(m,\alpha)}}$ and $N_{(m+1,\omega(p))}^{N_{(m,\alpha)}}$ indicate respectively the first q's and p's multiple-nodes left to $N_{(m+1,2^m-1)}^{N_{(m,\alpha)}}$, $N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}}$ be the node that is left to and $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ nodes away from $N_{(m+1,2^m-1)}^{N_{(m,\alpha)}}$, and $N_{(m+1,2^{m-1}-1)}^{N_{(m,\alpha)}}$ be the mid-node that is right to and 2^{m-1} nodes away from $N_{(m+1,0)}^{N_{(m,\alpha)}}$; then it holds*

(1) Nodes $N_{(m+1,2^m-1)}^{N_{(m,\alpha)}} = 2^{m+1}N_{(m,\alpha)} - 1$;

(2) There are exact $\frac{p+1}{2}$ *nodes from* $N^{N_{(m,\alpha)}}_{(m+1,\omega(p))}$ *to* $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$ *and exact* $\frac{q+1}{2}$ *nodes from* $N^{N_{(m,\alpha)}}_{(m+1,\omega(q))}$ *to* $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$*;*

(3) the distribution of $N^{N_{(m,\alpha)}}_{(m+1,0)}$, $N^{N_{(m,\alpha)}}_{(m+1,\omega(q))}$, $N^{N_{(m,\alpha)}}_{(m+1,2^{m-1}-1)}$, $N^{N_{(m,\alpha)}}_{(m+1,\xi(qp))}$, $N^{N_{(m,\alpha)}}_{(m+1,\omega(p))}$ *and* $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$ *on level m+1 is as figure 1 illustrates.*

Fig.1 Distribution of Critical Nodes (m>2)



Lemma 3(see in [8]) *The floor function of a real number x, denoted by* $\lfloor x \rfloor$ *that is defined by* $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$ *satisfies*

(1) $\lfloor x \rfloor - \lfloor y \rfloor - 1 \le \lfloor x - y \rfloor \le \lfloor x \rfloor - \lfloor y \rfloor$

(2) $\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor$

(3) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ *for integer n.*

III. Theoretic Conclusions and Proofs

Corollary 1. *Let* $N_{(m,\alpha)} = pq$ *be an odd composite such that* $2^{m+1}+1 \le N_{(m,\alpha)} \le 2^{m+2}-1$ *and* $m > 2$*, where p and q are odd numbers that fit* $3 \le p < q$*; then* $2^{m-2}+2 \le q-p \le 2^{m+1}-6$.

Proof. By Lemma 2, it is easily to know $2^{m-1} \le \frac{q+1}{2} \le 2^m$, namely, $2^m - 1 \le q \le 2^{m+1}-1$. Similarly, it yields

$$1 \le \frac{p+1}{2} \le \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \le \frac{\sqrt{2^{m+2}-1}+1}{2} < 2^{\frac{m}{2}} + \frac{1}{2}$$

That is

$$3 \le p \le 2^{\frac{m}{2}+1} - 1 \Rightarrow -2^{\frac{m}{2}+1} + 1 \le -p \le 3$$

Thus

$$2^m - 2^{\frac{m}{2}+1} \le q - p < 2^{m+1} - 4$$

Note that, when m>2 it yields

$$\frac{2^m - 2^{\frac{m}{2}+1}}{2^{m-2}} = 4 - 2^{3-\frac{m}{2}} = 4 - \frac{8}{2^{\frac{m}{2}}} > 1$$

Consequently

$$2^{m-2} < q - p < 2^{m+1} - 4$$

Since *p* and *q* are both odd numbers, the corollary obviously holds.

□

Corollary 2. *Let m>2 and* $N_{(m,\alpha)} = pq$ *be a large composite integer of decimal digit length* $l \ge 5$ *and difference* $|p-q| = d \ge 0$*; then p and q respectively are divisors of nodes in intervals* $[N^{N_{(m,\alpha)}}_{(m+1,I_q^L)}, N^{N_{(m,\alpha)}}_{(m+1,I_q^R)}]$ *and* $[N^{N_{(m,\alpha)}}_{(m+1,I_p^L)},\ N^{N_{(m,\alpha)}}_{(m+1,I_p^R)}]$*, where*

$I_q^L = 2^{m-1} - 1 - \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m - 3)^2} \right\rfloor$

$I_q^R = 2^m - 1 - \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^{m-3} + 1)^2} + 2^{m-4} \right\rfloor$

$I_p^L = 2^{m-1} - \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m - 3)^2} - 2^{m-4} \right\rfloor$

