*Advances in Pure Mathematics*, 2013, 3, 24-28
http://dx.doi.org/10.4236/apm.2013.31005 Published Online January 2013 (http://www.scirp.org/journal/apm)

# Integral Sequences of Infinite Length Whose Terms Are Relatively Prime

**Kazuyuki Hatada**
Department of Mathematics, Faculty of Education, Gifu University, Gifu, Japan
Email: hatada@gifu-u.ac.jp

Received September 7, 2012; revised October 10, 2012; accepted November 13, 2012

## ABSTRACT

It is given in Weil and Rosenlicht ([1], p. 15) that G.C.D.$\left(c^{2^m}+1, c^{2^n}+1\right)=1$ (resp. 2) for all non-negative integers $m$ and $n$ with $m \neq n$ if $c$ is any even (resp. odd) integer. In the present paper we generalize this. Our purpose is to give other integral sequences $\{y_n\}_{n=1}^{\infty}$ such that G.C.D.$(y_m, y_n)=1$ for all positive integers $m$ and $n$ with $m \neq n$. Roughly speaking we show the following 1) and 2). 1) There are infinitely many polynomial sequences $\{f_n(X)\}_{n=1}^{\infty} \subset \boldsymbol{Z}[X]$ such that G.C.D.$\left(f_m(a), f_n(a)\right)=1$ for all positive integers $m$ and $n$ with $m \neq n$ and infinitely many rational integers $a$. 2) There are polynomial sequences $\{g_n(X,Y)\}_{n=1}^{\infty} \subset \boldsymbol{Z}[X,Y]$ such that G.C.D.$\left(g_m(a,b), g_n(a,b)\right)=1$ for all positive integers $m$ and $n$ with $m \neq n$ and arbitrary (rational or odd) integers $a$ and $b$ with G.C.D.$(a,b)=1$. Main results of the present paper are Theorems 1 and 2, and Corollaries 3, 4 and 5.

**Keywords:** Relatively Prime; Integral Sequences of Infinite Length; Sets of Infinitely Many Prime Numbers

## 1. Introduction

The numbers $F_n=2^{2^n}+1 (n=0,1,2,3,\cdots)$ are called Fermat numbers. Fermat conjectured that $F_n$ were all prime numbers. One has $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ and $F_5=641\times 6700417$. By now, no Fermat prime has been found except for $F_j\,(j=0,1,2,3,4)$. In Euclid's books was given the proof of existence of infinitely many prime numbers. By proving G.C.D. $(F_m, F_n)=1$ if $m \neq n$, Pólya gave another proof of that, cf. ([2], Theorem 16, p. 14) and ([3], exercise (viii), p. 7). Weil and Rosenlicht ([1], p. 15) considered not only $F_n$ but also $c^{2^n}+1$ for any rational integer $c$.

Let $n$ be any positive integer, and let $\zeta_n$ be any primitive $n$-th root of unity. Let $S(n)=\{\zeta \in \boldsymbol{C} \mid \zeta$ is a primitive $n$-th root of unity$\}$. Then *the number of* $S(n)=\varphi(n)$ where $\varphi$ denotes the Euler function. Let $\Phi_n(T)$ denote the $n$-th cyclotomic polynomial over $\boldsymbol{Q}$. Namely, $\Phi_n(T)$ denotes the polynomial $\in \boldsymbol{Q}[T]$ of the minimum degree whose roots contain $\zeta_n$ and whose leading coefficient is 1. One has that $\Phi_n(T)$ does not depend on choice of $\zeta_n$ in $S(n)$, that $\Phi_n(T) \in \boldsymbol{Z}[T]$ and that $\Phi_n(T)=\prod_{\zeta \in S(n)}(T-\zeta)$, (see e.g. [4-8]). Below in this paper we write $\Phi(n,T)=\Phi_n(T)$.

We let G.C.D. denote "greatest common divisor" as usual. One has $\Phi\left(2^n,T\right)=T^{2^{n-1}}+1$. Then exercise IV.3 in [1] asserts G.C.D.$\left(\Phi\left(2^n,c\right),\Phi\left(2^m,c\right)\right)=1$ (resp. 2) for all positive integers $m$ and $n$ with $m \neq n$ if $c$ is even (resp. odd).

