On the upper bound of number-theoretic function $F_f(h)$

Shenghan Lu
Guided by: Jinsong Li
The high school attached to Tsinghua University

Abstract: The problem of the existence of infinitely many prime values of a number-theoretic function $f(x)$ has been one of the most important topics in Number Theory. Note that if $f(x)$ represents infinitely many primes, then we can get this necessary condition: for any positive integer h, there exists a positive integer k such that $(f(k),h)=1$ and $f(k)>1$. Naturally, we are interested in the number-theoretic functions $f(x)$ that satisfy the aforementioned necessary condition. Thus, there must exist the least positive integer n such that $(f(n),h)=1$ and $f(n)>1$. Denote this least positive integer n by $F_f(h)$. In this paper, we mainly focus on three famous number-theoretic functions: $f(x)=2^{2^x}+1$, $m(x)=2^x-1$ and $l(x)=x^2+1$, proving they satisfy the aforementioned necessary condition respectively. Furthermore, we approximately estimate the upper bound of $F_{f(x)}(h), F_{m(x)}(h), F_{l(x)}(h)$ respectively, and obtain some interesting results.

Ⅰ. Introduction

Let $f(x)$ be a number-theoretic function. Whether $f(x)$ represents infinitely many primes has always been a problem that attracts great interests among many famous mathematicians. As early as 2000 years ago, Euclid has proved that $f(x)=x$ represents infinitely many primes. In 1837, Dirichlet proved that $f(x)=ax+b$ also represents infinitely many prime values, where a and b are integers with $(a,b)=1$, either $a>0, b\neq 0$ or $a=1, b=0$. By proving this, he completely solved this problem in the case of linear polynomial with integral coefficients. Apart from this case of linear polynomial, however, the problem becomes complex and there is still no complete solution by now. For example, whether functions such as $f(x)=2^{2^x}+1$, $m(x)=2^x-1$ and $l(x)=x^2+1$ represent infinitely many primes has not been verified until today. Actually, these functions are respectively related to the problem of Fermat number, Mersenne number and the first conjecture of Landau. Readers can refer to [6] for some other information. [6] is a paper that summaries the research history from Euclid to Green-Tao Theorem, studies the infinitude of some special kinds of prime and brings up some interesting questions. Our paper is just based on one of these questions. I thank Doctor Shaohua Zhang here for suggesting this interesting topic to us.

Note that if a number-theoretic function $f(x)$ represents infinitely many primes, we can get the following necessary condition: for every positive integer h, there exists a positive integer k, such that $(f(k),h)=1$, $f(k)>1$. Consequently, we are interested in functions that satisfy this necessary condition. Thus, if $f(x)$ satisfies this condition, there exists the smallest integer n such that $(f(n),h)=1$, $f(n)>1$. Denote n by $F_f(h)$. In this paper, we mainly focus on the three aforementioned functions, proving that they all satisfy this necessary condition, and approximately estimate the upper bound of $F_{f(x)}(h), F_{m(x)}(h), F_{l(x)}(h)$. Here are the results obtained.

Theorem 1 If $m(x)=2^x-1$, then for every positive integer h, there exists a least positive integer n such that $(m(n),h)=1$ and $m(n)>1$. In addition, there exists a constant C such that for every $h>C$, $n=F_{m(x)}(h)<\frac{3}{4}\log_2 h$.

Theorem 2 If $f(x)=2^{2^x}+1$, then for every positive integer h, there exists a least positive integer n such that for every $h>5$, $n=F_{f(x)}(h)\le \log_2(h-1)-1$.

Theorem 3 If $l(x)=x^2+1$, then for every positive integer h, there exists a least positive integer n, such that $(l(n),h)=1$, $l(n)>1$. In addition, for every $h>2$, $n=F_{l(x)}(h)\le \frac{h}{2}$.

Ⅱ. Proof of the theorems

In this paper, we denote the greatest common divisor of a and b by (a,b).

Lemma 1[5] For every positive integer m,n, $(2^i-1,2^j-1)=2^{(i,j)}-1$.

Lemma 2[4,5] Let p be an odd prime. If q is a prime factor of 2^p-1, $q\equiv 1(\bmod 2p)$.