$I_p^R = 2^{m-1} - \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^{m-3} + 1)^2} \right\rfloor$

Proof. By Lemma 1, *p* and *q* are approximately calculated respectively by

$$p = \sqrt{N_{(m,\alpha)} + (\frac{d}{2})^2} - \frac{d}{2} \text{ and } q = \sqrt{N_{(m,\alpha)} + (\frac{d}{2})^2} + \frac{d}{2}$$

Therefore it yields

$$\frac{p+1}{2} = \frac{1}{2}\sqrt{N_{(m,\alpha)} + (\frac{d}{2})^2} - \frac{d}{4} \text{ and } \frac{q+1}{2} = \frac{1}{2}\sqrt{N_{(m,\alpha)} + (\frac{d}{2})^2} + \frac{d}{4}$$

Let $D_p = \frac{p+1}{2}$ and $D_q = \frac{q+1}{2}$; from $2^{m-2} + 2 \le q - p \le 2^{m+1} - 6$, then it yields

$$\frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^{m-3}+1)^2} + \frac{2^{m-3}+1}{2} \le D_q \le \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} + \frac{2^m-3}{2} \quad (1)$$

$$\frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^{m-3}+1)^2} - \frac{2^m-3}{2} \le D_p \le \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} - \frac{2^{m-3}+1}{2} \quad (2)$$

By Lemma 3, it yields

$$\left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^{m-3}+1)^2} + \frac{2^{m-3}+1}{2} \right\rfloor \le D_q < \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} + \frac{2^m-3}{2} \right\rfloor + 1 \quad (3)$$

and

$$\left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^{m-3}+1)^2} + \frac{2^m-3}{2} \right\rfloor \le D_p < \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} + \frac{2^{m-3}+1}{2} \right\rfloor + 1 \quad (4)$$

Now simplify the inequalities (1) and (2). Note that

$$\begin{aligned}
\left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} + \frac{2^m-3}{2} \right\rfloor &= \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} + 2^{m-1} - 2 + \frac{1}{2} \right\rfloor \\
&= \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} + \frac{1}{2} \right\rfloor + 2^{m-1} - 2 \\
&= \left\lfloor \sqrt{N_{(m,\alpha)} + (2^m-3)^2} \right\rfloor - \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} \right\rfloor + 2^{m-1} - 2 \\
&\le \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} \right\rfloor + 2^{m-1} - 1
\end{aligned}$$

it knows

$$D_q \le \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} \right\rfloor + 2^{m-1} \quad (5)$$

Similarly it yields

$$D_q \ge \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^{m-3}+1)^2} + 2^{m-4} \right\rfloor \quad (6)$$

and

$$\left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^{m-3}+1)^2} \right\rfloor - 2^{m-1} + 1 \le D_p \le \left\lfloor \frac{1}{2}\sqrt{N_{(m,\alpha)} + (2^m-3)^2} - 2^{m-4} \right\rfloor + 1 \quad (7)$$

Now consider D_p and D_q are number of nodes left to the node $N_{(m+1,2^m-1)}^{N_{(m,\alpha)}}$, the corollary surely holds when translating D_p and D_q into I_p^L, I_p^R, I_q^L and I_p^R.

□

IV. Algorithm Design and Experiments

According to the corollaries that are proved in previous section, algorithm to search p and search p (SpSq) for factorization of odd numbers can be designed and experiments can be made as follows.

4.1 Algorithm Design

======== SpSq Algorithm=========

Input: Odd composite number $N_{(0,0)}$

Step 1. Calculate searching level: $K = \lfloor \log_2 N_{(0,0)} \rfloor - 1$;

Step 2. Calculate: $I_q^L = 2^{m-1} - 1 - \left\lfloor \frac{1}{2}\sqrt{N_{(0,0)} + (2^K - 3)^2} \right\rfloor$,

$$I_q^R = 2^K - 1 - \left\lfloor \frac{1}{2}\sqrt{N_{(0,0)} + (2^{K-3} + 1)^2} + 2^{K-4} \right\rfloor,$$

$$I_p^L = 2^{K-1} - \left\lfloor \frac{1}{2}\sqrt{N_{(0,0)} + (2^K - 3)^2} - 2^{K-4} \right\rfloor,$$

$$I_p^R = 2^{K-1} - \left\lfloor \frac{1}{2}\sqrt{N_{(0,0)} + (2^{K-3} + 1)^2} \right\rfloor;$$

Step 3. Calculate reference node: $ul = N^{N_{(0,0)}}_{(K,2^{K-1}-1)} = 2^{K+1}N_{(0,0)} - 1$;

Step 4. Calculate: $I_p^L = ul - 2I_p^L, I_p^R = ul - 2I_p^R$, $I_q^L = ul - 2I_q^L, I_q^R = ul - 2I_q^R$;

Step 5. Search in $[I_p^L, I_p^R],[I_q^L, I_q^R]$ the first odd number that has common divisor with $N_{(0,0)}$.

