Hypothesis of Schinzel and Sierpiński and Cyclotomic Fields with Isomorphic Galois Groups

By

Shin-ichi KATAYAMA

Department of Mathematical Sciences,
Graduate School of Science and Engineering
Tokushima University,
Minamijosanjima-cho 2-1, Tokushima 770-8506, JAPAN
e-mail address : *shinkatayama@tokushima-u.ac.jp*
(Received September 30, 2016)

Abstract

In 1922 R. D. Carmichael conjectured that for any natural number n there exist infinitely many natural numbers m such that $\varphi(n) = \varphi(m)$. It is well known that this conjecture can be proved under the assumption of the famous unproved hypothesis of Schinzel and Sierpiński. In this short note, we shall show the Hypothesis of Schinzel and Sierpiński implies more precisely that the existence of infinitely many cyclotomic fields $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)$ with isomorphic absolute Galois groups. Here ζ_n and ζ_m are primitive nth and mth roots of unity with $m \neq n$.

2010 Mathematics Subject Classification. Primary 11R18; Secondary 11C08

Introduction

The following conjecture of Carmichael on the values of Euler's function φ is well known:

(**C**) *For any natural number n, there exists a natural number $m \neq n$, such that $\varphi(n) = \varphi(m)$.*

It is known that this conjecture can be proved under the assumption of the following unproved hypothesis of Schinzel and Sierpiński:

(**S**) *Let $f_1(x), \ldots, f_s(x)$ be irreducible polynomials, with integral coefficients and*

positive leading coefficients. Assure that $f_1(x), \ldots, f_s(x)$ satisfy the following condition:

$(*)$ *There does not exist any integer $d > 1$ dividing all the products $f_1(k) \cdots f_s(k)$, for every integer k.*

Then there exist infinitely many natural numbers l such that all numbers $f_1(l), \ldots, f_s(l)$ are primes.

In the following, we call this unproved hypothesis of Schinzel-Sierpiński by (**S**) and we shall investigate a problem closely related to the above Carmichael's conjecture (**C**). Let n be an integer greater than 2 and ζ_n be a positive nth root of unity. We denote the nth cyclotomic field $\mathbb{Q}(\zeta_n)$ by K_n and the Galois group of $K_n/\mathbb{Q}$ by $G(n)$. Then $G(n)$ is isomorphic to $(\mathbb{Z}/n\,Z)^\times$, the multiplicative group of residue classes (mod n), prime to n. In this paper, we shall consider several conditions for m and n such that $G(n) \cong G(m)$ but $K_n \neq K_m$. Since the order of the Galois group $G(n)$ equals to $\varphi(n)$, one can easily see this problem is closely related to Carmichael's conjecture (**C**) and a precise version of (**C**).

1 Main Theorem

Note that, for any odd n, the fields K_n and K_{2n} coincide, whence it suffices to deal in the sequel with the cases $n \not\equiv 2 \pmod 4$. Hence $n \neq m$ implies $K_n \neq K_m$ for these cases and our problem is nothing but to find $n > m$ such that $G(n) \cong G(m)$.

First we consider the case when $G(n)$ is cyclic, that is, $n = 4$ or p^r, where p is an odd prime and $r \geq 1$. Then we have

Lemma 1. *With the above notation, the following conditions are equivalent.*

i) *$n > m$ and $G(n)$ and $G(m)$ are cyclic groups of the same order.*

ii) *$\{n, m\} = \{4, 3\}$ or $(\{p^r, p^r - p^{r-1} + 1\}$, where p and $p^r - p^{r-1} + 1$ are odd primes $(r \geq 2)$.*

Proof. Since it is obvious that (ii) implies (i), it suffices to show that (i) implies (ii). If $n = 4$, then $(\mathbf{Z}/m\mathbf{Z})^\times \cong (\mathbf{Z}/4\mathbf{Z})^\times$ $(m \neq 4)$ only for $m = 3$. If $n = p^r$ and $m = q^s$, where q is also an odd prime, then $G(n) \cong G(m)$ implies $p^{r-1}(p-1) = q^{s-1}(q-1)$. In the case $r = s = 1$ or $r \geq 2$ and $s \geq 2$, we have $p = q$ and $r = s$, that is, $n = m$. Hence $r = 1$, $s \geq 2$ or $r \geq 2$, $s = 1$. From the assumption $n > m$, one sees $r \geq 2$ and $s = 1$, that is, $n = p^r$ and $m = q = p^r - p^{r-1} + 1$ $(r \geq 2)$, which completes the proof.

Let $g_r(x)$ $(r \geq 2)$ be the polynomial $x^r - x^{r-1} + 1$. Modifying Selmar's reault (c.f. exm.1.22 in [2]), one can easily show the following lemma.