Remark 1: From Lemma 2, we can get that for every positive integer h, $n=F_{m(x)}(h)\le\left[\frac{h+1}{2}\right]+1$.We give a stronger bound in the proof of Theorem 1.

Lemma 3[1] For integer $x\ge 487381$, $\sum_{p\le x}\log p>0.998x$, where $\log p$ represents the nature log of p.

Lemma 4[2] For every integer $x>117$, there exists at least one prime in $(x,\frac{14}{13}x]$.

Lemma 5[3] For $k>1$, the smallest prime factor of $f(k)=2^{2^k}+1$ is no less than $2^{k+2}+1$.

Proof of theorem 1: Remark 1 actually indicates that the first half of theorem 1 is true, so we only need to prove that there exists a constant C such that for every $h > C$, $n = F_{m(x)}(h) < \frac{3}{4}\log_2 h$ here. Let p_r be the r_{th} prime. If $2^{p_r} = h^{3/4}$, there is only one solution $p_r = 3$, $h = 16$, and $n = F_{m(x)}(h) = 2 < \frac{3}{4}\log_2 h$. Thus, we can let $2^{p_r} < h^{\frac{3}{4}} < 2^{p_{r+1}}$.

If there exists an i, $1 \le i \le r$, such that $(2^{p_i} - 1, h) = 1$, then $1 < 2^{p_i} - 1 < 2^{p_r} < h^{3/4}$. As a result, $n = F_{m(x)}(h) \le p_i \le p_r < \frac{3}{4}\log_2 h$. This means we only have to consider the case that for every $1 \le i \le r$, $(2^{p_i} - 1, h) > 1$. From Lemma 1 we know that for every $1 \le i \ne j \le r$, $(2^{p_i} - 1, 2^{p_j} - 1) = 1$. And from Lemma 2, we know that for every $i \ge 2$, the smallest prime factor of $2^{p_i} - 1$ is no less then $2p_i + 1$. Hence, $h \ge 3\prod_{i=2}^{r}(2p_i + 1)$. When $r \ge 2$, it leads to $h > \prod_{i=1}^{r} p_i$. As we have already assumed $h < 2^{4p_{r+1}/3}$ before, we can lead to a contradiction by proving that $\prod_{i=1}^{r} p_i > 2^{4p_{r+1}/3}$, thus finishing our proof. But to prove this was then beyond my ability. Thank to my teacher Jinsong Li, who introduced some beautiful results of analytic number theory to me, especially on the bound of Chebyshev function $\theta(x) = \sum_{p \le x} \log p$, which shed new light on my proving this problem. From Lemma 3, we know that for $p_r \ge 487381$, $\sum_{1 \le i \le r} \log p_i > 0.998 p_r$. Because $\frac{0.998 \times 13}{14} > \frac{4}{3}\log 2$, and from Lemma 4: when $p_r > 117$, $p_{r+1} \le \frac{14}{13} p_r$, we have that $\sum_{1 \le i \le r} \log p_i > 0.998 p_r > \frac{4}{3} p_{r+1} \log 2$. Thus, for $p_r \ge 487381$, $\prod_{i=1}^{r} p_i > 2^{4p_{r+1}/3}$. Because 487381 is a prime, let $C = 2^{1949524/3}$, then for every $h > C$, $n = F_{m(x)}(h) < \frac{3}{4}\log_2 h$.

Remark 2: we can prove that it is not easy to strengthen $\frac{3}{4}$, for instance, to $\frac{2}{3}$. From [1], we can get that $\sum_{1 \le i \le r} \log p_i < 1.001102 p_r < (\frac{3}{2}\log 2) p_r < (\frac{3}{2}\log 2) p_{r+1}$. This result increase the difficulty of strengthening this bound.

From the proof above we also know that $2^{3p_{n+1}/2} > \prod_{i=1}^{n} p_i$. Hence, for $p_n \geq 487381$, we have this result: $2^{2p_n} > 2^{3p_{n+1}/2} > 2^{3p_n/2} > \prod_{i=1}^{n} p_i > 2^{4p_{n+1}/3} > 2^{p_{n+1}}$. This inequality again demonstrates the famous result that for every $x > 1$, $(x, 2x)$ contains at least one prime.

