

# Arithmetic puzzles for children

Yoichi Maeda

[maeda@tokai.ac.jp](mailto:maeda@tokai.ac.jp)

Department of Mathematics

Tokai University

Japan

**Abstract:** In this paper, we introduce arithmetic puzzles for elementary school students based on Galois field  $F_p (= \mathbb{Z}/p\mathbb{Z})$  where  $p$  is a prime number. For every prime number  $p$ , there exists a circular picture of prime  $p$ , and with this picture, we can make puzzles. There are infinitely many prime numbers, we can easily create lots of puzzles as we like. We also discuss about picture of  $\mathbb{Z}/p^n\mathbb{Z}$  where  $p$  is an odd prime number and  $n$  is a natural number. We hope that children all over the world will be able to draw pictures of prime numbers themselves in the near future.

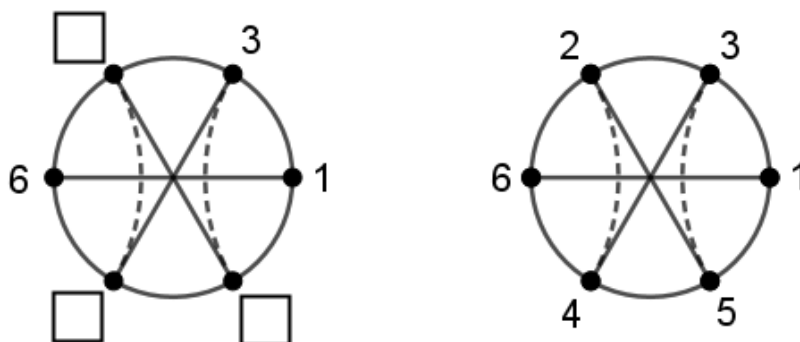
## 1. Introduction

We would like to start this paper from the following puzzle with prime number 7.

< Puzzle with prime number 7 >

Fill each blank with a natural number such that any pairs of numbers satisfy the following two conditions;

1. The sum of the two numbers at the end points of any diameter is equal to 7,
2. The product of the two numbers at the end points of any dashed arc is congruent to 1 modulo 7 (i.e., the remainder of the product divided by 7 is equal to 1).



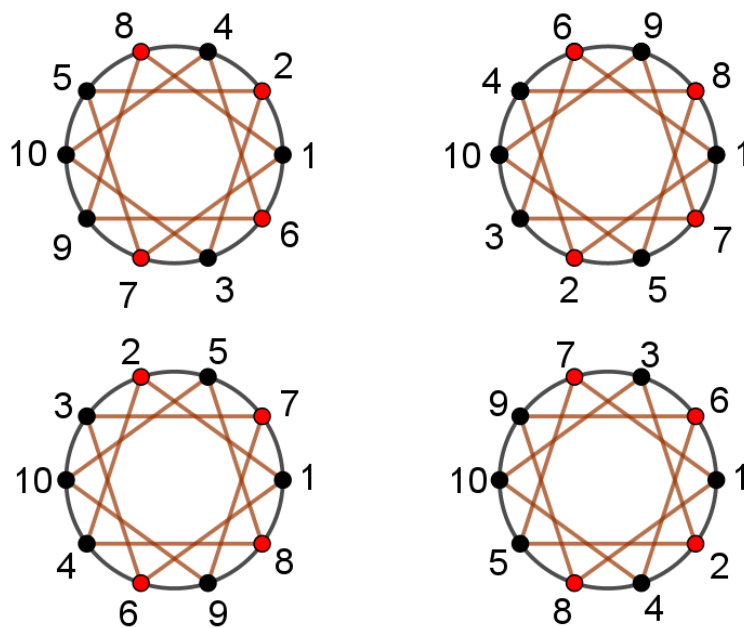
**Figure 1.1** Arithmetic puzzle (left) and its answer (right).

