

## A REFINEMENT OF THE FUNCTION $g(x)$ ON GRIMM'S CONJECTURE

SHAOHUA ZHANG

**ABSTRACT.** In this paper, we refine the function  $g(x)$  on Grimm's conjecture and improve a result of Erdős and Selfridge without using Hall's theorem.

**1. Some basic notation.** Let  $\pi(x)$  be the prime counting function which represents the number of primes not exceeding the real number  $x$ . We write  $f(x) = O(g(x))$ , or equivalently  $f(x) \ll g(x)$  when there is a constant  $C$  such that  $|f(x)| \leq Cg(x)$  for all values of  $x$  under consideration. We write  $f(x) = o(g(x))$  when  $\lim_{x \rightarrow \infty} f(x)/g(x) = 0$ . We let  $[x]$  denote the largest integer not exceeding the real number  $x$ .

Let  $\binom{m+n}{n}$  be the binomial coefficient. For a prime  $p$  and a positive integer  $n > 1$ , we define  $v_p(n)$  to be the largest exponent of  $p$  that divides  $n$ . In this paper, we always denote by  $p$  a prime number. Denote the set of all prime numbers by  $P$ , and denote the set of all composite numbers by  $C$ . Let  $H_n = \{x : x \in C, \text{ for all } p \mid x, p^{v_p(x)} \leq n\}$ .

**2. Introduction.** In 1969, Grimm [9] made an important conjecture that if  $m+1, \dots, m+n$  are consecutive composite numbers, then there exist  $n$  distinct prime numbers  $p_1, \dots, p_n$  such that  $m+j$  is divisible by  $p_j$ ,  $1 \leq j \leq n$ . This implies that the product of any  $n$  consecutive composite numbers must have at least  $n$  distinct prime factors.

Grimm proved the conjecture for two special cases: (i) For all  $n$  in the sequence of consecutive composites,  $\{n! + i\}$ ,  $i = 2, \dots, n$ . (ii) For all  $m$ , when  $m > n^{n-1}$ . This was improved to  $m > n^{\pi(n)}$  by Erdős and

---

2010 AMS *Mathematics subject classification.* Primary 11A41, 11A99, 11B65.

*Keywords and phrases.* Consecutive composite numbers, Grimm's conjecture, Cramér's conjecture, binomial coefficient.

This work was partially supported by the Scientific Research Foundation of Yangtze Normal University, the Science and Technology Research Project of Chongqing City Board of Education (Nos. KJ121316, KJ121312) and the Doctoral Fund of Ministry of Education of China (No. 20090131120012).

Received by the editors on November 3, 2009, and in revised form on June 25, 2010.

DOI:10.1216/RMJ-2013-43-1-385 Copyright ©2013 Rocky Mountain Mathematics Consortium

Selfridge [7] who used Hall's theorem [10]. Moreover, they obtained the following typical theorem:

*Let  $v(m, n)$  be the number of distinct prime factors of  $\prod_{i=1}^{i=n} (m + i)$ , and let  $f(m)$  be the largest  $n$  for which  $v(m, n) \geq n$ , then  $f(m) < c(m/\log m)^{1/2}$  for all  $m$ , where  $c$  is a positive absolute constant.*

Thus, Grimm's conjecture implies  $p_{r+1} - p_r \ll (p_r/\log p_r)^{1/2}$  which is out of bounds for even the Riemann hypothesis [14] which implies that  $p_{r+1} - p_r \ll p_r^{1/2} \log p_r$ , where  $p_{r+1}$  and  $p_r$  are consecutive primes. It implies particularly that there are primes between  $n^2$  and  $(n + 1)^2$  for all sufficiently large  $n$ , a conjecture which is still open. For the details of its proof, see also [17]. Furthermore, by [7, Theorem 1], it is not difficult to prove that Grimm's conjecture implies that there are primes between  $x^2$  and for  $x^2 + x$  all sufficiently large  $x$  and there are primes between  $y^2 - y$  and  $y^2$  for all sufficiently large  $y$ . Let  $x = n$  and  $y = n + 1$ ; then, Grimm's conjecture implies that, for all sufficiently large  $n$ , there are two primes between  $n^2$  and  $(n + 1)^2$  which implies that there are four primes between  $n^3$  and  $(n + 1)^3$  for all sufficiently large  $n$  [18].

