A paper on the Twin Prime Conjecture

Minoru TANAKA*, Kaoru TANAKA

**School of Network and Information, Senshu University*
2-1-1 Higashi-mita, Tama-ku, Kawasaki-shi, Kanagawa, 214-8580, Japan
E-mail: mtanaka@isc.senshu-u.ac.jp

Abstract

The conjecture that there are infinitely many twin primes such as (3, 5), (5, 7), (11, 13) is still open problem in number theory. This paper introduces an unpublished paper written about 20 years ago which is intended to give the proof of the conjecture by constructing new larger twin primes from given twin primes.

Key words: Twin primes; Modulus; Congruence; Principal ideal; Ring.

Preface

Twin primes are pairs of primes of the form (p-1, p+1) such that (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), ... There are, for example, 1224 such pairs below 100,000, and 8169 below 1,000,000. Then it is conjectured that there are infinitely many twin primes, which is still one of the open problems of twin prime conjectures in number theory. It is also said that its proof or disproof is at present beyond the resources of mathematics (see Hardy and Wrigtht; An Introduction to the Theory of Numbers, 1979, Oxford). In this paper the even number p between the primes will be called a "prime pair" of the twin primes (p-1, p+1). The first few prime pairs are 4, 6, 12, 18, 30, ... , and it is easily seen that all prime pairs except 4 are of the form 6n, a multiple of 6. The largest known prime pair will be 16869987339975x2^171960 presented by Jarai et al. in 2005 (for further details, see Wolfram research; http://mathworld.wolfram.com /TwinPrimes.html).

The objective of this paper is to introduce a paper entitled "Existence of Infinitely Many Prime Pairs" which was written by Kaoru Tanaka about 20 years ago. It must be fairly rare to give a proof of the conjecture that a new prime pair will be constructed in a systematic way from a given prime pair. But the paper has not published yet, because it may be impossible to find reviewers of it (the similar comment was seen in the referee's comments for the paper sent from H. Zassenhaus, an editor of Journal of Number Theory in 1988). If you have any interests in this material, please try to read the following Chapters 1-3 below and understand elementary number theoretic attempts to solve the twin prime conjecture.

1. Introduction

Let q be a positive integer. If (q-1, q+1) is a pair of primes (or twin prime numbers), then we say q is a prime pair. In this paper we prove that given a sufficiently large prime pair q there is at least one positive integer g such that $g \cdot q$ is again a prime pair satisfying $q < g \cdot q < 385 \cdot q$.

Throughout the paper, we ask about the structure of the group of units $Z_\Omega{}^*$ in a ring of integers Z_Ω. Let

(1) q be a sufficiently large prime pairs and (q-1, q+1) = $(p_\epsilon, p_{\epsilon+1})$.

Note that the prime pairs q $\geq$ 6 must be a multiple of 6.

(2) Φ_1, Φ_2 be the sets of primes such that

$$\Phi_1 = \{\, p_i \mid p_i \nmid q,\ 11 < p_i < p_\epsilon \,\},$$

$$\Phi_2 = \{\, p_j \mid p_j \mid q,\ 11 < p_i < p_\epsilon \,\}.$$

(3) ω, Ω be the product of primes such that

$$\omega = (\textstyle\prod_{\Phi_1} p_i)\, p_\epsilon\, p_{\epsilon+1},$$

$$\Omega = 5 \times 7 \times 11 \times \omega = 385\, \omega.$$

(4) Z be the ring of integers and I be the set of non-negative integers.

(5) Z_m be the ring of integers modulo m and $Z_m{}^*$ be the groups of units in Z_m.

Customarily the identity will be denoted by 1 and the zero element by 0 in every Z_m.

(6) $G_2\,\{Z_m\}$ be the subgroup of $Z_m{}^*$ such that

$$G_2\,\{Z_m\} = \{\, g \in Z_m{}^* \mid g^2 - 1 = 0\ (Z_m) \,\}.$$

(7) $S_2\,\{Z_m\}$ be the subset of Z_m such that

$$S_2\,\{Z_m\} = \{\, \mathrm{s} \in Z_m \mid s^2 - 1 \neq 0\ (Z_p) \text{ for all prime } \mathrm{p} \mid \mathrm{m} \,\}.$$

(8) $\eta : Z_\Omega \to Z_\omega$ be a natural homomorphism given by $\eta(\mathrm{z}) = \tilde{z}$ and

$\eta_p : Z_\omega \to Z_p$ be a homomorphism given by $\eta_p(\tilde{z}) = \tilde{\tilde{z}}$ for every prime factor p of ω.

(9) $\varphi : Z_\Omega \to Z_{385}$ be a natural homomorphism given by $\varphi(\mathrm{z}) = \bar{z}$ and

$\varphi_p : Z_{385} \to Z_p$ be a homomorphism given by $\varphi_p(\bar{z}) = \bar{\bar{z}}$ for every prime factor p of 385.

(10) H be the subgroup of $G_2\ \{Z_\Omega\}$ such that

$$H = \{\ h \in G_2\ \{Z_\Omega\} \mid\ \eta(h) = \tilde{h} = 1\ \ (Z_\omega)\},$$

where we use 1 instead of $\tilde{1}$, the identity of Z_ω.

For example, let the prime pairs q = 18, then $(p_\epsilon,\ p_{\epsilon+1}) = (17,\ 19\ )$, $\omega = 13\times17\times19 = 4199$ and $\Omega = 385\ \omega = 1616615$. Thus in this case we have

$$H = \{\ 1,\ 1478049,\ 1154726,\ 323324,\ 449294,\ \ 587861,\ 911184,\ 125971\ \} \subset G_2\ \{Z_\Omega\},$$

and $G_2\ \{Z_\Omega\}$ always contains ±1 of $Z_\Omega{}^*$ and also $S_2\ \{Z_\Omega\}$ always contains zero element of Z_Ω. In Z_{385},

$$G_2\ \{Z_{385}\} = \{\ 1,\ 34,\ 111,\ 309,\ 384,\ 351,\ 274,\ 76\ \}.$$

Note that H is contained in $1+A_\omega$ where $A_\omega = (\omega)$ is the principal ideal of Z_Ω generated by an element ω, and H is mapped onto $G_2\ \{Z_{385}\}$ by the natural epimorphism φ from Z_Ω to Z_{385}. We know that the order of $G_2\ \{Z_{385}\}$ is 2^3 (see K. Tanaka [3]).