Figure 1.1 (right) is an example of the pictures of prime number  $p$ , that is a simple visualization of the fact;  $F_p^* (= F_p \setminus \{0\})$  is a cyclic group with a certain primitive root (generator of the cyclic group) (see, [1] p.98, [2] p.71, [3] p.132, [4] pp.50-51). In the case of prime number 7, there are two primitive roots, 3 and 5. With one primitive root 3, we can make a cycle with period 6;  $3^0 = 1, 3^1 = 3, 3^2 = 9 \equiv 2, 3^3 \equiv 2 * 3 = 6, 3^4 \equiv 6 * 3 = 18 \equiv 4, 3^5 \equiv 4 * 3 = 12 \equiv 5, 3^6 \equiv 5 * 3 = 15 \equiv 1$ , where symbol  $\equiv$  means “modulo 7”. As for another primitive root 5, the cycle is,  $5^0 = 1, 5^1 = 5, 5^2 = 25 \equiv 4, 5^3 \equiv 4 * 5 = 20 \equiv 6, 5^4 \equiv 6 * 5 = 30 \equiv 2, 5^5 \equiv 2 * 5 = 10 \equiv 3, 5^6 \equiv 3 * 5 = 15 \equiv 1$ . With this simple rule, it is easy for students to solve the puzzle by calculating counterclockwise using multiplication and division.

## 2. Pictures of prime number

For every prime number  $p$ , a picture of  $p$  is given as a diagram in which  $(p-1)$  vertices of a regular  $(p-1)$ -sided polygon are arranged on a circle, because the order of cyclic group  $F_p^* (= F_p \setminus \{0\})$  is  $p-1$ . The problem of seeking primitive roots seems to be an open problem, which is related to “Artin’s conjecture on primitive roots”. However, once a primitive root is found, all primitive roots and all pictures of prime number  $p$  can be automatically obtained. Let’s show this fact with several examples.

The first example is the case of  $p=11$ . Figure 2.1 shows four pictures of prime number 11. With the smallest primitive root 2 as shown in Table 2.1, the picture in left-upper is obtained by doubling 1 and then continuing to double. Here, note that the integers that are relatively prime to  $p-1=10$  are 1, 3, 7, and 9. The picture in right-upper is obtained by skipping 3 vertices from the picture in left-upper. In the similar way, the picture in left-lower is obtained by skipping 7 vertices from the picture in left-upper. The picture in right-lower is obtained by skipping 9 vertices from the picture in left-upper, which is the rearrangement of the picture in left-upper in reverse.



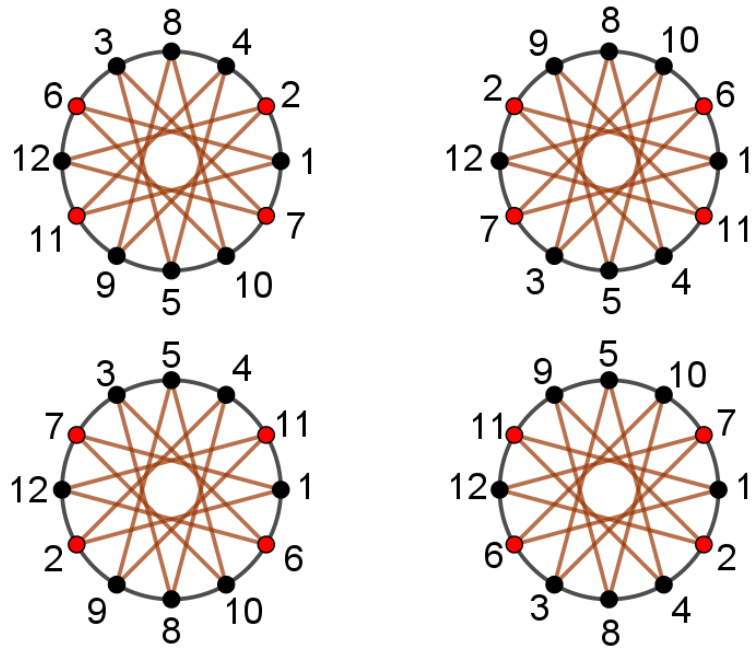
**Figure 2.1** There are four pictures of prime number 11 in total.