These surprising consequences motivate the study of the function  $g(m)$  which is the largest integer  $n$  such that Grimm's conjecture holds for the interval  $[m + 1, m + n]$ . Theorem 1 in [7] said that  $g(m) = O(\sqrt{m/\log m})$ . By using a result of Ramachandra [15], Erdős and Pomerance [6] pointed out that  $g(m) < m^{(1/2)-c}$  for some fixed  $c > 0$  and all large  $m$ . Thus, an interesting problem of research has been to obtain upper and lower bounds for  $g(m)$ .

In 1971, Erdős and Selfridge [7] proved  $g(m) \geq (1 + o(1)) \log m$ . In 1975, as an improvement of results of Cijssouw, Tijdeman [3] and Ramachandra [14], Ramachandra, Shorey and Tijdeman [16] obtained an important result which states that  $(\log m/\log \log m)^3 \ll g(m)$  by using Gelfond-Baker's theory. This implies that Grimm's conjecture would follow from Cramér's conjecture [5] which states that  $p_{r+1} - p_r = O((\log p_r)^2)$ . In 2006, Laishram and Shorey [12] confirmed that Grimm's conjecture is true for  $m \leq 1.9 \times 10^{10}$  and for all  $n$  by using Mathematica.

The object of this section is to study a stronger function  $w(m)$  which is the largest integer  $n$  such that the binomial coefficients  $\binom{m+n}{n}$

may be written as  $\binom{m+n}{n} = \prod_{i=1}^{i=n} a_i, a_i \mid (m+i), a_i \in N, a_i > 1, (a_i, a_j) = 1, 1 \leq i \neq j \leq n$ . By a result of the author [20], we see that every binomial coefficient has the representation:  $\binom{m+n}{n} = \prod_{i=1}^{i=n} a_i, a_i \mid (m+i), a_i \in N, (a_i, a_j) = 1, 1 \leq i \neq j \leq n$ . Naturally, we want to know what condition  $m$  satisfies so that each  $a_i > 1$  since it will imply that  $\binom{m+n}{n}$  must have at least  $n$  distinct prime factors in this case. In this paper, we will prove the following theorem without using Hall's theorem:

**Theorem 1.** *When  $m > \prod_{p \leq n} p^{\lfloor \log_p n \rfloor}$ , the binomial coefficient  $\binom{m+n}{n}$  has the representation:*

$$\binom{m+n}{n} = \prod_{i=1}^n a_i, a_i \mid (m+i), a_i \in N, a_i > 1, (a_i, a_j) = 1, 1 \leq i \neq j \leq n.$$

Note that  $w(m) \leq g(m), n^{\pi(n)} > \prod_{p \leq n} p^{\lfloor \log_p n \rfloor}$ , and it is easy to show by [19] that  $\pi(n) \log n \geq n$  when  $n \geq 17$ . Hence, we have  $\log m \ll w(m) \ll \sqrt{m/\log m}$ . So, by this lower bound, we have obtained an analogical result of Theorem 3 in [7].

In Section 3, we will give the proof of Theorem 1. In Section 4, we will try to point out that it is not easy to improve the lower bound of  $w(m)$  to  $(\log m)^2$ .

**3. Proof of Theorem 1.** To prove the theorem, we need some lemmas which reflect that the binomial coefficients have some fascinating and remarkable arithmetic properties again.

**Lemma 1.** *Let  $\binom{m+n}{n}$  be the binomial coefficient with  $m, n \in N$ . Then, for any prime  $p, v_p\left(\binom{m+n}{n}\right) \leq t$ , where  $t = \max_{1 \leq i \leq n} \{v_p(m+i)\}$ .*

*Proof.* For the proof of Lemma 1, see [20].