===============End of Algorithm ==============

4.2 Numerical Experiments

To test the new algorithm, numerical experiments are made on a Dell PC with 2.99Ghz CPU and 8G memories. For comparative purpose, 10 big numbers are tested by both Pullard's Rho algorithm and the new algorithm designed previously and the results are list in table 1. Seen from figure 2, it knows that, the two algorithms are almost equally efficient.

Table 1 Experiment on Some Big Integers

N's Factorization	Computing time(in seconds)	
	Pollard's Rho	SpSqAlgorithm
N1= 1123877887715932507=299155897×3756830131	*15*	*70*
N2=1129367102454866881=25869889×43655660929	*1*	*4*
N3=29742315699406748437=372173423×79915205819	*139*	*5*
N4=35249679931198483=59138501×596052983	*4*	*16*
N5=208127655734009353=430470917×483488309	*148*	*190*
N6=331432537700013787=114098219×2904800273	*14*	*66*
N7=3070282504055021789=1436222173×2137748993	*240*	*281*
N8=3757550627260778911=16053127×234069700393	*6*	*16*
N9=24928816998094684879=347912923×71652460573	*40*	*155*
N10=10188337563435517819=70901851×143696355169	*31*	*42*

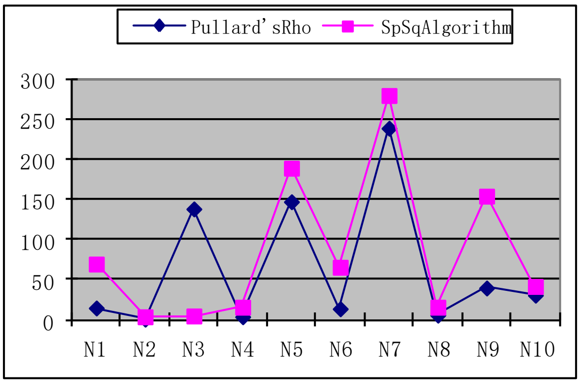


Fig.2 Pullard'sRho vs. SpSq Algorithm

V. Conclusion

It is necessary for a scientific researcher to implement and make test of his theoretic idea. Comparisons or comparative study of kinds of different models can make it clear for a decision. For this purpose, this article combines the idea that was raised in article [3] and the theory that was put forward in article [7] and realizes an approach to factorize integers. The author hope it could be a useful exploration and a valuable reference in theoretic study and technical development.

Acknowledgment

The research work is supported by Foshan Bureau of Science and Technology under projects 2016AG100652, 2016AG100792 and 2016AG100382. The author sincerely presents thanks to them all.

References

[1] Sonal Sarnaik, Dinesh Gadekarand Umesh Gaikwad, "*An overview to Integer factorization and RSA in Cryptography*", INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY,2(9),21-26(2014)

[2] Jongsoo Park,Mathology Sys, "*Prime Sieve and Factorization Using Multiplication Table*", Journal of Mathematics Research,4(3):7-12(2012)

[3] W Aldrin, Wanambisi Shem Aywa, Cleophas Maende and Geoffrey Muchiri Muketha, "*Factorization of Large Integers*". International Journal of Mathematics and Statistics Studies,1(1):39-44(2013)

[4] Xingbo WANG. "*Seed and Sieve of Odd Composite Numbers with Applications In Factorization of Integers*", OSR Journal of Mathematics (IOSR-JM), 12(5, Ver. VIII), 01-07(2016)

[5] Xingbo WANG, "*Factorization of Large Numbers via Factorization of Small Numbers*", Global Journal of Pure and Applied Mathematics, 12(6), 5157-5173 (2016)

[6] WANG Xingbo, "*Valuated Binary Tree: A New Approach in Study of Integers*", International Journal of Scientific and Innovative Mathematical Research (IJSIMR), 4(3), 63-67(2016)(DOI:10.20431/2347-3142.0403008)

[7] Xingbo WANG, "*Genetic Traits of Odd Numbers With Applications in Factorization of Integers*", Global Journal of Pure and Applied Mathematics,13(1):318-333(2017)

[8] Wang Xingbo, "*A mean-value formula for the floor function on integers*", Mathproblems Journal, 2(4),136-143(2012)