Lemma 2. *When $r \not\equiv 2 \pmod 6$, $g_r(x)$ is irreducible. When $r \equiv 2 \pmod 6$, $(x^2 - x + 1) \mid g_r(x)$ and the quotient $g_r(x)/(x^2 - x + 1)$ is irreducible.*

Proof. Let $h(x) = x^r + c_1 x^{r-1} + \cdots + c_r = (x - \alpha_1) \cdots (x - \alpha_r)$ be the polynomial such that $h(x) \in \mathbf{Z}[x]$ and $c_r \neq 0$, with the roots $\alpha_1, \ldots, \alpha_r \in \mathbf{C}$. We put $S(h) = \sum_{i=1}^r \alpha_i -$

α_i^{-1}. Then one sees $S(h) \in \mathbf{Q}$ and, for the case $c_r = \pm 1$, one sees $S(h) \in \mathbf{Z}$. When $h(x) = h_1(x)h_2(x)$, with monic polynomials $h_i(x) \in \mathbf{Z}[x]$ and $\deg h_i \geq 1$, it is obvious that $S(h) = S(h_1)+S(h_2)$. In the case $g_r(x)$ with $r \not\equiv 2 \pmod 6$, one sees $S(g_r) = -1$. Using the fact that $|\alpha_i| \neq 1$ for $1 \leq i \leq r$, one sees $S(h) \leq -1$ for any factor $h(x)|g_r(x)$, where $h(x)$ is a monic polynomial in $\mathbf{Z}[x]$. Hence for the case $g_r(x) = p(x)q(x)$, with monic polynomials $p(x), q(x) \in \mathbf{Z}[x]$, one sees $S(g_r) = S(p) + S(q) \leq -2$, which contradicts the fact $S(g_r) = -1$. Therefore $g_r(x)$ is irreducible for the case $r \not\equiv 2 \pmod 6$. In the case $r \equiv 2 \pmod 6$, we can show the desired results in the same way as above.

Combining these lemmas, we have the following theorem.

Theorem 1. *Under the assumption of Schinzel-Sierpiński hypothesis, there exist infintely many pairs of cyclic cyclotomic fields $K_n \neq K_m$ such that $G(n) \cong G(m)$.*

Proof. Put $f_1(x) = x$ and $f_2(x) = g_r(x)$, where $r(\not\equiv 2 \pmod 6)$ is an arbitrary integer greater than 2 or $= 2$. From the fact $f_1(1) = f_2(1) = 1$ and Lemma 2, $f_1(x)$ and $f_2(x)$ satisfy the condition $(*)$ of $(\mathbf{S})$

Hence, from Schinzel-Sierpiński hypothesis, there are infinitely many pairs of odd primes p, q such that $q = f_2(p) = p^r - p^{r-1} + 1$. Putting $n = p^r$ and $m = q = p^r - p^{r-1} + 1$, one can take infinitely many pairs of cyclotomic fields $K_n \neq K_m$ with isomorphic cyclic Galois groups $G(n) \cong G(m)$. Under the same assumption, one can get the following more general result:

Theorem 2. *Let t be any integer greater than 2. Then, under the assumption of Schinzel-Sierpiński hypothesis, there exist infinitely many different cyclotomic fields $K_{n_1}, \ldots, K_{n_t}$ such that $G(n_1) \cong G(n_2) \cong \cdots \cong G(n_t)$.*

Proof. From Theorem 1, there exist n_{01}, n_{11} such that $(n_{01}, n_{11}) = 1$ and $G(n_{01})$ and $G(n_{11})$ are isomorphic cyclic groups. Let a be a mininal integer such that $t \leq 2^a$. Then, inductively one gets the two sets of integers $\{n_{01}, n_{02}, \ldots, n_{0a}\}$ and $\{n_{11}, n_{12}, \ldots, n_{1a}\}$ which satisfy the following conditions,

$(n_{ij}, n_{kl}) = 1$ for $(i, j) \neq (k, l)$ and $G(n_{0j}) \cong G(n_{1j})$ $(1 \leq j \leq a)$.

For any $v = (v_1, \ldots, v_a) \in (\mathbf{Z}/2\mathbf{Z})^a$, we put $N(v) = n_{v_1 1} \times n_{v_2 2} \times \cdots \times n_{v_a a}$. We denote $n_{01} \times n_{02} \times \cdots \times n_{0a}$ by N_0. Then for any $v \neq v' \in (\mathbf{Z}/2\mathbf{Z})^a$, we have $K_{N(v)} \neq K_{N(v')}$ and $G(N(v)) \cong G(N(v')) \cong G(N_0)$, which completes the proof.