2. Lemmas

Given the subgroup H of $Z_\Omega{}^*$ such that

$$H = \{\ h \in G_2\ \{Z_\Omega\} \mid\ \eta(h) = \tilde{h} = 1\ \ (Z_\omega)\ \},$$

let $\tilde{H}$, $\overline{H} = \varphi(H)$ be the image of H in Z_ω, Z_{385} respectively such that

$$\tilde{H} = \{\ 1\ \},\quad \overline{H} = \ \ \{\ \overline{h} \in G_2\ \{Z_{385}\}\ \}.$$

Suppose the sequence of primes,

$$5 < 7 < 11 <\ p_1 < \ldots < p_i < \ldots <\ p_\epsilon\ < p_{\epsilon+1}$$

with $p_i \in \Phi_1$, let $A_5, A_7, A_{11}, A_{p_1}, \ldots, A_{p_{\epsilon+1}}$ denote the principal ideal of Z_Ω generated by the associated primes. Then we can find an element $r \in Z_\Omega$ satisfying the following conditions:

$$\begin{aligned}
r &\equiv 1 && (\bmod A_5\ ) \\
r &\equiv 1 && (\bmod A_7\ ) \\
r &\equiv 1 && (\bmod A_{11}) \\
r &\equiv q^{\lambda_1} && (\bmod A_{p_1})
\end{aligned}$$

$$\begin{array}{lll}\vdots & & \\ r \equiv q^{\lambda_i} & (\bmod A_{p_i}) & \\ \vdots & & \\ r \equiv q & (\bmod A_{p_\epsilon}) & \\ r \equiv q & (\bmod A_{p_{\epsilon+1}}) & \end{array} \qquad (1)$$

for some $\lambda_i \in$ I. Clearly r is a unit of Z_Ω, because the given prime pair q is a unit of Z_Ω.

Suppose here the cosets of H generated by r in Z_Ω such that

$$Z_\Omega \mid \quad \{ \mathrm{H}, \ r\mathrm{H}, \ \cdots, \ r^{N-1}\mathrm{H} \},$$

where N denotes the least positive integer such that $r^N = 1 \ (Z_\Omega)$. Let $q_n \in r^n$H for any n∈I, then the image $\varphi(q_n)$ in Z_{385} may be mapped onto $\overline{h}$, that is

$$Z_{385} \mid \quad \varphi(q_n) = \overline{q_n} = \overline{r^n h} = \overline{h} \in Z_{385}^*$$

for each h ∈ H. Suppose further an element s ∈ Z_Ω satisfying the following conditions:

$$\begin{array}{ll} s \equiv 1 & (\bmod A_5) \\ s \equiv 1 & (\bmod A_7) \\ s \equiv q & (\bmod A_{11}) \\ s \equiv 1 & (\bmod A_{p_1}) \\ \vdots & \\ s \equiv 1 & (\bmod A_{p_i}) \\ \vdots & \\ s \equiv 1 & (\bmod A_{p_\epsilon}) \\ s \equiv 1 & (\bmod A_{p_{\epsilon+1}}) \end{array} \qquad (2)$$

where q is the given prime pairs. Note that s is not always a unit of Z_Ω. Then we have, for any k∈I,

$$Z_\Omega \mid \quad \{ s^k\mathrm{H}, \ s^k r\mathrm{H}, \ \cdots, \ s^k r^{N-1}\mathrm{H} \}$$

and for any s^kh ∈ s^kH and $\overline{s^k h} \in Z_{385}$ it follows

$$Z_{385} \mid \quad \varphi(s^k h \cdot \overline{s^k h}) = \overline{s^k h} \cdot \overline{s^k h} = \overline{s}^{2k}.$$

Note that the product $s^k h \cdot \overline{s^k h}$ in Z may be embedded in Z_Ω, and $\varphi(s^k h \cdot \overline{s^k h})$ arises in Z_{385}.

On the other hand, for any n ∈ I,

$$Z_{385} \mid \quad \varphi(s^{2k} r^n) = \overline{s}^{2k} \overline{r}^n = \overline{s}^{2k}.$$

Whence we can find some g_n in Z_Ω such that for any n ∈ I,

$$Z_\Omega \mid \quad s^k h \cdot \overline{s^k h} + g_n = s^{2k} r^n$$

and

$$Z_{385} \mid \quad \varphi(g_n) = \varphi(s^{2k}\, r^n) - \varphi\left(s^k\, h \cdot \overline{s^k\, h}\right) = 0,$$

$$Z_\omega \mid \quad \eta(g_n) = (s^{2k}\, r^n)^\sim - \left(s^k\, h \cdot \overline{s^k\, h}\right)^\sim = (r^n)^\sim - (\overline{s^k\, h})^\sim .$$

Analogously, for any $q_n \in r^n\, H$ we have

$$Z_{385} \mid \quad \varphi(s^k\, q_n - \overline{s^k\, q_n}) = 0 .$$

$$Z_\omega \mid \quad \eta\left(s^k\, q_n - \overline{s^k\, q_n}\right) = (s^k\, r^n\, h)^\sim - (\overline{s^k\, r^n\, h})^\sim = (r^n)^\sim - (\overline{s^k\, h})^\sim .$$

for $(s^k\, h)^\sim = 1\ (Z_\omega)$ and $\bar{r}^n = 1\ (Z_{385})$. Thus we have

$$Z_{385} \mid \quad \varphi\left(\left[s^k\, q_n - \overline{s^k\, q_n}\right] - g_n\right) = 0,$$

$$Z_\omega \mid \quad \eta\left(\left[s^k\, q_n - \overline{s^k\, q_n}\right] - g_n\right) = 0,$$

and consequently we have

$$Z_\Omega \mid \quad s^k\, q_n - \overline{s^k\, q_n} = s^{2k}\, r^n - s^k\, h \overline{s^k\, h} .$$

Assume here that whenever s is a nonunit of Z_Ω, we will take k = 0 and s^k may be contained in $Z_\Omega{}^*$ for any s.

