TAIWANESE JOURNAL OF MATHEMATICS
Vol. 2, No. 3, pp. 303-312, September 1998

ON THE TRIPLET-DIVISIONS OF THE SET $\{1, 2, 3, \cdots, p-2\}$

Chyi-Lung Lin

Abstract. In this paper, we give a number theoretical application of a simple discrete map. For any prime $p \geq 5$, we show that the numbers in the set $G(1, p-2) = \{1, 2, 3, \cdots, p-2\}$ can be divided into disjoint triplets $\langle a, b, c\rangle$, such that $a \cdot b \cdot c \equiv 1 \pmod{p}$. This is a generalization of the well known doublet–division, that is, the numbers in the set $\{1, 2, 3, \cdots, p-1\}$ can be divided into disjoint pairs $\langle a, a^*\rangle$, such that $a \cdot a^* \equiv 1 \pmod{p}$. The reason that we can perform the triplet-division is because there exists a simple map F defined on the set $G(1, p-2)$ such that any number $a \in G(1, p-2)$ is a period-3 point of the map. Furthermore, the triplet $\langle a,\ F(a),\ F^2(a)\rangle$ has the property that $a \cdot F(a) \cdot F^2(a) \equiv 1 \pmod{p}$.

1. Introduction

Our goal in this paper is to introduce an interesting application of iterated maps. It is surprising that there are many different areas whose dynamics can be expressed as iterated maps. It is then natural to see that iterated maps have many applications in large areas, including mathematics, physics, biology, etc. We show in this paper an application of iterated maps to number theory.

It is known that one of the interesting properties of a prime p is that the numbers in the set $\{1, 2, 3, \cdots, p-1\}$ can be divided into disjoint pairs $\langle a, a^*\rangle$, such that $a \cdot a^* \equiv 1 \pmod{p}$ [1]. We call this the *doublet-division*. This property was used to prove the well-known Wilson's theorem: $(p-1)! \equiv -1 \pmod{p}$, for p a prime [1, 2, 3]. We call $\langle a, a^*\rangle$ a *doublet*, and a^* the *associate* of a [2 p.5]. For every $a < p$, the existence of a unique $a^* < p$ such that

Received November 4, 1996.
Communicated by M. Eie.
1991 *Mathematics Subject Classification*: 11A05, 11A41, 11B75.
Key words and phrases: Prime, doublet-division, triplet-division, iterated maps.

$a \cdot a^* \equiv 1 \pmod{p}$ is guaranteed by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$, which implies that $a^* \equiv a^{p-2} \pmod{p}$.

We can easily generalize a doublet to a triplet $\langle a, b, c\rangle$ for which $a \cdot b \cdot c \equiv 1 \pmod{p}$. For any $a < p$, it is easy to derive from Fermat's little theorem triplets that contain a. For instance, $\langle a, a^2, a^{p-4}\rangle$ and $\langle a, a^3, a^{p-5}\rangle$ are triplets containing a. However, it is deeper to divide all the numbers less than p into *disjoint* triplets. If this can be done, we shall call this the *triplet-division*. For convenience, we denote by $G(1, k)$ the set of numbers from 1 to k, i.e.,

$$G(1, k) = \{1, 2, 3, \cdots, k\}.$$

Therefore, $G(1, p-1) = \{1, 2, 3, \cdots, p-1\}$ and $G(1, p-2) = \{1, 2, 3, \cdots, p-2\}$. The doublet-division is on the set $G(1, p-1)$, while the triplet-division will be shown to be on the set $G(1, p-2)$. In this paper, we are to introduce a generalization of doublet-division to the triplet-division, exploring another interesting property of a prime.

