Journal of Mathematics Research; Vol. 10, No. 3; June 2018
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

Some New Inequalities With Proofs and Comments on Applications

Xingbo WANG[1,2,3], Zhikui DUAN[1,3] & Wen WAN[3]

[1] Department of Mechatronic Engineering, Foshan University, Foshan, China

[2] State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi, China

[3] National Supercomputer Center in Guangzhou, Guangzhou, China

Correspondence: Xingbo WANG, Department of Mechatronic Engineering, Foshan University, No.18, Jiangwanyi Road, Foshan, China.

Received: February 22, 2018 Accepted: March 12, 2018 Online Published: March 19, 2018

doi:10.5539/jmr.v10n3p15 URL: https://doi.org/10.5539/jmr.v10n3p15

Abstract

This article proves several new inequalities. The proved inequalities are all integrated with the floor function and one of them gives a bound estimation for the Euler's totient of the semiprimes. Detail mathematical deductions are presented and applicable cases for each inequality are also given with technical comments.

Keywords: Inequality, Euler's totient, floor function

1. Introduction

The importance of the inequalities and their applications are widely known by researchers of science and technology. Among the thousands of inequalities, those that incorporate the floor function are of very special individuality because of their discrete traits and their wide applications in computer science and various technological aspects. Discovering and proving such inequalities always accompany with mathematical skills and smartness, as seen in chapter 3 of Graham's book (Graham, 1994), in chapter 2 of KUANG's book (Jichang Kuang,2010) and in WANG's article (Xingbo WANG,2017). A recent study came across several new such inequalities. This article introduces , proves them and makes comments on their applications.

2. Preliminaries

This section lists notations, symbols and lemmas that are adopted in this article.

Definition 1 *The floor function of a real x, denoted by* $\lfloor x \rfloor$*, is an integer that satisfies inequality* $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$*, or equivalently,* $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$*.The fraction part* $x - \lfloor x \rfloor$ *is denoted by* $\{x\}$*.*

Symbols *Symbol* $A \Longrightarrow B$ *means A can derive out B or B is obtained from A.*

Lemma 1 *For arbitrary positive real numbers x and y, it holds* $\frac{x+y}{2} \geq \sqrt{xy}$, where the equal sign '=' holds if and only $x = y$.

Lemma 2 (See in Xingbo WANG,2017) *The floor function* $\lfloor x \rfloor$ holds the following properties (P8) and (P12).

(P8). $n \lfloor x \rfloor \leq \lfloor nx \rfloor$, *where n is a positive integer*;

(P12). $\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor, x \in Z \\ -\lfloor x \rfloor - 1, x \notin Z \end{cases}$, *where symbol* $\mathbf{Z}$ *means set of integers.*

Lemma 3 *For arbitrary positive integer* $n > 13$*, it holds* $n^2 < 2^{n-3}$.

Proof. The lemma obviously holds for $n = 14$ because $8 \times 14^2 = 8 \times 196 = 1568$ and $2^{14-3} = 2^{11} = 2048$. Now assume it holds for $n = k$ with $k > 14$; then it yields

$$k < \sqrt{2^{k-3}}$$

and

$$(k+1)^2 = k^2 + 2k + 1 < 2^{k-3} + 2k + 1 \tag{1}$$

Note that when $k > 14$,

$$\frac{2^{k-3} + 2k + 1}{2^{(k+1)-3}} = \frac{1}{2} + 2\frac{k}{2^{k-2}} + \frac{1}{2^{k-2}} < \frac{1}{2} + \frac{1}{2^{\frac{k-3}{2}}} + \frac{1}{2^{k-2}} < \frac{1}{2} + \frac{1}{2^{\frac{14-3}{2}}} + \frac{1}{2^{14-2}} < 1 \tag{2}$$

Then (1) and (2) result in

$$(k+1)^2 < 2^{k-2} = 2^{(k+1)-3}$$

By principle of mathematical induction, the lemma holds.