**Lemma 2.** *If  $m+i \notin H_n$  for some  $1 \leq i \leq n$ , then there is a prime number  $p$  such that  $p^{v_p(m+i)} > n$ . Moreover,  $1 \leq v_p\left(\binom{m+n}{n}\right) \leq v_p(m+i)$ .*

*Proof.* By our assumption and the definition of  $H_n$ , clearly, there is a prime  $p$  such that  $p^{v_p(m+i)} > n$ . Note that  $v_p(m+j) < v_p(m+i)$  when  $j \neq i$ . Otherwise,  $p^{v_p(m+i)} | (j-i)$ . But  $|j-i| < n$ , which is impossible. Thus,  $v_p(m+i) = \max_{1 \leq j \leq n} \{v_p(m+j)\}$  and  $v_p\left(\binom{m+n}{n}\right) \leq v_p(m+i)$  by Lemma 1. On the other hand, if we write  $m = p^{v_p(m+i)}x + y$ , where  $x, y \in N \cup \{0\}$  with  $0 \leq y < p^{v_p(m+i)}$ , then we have  $p^{v_p(m+i)} | (y+i)$  and  $[(m+n)/p^{v_p(m+i)}] - [m/p^{v_p(m+i)}] = 1$  since  $[n/p^{v_p(m+i)}] = 0$  and  $n+y \geq i+y$ . Hence,  $\sum_{j=1}^{\infty} ([m+n/p^j] - [m/p^j] - [n/p^j]) \geq 1$ , and  $1 \leq v_p\left(\binom{m+n}{n}\right)$ . This completes the proof of Lemma 2.  $\square$

It is worthwhile pointing out that  $H_n$  has many interesting properties which should be given further consideration. For example,  $H_2$  is an empty set,  $H_3 = \{6\}$ ,  $H_4 = \{4, 6, 12\}$  and so on.  $H_n \subseteq H_{n+1}$ ;  $|H_n| = \prod_{p \leq n} (1 + [\log_p n]) - 1 - \pi(n)$ ;  $H_n \subseteq \psi(x, n)$ , where  $\psi(x, n)$  is the set of  $n$ -smooth integers in  $[1, x]$  with  $x = \prod_{p \leq n} p^{[\log_p n]}$ . For some details on smooth integers which relate to factorization of integers, see [4]. For applications of smooth numbers to various problems in different areas of number theory, see [2, 8, 11, 13].

**Lemma 3.** *If  $m+i \notin H_n$  for every  $1 \leq i \leq n$ , then  $\binom{m+n}{n}$  has the representation:*

$$\binom{m+n}{n} = \prod_{i=1}^n a_i, \quad a_i | (m+i), \quad a_i \in N, \quad a_i > 1, \quad (a_i, a_j) = 1, \\ 1 \leq i \neq j \leq n.$$

*Proof.* Write  $B = \binom{m+n}{n} = \prod_{i=1}^{i=k} p_i^{e_i}$  by the fundamental theorem of arithmetic, where  $k$  is the number of distinct prime factors of  $B$ . Clearly, for every prime factor  $p_i$  of  $B$ , there must be a number  $i_j$  with  $1 \leq i_j \leq n$ , such that  $v_{p_i}(m+i_j) = \max_{1 \leq r \leq n} \{v_{p_i}(m+r)\}$ . By Lemma 1, we have  $e_i \leq v_{p_i}(m+i_j)$  for every  $1 \leq i \leq n$ . Therefore, we can choose the number  $m+i_j$  such that

$$\frac{(m+1) \cdots (m+n)}{n!} \\ = \frac{m+1}{p_i^{v_{p_i}(m+1)}} \cdots \frac{m+i_j-1}{p_i^{v_{p_i}(m+i_j-1)}} \frac{m+i_j}{p_i^{v_{p_i}(m+i_j)-e_i}} \frac{m+i_j+1}{p_i^{v_{p_i}(m+i_j+1)}} \cdots \frac{m+n}{p_i^{v_{p_i}(m+n)}} \\ = \frac{n!}{p_i^{v_{p_i}(n!)}}$$