We generalize this. Let $p$ denote any odd prime number, and let $v$ denote any rational integer. In Theorem 2 in Section 3 below we show that G.C.D.$\left(\Phi\left(p^n,v\right),\Phi\left(p^m,v\right)\right)=1$ (resp. $p$) for all positive integers $m$ and $n$ with $m \neq n$ if $v$ is not congruent modulo $p$ to 1 (resp. if $v$ is congruent modulo $p$ to 1). Our first proof of Theorem 2 uses Elementary Number Theory. Our second proof of Theorem 2 uses Algebraic Number Theory and Theory of Cyclotomic Fields. In Corollary 5 in Section 4 we also show that G.C.D.$\left(\Phi\left(2^n p,v\right),\Phi\left(2^m p,v\right)\right)=1$ for all positive integers $m$ and $n$ with $m \neq n$ and all rational integers $v$. In Corollary 4 in Section 3 we study also G.C.D.$\left(\Phi\left(p^n q,v\right),\Phi\left(p^m q,v\right)\right)$ where $p$ and $q$ are arbitrary odd prime numbers with $p \neq q$. The case of G.C.D.$\left(\Phi\left(2p^n,v\right),\Phi\left(2p^m,v\right)\right)$ is reduced to Theorem 2 since $\Phi\left(2p^u,v\right)=\Phi\left(p^u,-v\right)$ for any non-negative integer $u$. Cf. Corollary 3 in Section 3.

 

In Section 2 (resp. 4) we consider

$$h_n(X,Y) = X^{2^n} - X^{2^{n-1}}Y^{2^{n-1}} + Y^{2^n}$$
$$\left(\text{resp. } H_n(X,Y) = X^{2^{n-1}} + Y^{2^{n-1}}\right).$$

In Theorem 1 in Section 2 we show $\text{G.C.D.}\left(h_n(a,b), h_m(a,b)\right) = 1$ for all positive integers *m* and *n* with $m \neq n$ and all rational integers *a* and *b* with $\text{G.C.D.}(a,b) = 1$. In Theorem 3 in Section 4 we show $\text{G.C.D.}\left(H_n(a,b), H_m(a,b)\right) = 1$ (resp. 2) for all positive integers *m* and *n* with $m \neq n$ and all rational integers *a* and *b* with $ab \equiv 0 \pmod 2$ (resp. $ab \equiv 1 \pmod 2$) and $\text{G.C.D.}(a,b) = 1$. The case $(b = 1)$ of Theorem 3 gives a proof of Exercise IV.3 in [1].

## 2. On $a^{2^n} - a^{2^{n-1}}b^{2^{n-1}} + b^{2^n}$ $(n = 1,2,3,\cdots)$

Recall $h_n(X,Y) = X^{2^n} - X^{2^{n-1}}Y^{2^{n-1}} + Y^{2^n}$. We show first

**Theorem 1.** *Let a and b be arbitrary rational integers with* $\text{G.C.D.}(a,b) = 1$. *Let* $\{x_n\}_{n=1}^{\infty}$ *denote the sequence given by* $x_n = h_n(a,b)$ *for all positive integers n. Then we have* $\text{G.C.D.}(x_m, x_n) = 1$ *for all positive integers m and n with* $m \neq n$.

**Proof.** We have

$$a^{2^{n+1}} + a^{2^n}b^{2^n} + b^{2^{n+1}}$$
$$= \left(a^{2^n} + a^{2^{n-1}}b^{2^{n-1}} + b^{2^n}\right)\left(a^{2^n} - a^{2^{n-1}}b^{2^{n-1}} + b^{2^n}\right)$$

and

$$a^{2^{n+1}} + a^{2^n}b^{2^n} + b^{2^{n+1}}$$
$$= \left(a^2 + ab + b^2\right)\cdot\prod_{j=1}^{n}\left(a^{2^j} - a^{2^{j-1}}b^{2^{j-1}} + b^{2^j}\right).$$

Hence $x_m \left| \left(a^{2^{n+1}} + a^{2^n}b^{2^n} + b^{2^{n+1}}\right)\right.$ for all integers $1 \le m \le n$. We have also

$$\text{G.C.D.}\left(a^{2^{n+1}} + a^{2^n}b^{2^n} + b^{2^{n+1}}, a^{2^{n+1}} - a^{2^n}b^{2^n} + b^{2^{n+1}}\right)$$
$$= \text{G.C.D.}\left(2a^{2^n}b^{2^n}, a^{2^{n+1}} - a^{2^n}b^{2^n} + b^{2^{n+1}}\right).$$