Thus, multiplying both sides by $(s^k\, h)^{-1}$, we have

$$Z_\Omega \mid \ r^n - (s^k\, h)^{-1}\, \overline{s^k\, h} = s^k\, r^n\, h^{-1} - \overline{s^k\, h} = s^k\, r^n\, h - \overline{s^k\, r^n\, h},$$

because $h^{-1} = \mathrm{h}\ (Z_\Omega\ )$ and $\overline{s^k\, h} = \overline{s^k\, r^n\, h}\ (Z_{385})$ for any n $\in$ I.

Hence we get

LEMMA 1. For any n $\in$ I, h$\in$ H and for some k $\in$ I

$$Z_\Omega \mid \quad s^k\, r^n\, h - \overline{s^k\, r^n\, h} = r^n - (s^k\, h)^{-1} \cdot \overline{s^k\, h} . \qquad (3)$$

Next suppose the cyclic subgroup of $Z_\Omega{}^*$ such that

$$Z_\Omega \mid \quad \mathrm{R} = \{\, 1, \mathrm{r}, \ldots, r^k, \ldots, r^{N-1} \,\},$$

where r $\in Z_\Omega$ is defined by (1) and N is the least positive integer with $r^N = 1$ (Z_Ω). Assume further that $(r^x)^\sim = \tilde{q}$ over Z_ω where q is the given prime pair. We can always find such $r^x \in Z_\Omega$ by taking properly selected λ_i defined by (1), e.g. we may take λ_1 with (λ_i, p_i-1) = 1 and $\lambda_i = 1$ for every i > 1.

Let Rα be the subgroup of R in Z_Ω such that

$$Z_\Omega \quad | \qquad \mathrm{R}\alpha = \{ 1, r^\alpha, \ldots, r^X, \ldots, r^{N-\alpha} \},$$

where α = (X, N), X = jα and (j, N/α) = 1. Let N_ϵ be the least positive integer such that $r^{N_\epsilon} = 1$ over $Z_{\Omega/p_\epsilon\, p_{\epsilon+1}}$ and let X ≡ x (mod N_ϵ), so that $r^X = r^x$ over $Z_{\Omega/p_\epsilon\, p_{\epsilon+1}}$. Thus we obtain

$$Z_\Omega \quad | \qquad R = \{ 1, r, \ldots, r^x, \ldots, r^{N_\epsilon} \ldots, r^X \ldots, r^{N-1} \}.$$

Given $s^k \in Z_\Omega{}^*$ for some k ∈ I, suppose an element $(s^k\, h)^{-1} \cdot \overline{s^k\, h} \in Z_\Omega$ for some h ∈ H. Assume now that

$$Z_\Omega \quad \Big| \qquad \left\{(s^k\, h)^{-1} \cdot \overline{s^k\, h} + 385\, m\right\} (r^X - 1) \in (r^x - 1)\, \mathrm{R}\alpha$$

holds for some m ∈ Z, where $(r^x - 1)\, \mathrm{R}\alpha$ is defined as follows:

$$Z_\Omega \quad | \qquad (r^x - 1)\, \mathrm{R}\alpha = \begin{pmatrix} (r^x - 1) \\ (r^x - 1)\, r^\alpha \\ \vdots \\ (r^x - 1)\, r^X \\ \vdots \\ (r^x - 1)\, r^{N-\alpha} \end{pmatrix}.$$

Then for some n ∈ I we have

$$Z_\Omega \;\Big| \qquad \left\{(s^k\, h)^{-1} \cdot \overline{s^k\, h} + 385\, m\right\} (r^X - 1) = (r^x - 1)\, r^{n\alpha},$$

$$Z_\Omega \;\Big| \qquad \left\{(s^k\, h)^{-1} \cdot \overline{s^k\, h} + 385\, m - r^{n\alpha}\right\} (r^X - 1) = (r^x - r^X)\, r^{n\alpha}.$$

Hence by the LEMMA 1 it follows

$$Z_{\Omega/p_\epsilon\, p_{\epsilon+1}} \;\Big| \qquad \left\{385\, m - \left(s^k\, r^{n\alpha}\, h - \overline{s^k\, r^{n\alpha}\, h}\right)\right\} (r^X - 1) = 0,$$

for $r^X = r^x$ over $Z_{\Omega/p_\epsilon\, p_{\epsilon+1}}$, and also

$$Z_{\omega/p_\epsilon\, p_{\epsilon+1}} \quad \Big| \quad \{(385\, m)^{\sim} - \big((s^k r^{n\alpha} h)^{\sim} - (\overline{s^k r^{n\alpha} h})^{\sim}\big)\}(r^X - 1)^{\sim} = 0.$$

Since $(r^X - 1)^{\sim} = (q-1)^{\sim} = p_\epsilon^{\sim}$ is a unit of $Z_{\Omega/p_\epsilon\, p_{\epsilon+1}}{}^{*}$, it follows that

$$Z_{\omega/p_\epsilon\, p_{\epsilon+1}} \quad \Big| \quad (385\, m)^{\sim} - \big((s^k r^{n\alpha} h)^{\sim} - (\overline{s^k r^{n\alpha} h})^{\sim}\big) = 0. \qquad (4)$$

On the other hand,

$$Z_{385} \quad \Big| \quad \overline{385\, m} - \overline{\big(s^k r^{n\alpha} h - \overline{s^k r^{n\alpha} h}\big)} = 0, \qquad (5)$$

and from (4) and (5) we obtain

$$Z_{\Omega/p_\epsilon\, p_{\epsilon+1}} \quad \Big| \quad 385\, m - \big(s^k r^{n\alpha} h - \overline{s^k r^{n\alpha} h}\big) = 0.$$

for some m, n ∈ I.