For an easy example, consider $p = 11$. The doublet-division is: $\langle 1, 1\rangle$, $\langle 2, 6\rangle$, $\langle 3, 4\rangle$, $\langle 5, 9\rangle$, $\langle 7, 8\rangle$, $\langle 10, 10\rangle$. While, there are two ways for performing the triplet-division on the set $G(1, p-2) = \{1, 2, 3, \cdots, 9\}$, namely:

$\langle 1, 9, 5\rangle$	$\langle 1, 3, 4\rangle$
$\langle 2, 4, 7\rangle$	$\langle 8, 9, 2\rangle$
$\langle 3, 6, 8\rangle$	$\langle 5, 7, 6\rangle$
(A1)	(A2)

Next, consider $p = 13$. The doublet-division is: $\langle 1, 1\rangle$, $\langle 2, 7\rangle$, $\langle 3, 9\rangle$, $\langle 4, 10\rangle$, $\langle 5, 8\rangle$, $\langle 6, 11\rangle$, $\langle 12, 12\rangle$. The triplet-division on the set $G(1, p-2) = \{1, 2, 3, \cdots, 11\}$ is:

$\langle 1, 11, 6\rangle$	$\langle 1, 7, 2\rangle$
$\langle 2, 5, 4\rangle$	$\langle 6, 5, 10\rangle$
$\langle 7, 10, 8\rangle$	$\langle 11, 4, 8\rangle$
$\langle 3, 3, 3\rangle$	$\langle 9, 9, 9\rangle$
$\langle 9, 9, 9\rangle$	$\langle 3, 3, 3\rangle$
(B1)	(B2)

There are two triplets whose three numbers are equal in either (B1) or (B2). We will show that, for a prime of the type $p = 6m + 1$, the triplet-division of $G(1, p-2)$ always contains two such triplets.

In general, if we find a triplet-division, we can then generate other triplet-divisions by raising each number in the triplets to the power j, where j is a number $< p$ and relatively prime to $p-1$; the same as if we find a primitive root g for a prime p, then we can generate all the other primitive roots by g^j. It is interesting to note that it is possible to find the first or the basic triplet-division, called the 3-cycle-division, which can be easily derived from a simple *map*. In Section 2, we introduce this map F which is defined on $G(1, p-2)$, and we show that every $a \in G(1, p-2)$ is a period-3 point of F. Accordingly, the numbers in $G(1, p-2)$ can be divided into disjoint 3-cycles, namely, the 3-cycle-division. In Section 3, we show that different triplet-divisions of $G(1, p-2)$ can be derived from the basic 3-cycle-division, and in fact there are $\varphi(p-1)/2$ ways for performing the triplet-division. In Section 4, we generalize the above discussions to the more general F_k-map.

2. The F-map and the 3-cycles for F

In the following, we consider p a prime ≥ 5; as the case for $p = 3$ is trivial.

Lemma 2.1. *For any $a \in G(1, p-2)$, there exists a unique number $b \in G(1, p-2)$ such that $a \cdot (1+b) \equiv -1 \pmod{p}$.*

Proof. Let $b = p - 1 - a^*$, where $a^* \equiv a^{p-2} \pmod{p} < p$ is the associate of a. Then we easily have $b \in G(1, p-2)$, and $a \cdot (1+b) \equiv -a \cdot a^* \equiv -1 \pmod{p}$. ∎

Definition 2.2. We define a map F: $G(1,\ p-2) \to G(1,\ p-2)$ such that for any $a \in G(1, p-2)$,

$$F(a) = p - 1 - a^*.$$

This map is one-to-one and onto. We define $F^2 = F \circ F$ and $F^n = F \circ F^{n-1}$.

Theorem 2.3.

(T1) *Any $a \in G(1, p-2)$ is a period-3 point of F, i.e., $F^3(a) = a$.*

(T2) *Each 3-cycle for F, i.e., $\langle a, F(a), F^2(a)\rangle$, is a triplet with $a \cdot F(a) \cdot F^2(a) \equiv 1 \pmod{p}$.*

(T3) *The numbers in $G(1, P-2)$ can be divided into disjoint 3-cycles for F.*

Proof. To prove (T1) and (T2), consider

$$F : a \to b, \qquad \text{which yields } a \cdot (1+b) \equiv -1 \pmod{p}, \tag{2.1}$$

$$F : b \to c, \qquad \text{which yields } b \cdot (1 + c) \equiv -1 \pmod{p}, \tag{2.2}$$

$$F : c \to d, \qquad \text{which yields } c \cdot (1 + d) \equiv -1 \pmod{p}. \tag{2.3}$$