Besides, our inequality $2^{3p_n/2} > p_1 ... p_n$ strengthens the inequality $2^{2p_n} > p_1 ... p_n$ in [4, pp389].

Proof of theorem 2: When $h > 5$, we can let $k = [\log_2(h-1)] - 1$, and $f(k) = 2^{2^{[\log_2(h-1)]-1}} + 1$. From Lemma 5, we know that the smallest divisor of $f(k)$ is greater than h. Hence we have $(2^{2^{[\log_2(h-1)]-1}} + 1, h) = 1$. Therefore, when $h > 5$, $n = F_{f(x)}(h) \leq k \leq \log_2(h-1) - 1$. When $1 \leq h \leq 5$, we can prove that the first half is true directly.

Proof of theorem 3: The proof of the first half of the theorem is obvious, so we only need to prove that when $h > 2$, $n = F_{l(x)}(h) \leq \frac{h}{2}$. When h is odd, $n = F_{l(x)}(h) = 1 < \frac{h}{2}$. When h is even, we first consider the case when $4 | h$. Let $h = 4t$, where t is a positive integer. Because $((2t)^2 + 1, 4t) = 1$, we have $n = F_{l(x)}(h) \leq 2t = \frac{h}{2}$. If $2 \| h$, because $h > 2$, we let $h = 4t + 2$, where t is a positive integer. Since $((2t)^2 + 1, 4t + 2) = 1$, $n = F_{l(x)}(h) \leq 2t < \frac{h}{2}$. Thus we have proved theorem 3.

Ⅲ. Some related questions

Question 1: In the proof of Theorem 1, $C = 2^{1949524/3}$ is obviously a very approximate bound. By observation and computation, however, we conjecture that C is very likely to be 84, yet we have not finished verifying this.

Question 2: We don’t know how to strengthen the result in Theorem 2, but we know it is related to the smallest prime divisor of Fermat number. Up to now, however, Lemma 5 has not been improved. Besides, it is easy to prove that $F_{f(x)}(h)$ cannot be always less than $\log_2 \log_2(h+1)$.

Question 3: By calculating, we conjecture that for $h > 10$, $n = F_{l(x)}(h) < \sqrt{h-1}$. We will consider this problem further. More generally, Doctor Shaohua Zhang pointed out that if $l(x) = a_k x^k + \cdots + a_1 x + a_0$ represents infinitely many primes, there might be

$n = F_{l(x)}(h) < \sqrt[k]{h/a_k}$ for every sufficiently large h. He also told me it is interesting to study the primality of $F_f(h)$, $f(F_f(h))$, $F_f(h!)$, $f(F_f(h!))$. For example, for every positive integer h, $F_{m(x)}(h)$ is a prime while $m(F_{m(x)}(h))$ is not always one; $F_{l(x)}(h)$ and $l(F_{l(x)}(h))$ are not always prime. As for $f(F_f(h!))$, we don't know whether $m(F_{m(x)}(h!))$ and $l(F_{l(x)}(h!))$ are always primes now. However, we know that $f(F_{f(x)}(h!))$ is not always a prime.

In the end of my paper, I want to first thank Professor Shing-Tung Yau for offering middle school students this valuable opportunity of exploring further into math. Although the result I've obtained is a small one, it is my first try in mathematic study. It is an experience completely different from tests in school, in which I understood both the hardship and happiness of research. Here I also want to thank my mother. It is she who helped me proofread the paper, test some of the data, adjust the format, and get access to many papers and books of number theory. By reading these, I deeply appreciated the beauty of Number Theory.

References

[1] Rosser J. Barkley, Schoenfeld Lowell, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, Math. Comp., 29, pp243-269, 1975

[2] H. Rohrbach and J. Weis, Zum finiten Fall des Bertrandschen Postulats, J. Reine Angew. Math. 214/215, pp432-440, 1964

[3] 柯召，孙琦，初等数论100例，上海教育出版社，1980

[4] 潘承洞，潘承彪，初等数论，北京大学出版社，1992

[5] 柯召， 孙琦， 数论讲义， 高等教育出版社， 1987

[6] Shao-hua Zhang, On the infinitude of some special kinds of primes, (http://arxiv.org/abs/0905.1655)