From $\text{G.C.D.}(a,b) = 1$, factoring *a* and *b* into products of prime numbers, we have

$$\text{G.C.D.}\left(2a^{2^n}b^{2^n}, a^{2^{n+1}} - a^{2^n}b^{2^n} + b^{2^{n+1}}\right) = 1.$$

Hence $\text{G.C.D.}\left(x_m, a^{2^{n+1}} - a^{2^n}b^{2^n} + b^{2^{n+1}}\right) = 1$ for all rational integers $1 \le m \le n$. Namely $\text{G.C.D.}(x_m, x_{n+1}) = 1$ for all rational integers $1 \le m \le n$.

In Euclid's books was given the proof of the classical well known theorem that there are infinitely many prime numbers. Theorem 1 above gives another proof of this theorem. For each positive integer *m*, let $p_m$ denote a prime number dividing $x_m$ in Theorem 1.

**Corollary 1.** *We have* $p_m \neq p_n$ *if* $m \neq n$. *There are infinitely many prime numbers.*

## 3. On $\Phi\left(p^n, v\right)$ $(n = 1,2,3,\cdots)$

Let *p* be any odd prime number and let *n* be any positive integer. Let $\zeta_{p^n}$ denote a primitive $p^n$-th root of unity in $\boldsymbol{C}$. Recall $\Phi\left(p^n, T\right) = \text{Irr}\left(\zeta_{p^n}, \boldsymbol{Q}, T\right)$. It is a polynomial in $\boldsymbol{Z}[T]$ whose leading coefficient is 1. One has $\Phi\left(p^n, T\right) = \prod_{\lambda \in S\left(p^n\right)}(T - \lambda)$, (see e.g. [4-8]). Let *m* and *n* be arbitrary positive integers with $1 \le m < n$. Since there are no common roots of $\Phi\left(p^m, T\right)$ and $\Phi\left(p^n, T\right)$ in $\boldsymbol{C}$, $\text{G.C.D.}\left(\Phi\left(p^m, T\right), \Phi\left(p^n, T\right)\right)$ in $\boldsymbol{Q}[T] = 1$.

We have

**Proposition 1.** $\text{G.C.D.}\left(\Phi\left(p^m, T\right), \Phi\left(p^n, T\right)\right)$ *in* $\boldsymbol{Z}[T] = 1$, *if* $1 \le m < n$.

**Proof.** We have $\Phi\left(p^m, T\right)$ and $\Phi\left(p^n, T\right)$ are polynomials in $\boldsymbol{Z}[T]$ whose leading coefficients are 1, (see e.g. [4-8]). Use Gauss Lemma for polynomials over the quotient ring of a factorial ring, (see e.g. ([5], pp. 181-182)). By applying it to $\boldsymbol{Z}[T]$ and $\boldsymbol{Q}[T]$, $\boldsymbol{Z}[T]$ is factorial. We may put $d_{m,n}(T) = \text{G.C.D.}\left(\Phi\left(p^m, T\right), \Phi\left(p^n, T\right)\right)$ in $\boldsymbol{Z}[T]$. If $\deg d_{m,n}(T) \ge 1$, this contradicts $\text{G.C.D.}\left(\Phi\left(p^m, T\right), \Phi\left(p^n, T\right)\right)$ in $\boldsymbol{Q}[T] = 1$. We have $d_{m,n}(T) \in \boldsymbol{Z}$. Since the leading coefficient of $\Phi\left(p^m, T\right) \in \boldsymbol{Z}[T]$ is 1, $d_{m,n}(T) = \pm 1$. Proposition 1 is proven.

Note

$$\left(T^{p^m} - 1\right)\left|\left(\left(T^{p^m}\right)^{p^{n-m}} - 1\right) = \left(T^{p^n} - 1\right),\right.$$

and

$$\Phi\left(p^m, T\right)\left|\left(T^{p^m} - 1\right)\right|\left(T^{p^n} - 1\right)$$

in $\boldsymbol{Z}[T]$ if $n \ge m \ge 1$. We have $\Phi\left(p^m, v\right)\left|\left(v^{p^n} - 1\right)\right.$ in $\boldsymbol{Z}$ if $v \in \boldsymbol{Z}$ and $n \ge m \ge 1$. One has

$$\Phi\left(p^n, T\right) = \Phi\left(p, T^{p^{n-1}}\right)$$

and $\Phi(p,T) = \sum_{j=0}^{p-1} T^j$, see e.g. [4-8]. We give

**Theorem 2.** *Let p be any odd prime number, and let v be any rational integer. Then we have the following.*

*Case* 1 *that v is not congruent modulo p to* 1:

$$\text{G.C.D.}\left(\Phi\left(p^m, v\right), \Phi\left(p^n, v\right)\right) = 1$$

*for all rational integers m and n with* $1 \le m < n$.