Thus we get the following result.

LEMMA 2. Suppose that for some m ∈ I

$$Z_\Omega \quad \Big| \quad \big\{(s^k h)^{-1}\, \overline{s^k h} + 385\, m\big\}(r^X - 1) \in (r^x - 1)\mathrm{R}\alpha$$

holds, then

$$Z_{\Omega/p_\epsilon\, p_{\epsilon+1}} \quad \Big| \quad s^k r^{n\alpha} h - \overline{s^k r^{n\alpha} h} = 385\, m,$$

holds for some n ∈ I.

From the above result we have our final LEMMA:

LEMMA 3. Suppose that

$$Z_\Omega \quad \Big| \quad \big\{(s^k h)^{-1}\, \overline{s^k h}\big\}(r^X - 1) \not\subset (r^x - 1)\mathrm{R}\alpha,$$

then

$$Z_{\Omega/p_\epsilon\, p_{\epsilon+1}} \quad \Big| \quad s^k r^{n\alpha} h \neq \overline{s^k r^{n\alpha} h}$$

holds for all n ∈ I, provided $\overline{s^k r^{n\alpha} h} \neq 1$ in Z_{385}.

Proof. Assume that

$$Z_{\Omega/p_\epsilon\, p_{\epsilon+1}} \quad \Big| \quad s^k r^{n\alpha} h = \overline{s^k r^{n\alpha} h}$$

for some $n_0 \in \mathrm{I}$ and $r^X = r^x$ in $Z_{\Omega/p_\epsilon\, p_{\epsilon+1}}$. Then it follows

$$Z_{\Omega/p_\epsilon\, p_{\epsilon+1}} \;\Big|\quad (s^k\, h)^{-1} \cdot \overline{s^k\, r^{n_0\, \alpha}\, h} \cdot (r^X - 1) \;=\; r^{n_0\, \alpha}(r^x - 1). \qquad (6)$$

Hence for the given n_0 we can find some $m_0 \in \mathrm{I}$ such that

$$Z_\Omega \;\Big|\quad (s^k\, h)^{-1} \cdot \overline{s^k\, h}(r^X - 1) + 385\, m_0 \;=\; r^{n_0\, \alpha}(r^x - 1). \qquad (7)$$

Indeed, let $\mathrm{y} = \{ (s^k\, h)^{-1} \cdot \overline{s^k\, h}(r^X - 1) - r^{n_0\, \alpha}(r^x - 1)\}$ over Z_Ω, then

$$Z_{385} \;|\quad \varphi(\mathrm{y}) = (s^k\, h)^{-1} \cdot \overline{s^k\, h} \cdot \overline{(r^X - 1)} - \overline{s^k\, r^{n_0\, \alpha}\, h} \cdot \overline{(r^X - 1)} \;=\; 0,$$

and y must be contained in the principal ideal $A_{385} = (385)$ of Z_Ω.

Thus from (6) and (7) we have

$$Z_{\Omega/p_\epsilon\, p_{\epsilon+1}} \;|\quad 385\, m_0 \;=\; 0,$$

so that

$$Z \;|\quad 385\, m_0 \equiv 0 \;\left(\mathrm{mod}\ \tfrac{\Omega}{p_\epsilon\, p_{\epsilon+1}}\right). \qquad (8)$$

Again from (7), since $\tilde{\tilde{r}} = 1\ (Z_{p_\epsilon})$, we have $((385\, m_0)^{\sim})^{\sim} = 1\ (Z_{p_\epsilon})$ and

$$Z \;|\quad 385\, m_0 \equiv 0 \;\;(\mathrm{mod}\ p_\epsilon). \qquad (9)$$

From (8) and (9) it follows that

$$Z \;|\quad 385\, m_0 \equiv 0 \;\left(\mathrm{mod}\ \tfrac{\Omega}{p_{\epsilon+1}}\right).$$

Thus from (7) we have

$$Z_\Omega \;\Big|\quad (s^k\, h)^{-1} \cdot \overline{s^k\, h} \cdot (r^X - 1) + t_0 \cdot \tfrac{\Omega}{p_{\epsilon+1}} \;=\; r^{n_0\, \alpha} \cdot (r^x - 1) \qquad (10)$$

for some $t_0 \in I$. Therefore, let $\delta = (s^k\, h)^{-1} \cdot \overline{s^k\, h} \cdot (r^X - 1)$ of Z_Ω, then

$$Z_{\Omega/p_{\epsilon+1}} \;|\quad \delta = r^{n_0\, \alpha} \cdot (r^X - 1) \in (r^x - 1)\,\mathrm{R}\alpha \subset (r^x - 1)\, R. \qquad (11)$$