From (2.1), (2.2), and (2.3), we have

$$a + a \cdot b \equiv -1 \pmod{p}, \tag{2.4}$$

$$b + b \cdot c \equiv -1 \pmod{p}, \tag{2.5}$$

$$c + c \cdot d \equiv -1 \pmod{p}. \tag{2.6}$$

Multiplying both sides of (2.5) with a, we have $a \cdot b + a \cdot b \cdot c \equiv -a \pmod{p}$. Comparing this with (2.4), we have

$$a \cdot b \cdot c \equiv 1 \pmod{p}. \tag{2.7}$$

Since $b = F(a)$ and $c = F^2(a)$, the three numbers a, $F(a)$, $F^2(a)$ form a triplet. We now prove that $d = a$. This can be seen by multiplying both sides of the equation in (2.3) with $a \cdot b$, then we have $1 + d \equiv -a \cdot b \pmod{p}$. Comparing this with (2.4), we have $d = a$. As $d = F^3(a)$, we find that

$$F^3(a) = a. \tag{2.8}$$

The map F is therefore interesting, since every $a \in G(1, p-2)$ is a period-3 point of F, and $\langle a, F(a), F^2(a)\rangle$ is a 3-cycle for F and is certainly a triplet, as $a \cdot F(a) \cdot F^2(a) \equiv 1 \pmod{p}$.

We next prove (T3). It is known that any two distinct cycles are disjoint, and so an $a \in G(1, p-2)$ must belong to one and only one 3-cycle for F. As a result, the numbers in $G(1, p-2)$ can be divided into disjoint 3-cycles for F. We complete the proof by showing that, for a prime p, there exists a 3-cycle-division on the set $G(1, p-2)$. We then obtain the first triplet-division, i.e., the 3-cycle-division, from the simple map F.

We easily check that, for instance, $\langle 1, p-2, (p-1)/2\rangle$ is a 3-cycle for F. Also $\langle 2, (p-3)/2, (2p-1)/3\rangle$ is a 3-cycle for F if $p = 6m - 1$, and $\langle 2, (p-3)/2, (p-1)/3\rangle$ is a 3-cycle for F if $p = 6m + 1$. In general, if $\langle a, b, c\rangle$ is a 3-cycle for F, then $\langle a+1, c-1, -(a+2)^*\rangle$ is a 3-cycle for F.

A 3-cycle for F should contain either three distinct numbers or three identical numbers. In the latter case, F has fixed points. If e is a fixed point of F, then $F(e) = e$, and we have the 3-cycle $\langle e, e, e\rangle$. We call $\langle e, e, e\rangle$ the identical 3-cycle. Since $F(e) = e$, then $e \cdot (1 + e) \equiv -1 \pmod{p}$, i.e.,

$$e^2 + e + 1 \equiv 0 \pmod{p}. \tag{2.9}$$

As $p \geq 5$, (2.9) is equivalent to

$$e^3 \equiv 1 \pmod{p} \text{ and } e \neq 1. \tag{2.10}$$

This result is expected, since $\langle e, e, e \rangle$ is a 3-cycle for F and therefore must be a triplet and hence e^3 is congruent to one. From (2.10), we see that e is of order 3. From Fermat's little theorem, $e^{p-1} \equiv 1 \pmod{p}$, and hence $3|(p-1)$, i.e., $p = 3n + 1$. Note that n must be even. Therefore, p must be a prime of the type $p = 6m + 1$. Consider then $p = 6m + 1$, and let the two solutions of (2.9) be e_1 and e_2. From $(e_1)^3 \equiv 1 \pmod{\text{p}}$ and $(e_2)^3 \equiv 1 \pmod{\text{p}}$, we have $(e_1 \cdot e_2)^3 \equiv 1 \pmod{\text{p}}$. Since $e_1 \cdot e_2$ cannot be congruent to either e_1 or e_2, we have

$$e_1 \cdot e_2 \equiv 1 \pmod{p}. \tag{2.11}$$

From (2.10) and (2.11), we have: $e_2 \equiv (e_1)^2 = p - e_1 - 1$, and $e_1 \equiv (e_2)^2 = p - e_2 - 1$. That is,

$$e_1 + e_2 = p - 1. \tag{2.12}$$

We conclude that there are always two identical 3-cycles: $\langle e_1, e_1, e_1 \rangle$ and $\langle e_2, e_2, e_2 \rangle$ for a prime of the type $p = 6m + 1$ ∎

We have the following corollaries:

Corollary 2.4. *If p is a prime, then $(p-2)! \equiv 1 \pmod{p}$.*

Proof. This is the well-known Wilson's theorem. We may discuss this in the following two cases:

(a) If p is a prime of the type $p = 6m - 1$, then $G(1, p-2)$ can be divided into $(2m-1)$ 3-cycles and each 3-cycle is a triplet. Therefore we have $(p-2)! \equiv (1)^{2m-1} \equiv 1 \pmod{p}$.