□

3. Main Results and Proofs

Theorem 1 *For arbitrary odd integer $n \geq 7$, it holds*

$$1 + \lfloor \log_2 n \rfloor \leq \frac{n-1}{2} \tag{3}$$

Proof. Direct calculation shows that, inequality (3) hold for $n = 7, 9, 11, 13$ because $1 + \lfloor \log_2 7 \rfloor = 3 = \frac{7-1}{2}$, $1 + \lfloor \log_2 9 \rfloor = 4 = \frac{9-1}{2}$, $1 + \lfloor \log_2 11 \rfloor = 4 < \frac{11-1}{2}$ and $1 + \lfloor \log_2 13 \rfloor = 4 < \frac{13-1}{2}$. Now consider $n > 13$. Use proof by contradiction. Assume $1 + \lfloor \log_2 n \rfloor > \frac{n-1}{2}$; then it leads to $1 + \log_2 n > \frac{n-1}{2}$ since $\log_2 n \geq \lfloor \log_2 n \rfloor$. That is

$$\log_2 n > \frac{n-3}{2} \Rightarrow \log_2 n^2 > n - 3 \Rightarrow n^2 > 2^{n-3}$$

which is contradictory to Lemma 3. Thus when $n > 13$ the inequality (3) holds. Consequently the theorem holds.

□

Theorem 2 *Let α and x be positive real numbers; then it holds*

$$\alpha \lfloor x \rfloor - 1 < \lfloor \alpha x \rfloor < \alpha(\lfloor x \rfloor + 1) \tag{4}$$

Particularly, if α is a positive integer, say $\alpha = n$, then it yields

$$n \lfloor x \rfloor \leq \lfloor nx \rfloor \leq n(\lfloor x \rfloor + 1) - 1 \tag{5}$$

Proof. The definition of the floor function shows that $\alpha x - 1 < \lfloor \alpha x \rfloor \leq \alpha x$ and $x - 1 < \lfloor x \rfloor \leq x$. Hence $\lfloor \alpha x \rfloor - \alpha \lfloor x \rfloor \leq \alpha x - \alpha \lfloor x \rfloor < \alpha x - \alpha(x-1) = \alpha$, namely

$$\lfloor \alpha x \rfloor < \alpha \lfloor x \rfloor + \alpha \tag{6}$$

Again by $\lfloor \alpha x \rfloor > \alpha x - 1$ and $\lfloor x \rfloor \leq x$, it yields

$$\lfloor \alpha x \rfloor - \alpha \lfloor x \rfloor \geq \lfloor \alpha x \rfloor - \alpha x > \alpha x - 1 - \alpha x = -1$$

namely,

$$\lfloor \alpha x \rfloor > \alpha \lfloor x \rfloor - 1 \tag{7}$$

Obviously, when α is a positive integer, say $\alpha = n$, then (7) turns to be

$$n \lfloor x \rfloor < \lfloor nx \rfloor + 1$$

That is $n \lfloor x \rfloor \leq \lfloor nx \rfloor$, as Lemma 2(P8) states.

□

Corollary 1 *For arbitrary positive real numbers α,x and y with $x > y$, it holds*

$$\lfloor \alpha(x-y) \rfloor + \alpha \lfloor y - x \rfloor \leq 0 \tag{8}$$

Proof. There are two cases to investigate. One is that $|x-y| = n$ is a positive integer, and the other is not. For the first case, $\lfloor \alpha(x-y) \rfloor = \lfloor \alpha n \rfloor \leq \alpha n$ and by Lemma 2 (P12) $\alpha \lfloor y - x \rfloor = -\alpha n$; then it yields $\lfloor \alpha(x-y) \rfloor + \alpha \lfloor y - x \rfloor \leq \alpha n - \alpha n = 0$. For the second case, $x - y$ is not an integer, then by Theorem 2 and Lemma 2(P12)

$$\lfloor \alpha(x-y) \rfloor + \alpha \lfloor y - x \rfloor < \alpha \lfloor (x-y) \rfloor + \alpha - \alpha(\lfloor x - y \rfloor + 1) = 0$$