Remark 1. The proofs of above theorems give a method of construction of the cyclotomic fields with isomorphic Galois groups.
For example $n_{01} = 3 = 2^2 - 2 + 1$, $n_{02} = 43 = 7^2 - 7 + 1$, $n_{03} = 101 = 5^3 - 5^2 + 1$ and
$n_{11} = 4 = 2^2$, $n_{12} = 49 = 7^2$, $n_{13} = 125 = 5^3$ satisfy the conditions in the proof of Theorem 2. Therefore, putting $N_0 = 13029 = 3 \times 43 \times 101$, $N_1 = 14847$,$N_2 = 16125$, $N_3 = 17372$, $N_4 = 18375$, $N_5 = 19796$, $N_6 = 21500$, $N_7 = 24500$, one gets 8 cyclotomic fields $K_{N_i} \neq K_{N_j}$
$(0 \leq i \neq j \leq 7)$ with isomorphic Galois proups $G(N_i) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/42\mathbf{Z} \times \mathbf{Z}/100\mathbf{Z}$.

2 Several Applications

In this section, we shall consider the integer solutions (x, y) which satisfy the equation

$$(E_a) \quad \varphi(x) = y^a,$$

where a is a fixed integer greater than 2.
Since $\varphi(2^{a+1}) = 2^a$, one sees $(x, y) = (2^{a+1}, 2)$ satisfies the equation (E_a). Hence (E_a) has at least one integer solution for any a.
Let (x, y) be a solution of (E_a), then, for any prime divisor p of x, we have $\varphi(p^a x) = p^a \varphi(x) = (py)^a$. Hence $(p^a x, py)$ is also a solution of (E_a).
Moreover, let (x_1, y_1), (x_2, y_2) be the solutions of (E_a) and $(x_1, x_2) = 1$, then $\varphi(x_1 x_2) = \varphi(x_1)\varphi(x_2) = (y_1 y_2)^a$. Hence $(x_1 x_2, y_1 y_2)$ is a new solution of (E_a). Hence we have shown the following lemma.

Lemma 3. *The solutions of (E_a) satisfy the following properties.*

(1) *Let (x, y) be a solution of (E_a) and p is a prime divisor of x, then $(p^a x, py)$ is a solution of (E_a).*

(2) *Let (x_1, y_1) and (x_2, y_2) be solutions of (E_a) and $(x_1, x_2) = 1$, then $(x_1 x_2, y_1 y_2)$ is a solution of (E_a)*

Let (x_1, y_1) and (x_2, y_2) be the solutions of (E_a). By abuse of language, we call two solutions (x_1, y_1) and (x_2, y_2) are coprime when $(x_1, x_2) = 1$. From Lemma 3 (1) and the fact $\varphi(2^{a+1}) = 2^a$, one sees (E_a) has infinitely many integer solutions $(2^{ab+1}, 2^b)$, where $b \geq 0$. But, it is not obvious that (E_a) has infinitely many coprime solutions.
First, we consider the case $a = 2$. Then the equation (E_2) has a solution (x, y) with a prime x, if and only if x is a prime of the form $y^2 + 1$. Hence, if one assumes Hardy-Littlewood's conjecture on the prime values of the irreducible quadratic polynomials, the equation (E_2) has infinitely many coprime integer solutions (x, y) with primes x. Moreover, using Theorem 1, one can also show (E_2) has infinitely many coprime integer solutions as follows.
Let p and q are odd primes such that $q = p^r - p^{r-1} + 1$ $(r \geq 2)$. Put $x = p^r q$. Then $\varphi(x) = \varphi(p^r)\varphi(q) = (p^{r-1}(p-1))^2$. Therefore, under the assumption of Shinzel-Sierpiński hypothesis (S), one can show the equation (E_2) has infinitely many coprime integer solutions with composite number x.
In the same way as (E_2), we have the following theorem.

Theorem 3. *Under the assmption of Shinzel-Sierpińshi hypothesis, the equation E_a has infinitely many coprime integer solution (x, y) for any $a \geq 2$.*

Proof. Put $f_1(x) = x, f_2(x) = g_{r_2}(x), \ldots, f_a(x) = g_{r_a}(x)$, where $r_2, \ldots, r_a$ are natural numbers $\not\equiv (\mathrm{mod}\ 6)$ or 2 and $2 \leq r_2 \leq \cdots \leq r_a$. Let b be a nutulal number such that $b \equiv -1 - r_2 - \cdots - r_a \ (\mathrm{mod}\ a)$. We denote the quotient $(b + 1 + r_2 + \cdots + r_a)/a$ by c. From the assumption, there are infinitely many primes p such that $q_2 = f_2(p) = p^{r_2} - p^{r_2 - 1} + 1, \ldots, q_a = f_a(p) = p^{r_a} - p^{r_a - 1} + 1$, are also primes. Put $n = p^{b+1} \cdot q_2 \cdots \cdots q_a$. Then $\varphi(n) = \varphi(p^{b+1})\varphi(q_2) \cdots \varphi(q_a) = p^b(p-1) \times p^{r_2 - 1}(p-1) \times \cdots \times p^{r_a}(p-1) = (p-1)^a p^{b + (r_2 - 1) + \cdots + (r_a - 1)} = (p-1)^a p^{b+1+r_2+\cdots+r_a - a} = ((p-1)p^{c-1})^a$. Hence (E_a) has infinitely many coprime integer solutions.