(b) If p is a prime of the type $p = 6m + 1$, then $G(1, p-2)$ can be divided into $(2m-1)$ 3-cycles and two identical 3-cycles. Therefore $(p-2)! \equiv (1)^{2m-1} \cdot e_1 \cdot e_2 \equiv 1 \pmod{p}$. ∎

Corollary 2.5. *If $\langle a, b, c \rangle$ is a 3-cycle for F, then $\langle a^*, c^*, b^* \rangle$ is also a 3-cycle for F, where a^*, b^*, c^* are, respectively, the associates of the numbers a, b, c.*

Proof. This is directly derived from Theorem 2.3, as

$$a \cdot (1+b) \equiv -1 \pmod{p}, \text{ therefore } a^* = p-1-b,$$
$$b \cdot (1+c) \equiv -1 \pmod{p}, \text{ therefore } b^* = p-1-c,$$
$$c \cdot (1+a) \equiv -1 \pmod{p}, \text{ therefore } c^* = p-1-a.$$

We then easily check that $F(a^*) = c^*$, as $a^* \cdot (1+c^*) \equiv -1 \pmod{\text{p}}$. And similarly, we have $F(c^*) = b^*$ and $F(b^*) = a^*$. Hence $\langle a^*, c^*, b^* \rangle$ is a 3-cycle for F. ∎

We call $\langle a^*, c^*, b^* \rangle$ the associate 3-cycle of $\langle a, b, c \rangle$. In general, a 3-cycle and its associate 3-cycle are different; they are equal only when $a = 1,\ b = p-2$, and $c = (p-1)/2$. Hence

$$\langle 1, p-2, (p-1)/2 \rangle$$

is the only 3-cycle for F that is equal to its associate 3-cycle. We call $\langle 1, p-2, (p-1)/2 \rangle$ the self-associate 3-cycle. For $p = 6m \pm 1$, the number of 3-cycles is $2m \pm 1$, which is odd, due to the existence of the self-associate 3-cycle. From Corollary 2.5, we have $(a+b+c)+(a^*+b^*+c^*) = 3(p-1)$, and the sum of the numbers in the self-associate 3-cycle is $3(p-1)/2$. We can therefore calculate the total sum of all the numbers in $G(1, p-2)$, which is trivially calculated to be $(p-1)(p-2)/2$; as expected from $1+2+3+\cdots+p-2$.

3. The Triplet-Divisions of $G(1, p-2)$

We now discuss the division of the numbers in $G(1, p-2)$ into disjoint triplets $\langle a, b, c \rangle$. This can be obtained from the basic 3-cycle-division. We write the 3-cycle-division of the set $G(1, p-2)$ as:

$$\{\langle a_i, b_i, c_i \rangle | i = 1, 2, \cdots, n\}, \tag{3.1}$$

where $\langle a_i, b_i, c_i \rangle$ represents the ith 3-cycle for F, and $n = 2m \pm 1$ for $p = 6m \pm 1$. In what follows, the number a^j is to mean that it is in fact "$a^j \pmod{p}$", a number $\in G(1, p-2)$. We have the following theorem:

Theorem 3.1. *For j a number relatively prime to $p-1$,*

$$\{\langle a_i^j, b_i^j, c_i^j \rangle | i = 1, 2, \cdots, n\} \tag{3.2}$$

is a triplet-division of $G(1, p-2)$.

