Commun. Korean Math. Soc. **19** (2004), No. 2, pp. 205–210

INFINITELY MANY PRIMES OF THE FORM $An+1$ ANOTHER ELEMENTARY PROOF

Jisang Yoo

Abstract. According to Diriclet's Theorem, there are infinitely many primes of the form $An+1$ for any fixed positive integer A. For this, there already exists a classical simple proof using cyclotomic polynomials. In this paper, we develop another elementary proof of this statement.

1. Introduction

Dirichlet's Theorem is the following.

Theorem 1.1 (Dirichlet's Theorem). *If A and B are relatively prime positive integers, there are infinitely many primes of the form $An + B$. In other words, the set $\{An + B : \quad n \in \mathbb{N}\}$ contains infinitely many primes.*

This theorem is known to be proved by P. G. L. Dirichlet using analysis. Here we give an elementary proof of the restricted case when $B = 1$. This restricted case is that for any fixed positive integer A, there are infinitely many primes of the form $An + 1$. Actually, there already is a well-known classical and simple proof of this fact using cyclotomic polynomials and the proof can be found in [1] and [2].

The purpose of this paper is to provide another elementary proof without using cyclotomic polynomials. We concentrate on constructing an irreducible fraction such that every prime factor of the numerator of it is of the form $An + 1$ and that the numerator is greater than one so that the numerator has at least one prime factor.

Received September 12, 2002.

2000 Mathematics Subject Classification: 11A41.

Key words and phrases: prime number, Dirichlet's theorem.

2. Lemmas

To achieve our goal, we need two lemmas. The first lemma is about polynomials over $\mathbb{Z}$. And the second lemma is about $\frac{(Ax)^A-1}{(Ax)^a-1}$ where a is a factor of the integer $A > 1$ and x is a positive integer. The fraction $\frac{(Ax)^A-1}{\prod_{a|A,a<A}((Ax)^a-1)}$ plays a key role in our main proof.

LEMMA 2.1. *Let $f(x), g(x) \in \mathbb{Z}[x]$ be nonzero polynomials over $\mathbb{Z}$ such that there is no polynomial $h(x) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ satisfying $h(x)g(x) = f(x)$. Then the set defined by*

$$D(g,f) = \{i \in \mathbb{N} : \quad g(i) \text{ divides } f(i)\}$$

is finite.

PROOF. There exist polynomials $q'(x), r'(x) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ such that: $f(x) = q'(x)g(x) + r'(x), 0 < \deg(r') < \deg(g)$ and $r'(x)$ is a nonzero polynomial.

Then there is a number $M \in \mathbb{N}$ such that $Mq'(x) \in \mathbb{Z}[x], Mr'(x) \in \mathbb{Z}[x]$.

Let $q(x) = Mq'(x), r(x) = Mr'(x)$, then we have:

$$Mf(x) = q(x)g(x) + r(x), \quad g(x), r(x) \in \mathbb{Z}[x].$$

And $r(x)$ is still a nonzero polynomial such that $0 < \deg(r) < \deg(g)$. Since $r(x), g(x)$ are nonzero polynomials, they have a finite number of zeros, so that there exists $N_1 \in \mathbb{N}$ such that:

$$i > N_1 \Longrightarrow \frac{r(i)}{g(i)} \neq 0.$$

Since $0 < \deg(r) < \deg(g)$, we have $\lim_{i\to\infty} \frac{r(i)}{g(i)} = 0$, so that there exists $N_2 \in \mathbb{N}$ such that:

$$i > N_2 \Longrightarrow -\frac{1}{2} < \frac{r(i)}{g(i)} < \frac{1}{2}.$$

If we let $N = \max(N_1, N_2)$, we have:

$$i > N \Longrightarrow 0 < \left|\frac{r(i)}{g(i)}\right| < \frac{1}{2}.$$

Then for each integer i with $i > N$, $\frac{r(i)}{g(i)}$ is not an integer so that $g(i) \nmid r(i)$. Thus,

$$i > N \Longrightarrow g(i) \nmid r(i).$$

From $Mf(i) = q(i)g(i) + r(i)$, we see that $g(i) \nmid r(i)$ implies $g(i) \nmid Mf(i)$ and further $g(i) \nmid f(i)$. Therefore we have:

$$i > N \Longrightarrow g(i) \nmid f(i).$$

This shows that any element of $D(g, f)$ is less than or equal to N, therefore the set $D(g, f)$ is finite. □