Notice that  $(m + 1)/p_i^{v_{p_i}(m+1)}, \dots, (m + i_j - 1)/p_i^{v_{p_i}(m+i_j-1)}, (m + i_j)/p_i^{v_{p_i}(m+i_j)-e_i}, (m + i_j + 1)/p_i^{v_{p_i}(m+i_j+1)}, \dots, (m + n)/p_i^{v_{p_i}(m+n)}, n!/p_i^{v_{p_i}(n!)}$  are all integers. Thus, by reduction,  $B$  has the representation:

$$B = \prod_{i=1}^n a_i, \quad a_i \mid (m + i), \quad a_i \in N, \quad (a_i, a_j) = 1, \quad 1 \leq i \neq j \leq n.$$

On the other hand, since  $m + i \notin H_n$  for every  $1 \leq i \leq n$ , there is a prime number  $p_i$  such that  $p_i^{v_{p_i}(m+i)} > n$ . By Lemma 2, we have  $v_{p_i}(m+i) = \max_{1 \leq r \leq n} v_{p_i}(m+r)$  and  $p_i \mid a_i$ . Note that prime numbers  $p_1, \dots, p_n$  are distinct. This completes the proof of Lemma 3.

*Proof of Theorem 1.* For every  $1 \leq i \leq n$ , we write  $m + i = (\prod_{p^{v_p(m+i)} > n} p^{v_p(m+i)}) (\prod_{p^{v_p(m+i)} \leq n} p^{v_p(m+i)})$ . If  $m + i \in H_n$  for some  $1 \leq i \leq n$ , then we have  $m + i = \prod_{p^{v_p(m+i)} \leq n} p^{v_p(m+i)} \leq \prod_{p^{v_p(m+i)} \leq n} p^{\lceil \log_p n \rceil}$ . It is a contradiction by our assumption. Therefore,  $m + i \notin H_n$  for all  $1 \leq i \leq n$ , and by Lemma 3, we get the assertion of Theorem 1.

**Corollary 1.** *If  $2 \leq n \leq 7$  and  $m + 1, \dots, m + n$  are consecutive composite numbers, then  $\binom{m+n}{n}$  can be written as*

$$\binom{m+n}{n} = \prod_{i=1}^n a_i, \quad a_i \mid (m+i), \quad a_i \in N, \quad a_i > 1, \quad (a_i, a_j) = 1, \\ 1 \leq i \neq j \leq n.$$

Namely, the conjecture in [20] is true when  $2 \leq n \leq 7$ .

*Proof.* Corollary 1 holds when  $2 \leq n \leq 6$  by computations since  $m \leq 2^2 \times 3 \times 5 = 60$  by Theorem 1. Next, we consider the case of  $n = 7$ . By Theorem 1, when  $m > 2^2 \times 3 \times 5 \times 7 = 420$ , Corollary 1 holds. When  $m \leq 420$ , by the table of prime numbers, the set of 7 consecutive composite numbers must be a subset of one of the following 13 sets:

- {90, 91, 92, 93, 94, 95, 96},
- {114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126},
- {182, 183, 184, 185, 186, 187, 188, 189, 190},

$\{200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210\}$ ,  
 $\{212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222\}$ ,  
 $\{242, 243, 244, 245, 246, 247, 248, 249, 250\}$ ,  
 $\{284, 285, 286, 287, 288, 289, 290, 291, 292\}$ ,  
 $\{318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330\}$ ,  
 $\{338, 339, 340, 341, 342, 343, 344, 345, 346\}$ ,  
 $\{360, 361, 362, 363, 364, 365, 366\}$ ,  
 $\{390, 391, 392, 393, 394, 395, 396\}$ ,  
 $\{402, 403, 404, 405, 406, 407, 408\}$ ,  
 $\{410, 411, 412, 413, 414, 415, 416, 417, 418\}$ .

We have  $204 \times 205 \times 206 \times 207 \times 208 \times 209 \times 210/1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 = 17 \times 41 \times 103 \times 207 \times 208 \times 209 \times 5$ . The remaining cases satisfy  $m + i \notin H_7$  for every  $1 \leq i \leq 7$  when  $n = 7$ . By Lemma 3, Corollary 1 holds.