Proof. Since $\langle a_i, b_i, c_i\rangle$ is a 3-cycle for F, then $a_i \cdot b_i \cdot c_i \equiv 1$, and hence $\langle a_i^j, b_i^j, c_i^j\rangle$ is a triplet, as $a_i^j \cdot b_i^j \cdot c_i^j = (a_i \cdot b_i \cdot c_i)^j \equiv 1$. Also as j and $p-1$ are relatively prime, it is known that $1^j, 2^j, 3^j, \cdots, (p-2)^j$ are just the permutation of the numbers $1, 2, 3, \cdots, p-2$. Hence, $\{\langle a_i^j, b_i^j, c_i^j\rangle \,|\, i = 1, 2, \cdots, n\}$ represents the division of the numbers in $G(1, p-2)$ into disjoint triplets, and hence is a triplet-division of $G(1, p-2)$. The triplet-division in (3.2) with $j = 1$ is just the 3-cycle-division. ∎

The number of such $j < p$ relatively prime to $p-1$ is known to be $\varphi(p-1)$, which is the Euler φ-function of $p-1$. We have the following theorem:

Theorem 3.2. *There are $\varphi(p-1)/2$ triplet-divisions for $G(1, p-2)$ derived from the 3-cycle-division.*

Proof. Naively, we would think that there are $\varphi(p-1)$ different triplet-divisions for the set $G(1, p-2)$, since in general the triplet-divisions in (3.2) with $j = j_1$ and $j = j_2$ are different if $j_1 \neq j_2$. However, we know that if j is relatively prime to $p-1$, so is $p-1-j$. Hence if there is a triplet-division of $G(1, p-2)$ in (3.2), there will be also a triplet-division

$$\{\langle a_i^{p-1-j},\ b_i^{p-1-j},\ c_i^{p-1-j}\rangle \,|\, i = 1, 2, \cdots, n\} \tag{3.3}$$

of $G(1, p-2)$. But (3.2) and (3.3) are equivalent. As $(a_i)^j \cdot a_i^{p-1-j} \equiv 1$, therefore, $a_i^{p-1-j} = (a_i^*)^j$. Therefore (3.3) is equivalent to

$$\begin{aligned} &\{\langle (a_i^*)^j,\ (b_i^*)^j,\ (c_i^*)^j\rangle \,|\, i = 1, 2, \cdots, n\} \\ &= \{\langle (a_i^*)^j,\ (c_i^*)^j,\ (b_i^*)^j\rangle \,|\, i = 1, 2, \cdots, n\}. \end{aligned} \tag{3.4}$$

However, as we know that $\langle a^*, c^*, b^*\rangle$ is also a 3-cycle for F, $\langle (a_i^*)^j,\ (c_i^*)^j,\ (b_i^*)^j\rangle$ are triplets that are already contained in (3.2). This then means that the triplet-division in (3.3) is the same as the triplet-division in (3.2). Therefore the number of different triplet-divisions obtained from the 3-cycle-division is only $\varphi(p-1)/2$. ∎

We give an example. If $p = 17$, then $\varphi(p-1)/2 = 4$. There should then be four different ways for performing the triplet-division for $G(1, p-2)$. The basic 3-cycle–division (with $j = 1$) and the triplet-division with $j = 15$ are:

$\langle 1, 15, 8\rangle$	$\langle 1, 8, 15\rangle$
$\langle 2, 7, 11\rangle$	$\langle 9, 5, 14\rangle$
$\langle 3, 10, 4\rangle$	$\langle 6, 12, 13\rangle$
$\langle 5, 9, 14\rangle$	$\langle 7, 2, 11\rangle$
$\langle 6, 13, 12\rangle$	$\langle 3, 4, 10\rangle$
3-cycle-division	Triplet-division with $j = 15$

We see the triplet-division with $j = 15$ is the same as the 3-cycle division. Other triplet-divisions for $G(1, p-2)$ obtained from the basic 3-cycle-division are:

$\langle 1, 9, 2\rangle$	$\langle 1, 2, 9\rangle$	$\langle 1, 8, 15\rangle$
$\langle 8, 3, 5\rangle$	$\langle 15, 11, 10\rangle$	$\langle 9, 12, 3\rangle$
$\langle 10, 14, 13\rangle$	$\langle 5, 6, 4\rangle$	$\langle 11, 5, 13\rangle$
$\langle 6, 15, 7\rangle$	$\langle 14, 8, 12\rangle$	$\langle 10, 2, 6\rangle$
$\langle 12, 4, 11\rangle$	$\langle 7, 13, 3\rangle$	$\langle 14, 4, 7\rangle$
$j = 3,\ 13$	$j = 5,\ 11$	$j = 7,\ 9$