*Case* 2 *that v is congruent modulo p to* 1:

 

$$\text{G.C.D.}\left(\Phi\left(p^m,v\right),\Phi\left(p^n,v\right)\right)=p$$

*for all rational integers m and n with* $1\le m<n$.

We give two proofs. The first one uses Elementary Number Theory. The second one uses (local and global) Algebraic Number Theory and Theory of Cyclotomic Fields for which cf. [4-9].

**Proof 1.** We have $1\le m\le n-1$. Put $\tau=v^{p^m}-1$. We have

$$v^{p^{n-1}}=v^{p^m p^{n-1-m}}=\left(v^{p^m}\right)^{p^{n-1-m}}=(\tau+1)^{p^{n-1-m}}\equiv 1(\bmod \tau)$$

and

$$\Phi\left(p^n,v\right)=\Phi\left(p,v^{p^{n-1}}\right)\equiv\Phi(p,1)(\bmod\tau)\equiv p(\bmod\tau).$$

There is a rational integer $y$ with $\Phi\left(p^n,v\right)+\tau y=p$. We have $\text{G.C.D.}\left(\Phi\left(p^n,v\right),\tau\right)=\text{G.C.D.}\left(p,\tau\right)=1$ or $p$. Since $\Phi\left(p^m,v\right)\Big|\tau,\text{G.C.D.}\left(\Phi\left(p^n,v\right),\Phi\left(p^m,v\right)\right)$ divides $\text{G.C.D.}\left(\Phi\left(p^n,v\right),\tau\right)$. Hence

$$\text{G.C.D.}\left(\Phi\left(p^n,v\right),\Phi\left(p^m,v\right)\right)=1 \text{ or } p. \quad (1)$$

In Case 2: We have

$$\Phi\left(p^m,v\right)\equiv\Phi\left(p^m,1\right)(\bmod p)\equiv p(\bmod p)$$
$$\equiv 0(\bmod p).$$

We have also $\Phi\left(p^n,v\right)\equiv 0(\bmod p)$. Hence $\text{G.C.D.}\left(\Phi\left(p^n,v\right),\Phi\left(p^m,v\right)\right)=p$. Case 2 of Theorem 2 is proven.

In Case 1: Let $\delta>1$ be any divisor of $\tau$. Then $v^{p^{n-1}}\equiv 1(\bmod\tau)\equiv 1(\bmod\delta)$. We have

$$\Phi\left(p^n,v\right)=\Phi\left(p,v^{p^{n-1}}\right)\equiv\Phi(p,1)(\bmod\delta)\equiv p(\bmod\delta).$$

We shall show $\delta$ does not divide $p$. Assume it were true that $\delta\,|\,p$. Then we would have $\delta=p$. We have $v^{p^m}-1\equiv 0(\bmod\delta)$. Therefore

$\left(v(\bmod p)\right)^{p^m}\equiv 1(\bmod p)$ and $p$ would not divide $v$. It follows that $\left(v(\bmod p)\right)^{p-1}\equiv 1(\bmod p)$. The order of $v(\bmod p)$ divides $p^m$ and $p-1$. Hence $v(\bmod p)\equiv 1(\bmod p)$, which is a contradiction. Hence we have $\delta\ne p$ and $\delta$ does not divide $p$. Hence $\delta$ does not divide $\Phi\left(p^n,v\right)$. Hence we get $\text{G.C.D.}\left(\Phi\left(p^n,v\right),v^{p^m}-1\right)=1$. Since $\Phi\left(p^m,v\right)\Big|\left(v^{p^m}-1\right)$, we have $\text{G.C.D.}\left(\Phi\left(p^n,v\right),\Phi\left(p^m,v\right)\right)=1$ if $1\le m<n$. Case 1 of Theorem 2 is proven.

We give another proof of Theorem 2.