LEMMA 2.2. *Let $A \in \mathbb{N}$ be a number with $A > 1$. Let $a \in \mathbb{N}$ be a factor of A, i.e. $a \mid A$. Let $x \in \mathbb{N}$ be a number. Then $\frac{(Ax)^A-1}{(Ax)^a-1}$ is a positive integer and*

$$\gcd\left(\frac{(Ax)^A - 1}{(Ax)^a - 1}, (Ax)^a - 1\right) = 1.$$

PROOF. First, $(Ax)^A - 1$ and $(Ax)^a - 1$ are positive integers. And there exists $b \in \mathbb{N}$ such that $ab = A$. Now we observe :

$$\frac{(Ax)^A - 1}{(Ax)^a - 1} = \sum_{i=0}^{b-1} ((Ax)^a)^i.$$

This equation shows that $\frac{(Ax)^A-1}{(Ax)^a-1}$ is a positive integer. From this equation, we get:

$$\frac{(Ax)^A - 1}{(Ax)^a - 1} \equiv \sum_{i=0}^{b-1} 1 \equiv b \pmod{(Ax)^a - 1}$$

$$(Ax)^a - 1 \equiv 0 - 1 \equiv -1 \pmod{b}.$$

Consequently,

$$\gcd\left(\frac{(Ax)^A - 1}{(Ax)^a - 1}, (Ax)^a - 1\right) = \gcd(b, (Ax)^a - 1) = \gcd(b, -1) = 1.$$

□

3. The proof

Now, we are going to prove the main theorem after introducing the function num.

DEFINITION 3.1. (Here $\mathbb{Q}_+$ denotes the set of all positive rational numbers.) We define the function num : $\mathbb{Q}_+ \longrightarrow \mathbb{N}$ as follows ('num' is the abbreviation of 'numerator'). For each $r \in \mathbb{Q}_+$, define $\text{num}(r) = m$, where $m, n \in \mathbb{N}$ is the unique pair such that $\gcd(m, n) = 1$ and $r = \frac{m}{n}$.

For arbitrary two numbers $a, b \in \mathbb{N}$, we have:

1. $a \mid b \iff \mathrm{num}(\frac{a}{b}) = 1$,
2. $\mathrm{num}(a) = a$,
3. $\mathrm{num}(\frac{a}{b}) \mid a$.

Now, we declare and prove a theorem which will be proved to be equivalent to our main theorem. The proof of the following theorem saying the existence of at least one prime of the form $An+1$ is the main part of this paper. Proving the fact that the following theorem implies the existence of infinitely many primes of the form $An+1$ is easy as we shall see.

THEOREM 3.2. *Let $A \in \mathbb{N}$ be a number with $A > 1$. Then there exists a prime number p of the form $An+1$.*

PROOF. This proof consists of three steps. In *Step 1*, we construct a particular positive rational number S with $\mathrm{num}(S) > 1$. In *Step 2*, we prove some properties of $\mathrm{num}(S)$. And finally in *Step 3*, we fix an arbitrary prime factor p of $\mathrm{num}(S)$ and prove that p is of the form $An+1$.

Step 1 :

Define two polynomial $E(x), F(x) \in \mathbb{Z}[x]$ as follows:

$$E(x) = x^A - 1, \quad F(x) = \prod_{a \mid A, a < A} (x^a - 1).$$

If the polynomial $E(x)$ is a factor of the polynomial $F(x)$ as element of $\mathbb{Q}[x]$, every zero of $E(x)$ would be also a zero of $F(x)$. But $e^{\frac{2\pi\sqrt{-1}}{A}}$ is a zero of $E(x)$ and is not a zero of $F(x)$. Therefore the polynomial $E(x)$ is not a factor of the polynomial $F(x)$. By Lemma 2.1, the set defined by

$$D(E,F) = \{i \in \mathbb{N} : \quad E(i) \mid F(i)\}$$

is finite. Since $D(E,F)$ is finite, we can choose a number $k \in \mathbb{N}$ such that $Ak \notin D(E,F)$. Then we have $E(Ak) \nmid F(Ak)$. If we define S as follows,

$$S = \frac{E(Ak)}{F(Ak)} = \frac{(Ak)^A - 1}{\prod_{a \mid A, a < A}((Ak)^a - 1)}.$$

We get $S \in \mathbb{Q}_+$ and $\mathrm{num}(S) > 1$.