However, since we assume that $\delta \not\subset (r^x - 1)\,\mathrm{R}\alpha$ in Z_Ω, we must have

$$Z_\Omega \;|\quad \delta \in (r^x - 1)\, R. \qquad (12)$$

On the other hand, since $\overline{\overline{R}} = \{1, \overline{\overline{r}}\} = \{1, \overline{\overline{q}}\} = \{1, -1\} = \overline{\overline{\mathrm{R}\alpha}}$ over $Z_{p_{\epsilon+1}}$

with $((r^{\sim})^{\sim})^X = ((r^{\sim})^{\sim})^x = ((r^{\sim})^{\sim})^\alpha = (q^{\sim})^{\sim} = -1$, we have from (12)

$$Z_{p_{\epsilon+1}} \quad | \qquad (\delta^{\sim})^{\sim} = \eta_{p_{\epsilon+1}} \circ \eta(\delta) = \left((\overline{s^k h})^{\sim} \right)^{\sim} \cdot (p_\epsilon{}^{\sim})^{\sim} \qquad (13)$$

$$\in \; ((r^x - 1)^{\sim})^{\sim} \cdot (R^{\sim})^{\sim} = (p_\epsilon{}^{\sim})^{\sim} \cdot (R^{\sim})^{\sim} \; .$$

Therefore it follows

$$Z_{p_{\epsilon+1}} \quad | \qquad \left((\overline{s^k h})^{\sim} \right)^{\sim} \in (R^{\sim})^{\sim} = \{1, \; (q^{\sim})^{\sim}\},$$

where q = $p_\epsilon + 1 = p_\epsilon - 1$. But this is a contradiction over $Z_{p_{\epsilon+1}}$ as we assume that

$$Z \quad | \qquad 1 < \overline{s^k h} < 385 < p_\epsilon < q < p_{\epsilon+1} .$$

Thus if $\delta \not\subset (r^x - 1)$ Rα over Z_Ω, then $\overline{s^k r^{n\alpha} h} \neq s^k r^{n\alpha} h$ over $Z_{\Omega/p_\epsilon \, p_{\epsilon+1}}$ for all n $\in$ I and some h $\in$ H, provided $\overline{s^k r^{n\alpha} h} \neq 1$ (Z_{385}).

3. Existence Theorem

As a starting point we adopt the LEMMA 3 and we will prove the following theme.

THEOREM. There are infinitely many prime pairs.

Proof. Without loss of generality let q be a sufficiently large prime pair such that q > 770 and (q-1, q+1) = $(p_\epsilon, p_{\epsilon+1})$. If we assume now, for h_1, h_2 $\in$ H and n_1, n_2 $\in$ I,

$$Z_\Omega \quad | \qquad \text{(A1)} \quad (s^k h_1)^{-1} \cdot \overline{s^k h_1} \cdot (r^X - 1) = r^{n_1 \alpha} \cdot (r^x - 1)$$

$$\text{(A2)} \quad (s^k h_2)^{-1} \cdot \overline{s^k h_2} \cdot (r^X - 1) = r^{n_2 \alpha} \cdot (r^x - 1)$$

hold, then

$$Z_\omega \quad | \qquad \text{(A1)} \quad (\overline{s^k h_1})^{\sim} \cdot p_\epsilon{}^{\sim} = (r^{\sim})^{n_1 \alpha} \cdot (r^x - 1)^{\sim}$$

$$\text{(A2)} \quad (\overline{s^k h_2})^{\sim} \cdot p_\epsilon{}^{\sim} = (r^{\sim})^{n_2 \alpha} \cdot (r^x - 1)^{\sim}$$

and thus

$$Z_\omega \quad | \qquad \left((\overline{s^k h_1})^{\sim} - (\overline{s^k h_2})^{\sim} \right) \cdot p_\epsilon{}^{\sim} = \left((r^{\sim})^{n_1 \alpha} - (r^{\sim})^{n_2 \alpha} \right) \cdot (r^x - 1)^{\sim} .$$

Recall here that

$$Z_\Omega \quad | \qquad R\alpha = \{ 1, r^\alpha, \ldots, r^X, \ldots, r^{(N/\alpha - 1)\alpha} \},$$

denotes the cyclic subgroup of order N/α in $Z_\Omega{}^*$, where α = (X, N), X = jα, and (j, N/α) = 1.

Thus we have $\alpha = j^{-1}X$ with $j^{-1} \in Z_{N/\alpha}{}^*$, so that $r^{n\alpha} = r^{n j^{-1} X}$ in Z_Ω. Hence

$$Z_{\omega/p_{\epsilon+1}} \;\Big|\; \Big((\overline{s^k h_1})^{\sim} - (\overline{s^k h_2})^{\sim} \Big) \cdot p_\epsilon{}^{\sim} = \Big((r^{\sim})^{n_1 j^{-1} X} - (r^{\sim})^{n_2 j^{-1} X} \Big) \cdot (r^x - 1)^{\sim} . \quad (13)$$

This implies

$$Z \;\Big|\; \Big(\overline{s^k h_1} - \overline{s^k h_2} \Big) \cdot p_\epsilon = (r^{n_1 j^{-1} X} - r^{n_2 j^{-1} X}) \cdot (r^x - 1) + t_1 \cdot \tfrac{\omega}{p_\epsilon} \qquad (14)$$

for some $t_1 \in$ Z. However if $| \, n_1 - n_2 \, |$ is even then $r^{(n_1 - n_2) j^{-1} X} - 1$ or $r^{(n_2 - n_1) j^{-1} X} - 1$ must be divided by $r^X + 1$which is the multiple of $p_{\epsilon+1}$. Whence

$$r^{n_1 j^{-1} X} - r^{n_2 j^{-1} X} = t_2 \cdot p_{\epsilon+1}$$

for some $t_2 \in$ Z and from (14)

$$Z \;\Big|\; \Big(\overline{s^k h_1} - \overline{s^k h_2} \Big) \cdot p_\epsilon = p_{\epsilon+1} \cdot \Big[t_2 \cdot (r^x - 1) + t_1 \cdot \tfrac{\omega}{p_\epsilon \, p_{\epsilon+1}} \Big].$$

This shows that $p_{\epsilon+1}$ must divide $\overline{s^k h_1} - \overline{s^k h_2}$. But it is a contradiction, since we assume that $| \, \overline{s^k h_1} - \overline{s^k h_2} \, | < 770 < p_{\epsilon+1}$ over Z, hence the nonnegative integer $| \, n_1 - n_2 \, |$ must be odd.