This process indicates that all primitive roots can be derived from a single primitive root. For a prime number  $p$ ;

- (1) Find a primitive root through trial and error.
- (2) Draw a picture of  $p$ .
- (3) Enumerate integers  $[1, \dots, p-2]$  that are coprime to  $p-1$ .
- (4) The numbers of the elements in the list correspond to the vertices of the picture and the numbers at the vertices are all primitive roots.

Hence, the number of pictures of prime number  $p$  is equal to  $\varphi(p-1)$ , where  $\varphi(n)$  is the Euler’s function (see, [1] p.54, [2] pp.52-54, [3] p.105, p.110). Since  $\varphi(10) = \#\{1,3,5,9\} = 4$ , the numbers at the four red vertices are the primitive roots in each picture of Figure 2.1.

One more example is the case of  $p=13$ . The smallest primitive root is 2 as shown in Table 2.1. Since  $\varphi(12) = \#\{1,5,7,11\} = 4$ , we can draw 4 pictures as shown in Figure 2.2.



**Figure 2.2** There are four pictures of prime number 13 in total.

The following table shows the smallest primitive root for the prime numbers up to 101 and the number of pictures of the primes.

**Table 2.1** The smallest primitive root for prime number and the totient function.

p	primitive root	p-1	phi(p-1)	p	primitive root	p-1	phi(p-1)
2	1	1	1	43	3	42	12
3	2	2	1	47	5	46	22
5	2	4	2	53	2	52	24
7	3	6	2	59	2	58	28
11	2	10	4	61	2	60	16
13	2	12	4	67	2	66	20
17	3	16	8	71	7	70	24
19	2	18	6	73	5	72	24
23	5	22	10	79	3	78	24
29	2	28	12	83	2	82	40
31	3	30	8	89	3	88	40
37	2	36	12	97	5	96	32
41	6	40	16	101	2	100	40

### 3. Group structure and the picture of prime number

Now, let's check the facts in the puzzle introduced in Section 1;

1. The sum of the two numbers at the end points of any diameter is equal to  $p$ ,
2. The product of the two numbers at the end points of any dashed arc is congruent to 1 modulo  $p$  (i.e., the remainder of the product divided by  $p$  is equal to 1).

For a primitive root  $r$ , the list of cycle is given as

$$[1, r, r^2, r^3, \dots, r^{\frac{p-1}{2}-1}, r^{\frac{p-1}{2}}, r^{\frac{p-1}{2}+1}, r^{\frac{p-1}{2}+2}, r^{\frac{p-1}{2}+3}, \dots, r^{p-2}].$$

Here, recall that  $r^{p-1} \equiv 1$ , and  $r^{\frac{p-1}{2}} \equiv -1$  by Fermat's little theorem. Hence, the list is rewritten as

$$[1, r, r^2, r^3, \dots, r^{\frac{p-1}{2}-1}, -1, -r, -r^2, -r^3, \dots, -r^{\frac{p-1}{2}-1}],$$

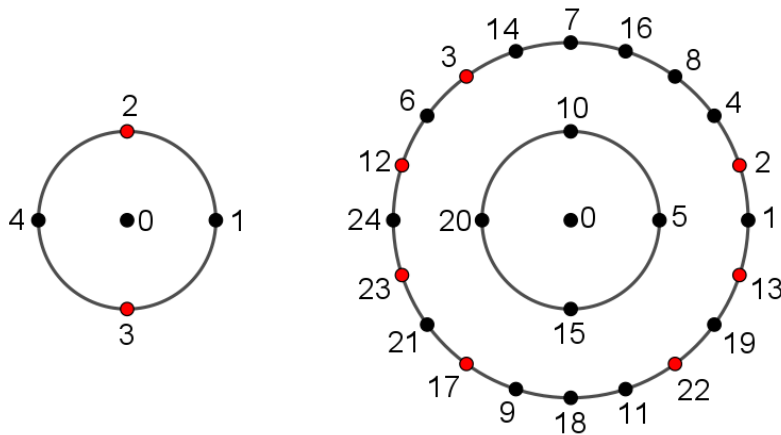
which means that the first fact is trivial. The second fact is also trivial because  $r^n \cdot r^{-n} \equiv 1$  for arbitrary integer  $n$ .