**Proof 2.** Let $1\le m<n$. Recall

$$\Phi\left(p^m,T\right)=\prod_{\lambda\in S\left(p^m\right)}(T-\lambda)$$

and

$$\Phi\left(p^n,T\right)=\prod_{\mu\in S\left(p^n\right)}(T-\mu).$$

Take $\lambda\in S\left(p^m\right)$ (resp. $\mu\in S\left(p^n\right)$) arbitrarily. Let $B$ denote the ring of the algebraic integers in $\boldsymbol{Q}\left(\zeta_{p^n}\right)$. Let $v\in\boldsymbol{Z}$.

In Case 1: Now assume that there is such a prime ideal $P$ of $B$ that satisfies $v-\lambda\in P$ and $v-\mu\in P$. Write $v-\lambda=(v-1)+(1-\lambda)$ and $v-\mu=(v-1)+(1-\mu)$. We have $\lambda-\mu\in P$ and $\lambda\left(1-\lambda^{-1}\mu\right)\in P$. Let $a\in\boldsymbol{Z}$. We have $\zeta_{p^n}\zeta_{p^n}^{ap^{n-m}}=\zeta_{p^n}^{1+ap^{n-m}}$ which is a primitive $p^n$-th root of unity since $p$ does not divide $1+ap^{n-m}$. So $\lambda^{-1}\mu$ is a primitive $p^n$-th root of unity. By the theory of cyclotomic fields (cf. [4-8]), $\lambda\left(1-\lambda^{-1}\mu\right)B$ is a unique prime ideal $P'$ of $B$ lying above $p\boldsymbol{Z}$, and $pB=P'^{(p-1)p^{n-1}}$. We have $\lambda\left(1-\lambda^{-1}\mu\right)B=P'\subset P$. Hence $P'=P$ and $P\,|\,p\boldsymbol{Z}$. We have $1-\mu\in P$ since $\mu\in S\left(p^n\right)$. From $v-\mu\in P$, we have $1-v\in P$. Since $v\in\boldsymbol{Z}$, we have $1-v\in p\boldsymbol{Z}$, namely, $v\equiv 1(\bmod p)$. This result implies the following. If $v$ is not congruent modulo $p$ to 1, there is no prime ideal $J$ with $v-\lambda\in J$ and $v-\mu\in J$. Since

$$\Phi\left(p^m,v\right)=\prod_{\lambda\in S\left(p^m\right)}(v-\lambda)$$

and

$$\Phi\left(p^n,v\right)=\prod_{\mu\in S\left(p^n\right)}(v-\mu),$$

the greatest common divisor ideal of $\Phi\left(p^n,v\right)B$ and $\Phi\left(p^m,v\right)B$ is $B$ if $v$ is not congruent modulo $p$ to 1. Therefore Case 1 of Theorem 2 is proven.

In Case 2: Let $v\equiv 1(\bmod p)$. Let $\mu\in S\left(p^n\right)$. Let $P$ denote the unique prime ideal in $B$ lying above $p\boldsymbol{Z}$, and let $B_P$ denote the localization of $B$ at $P$. Let $\hat{B}_P$ denote the completion of $B_P$ with respect to the $P$-adic (non-Archimedean) absolute value. We use local and global Algebraic Number Theory, cf. [5,9]. We have $P=(1-\mu)B$ and $(1-\mu)\left|(v-1+1-\mu)\right.$ in $B$. We have $(v-1+1-\mu)\left|(1-\mu)\right.$ in $\hat{B}_P$ since $\text{ord}_P\dfrac{v-1}{1-\mu}>0$. Hence we get $(v-\mu)\hat{B}_P=(1-\mu)\hat{B}_P$ using $v-\mu=v-1+1-\mu$. Then we have

$$\Phi\left(p^n,v\right)\hat{B}_P=\prod_{\mu\in S\left(p^n\right)}(v-\mu)\hat{B}_P$$
$$=(1-\mu)^{(p-1)p^{n-1}}\hat{B}_P=p\hat{B}_P.$$

In the same way we have

$$\Phi\left(p^m,v\right)\hat{B}_P=\prod_{\lambda\in S\left(p^m\right)}(v-\lambda)\hat{B}_P$$
$$=(1-\lambda)^{(p-1)p^{m-1}}\hat{B}_P=p\hat{B}_P$$

 

using $\boldsymbol{Q}\left(\zeta_{p^m}\right)\subset\boldsymbol{Q}\left(\zeta_{p^n}\right)$. Here we use (1) in Proof 1 above. Therefore we get

$$\text{G.C.D.}\left(\Phi\left(p^n,v\right),\Phi\left(p^m,v\right)\right)=p \quad \text{if} \quad v\equiv 1\left(\text{mod } p\right).$$

Case 2 of Theorem 2 is proven.