Therefore we may conclude that it is possible to stand at the same time by the following two conditions:

$$Z_\Omega \;\Big|\; \begin{array}{ll} \text{(A1)} & (s^k h_1)^{-1} \cdot \overline{s^k h_1} \cdot (r^X - 1) = r^{n_1 \alpha} \cdot (r^x - 1), \\[2ex] \text{(A2)} & (s^k h_2)^{-1} \cdot \overline{s^k h_2} \cdot (r^X - 1) = r^{n_2 \alpha} \cdot (r^x - 1), \end{array}$$

but it is impossible to expect the realization of more than two conditions. In fact if (A1), (A2) and

$$\text{(A3)} \quad (s^k h_3)^{-1} \cdot \overline{s^k h_3} \cdot (r^X - 1) = r^{n_3 \alpha} \cdot (r^x - 1)$$

hold for some $h_j \in$ H with $h_j \neq h_i \, (i \neq j : \; i, \; j$ = 1, 2, 3), then from (A1) and (A2) the nonnegative integer $| \, n_1 - n_2 \, |$ must be odd and also from (A1) and (A3) the nonnegative integer $| \, n_1 - n_3 \, |$ must be odd. Therefore if n_1 is even (odd) then n_2 and n_3 must be odd (even), so that $| \, n_1 - n_3 \, |$ must be even which follows a contradiction. Hence if any two conditions hold, then the last one does not occur in Z_Ω.

Thus we may assume that given $s^k \in Z_\Omega{}^*$ for some k ∈ I there exists at least one h ∈ H such that

$\overline{s^k h} \neq 1$ in Z_{385} (see K.Tanaka [3]) and

$$Z_\Omega \mid \quad (s^k h)^{-1} \cdot \overline{s^k h} \cdot (r^X - 1) \neq r^{n\alpha} \cdot (r^x - 1)$$

hold for all n ∈ I. Thus we have from LEMMA 3

$$Z_{\Omega/p_\epsilon\, p_{\epsilon+1}} \mid \quad \overline{s^k r^{n\alpha} h} \neq s^k r^{n\alpha} h$$

for all n ∈ I. However for every n ∈ I,

$$Z_{385} \mid \quad \overline{s^k r^{n\alpha} h} = s^k r^{n\alpha} h,$$

and it follows that

$$Z_{\omega/p_\epsilon\, p_{\epsilon+1}} \mid \quad (\overline{s^k r^{n\alpha} h})^{\sim} = (\overline{s^k h})^{\sim} \neq (s^k r^{n\alpha} h)^{\sim} = (r^{\sim})^{n\alpha} \in (\mathrm{R}\alpha)^{\sim},$$

and hence

$$Z_{\omega/p_\epsilon\, p_{\epsilon+1}} \mid \quad (\overline{s^k h})^{\sim}\, q^{\sim} \neq r^{\sim(n\alpha+X)} \in (\mathrm{R}\alpha)^{\sim}$$

for all n ∈ I and some h ∈ H. Since $\alpha = j^{-1} X$ with $j^{-1} \in Z_{N/\alpha}{}^*$ it follows that

$$Z_{\omega/p_\epsilon\, p_{\epsilon+1}} \mid \quad (\overline{s^k h})^{\sim}\, q^{\sim} = (\overline{s^k h})^{\sim}\, r^{\sim X} \neq r^{\sim(n j^{-1}+1)X} \in (\mathrm{R}\alpha)^{\sim}$$

for all n ∈ I. Thus for $p_i \in \Phi_1$ we have

$$Z_{p_i} \mid \quad \left((\overline{s^k h})^{\sim}\right)^{\sim} \cdot (q^{\sim})^{\sim} \neq ((r^{\sim})^{\sim})^{(n j^{-1}+1)X} \in ((\mathrm{R}\alpha)^{\sim})^{\sim} \qquad (15)$$

for all n ∈ I. Let $\phi_i = \phi(p_i) = p_i - 1$, $\boldsymbol{N_i}$ be the least positive integer such that $((r^{\sim})^{\sim})^{N_i} = 1 \ (Z_{p_i})$

and $X \equiv x_i \pmod{N_i}$. Note that $X \not\equiv 0 \pmod{N_i}$, for if $X \equiv x_i \equiv 0 \pmod{N_i}$, then

$((r^{\sim})^{\sim})^X = (q^{\sim})^{\sim} = 1$ and $((q^{\sim})^{\sim})^2 - 1 = (p_\epsilon{}^{\sim})^{\sim} \cdot (p_{\epsilon+1}{}^{\sim})^{\sim} = 0$ over Z_{p_i} and hence $p_\epsilon\, p_{\epsilon+1}$ must be

divided by $p_i \in \Phi_1$. But it is a contradiction. Therefore $(\mathrm{X}, N_i) = (x_i, N_i) = \alpha_i \neq N_i$ with $x_i = j_i\, \alpha_i$

and $(j_i, N_i/\alpha_i) = 1$. Hence we have $X = x_i + t_0 \cdot N_i$ for some $t_0 \in Z$, and for any $t_1 \in Z$ we have

$$Z_{p_i} \mid \quad ((r^{\sim})^{\sim})^{(n j^{-1}+1)X} = ((r^{\sim})^{\sim})^{(n j^{-1}+1)(x_i + t_0 \cdot N_i + t_1 \cdot \phi_i)}$$

$$= ((r^{\sim})^{\sim})^{(n j^{-1}+1)(x_i + t \cdot N_i)}$$

where $t = t_0 + t_1 \cdot \phi_i / N_i \in Z$. Thus

$$Z_{p_i} \mid \quad ((r^{\sim})^{\sim})^{(n j^{-1}+1) X} = ((r^{\sim})^{\sim})^{(n j^{-1}+1)(j_i + t \cdot N_i / \alpha_i) \cdot \alpha_i} \tag{15)'$$

$$= ((r^{\sim})^{\sim})^{(n j^{-1}+1) \cdot p \cdot \alpha_i}$$

where p denotes a sufficiently large prime such that $p = j_i + t \cdot N_i / \alpha_i$ with some t ∈ Z and

$(j_i, N_i/\alpha_i) = 1$. The existence of such primes may be guaranteed by DIRICHLET THEOREM.