For another example, consider $p = 19$. Then $\varphi(p-1)/2 = 3$. The 3-cycle-division and the other two triplet-divisions are:

$\langle 1, 17, 9\rangle$	$\langle 1, 9, 17\rangle$
$\langle 2, 8, 6\rangle$	$\langle 10, 12, 16\rangle$
$\langle 3, 5, 14\rangle$	$\langle 13, 4, 15\rangle$
$\langle 4, 13, 15\rangle$	$\langle 5, 3, 14\rangle$
$\langle 10, 16, 12\rangle$	$\langle 2, 6, 8\rangle$
$\langle 7, 7, 7\rangle$	$\langle 11, 11, 11\rangle$
$\langle 11, 11, 11\rangle$	$\langle 7, 7, 7\rangle$
3-cycle-division	Triplet-division with $j = 17$

$\langle 1, 6, 16\rangle$	$\langle 1, 5, 4\rangle$
$\langle 13, 12, 5\rangle$	$\langle 14, 8, 9\rangle$
$\langle 15, 9, 10\rangle$	$\langle 2, 16, 3\rangle$
$\langle 17, 14, 2\rangle$	$\langle 6, 10, 13\rangle$
$\langle 3, 4, 8\rangle$	$\langle 15, 17, 12\rangle$
$\langle 7, 7, 7\rangle$	$\langle 11, 11, 11\rangle$
$\langle 11, 11, 11\rangle$	$\langle 7, 7, 7\rangle$
$\mathrm{j} = 5, 13$	$\mathrm{j} = 7, 11$

4. The F_k-map on the Set $G(1, p-1|p-k)$

If we are interested in dividing numbers into disjoint triplets $\langle a_k, b_k, c_k\rangle$ such that $a_k \cdot b_k \cdot c_k \equiv k^3 \pmod p$, then we can generalize the above discussion to the set

$$G(1, p-1\,|\,p-k) = \{1, 2, 3, \cdots, p-k-1, p-k+l, \cdots, p-1\},$$

where $1 \le k \le p-1$. The set $G(1, p-1\,|\,p-k)$ contains numbers from 1 to $p-1$, except the number $p-k$. For $k = 1$, $G(1, p-1\,|\,p-1) = G(1, p-2)$. By similar discussions in Section 2, we can then define a map $F_k : G(1, p-1\,|\,p-k) \to G(1, p-1\,|\,p-k)$ such that

$$F_k(a_k) = b_k\,,$$

where $a_k \cdot (k + b_k) \equiv -k^2 \pmod p$, or $b_k \equiv -k^2 \cdot a_k^* - k \pmod p$. And we have

(T1) Any $a_k \in G(1, p-1\,|\,p-k)$ is a period-3 point of F_k, i.e., $F_k^3(a_k) = a_k$.

(T2) Each 3-cycle for F_k, $(a_k, F_k(a_k), F_k^2(a_k))$, is a triplet with
$a_k \cdot F_k(a_k) \cdot F_k^2(a_k) \equiv k^3 \pmod p$

(T3) The numbers in $G(1, p-1\,|\,p-k)$ can be divided into 3-cycles for F_k.

Finally, if (a, b, c) is a 3-cycle for F, then $(k{\cdot}a, k{\cdot}b, k{\cdot}c)$ and $(k{\cdot}a^*, k{\cdot}c^*, k{\cdot}b^*)$ are 3-cycles for F_k, where, for instance, $k \cdot a$ means $k \cdot a \pmod p$.

Acknowledgements

The author is deeply grateful to the anonymous referee who greatly improved the representation of this article and pointed out some errors. The auther would like to thank the National Science Council of the Republic of China for support (NSC Grant No. 85–2112–M–031–001).

References

1. O. Ore, Number Theory and Its History, Chapter 11, Dover Publications, Inc., New York, 1988.
2. C. F. Gauss, Disquisitiones Arithmeticae, Springer-Verlag, New York, 1986.
3. G. B. Mathews, Theory of Numbers, 2nd edition, Chapter 3, Chelsea Publishing Company, New York.

Department of Physics, Soochow University
Taipei, Taiwan