□

Theorem 3 *Let n be a semiprime and $\phi(n)$ be the Euler's totient function; then the inequalities (9) and (10) hold*

$$\sqrt{n} < \phi(n) < (\sqrt{n} - 1)^2 \tag{9}$$

$$\lfloor \sqrt{n} \rfloor < \phi(n) \leq n - 2\lfloor \sqrt{n} \rfloor \tag{10}$$

Proof. Let $n = pq$, where p and q are odd primes with $3 \leq p < q$; then $n > 6$. Now by definition of $\phi(n)$, see in chapter 4.9 of Graham's book(Graham, 1994), or chapter 7.1 of Rosen's book(Rosen,2011), it yields

$$\phi(n) = n(1 - \frac{1}{p})(1 - \frac{1}{q}) > \frac{4n}{9}$$

Considering $\frac{4n}{9\sqrt{n}} = \frac{4\sqrt{n}}{9}$, it knows that $\frac{4n}{9} > \sqrt{n}$ when $n > (\frac{9}{4})^2 = 2.25^2 = 5.0625$.

Therefore, it holds

$$\phi(n) > \sqrt{n} \tag{11}$$

The definition of the floor function shows $\sqrt{n} \geq \lfloor \sqrt{n} \rfloor$; hence it is sure

$$\phi(n) > \lfloor \sqrt{n} \rfloor \tag{12}$$

On the other hand,

$$\phi(n) = (p - 1)(q - 1) = n - (p + q) + 1$$

By Lemma 1 it holds $p + q > 2\sqrt{pq} = 2\sqrt{n}$; consequently

$$\phi(n) < n - 2\sqrt{n} + 1 = (\sqrt{n} - 1)^2 \tag{13}$$

Meanwhile, by $\lfloor \sqrt{n} \rfloor \leq \sqrt{n}$, it leads to

$$\phi(n) < n - 2\sqrt{n} + 1 \leq n - 2\lfloor \sqrt{n} \rfloor + 1$$

Since $\phi(n)$ is a positive integer, it yields

$$\phi(n) \leq n - 2\lfloor \sqrt{n} \rfloor \tag{14}$$

The inequalities (11) to (14) establish the theorem.

□

4. Applicable Cases & Comments

Theorems 1 to 3 might be thought very plain but in fact they are very important in certain areas. Here lists some of their applications.

4.1 Application of Theorem 1

When investigating the divisibility on a valued binary tree, as WANG introduced (Xingbo WANG, 2016), it can see that, the leftmost node of an $N_{(0,0)}$-rooted tree is calculated by

$$N_{(k,j)} = 2^k N_{(0,0)} - 2^k + 1; k = 0, 1, 2, ...$$

If $N_{(0,0)}$ is an odd prime number p, then it yields

$$N_{(k,j)} = 2^k p - 2^k + 1; k = 0, 1, 2, ... \tag{15}$$

By Fermat's Little Theorem,

$$2^{p-1} \equiv 1 (\mathrm{mod}\, p) \tag{16}$$

One can see from (15) and (16) that, $p | N_{(k,0)}$ when $k = p - 1$. That is to say, p's multiples periodically occur at the leftmost nodes of the tree. Theoretically, this provides an approach to find p's multiples in the tree; however when p is an unknown divisor of a composite odd number to be factorized and a search is performed to search the 'theoretical $p - 1$' along the

leftmost nodes of the tree, it will cost quite a lot of time when p is relatively big. Fortunately, WANG's article proves that, there is not a multiple-node before level $1 + \lfloor \log_2 p \rfloor$ and the congruence (16) indicates it might have $2^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod} p)$ or $2^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod} p)$. This time, Theorem 1 shows $1 + \lfloor \log_2 p \rfloor < \frac{p-1}{2}$, providing a mathematical foundation to reduce the searching distance.