For each positive integer $m$, let $q_m$ denote a prime number dividing $\Phi\left(p^m,v\right)$ in Case 1 of Theorem 2.

**Corollary 2.** *We have* $q_m\neq q_n$ *if* $m\neq n$. *There are infinitely many prime numbers.*

EXAMPLE of Theorem 2. Let $p=5$ and let $v$ be a rational integer which is not congruent modulo 5 to 1. Then we have that $1+v^{5^m}+v^{2\times 5^m}+v^{3\times 5^m}+v^{4\times 5^m}$ and $1+v^{5^n}+v^{2\times 5^n}+v^{3\times 5^n}+v^{4\times 5^n}$ are relatively prime for all rational integers $m$ and $n$ with $0\le m<n$.

We give some computations.

$$\Phi\left(5,2\right)=31,\ \Phi\left(5^2,2\right)=601\times 1801,$$

$$\Phi\left(5^3,2\right)=269089806001\times 4710883168879506001,$$

$$\Phi\left(5,-2\right)=11,\ \Phi\left(5^2,-2\right)=251\times 4051,$$

$$\Phi\left(5^3,-2\right)=229668251\times 5519485418336288303251.$$

(We used "Scientific WorkPlace", Version 5.5, MacKichan Software, 19307 8th Avenue NE, Suite C, Poulsbo, WA 98370, USA, for the computations).

**Corollary 3 of Theorem 2.** *Let* $p$ *be any odd prime number, and let* $v$ *be any rational integer. Then we have the following.*

*Case* 1 *that v is not congruent modulo* $p$ *to* $-1$:

$$\text{G.C.D.}\left(\Phi\left(2p^m,v\right),\Phi\left(2p^n,v\right)\right)=1$$

*for all rational integers* $m$ *and* $n$ *with* $1\le m<n$.

*Case* 2 *that v is congruent modulo* $p$ *to* $-1$:

$$\text{G.C.D.}\left(\Phi\left(2p^m,v\right),\Phi\left(2p^n,v\right)\right)=p$$

*for all rational integers m and n with* $1\le m<n$.

**Proof.** By ([6], p. 280), $\Phi\left(2p^u,T\right)=\Phi\left(p^u,-T\right)$ for any positive integer *u*. Then by Theorem 2, Corollary 3 follows.

**Corollary 4 of Theorem 2.** *Let p and q be arbitrary odd prime numbers with* $p\neq q$, *and let* $v$ *be any rational integer. Then we have the following.*

*Case* 1 *that* $v^q$ *is not congruent modulo* $p$ *to* 1:

$$\text{G.C.D.}\left(\Phi\left(p^mq,v\right),\Phi\left(p^nq,v\right)\right)=1$$

*for all rational integers m and n with* $1\le m<n$.

*Case* 2 *that* $v^q\equiv 1\left(\text{mod } p\right)$ *and* $v\equiv 1\left(\text{mod } p\right)$:

$$\text{G.C.D.}\left(\Phi\left(p^mq,v\right),\Phi\left(p^nq,v\right)\right)=1$$

*for all rational integers m and n with* $1\le m<n$.

*Case* 3 *that* $v^q\equiv 1\left(\text{mod } p\right)$ *and that v is not congruent modulo p to* 1:

*We have* $p\equiv 1\left(\text{mod } q\right)$ *and*

$$\text{G.C.D.}\left(\Phi\left(p^mq,v\right),\Phi\left(p^nq,v\right)\right)=1 \quad \textit{or } p$$

*for all rational integers m and n with* $1\le m<n$.

**Proof.** From ([6], p. 280) we have

$$\Phi\left(p^uq,T\right)=\Phi\left(p^u,T^q\right)\Big/\Phi\left(p^u,T\right)$$

for any positive integer *u*. Hence

$$\Phi\left(p^uq,v\right)=\Phi\left(p^u,v^q\right)\Big/\Phi\left(p^u,v\right)\in\boldsymbol{Z}.$$

In Case 1, we have

$$\text{G.C.D.}\left(\Phi\left(p^m,v^q\right),\Phi\left(p^n,v^q\right)\right)=1$$

from Theorem 2.