Let $\mu \cdot N_i / \alpha_i$ denote the integer such that

$$\mu \cdot N_i / \alpha_i = \begin{cases} 2^{-1} \cdot N_i / \alpha_i & \cdots \text{ if } N_i / \alpha_i \text{ is odd,} \\ \frac{1}{2} \cdot N_i / \alpha_i & \cdots \text{ if } N_i / \alpha_i \text{ is odd,} \end{cases}$$

where $2^{-1} \in Z^*_{N_i / \alpha_i}$. Then we may find integer $n = (\mu \cdot N_i / \alpha_i \cdot p^{-1} - 1) \cdot j$, where $p^{-1} \in Z^*_{N_i / \alpha_i}$ and $j \in Z^*_{N_i / \alpha_i}$. In fact, $p \in Z^*_{N_i / \alpha_i}$ implies $p^{-1} \in Z^*_{N_i / \alpha_i}$ and for $j = X / \alpha \in Z^*_{N_i / \alpha_i}$, $j_i = x_i / \alpha_i \in Z^*_{N_i / \alpha_i}$ with $X \equiv x_i \pmod{N_i}$ it follows that $(r^X)^{N/\alpha} = r^{jN} = 1$ (Z_Ω) and

$(((r^{\sim})^{\sim})^X)^{N_i / \alpha_i} = (((r^{\sim})^{\sim})^{x_i})^{N_i / \alpha_i} = ((r^{\sim})^{\sim})^{j_i N_i} = 1$ (Z_{p_i}), so that N_i / α_i must be a divisor of N/α,

and hence (j, N_i) = (j, N/α) = 1. Therefore from (15) and (15)' we have

$$Z_{p_i} \mid \quad ((\overline{s^k h})^{\sim})^{\sim} \cdot (q^{\sim})^{\sim} \neq ((r^{\sim})^{\sim})^{(n j^{-1}+1) X} \tag{16}$$
$$= ((r^{\sim})^{\sim})^{\mu \cdot N_i / \alpha_i \cdot p^{-1} \cdot p \cdot \alpha_i} = ((r^{\sim})^{\sim})^{\mu \cdot N_i} = -1.$$

Clearly we may take the integer $n = (N_i - 1) \cdot j$, so that

$$Z_{p_i} \mid \quad ((\overline{s^k h})^{\sim})^{\sim} \cdot (q^{\sim})^{\sim} \neq ((r^{\sim})^{\sim})^{(n j^{-1}+1) X} = ((r^{\sim})^{\sim})^{N_i \cdot X} = 1, \tag{17}$$

Thus for every $p_i \in \Phi_1$ it follows that

$$Z_{p_i} \mid \quad ((\overline{s^k h})^{\sim})^{\sim} \cdot (q^{\sim})^{\sim} = \eta_{p_i} ((\overline{s^k h})^{\sim} \cdot q^{\sim}) \in S_2 \{Z_{p_i}\}. \tag{18}$$

For the prime factors p_ϵ, $p_{\epsilon+1}$ of ω, we get $((\overline{s^k h})^{\sim})^{\sim} \cdot (q^{\sim})^{\sim} = ((\overline{s^k h})^{\sim})^{\sim}$ over Z_{p_ϵ} and $((\overline{s^k h})^{\sim})^{\sim} \cdot (q^{\sim})^{\sim} = -((\overline{s^k h})^{\sim})^{\sim}$ over $Z_{p_{\epsilon+1}}$, since $(q^{\sim})^{\sim} = 1$ (Z_{p_ϵ}) and $(q^{\sim})^{\sim} = -1$ $(Z_{p_{\epsilon+1}})$.

As the given $\overline{s^k h} \in Z_{385}$ satisfies the following conditions:

$$Z \mid \qquad 1 < \overline{s^k h} < 385 < p_\epsilon < p_{\epsilon+1}.$$

It follows that $\left((\overline{s^k h})^{\sim}\right)^{\sim} \cdot (q^{\sim})^{\sim} = \left((\overline{s^k h})^{\sim}\right)^{\sim} \neq \pm 1$ over Z_{p_ϵ} and also $\left((\overline{s^k h})^{\sim}\right)^{\sim} \cdot (q^{\sim})^{\sim} = -\left((\overline{s^k h})^{\sim}\right)^{\sim} \neq \pm 1$ over $Z_{p_{\epsilon+1}}$. Hence we obtain

$$Z_{p_\epsilon} \;\Big|\; \left((\overline{s^k h})^{\sim}\right)^{\sim} \cdot (q^{\sim})^{\sim} = \eta_{p_\epsilon}\left((\overline{s^k h})^{\sim} \cdot q^{\sim}\right) \in S_2\,\{Z_{p_\epsilon}\}, \tag{19}$$

$$Z_{p_{\epsilon+1}} \;\Big|\; \left((\overline{s^k h})^{\sim}\right)^{\sim} \cdot (q^{\sim})^{\sim} = \eta_{p_{\epsilon+1}}\left((\overline{s^k h})^{\sim} \cdot q^{\sim}\right) \in S_2\,\{Z_{p_{\epsilon+1}}\}. \tag{20}$$