4.2 Application of Theorem 2

When deducting a mathematical formula related with the floor function, it usually needs to move a coefficient c outside the floor symbol $\lfloor \rfloor$ into the symbol, or vice versa, as is shown below

$$c \lfloor x \rfloor \to \lfloor cx \rfloor, \lfloor cx \rfloor \to c \lfloor x \rfloor$$

Lemma 2(P8) shows $c \lfloor x \rfloor \leq \lfloor cx \rfloor$ when c is a positive integer. But this relationship does not hold when c is a positive real number. For example, $\lfloor 0.3 \times 23 \rfloor = 6 < 0.3 \times \lfloor 23 \rfloor = 6.9$. This time, Theorem 2 can solve the contradiction. By Theorem 2, it shall hold

$$0.3 \times \lfloor 23 \rfloor - 1 < \lfloor 0.3 \times 23 \rfloor < 0.3 \times (\lfloor 23 \rfloor + 1) \to 5.9 < 6 < 7.2$$

which matches to the fact.

Actually, Theorem 2 can have further more applicable occasions. Readers can see them in future works.

4.3 Application of Theorem 3

In cryptography, factoring a semiprime, especially a big semiprime, say a RSA number, means a successful step towards solving the difficult problem of integer factorization. There are a lot of literatures mentioning the topic. Among the published methods, the one that calculates or guesses the Euler's totient demonstrates particular individuality for its elementary traits, which is easily understood and relatively faster, as were stated in chapter 6.4 of YAN's book (Yan ,2008). Scholars developed several approaches to estimate the bound of $\phi(n)$, as Kloster (Kloster ,2010), Jie Fang (Jie Fang & Chenglian Liu,2018) and Kurzweg U H(Kurzweg .2012) did.

On reading Jie Fang's article, it is easy to find some errors in its mathematical deduction. For example, in proving Theorem 1 of the article, it alleged $p + q \geq 2\sqrt{n}$ under the assumption $n = pq$. Actutally, it is wrong because $p \neq q$ leads to that the equal sign '=' does not hold. This error directly results in a wrong upper bound of $\phi(n)$ in the article. Theorem 3 might provide a thought to its correction.

Acknowledgements

The research work is supported by the State Key Laboratory of Mathematical Engineering and Advanced Computing under Open Project Program No.2017A01, Department of Guangdong Science and Technology under project 2015A010104011, Foshan Bureau of Science and Technology under projects 2016AG100311, Project gg040981 from Foshan University. The authors sincerely present thanks to them all.

References

Graham, R. L., Knuth, D. E., & Patashnik, O. (1994). *Concrete Mathematics: A Foundation for Computer Science* (2nd ed). MA: Addison-Wesley, 1994, ISBN 0-201-55802-5.

Jichang Kuang. (2010). *Applied Inequalities*,Chinese Shandong: Shandong Science and technology Press. ISBN: 978-7-5331-5632-9.

Jie Fang, & Chenglian Liu. (2018). A Generalize Estimating the $\phi(n)$ of Upper/Lower Bound to RSA Public Key Cryptosystem,*International Journal of Network Security, 20*(2),332-336. https://doi.org/10.6633/IJNS.201803.20(2).14

Kloster, K. (2010). *Factoring a semiprime n by estimating* $\phi(n)$. Retrieved from: http://www.gregorybard.com/papers/phi_version_may_7.pdf.

Kurzweg, U. H. (2012). *More on Factoring Semi-primes*. Retrieved from: http://www2.mae.ufl.edu/ uhk/MORE-ON-SEMIPRIMES.pdf

Rosen, K. H. (2011). *Elementary Number Theory and Its Applications*(6th ed). New York: Addison-Wesley

Xingbo WANG. (2016). Valuated Binary Tree: A New Approach in Study of Integers, *International Journal of Scientific and Innovative Mathematical Research, 4*(3), 63-67.

Xingbo WANG. (2017). Brief Summary of Frequently-used Properties of the Floor Function, *IOSR Journal of Mathematics*, *13*(5 Ver. I1): 46-48. https://doi.org/10.9790/5728-1305024648

Yan, S. Y. (2008). *Cryptanalytic Attacks on RSA*. New York: Springer-Verlag New York Inc.