In Case 2: We have

$$\text{G.C.D.}\left(\Phi\left(p^m,v^q\right),\Phi\left(p^n,v^q\right)\right)=p$$

and

$$\text{G.C.D.}\left(\Phi\left(p^m,v\right),\Phi\left(p^n,v\right)\right)=p$$

from Theorem 2. Hence it follows that

$$\text{G.C.D.}\left(\Phi\left(p^mq,v\right),\Phi\left(p^nq,v\right)\right)=1.$$

In Case 3: From $\left(v\left(\text{mod } p\right)\right)^q\equiv 1\left(\text{mod } p\right)$, the order of $v\left(\text{mod } p\right)$ divides $q$ and $p-1$. Since $v$ is not congruent modulo $p$ to 1, the order of $v\left(\text{mod } p\right)$ is $q$. Hence $q\left|\left(p-1\right)\right.$. From Theorem 2, we have

$$\text{G.C.D.}\left(\Phi\left(p^m,v^q\right),\Phi\left(p^n,v^q\right)\right)=p$$

and

$$\text{G.C.D.}\left(\Phi\left(p^m,v\right),\Phi\left(p^n,v\right)\right)=1.$$

Here we use

$$\Phi\left(p^uq,v\right)=\Phi\left(p^u,v^q\right)\Big/\Phi\left(p^u,v\right)\in\boldsymbol{Z}.$$

It follows that $\text{G.C.D.}\left(\Phi\left(p^mq,v\right),\Phi\left(p^nq,v\right)\right)=1$ *or p.*

From Corollary 4 of Theorem 2 we obtain:

*Let* $p$ *and q be arbitrary odd prime numbers with* $p\neq q$, *and let* $v$ *be any rational integer. If p is not congruent modulo q to* 1,

$$\text{G.C.D.}\left(\Phi\left(p^mq,v\right),\Phi\left(p^nq,v\right)\right)=1$$

*for all rational integers m and n with* $1\le m<n$.

## 4. Proof of Exercise IV.3 in [1]

Let us quote the exercise.

Exercise IV.3 in [1]. *"If a, m, n are positive integers, and* $m\neq n$, *show that the* G.C.D. *of* $a^{2^m}+1$ *and* $a^{2^n}+1$ *is* 1 *or* 2 *according as a is even or odd. (Hint. use the fact that* $a^{2^n}-1$ *is a multiple of* $a^{2^m}+1$ *for* $n>m$*). From*

 

*this deduce the existence of infinitely many primes.*"

We give a proof of this in somewhat generalized form. Namely we show

**Theorem 3.** *Let a and b be arbitrary positive rational integers with* $\text{G.C.D.}(a,b)=1$. *Define* $H_n(X,Y)=X^{2^{n-1}}+Y^{2^{n-1}}$ *for any positive* $n\in\boldsymbol{Z}$. *Let m and n be arbitrary rational integers with* $0\le m<n$. *Write* $\Delta_{m,n}=\text{G.C.D.}\left(H_{m+1}(a,b),H_{n+1}(a,b)\right)$. *Then we have*:

$$\Delta_{m,n}=1 \text{ if } ab\equiv 0 \pmod 2;$$

$$\Delta_{m,n}=2 \text{ if } ab\equiv 1 \pmod 2.$$

**Proof.** We have

$$X^{2^n}-Y^{2^n}=\left(X^{2^{n-1}}+Y^{2^{n-1}}\right)\left(X^{2^{n-1}}-Y^{2^{n-1}}\right)$$

and

$$X^{2^n}-Y^{2^n}=(X-Y)\cdot\prod_{j=0}^{n-1}\left(X^{2^j}+Y^{2^j}\right).$$

Hence $\left(X^{2^m}+Y^{2^m}\right)\Big|\left(X^{2^n}-Y^{2^n}\right)$ for all integers $0\le m<n$. We have also

$$\Delta_n=\text{G.C.D.}\left(a^{2^n}-b^{2^n},a^{2^n}+b^{2^n}\right)$$
$$=\text{G.C.D.}\left(2a^{2^n},a^{2^n}+b^{2^n}\right)=\text{G.C.D.}\left(a^{2^n}-b^{2^n},2b^{2^n}\right).$$

Hence $\text{G.C.D.}\left(a^{2^m}+b^{2^m},a^{2^n}+b^{2^n}\right)\Big|\Delta_n$ for all integers $0\le m<n$. Assume that a prime number $p$ divides $a$. Then $p$ does not divide $a^{2^n}+b^{2^n}$ since $\text{G.C.D.}(a,b)=1$. Use $\Delta_n=\text{G.C.D.}\left(2a^{2^n},a^{2^n}+b^{2^n}\right)$.