**4. Remarks.** In this section, we will try to explain that it is not easy to improve the lower bound of  $w(m)$  to  $(\log m)^2$ . On one hand, we found two exceptions to the conjecture in [20] when  $m = 116$ ,  $n = 10$  or  $m = 118$ ,  $n = 8$ . This implies that the conjecture in [20] is not always true. On the other hand, if the lower bound of  $w(m)$  can be improved to  $(\log m)^2$ , then assuming Cramér's conjecture, there are only finitely many exceptions to the conjecture in [20]. which implies Grimm's conjecture (note that Grimm's conjecture follows from Cramér's conjecture). Namely, one would guess the following:

**Conjecture 1.** *For every sufficiently large integer  $n$ , the product of  $n$  consecutive composite numbers  $m + 1, \dots, m + n$  may be written as*

$$\prod_{i=1}^n (m+i) = n! \times \prod_{i=1}^n a_i, \quad a_i \mid (m+i), \quad a_i \in N, \quad a_i > 1, \quad (a_i, a_j) = 1, \\ 1 \leq i \neq j \leq n.$$

Obviously, if Conjecture 1 holds, then it also implies a surprising consequence that there are only finitely many exceptions to the following Conjecture 2.

**Conjecture 2.** (i) For every  $n > 1$ , there are primes in the intervals  $(d - n, d + n]$  and  $(d - q, d + q)$ , respectively, where  $d > 1$  is a factor of  $\prod_{n < p < 2n} p$ , and  $q$  is the least prime factor of  $d$ .

(ii) For every  $n > 2$ , let  $d > 1$  be a factor of  $\prod_{n/2 < p < n} p$ . If  $d = nt + r$  and  $d$  is coprime to each of  $nt + 1, \dots, nt + r - 1, nt + r + 1, \dots, nt + n$ , then there are primes in the interval  $[nt + 1, nt + n]$ .

*Proof.* (i) By the Bertrand-Chebyshev theorem which states that there exists a prime in interval  $(n, 2n)$  when  $n > 1$ , we see that  $\prod_{n < p < 2n} p$  has a prime factor  $> n$ . Let  $d > 1$  be a factor of  $\prod_{n < p < 2n} p$ . If there are no primes in the interval  $(d - n, d + n]$ , then  $d - n + 1, \dots, d - n + 2n$  are all composite numbers. By the assumption that Conjecture 1 holds, we have that  $\prod_{i=1}^{i=2n} (d - n + i) = (2n)! \times \prod_{i=1}^{i=2n} a_i$  with  $a_i | (d - n + i)$ ,  $a_i \in N$ ,  $a_i > 1$ ,  $(a_i, a_j) = 1$ ,  $1 \leq i \neq j \leq 2n$  for a sufficiently large integer  $n$ . But this is impossible since we obtain  $a_n = 1$  from  $v_p((2n)!) = 1$  and  $v_p((d - n + 1) \cdots (d - n + 2n)) = 1$ .

Let  $q$  be the least prime factor of  $d$ . If  $d$  is prime, then  $q = d$ . Clearly, there are primes, for example  $q$ , in the interval  $(d - q, d + q) = (0, 2q)$ . Now, we assume that  $d$  is not prime. If there are no primes in the interval  $(d - q, d + q)$ , then  $d - q + 1, \dots, d - q + 2q - 1$  are all composite numbers. Conjecture 1 holds, so we have that  $\prod_{i=1}^{i=2q-1} (d - q + i) = (2q - 1)! \times \prod_{i=1}^{i=2q-1} a_i$  with  $a_i | (d - q + i)$ ,  $a_i \in N$ ,  $a_i > 1$ ,  $(a_i, a_j) = 1$ ,  $1 \leq i \neq j \leq 2q - 1$  for a sufficiently large integer  $n$ . Note that, for any prime divisor  $r$  of  $d/q$ ,  $r > q$  since  $d > 1$  is a factor of  $\prod_{n < p < 2n} p$  and is square-free. Notice also that  $r < 2q$  since  $q > n$  and  $r < 2n$ . Therefore,  $a_q = 1$  since  $v_r((2q - 1)!) = 1$  and  $v_r((d - q + 1) \cdots (d - q + 2q - 1)) = 1$ . This contradiction shows that case (i) holds.