From (18), (19) and (20) we have

$$Z_\omega \;\Big|\; (\overline{s^k h})^{\sim} \cdot q^{\sim} \in S_2\,\{Z_\omega\} \tag{21}$$

for some $\overline{s^k h} \cdot q$ of Z_Ω. Moreover, for the element $\overline{s^k h} \cdot q$ of Z_Ω,

$$Z_{385} \;\Bigg|\; \overline{(\overline{s^k h}\cdot q)}^{\,2} = (\overline{s}^{\,k} \cdot \overline{h} \cdot \overline{q}\,)^2 = \overline{s}^{\,2k} \cdot \overline{q}^{\,2},$$

where $\overline{h}^{\,2} = 1\ (Z_{385})$. Let p $\in \{5,7\}$ then for each p

$$Z_p \;\Bigg|\; \varphi_p\left(\overline{(\overline{s^k h}\cdot q)}^{\,2}\right) = \varphi_p\,(\overline{s}^{\,2k}) \cdot \varphi_p\,(\overline{q}^{\,2}) = \overline{\overline{s}}^{\,2k} \cdot \overline{\overline{q}}^{\,2} = \overline{\overline{q}}^{\,2} \neq 1,$$

where $\overline{\overline{s}} = 1$ and $\overline{\overline{q}} \in S_2\,\{Z_p\}$. Therefore $\varphi_p(\,\overline{\overline{s^k h}\cdot q}\,) \in S_2\,\{Z_p\}$ for each p, and we have

$$Z_{35} \;\Big|\; \varphi_{35}(\,\overline{\overline{s^k h}\cdot q}\,) \in S_2\,\{Z_{35}\}. \tag{22}$$

In the similar way,

$$Z_{11} \;\Bigg|\; \varphi_{11}\left(\overline{(\overline{s^k h}\cdot q)}^{\,2}\right) = \varphi_{11}\,(\overline{s}^{\,2k}) \cdot \varphi_{11}\,(\overline{q}^{\,2}) = \overline{\overline{q}}^{\,2\,(k+1)},$$

where $\overline{\overline{s}} = \overline{\overline{q}}$ and $\overline{\overline{q}} \in S_2\,\{Z_{11}\}$.

Hence for k $\neq$ 5m+4 (m $\in$ I) it follows that $\overline{\overline{q}}^{\,2\,(k+1)} \neq 1$ over Z_{11} and that

$$Z_{11} \;\Big|\; \varphi_{11}(\,\overline{\overline{s^k h}\cdot q}\,) \in S_2\,\{Z_{11}\}. \tag{23}$$

Thus from (22) and (23) we have

$$Z_{385} \;\Big|\; \overline{\overline{s^k h}\cdot q} \in S_2\,\{Z_{385}\}. \tag{24}$$

Therefore from (21) and (24) we can conclude that

$$Z_\Omega \;\Big|\; \overline{\overline{s^k h}\cdot q} \in S_2\,\{Z_\Omega\}. \tag{25}$$

provided that, given $\overline{s^k h} \in Z_{385}$ with $\overline{s^k h} \neq 1$ and k $\neq$ 5m+4 (m $\in$ I), the following conditions hold for all n $\in$ I:

$$Z_\Omega \;\Big|\quad (s^k h)^{-1} \cdot \overline{s^k h} \cdot (r^X - 1) \neq r^{n\alpha} \cdot (r^x - 1).$$

Finally, we can show that $\overline{s^k h} \cdot q \in Z$ will be a new prime pair defined by the given prime pair q.

Since we assume that

$$Z \;\Big|\quad 1 < \overline{s^k h} < 770 < q,$$

it follows in the real field

$$\sqrt{\overline{s^k h} \cdot q + 1} < p_{\epsilon+1} < \overline{s^k h} \cdot q + 1 \leq q^2,$$

$$\sqrt{\overline{s^k h} \cdot q - 1} \leq p_\epsilon < \overline{s^k h} \cdot q - 1 < q^2.$$

Recall the sets of primes Φ_1 and Φ_2 such that

$$\Phi_1 = \{ p_i \mid p_i \nmid q, \quad 11 < p_i < p_\epsilon \},$$

$$\Phi_2 = \{ p_j \mid p_j \mid q, \quad 11 < p_j < p_\epsilon \}.$$

For all primes $p_i \in \{5, 7, 11\} \bigcup \Phi_1 \bigcup \{p_\epsilon, p_{\epsilon+1}\}$ and for k $\neq$ 5m+4 (m $\in$ I), from (25) we have

$$Z_{p_i} \;\Big|\quad \left(\overline{s^k h} \cdot q \right)^2 \neq 1,$$

so that $\overline{s^k h} \cdot q \pm 1$ must not be divided by every prime p_i over Z.

For any prime $p_j \in \{2, 3\} \bigcup \Phi_2$ we clearly have

$$Z_{p_j} \;\Big|\quad \left(\overline{s^k h} \cdot q \right)^2 - 1 = -1 \neq 1.$$

Hence $\overline{s^k h} \cdot q \pm 1$ must not be divided by every p_j over Z. Consequently we have proved that $\overline{s^k h} \cdot q \pm 1$ must not be devoid by every prime $p \leq \sqrt{\overline{s^k h} \cdot q + 1}$, and so

$$\left(\overline{s^k h} \cdot q - 1, \quad \overline{s^k h} \cdot q + 1 \right)$$

must be a new twin primes defined by a given prime pair q. This is our desired result, and we may say that there is a prime pair $\overline{s^k h} \cdot q$ satisfying

$$q < \overline{s^k h} \cdot q < 385 \cdot q$$

for a given prime pair q.

Acknowledgments

We take this opportunity to thank Prof. S. IKEHARA for his numerous suggested improvements.

References

[1] T.W. Hungerford, 1974, *Algebra*, Springer-Verlag, New York.

[2] B.R. Mcdonald, 1974, *Finite Rings with Identity*, Marcel Dekker, Inc. New York .

[3] K. Tanaka, 1967, "A Generalization of Euler's ϕ-function", Res. Rep. Tokyo Electrical Engrg. College, 15, 24-29.