Step 2 :

By the definition of S, we have:

$$\mathrm{num}(S) \mid \left((Ak)^A - 1\right). \tag{3.1}$$

For each $a_1 \in \mathbb{N}$ such that $a_1 \mid A, a_1 < A$, we can express S as follows:

$$S = \frac{((Ak)^A - 1)/((Ak)^{a_1} - 1)}{\prod_{a|A,a<A,a\neq a_1}((Ak)^a - 1)}.$$

Of the right-hand-side of the above expression, the numerator and the denominator are integers, so that $\mathrm{num}(S) \mid ((Ak)^A - 1)/((Ak)^{a_1} - 1)$. Since the choice of a_1 was arbitrary, we have

$$\text{(3.2)} \quad \mathrm{num}(S) \mid \frac{(Ak)^A - 1}{(Ak)^a - 1} \quad \text{for all} \quad a \quad \text{such that} \quad a \mid A \text{ and } a < A.$$

Therefore,

$$\gcd(\mathrm{num}(S), (Ak)^a - 1) \mid \gcd\left(\frac{(Ak)^A - 1}{(Ak)^a - 1}, (Ak)^a - 1\right)$$
$$\text{for all a such that} \quad a \mid A \text{ and } a < A.$$

Then by Lemma 2.2, we have

$$\text{(3.3)} \quad \gcd(\mathrm{num}(S), (Ak)^a - 1) = 1 \text{ for all } a \text{ such that } a \mid A \text{ and } a < A.$$

Step 3 :

Since $\mathrm{num}(S) > 1$, $\mathrm{num}(S)$ has at least one prime factor p. Now, we will show that the prime factor p is of the form $An + 1$. From the equations 3.1, 3.3, we have the following two results:

1. $p \mid \left((Ak)^A - 1\right)$,
2. $p \nmid ((Ak)^a - 1)$ for all a such that $a \mid A$ and $a < A$.

And these two results express the following two facts:

1. $(Ak)^A \equiv 1 \pmod{p}$,
2. $(Ak)^a \not\equiv 1 \pmod{p}$ for all a such that $a \mid A$ and $a < A$.

These show that the order of Ak in the multiplicative group $\mathbb{Z}_p^*$ is A. Since the order of each element of $\mathbb{Z}_p^*$ divides the order of the group $\mathbb{Z}_p^*$, namely $(p - 1)$, we have

$$A \mid (p - 1).$$

Therefore the prime p is of the form $An + 1$. □

Corollary 3.3. *Let $A \in \mathbb{N}$ be a number with $A > 1$. Then there are infinitely many primes of the form $An + 1$.*

Proof. Let $i \in \mathbb{N}$ be an arbitrary positive integer. Then by Theorem 3.2, there exists a prime number p_i of the form $(iA)n + 1$ and we get $iA \mid (p_i - 1)$. Since p_i is of the form $(iA)n + 1$, p_i is also of the form $An + 1$. We observe that $i < iA \leqq p_i - 1$ so that $i \leqq p_i$. Therefore p_i is a prime number of the form $An + 1$ greater than or equal to i. Since i

was arbitrary, we always have arbitrary large prime number of the form $An+1$. □

In the above corollary, we can easily get rid of the restriction $A > 1$.

ACKNOWLEDGEMENT. When I completed my proof while not aware of the classical proof, Sang Geun Hahn informed me of the classical proof [2]. And Hoju Lee informed me of the another classical one [1].

References

[1] Hua Loo Keng, *Introduction to Number Theory*, Springer-Verlag, New York (1982), 97–99.

[2] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York (1982), 12–13.

Department of Mathematics
KAIST
Daejon 305-701, Korea
E-mail: yoojisang@kaist.ac.kr