In the appendix of this paper, there are several puzzles. The readers can enjoy them even more by using the three properties of addition and multiplication. These puzzles must be a great introduction to number theory. Wilson's theorem ( $(p-1)! \equiv -1 \pmod{p}$ ) is also obvious at a glance by this picture of prime number (see, [1] pp.38-40, p.49, [2] pp.68-69, p.81). In the case of  $p=7$ ,

$$6! = 1 * 3 * 5 * 2 * 4 * 6 \equiv 6 \equiv -1.$$

### 4. Picture of $Z/p^nZ$

At the end of this paper, we will introduce the pictures of  $Z/p^nZ$  where  $p$  is an odd prime number and  $n$  is a natural number.



**Figure 3.1** A picture of  $Z/5Z$  (left) and a picture of  $Z/25Z$  (right).

Figure 3.1 shows how to create a picture of  $Z/25Z$  from a picture of  $Z/5Z$ . The left figure is a picture of prime number 5 with 0 at the center of the circle and 2 as a primitive root (see, Table 2.1). With this picture, we can make a picture of  $Z/25Z$ . First, multiply each number in the left picture by 5 which is embedded in the picture of  $Z/25Z$  as the maximal ideal of  $Z/25Z$ . Next, use 2 as a primitive root on the outer circle and repeat the process of doubling that number. With just this simple process, the picture of  $Z/25Z$  will be completed.

Figure 3.2 shows how to create a picture of  $Z/27Z$  from a picture of  $Z/3Z$ . The left figure is a picture of prime number 3 with 0 at the center of the circle and 2 as a primitive root (see, Table

2.1). With this picture, we can make a picture of  $Z/9Z$  in the middle. First, multiply each number in the left picture by 3 which is embedded in the picture of  $Z/9Z$  as the maximal ideal of  $Z/9Z$ . Next, use 2 as a primitive root on the outer circle and repeat the process of doubling that number. With just this simple process, the picture of  $Z/9Z$  will be completed. To get a picture of  $Z/27Z$  from the picture  $Z/9Z$ , multiply each number in the middle picture by 3 which is embedded in the picture of  $Z/27Z$  as the maximal ideal of  $Z/27Z$ . Then, use 2 as a primitive root on the outer circle and repeat the process of doubling that number. Now, you can make any picture of  $Z/p^nZ$  in a similar way.

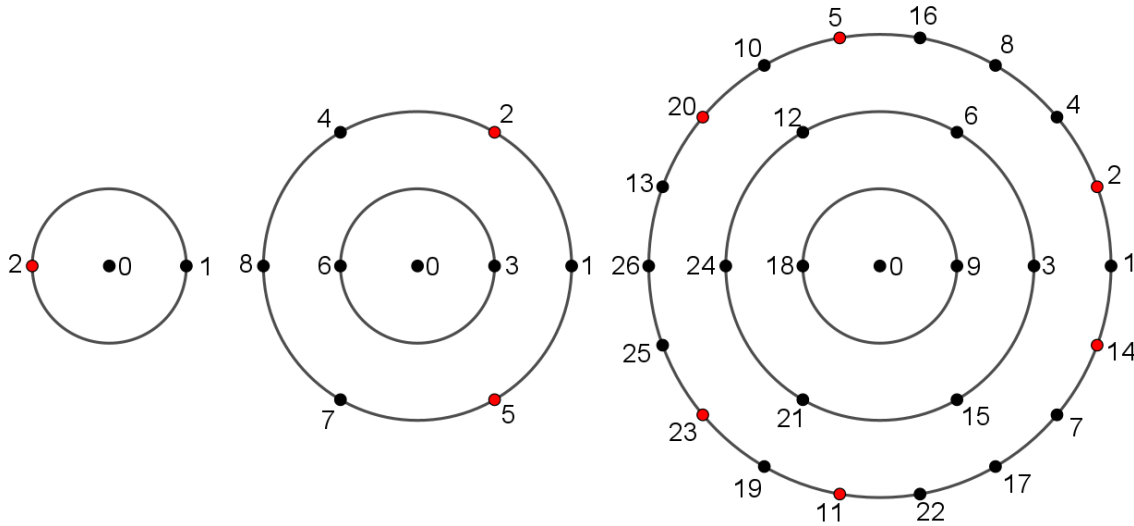


Figure 3.2 A picture of  $Z/3Z$  (left), a picture of  $Z/9Z$  (middle), and a picture of  $Z/27Z$  (right).