Similarly, one could deduce case (ii) in Conjecture 2 assuming Conjecture 1. In fact, if there are no primes in the interval  $[nt + 1, nt + n]$ , then by the assumption that Conjecture 1 holds, we have that  $\prod_{i=1}^{i=n} (nt + i) = n! \times \prod_{i=1}^{i=n} a_i$  with  $a_i | (nt + i)$ ,  $a_i \in N$ ,  $a_i > 1$ ,  $(a_i, a_j) = 1$ ,  $1 \leq i \neq j \leq n$  for every sufficiently large integer  $n$ . However, by our assumption and the known conditions, for any prime divisor  $p$  of  $d = nt + r$ , we have  $v_p(n!) = 1$  and  $v_p((nt + 1) \cdots (nt + n)) = 1$  since  $d = nt + r$  is square-free and coprime to each of  $nt + 1, \dots, nt + r - 1, nt + r + 1, \dots, nt + n$ . Therefore,  $a_r = 1$  since  $v_p\left(\binom{nt+n}{n}\right) = 0$ , which is a contradiction.

Conjecture 2 also implies that, for every  $n > 1$ , there are primes in the interval  $(d - q, d + q)$ , where  $d = \prod_{n < p < 2n} p$ , and  $q$  is the least prime factor of  $d$ . Of course, if  $d$  is prime, then there are primes in the interval  $(d - q, d + q) = (0, 2q)$ . When  $d$  is not prime, or equivalently, when  $n = 4$  or  $n > 5$  (by the refined Bertrand-Chebyshev theorem which states that there exist at least two distinct primes in interval  $(n, 2n)$  when  $n = 4$  or  $n > 5$ ), we have  $d - q \neq 0$ . Moreover, by the Chebyshev theorem which states that  $0.92129x/\log x < \pi(x) < 1.1056x/\log x$ , we have that  $2n < 2q < 4n < (((0.92 \times 2n/\log 2n) - (1.11n/\log n)) \log n)^2 < ((\pi(2n) - \pi(n)) \log q)^2 < (\log(\prod_{n < p < 2n} p - q))^2$  for every sufficiently large integer  $n$ . Thus,  $2q < (\log(d - q))^2$  which is out of bounds for even Cramér's conjecture, and it is hard to prove that there are primes in the interval  $(d - q, d + q)$ , say nothing of Conjecture 1. Therefore, we think that it is not easy to improve the lower bound of  $w(m)$  to  $(\log m)^2$ . Is Conjecture 1 true?

Based on Conjecture 2, one could obtain some interesting results. For instance, below is a fast algorithm for generating large primes by using small known primes.

### An algorithm for generating an $m$ -bit prime number.

**Input:** A natural number  $m$

**Step 1:** Choose  $p_1 < \dots < p_r < 2p_1$  such that  $r$  is appropriately large and  $p_i$  are all primes (not necessarily consecutive), for  $1 \leq i \leq r$  and  $2^{m-1} < k = \prod_{i=1}^{i=r} p_i < 2^m$ .

This step can be finished easily by pre-computing.

**Step 2:** Test whether each of  $k \pm 2, \dots, k \pm 2[p_1/2]$  is prime. If, for some  $i$ ,  $k + i$  or  $k - i$  is prime, terminate the algorithm. Otherwise, Conjecture 2 does not hold for  $n = 2[p_1/2] + 1$ .

Such a prime can be found quickly when  $r$  is appropriately large. On one hand, primality testing is comparatively easy since its running time is polynomial [1]. On the other hand, since  $k$  has many prime divisors, there is a high probability that either  $k + 2i$  or  $k - 2i$  is prime for some  $1 \leq i \leq [p_1/2] < p_1/2 < 2^{(m/r)-1}$ .