Therefore $\Delta_n=1$ or $2$. We have $\Delta_n=1$ if $a$ is even; $a^{2^n}+b^{2^n}$ is even and $\Delta_n=2$ if $a$ and $b$ are odd; $a^{2^n}+b^{2^n}$ is odd and $\Delta_n=1$ if $a$ is odd and $b$ is even. Recall $\Delta_{m,n}\Big|\Delta_n$. $\Delta_{m,n}=1$ if $ab$ is even. $\Delta_{m,n}=2$ if $ab$ is odd, since both $a^{2^m}+b^{2^m}$ and $a^{2^n}+b^{2^n}$ are even, and $2\Big|\Delta_{m,n}$.

**Corollary 5 of Theorem 3.** *Let p be any odd prime number, and let v be any rational integer. Then we have*

$$\text{G.C.D.}\left(\Phi\left(2^m p,v\right),\Phi\left(2^n p,v\right)\right)=1$$

*for all rational integers* $m$ *and* $n$ *with* $1\le m<n$.

**Proof.** By ([6], p. 280),

$$\Phi\left(2^u p,T\right)=\Phi\left(2^u,T^p\right)\Big/\Phi\left(2^u,T\right)$$

for any positive integer $u$. We have $\Phi\left(2^u,T\right)=T^{2^{u-1}}+1$. If $v$ is even,

$$\text{G.C.D.}\left(\Phi\left(2^m,v^p\right),\Phi\left(2^n,v^p\right)\right)=1$$

by Theorem 3. If $v$ is odd,

$$\text{G.C.D.}\left(\Phi\left(2^m,v^p\right),\Phi\left(2^n,v^p\right)\right)=2$$

and

$$\text{G.C.D.}\left(\Phi\left(2^m,v\right),\Phi\left(2^n,v\right)\right)=2$$

by Theorem 3. Then we have Corollary 5 using

$$\Phi\left(2^u p,v\right)=\Phi\left(2^u,v^p\right)\Big/\Phi\left(2^u,v\right)\in\boldsymbol{Z}.$$

In the case of $p=3$, Corollary 5 is derived also from Theorem 1. For we have

$$\Phi\left(2^u\times 3,T\right)=\Phi\left(2^u,T^3\right)\Big/\Phi\left(2^u,T\right)$$
$$=\left(T^{3\times 2^{u-1}}+1\right)\Big/\left(T^{2^{u-1}}+1\right)$$
$$=T^{2^u}-T^{2^{u-1}}+1.$$

## 5. Acknowledgements

The author concludes that the topic of the present paper relates to Algebraic Number Theory and Theory of Cyclotomic Fields. He would like to thank the referee for valuable suggestions for the important improvement of this paper.

## REFERENCES

[1] A. Weil and M. Rosenlicht, "Number Theory for Beginners," Springer Verlag, New York, 1979. doi:10.1007/978-1-4612-9957-8

[2] G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 4th Edition, Oxford University Press, Ely House, London, 1971.

[3] A. Baker, "A Concise Introduction to the Theory of Numbers," Cambridge University Press, Cambridge, 1984. doi:10.1017/CBO9781139171601

[4] B. J. Birch, "Cyclotomic Fields and Kummer Extensions," In: J. W. S. Cassels and A. Fröhlich, Eds., *Algebraic Number Theory*, Academic Press, London, 1967, pp. 85-93.

[5] S. Lang, "Algebraic Number Theory," Addison-Wesley Publishing Company, Massachusetts, 1970.

[6] S. Lang, "Algebra," 3rd Edition, Springer Verlag, New York, 2002. doi:10.1007/978-1-4613-0041-0

[7] E. Weiss, "Algebraic Number Theory," 2nd Edition, Chelsea Publishing Company, New York, 1976.

[8] H. Weyl, "Algebraic Theory of Numbers," Princeton University Press, Princeton, 1940.

[9] J.-P. Serre, "Local Fields," Springer Verlag, New York, 1979.

 