### 5. Appendix (Example of arithmetic puzzles)

< Puzzle with prime number 11 >

Fill each blank with a natural number such that any pairs of numbers satisfy the following two conditions;

1. The sum of the two numbers at the end points of any diameter is equal to 11,
2. The product of the two numbers at the end points of any dashed arc is congruent to 1 modulo 11 (i.e., the remainder of the product divided by 11 is equal to 1).

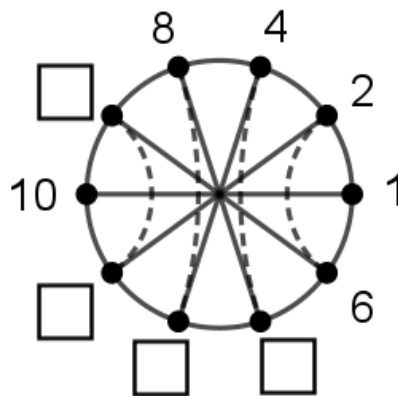
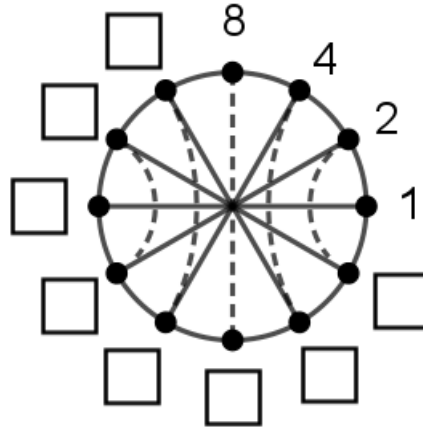


Figure A.1 Arithmetic puzzle with prime number 11.

< Puzzle with prime number 13 >

Fill each blank with a natural number such that any pairs of numbers satisfy the following two conditions;

1. The sum of the two numbers at the end points of any diameter is equal to 13,
2. The product of the two numbers at the end points of any dashed arc is congruent to 1 modulo 13 (i.e., the remainder of the product divided by 13 is equal to 1).

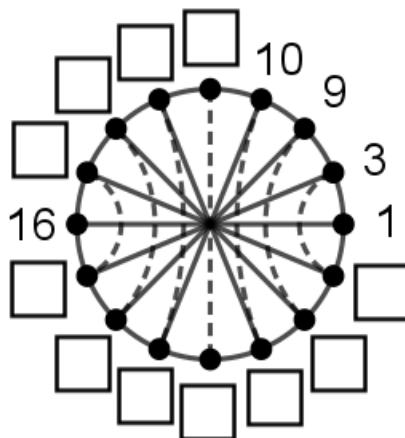


**Figure A.2** Arithmetic puzzle with prime number 13.

< Puzzle with prime number 17 >

Fill each blank with a natural number such that any pairs of numbers satisfy the following two conditions;

1. The sum of the two numbers at the end points of any diameter is equal to 17,
2. The product of the two numbers at the end points of any dashed arc is congruent to 1 modulo 17 (i.e., the remainder of the product divided by 17 is equal to 1).



**Figure A.3** Arithmetic puzzle with prime number 17.

## References

- [1] G. E. Andrews, *Number Theory*, Dover Publications, 1994.

- [2] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 2009.
- [3] N. Jacobson, *Basic Algebra I: Second Edition*, Dover Publications, 2009.
- [4] K. Kato, N. Kurokawa, T. Saito, *Number Theory 1: Fermat's Dream (Translations of Mathematical Monographs)*, American Mathematical Society, 2000.
- [5] Y. Maeda, *Suuron wo Tanoshimutame no Keisan Puzzle*. (in Japanese), RIMS Kokyuroku 2236, pp.81-89, 2022.