**Output:** An  $m$ -bit prime number. Due to the fact that it lies outside the scope of this paper, we omitted more details of this algorithm. As a



toy example, we can generate a 32-bit prime using small primes 29, 31, 37, 41, 43, 47. Note that  $2^{31} < 29 \times 31 \times 37 \times 41 \times 43 \times 47 < 2^{32}$ . By an exhaustive search, or a simple sieve, we find that  $29 \times 31 \times 37 \times 41 \times 43 \times 47 + 6 = 2756205449$  is a 32-bit prime. Unfortunately, we do not know whether Conjecture 2 is true or not, although we can test whether Conjecture 2 holds by the aforementioned algorithm. Moreover, we have not been able to work out a complete proof of Conjecture 2, still less Conjecture 1. But, all of these and related questions, specially, the lower bound of  $w(m)$ , we hope to investigate.

**Acknowledgments.** I am very thankful to the referees for their valuable comments and detailed revisions improving the presentation of the paper, and also to my supervisor Professor Xiaoyun Wang for her suggestions and encouragement. I thank the key lab of cryptography technology and information security in Shandong University and the Institute for Advanced Study in Tsinghua University, for providing me with excellent conditions.

## REFERENCES

1. M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, Ann. Math. **160** (2004), 781–793.
2. E.R. Canfield, P. Erdős and C. Pomerance, *On a problem of Oppenheim concerning 'faotonsatio numeroium'*, J. Number Theory **17** (1983), 1–28.
3. P.L. Cijsouw and R. Tijdeman, *Distinct prime factors of consecutive integers. Diophantine approximation and its applications*, (Proc. Conf., Washington, D.C., 1972, 59–76), Academic Press, New York, 1973.
4. D. Coppersmith, *Fermat's last theorem (case 1) and the Wieferich criterion*, Math. Comp. **54** (1990), 895–902.
5. H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2** (1936), 23–46.
6. P. Erdős and C. Pomerance, *An analogue of Grimm's problem of finding distinct prime factors of consecutive integers*, Util. Math. **24** (1983), 45–65.
7. P. Erdős and J.L. Selfridge, *Some problems on the prime factors of consecutive integers*, II. Proc. Washington State Univ. Conference on Number Theory, Pullman, WA, 1971, 13–21.
8. A. Granville, *Smooth numbers: Computational number theory and beyond*, in Proc. MSRI Conf. Algorithmic Number Theory: Lattices, Number Fields, Curves, and Cryptography, Berkeley, Cambridge University Press, 2000.
9. C.A. Grimm, *A conjecture on consecutive composite numbers*, Amer. Math. Month. **76** (1969), 1126–1128.

10. P. Hall, *On representatives of subsets*, J. Lond. Math. Soc. **10** (1935), 26–30.
11. H. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théor. Nombr. Bord. **2** (1993), 411–484.
12. S. Laishram and T.N. Shorey, *Grimm’s conjecture on consecutive integers*, Int. J. Number Theory **2** (2006), 207–211.
13. C. Pomerance, *Smooth numbers and the quadratic sieve*, in Proc. MSRI Conf. Algorithmic Number Theory: Lattices, Number Fields, Curves, and Cryptography, Berkeley, Cambridge University Press, 2000.
14. K. Ramachandra, *Application of Baker’s theory to two problems considered by Erdős and Selfridge*, J. Indian Math. Soc. **37** (1973), 25–34.
15. ———, *A note on numbers with a large prime factor*, J. London Math. Soc. **1** (1969), 303–306.
16. K. Ramachandra, T.N. Shorey and R. Tijdeman, *On Grimm’s problem relating to factorisation of a block of consecutive integers*, J. reine angew. Math. **273** (1975), 109–124.
17. P. Ribenboim, *The little book of the bigger primes*, Springer-Verlag, New York, 2004.
18. ———, *The book of prime number records*, Springer-Verlag, New York, 1988.
19. J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.
20. Y.X. You and S.H. Zhang, *A new theorem on the binomial coefficient  $\binom{m+n}{n}$* , J. Math. (Wuhan, China) **23** (2003), 146–148.

SCHOOL OF MATHEMATICS AND COMPUTER SCIENCE, YANGTZE NORMAL UNIVERSITY, FULING, CHONGQING, 408102, CHINA

**Email address:** safeprime@163.com