We note that the proof of the above thorem gives a method of constructing the coprime solutions for (E_a). To make a lang story short, we consider the numerical examples for the case $r = 3$.

Examples. In the case $p = 3$, one sees $g_2(3) = 7$, $g_3(3) = 19$ and $g_5(3) = 163$ are primes. Putting $N_0 = 3 \cdot 7 \cdot 19$ and $N_1 = 3 \cdot 19 \cdot 163$, we have $\varphi(N_0) = 6^3$ and $\varphi(N_1) = 18^3$.
In the case $p = 5$, one sees $g_3(5) = 101$ and $g_7(5) = 62501$ are primes. Putting $N_2 = 5^2 \cdot 101 \cdot 62501$, we have $\varphi(N_2) = 500^3$.
In the case $p = 7$, one sees $g_2(7) = 43$ and $g_5(7) = 14407$ are primes. Putting $N_3 = 7^2 \cdot 43 \cdot 14407$, we have $\varphi(N_3) = 294^3$.
In the case $p = 11$, one sees $g_{11}(11) = 259374246011$ and $g_{25}(11)$
$= 984973267580761109471184 11$ are primes. Putting $N_4 = 11^3 \cdot g_{11}(11) \cdot g_{25}(11)$, we have $\varphi(N_4) = (11^{12} \cdot 10)^3$.
In the case $p = 13$, one sees $g_2(13) = 157$ and $g_3(13) = 2029$ are primes. Putting $N_5 = 13 \cdot 157 \cdot 2029$, we have $\varphi(N_5) = 156^3$.
Thus we have obtained coprime solutions $(N_1, 18), \ldots, (N_5, 156)$ for (E_3).

In the same way as above, one might get other coprime solutions for each (E_a).

References

[1] R .D. Carmichael, Note on Euler's ϕ-function, Bull.Amer.Math.Soc, **28** (1922) 109-110.

[2] G. Fujisaki, Fields and Galois Theory (in Japanese), Iwanami-shoten, Tokyo, 1991.

[3] R. K. Guy, Unsolved Problems in Number Theory, 2nd ed., Springer-Verlag, New Yoek, 1994.

[4] P. Ribenboim, The Book of Prime Number Records, 2nd ed., Springer-Verlag, New York, 1989.

[5] A. Schinzel and W. Sierpiński, Sur certaines hypothèsis concernant les nombers premiers. Remarque, Acta Arith., **4** (1958) 185-208 and **5** (1959) 259.

[6] A. Schinzel, Remarks on the paper "Sur certaines hypothèsis concernant les nombers premiers", Acta Arith., **7** (1961) 1-8.

Groups of automorphisms of fields. Separable, normal, and Galois extensions. The fundamental theorem of Galois theory. Examples. Constructible numbers revisited. The Galois group of a polynomial. Solvability of equations. Exercises. 4 Computing Galois Groups. When is Gf in An? When does Gf act transitively on the roots? Polynomials of degree at most three.Â X Y X is a subset of Y (not necessarily proper). X Ddef Y X is dened to be Y , or equals Y by denition. X Y X is isomorphic to Y . X ' Y X and Y are canonically isomorphic (or there is a given or unique isomorphism). PREREQUISITES. Group theory (for example, GT), basic linear algebra, and some elementary theory of rings. References. Jacobson, N., 1964, Lectures in Abstract Algebra, Volume III, van Nostrand. Andrzej Schinzel. WacÅ‚aw SierpiÅ„ski. View. Stratified Morse Theory (Ergebnisse der Mathematik Und Ihrer Grenzgebiete.Â The Schinzel hypothesis essentially claims that finitely many irreducible polynomials in one variable over â„¤ simultaneously assume infinitely many prime values unless there is an obvious reason why this is impossible. We prove that under a restriction on the characteristic and a smoothness assumption, finitely many irreducible polynomials in one variable over the ring Fq[t] assume simultaneous prime values after a sufficiently large extension of the field of constants. View. Show abstract.Â â‰¥ 1. The techniques rely on a detailed analysis of the splitting field and Galois group, together with frequent use of Hilbert's Theorem 90. Read more. Article.