n進法での$\frac{1}{p}$の循環節の長さに現れる規則性

フェリス女学院高等学校　1年　山中　愛子

1　動機

『素数はめぐる　循環小数で語る数論の世界』という本を読んで、素数pの逆数の循環節の長さやそこに現れる数字についての性質を知り、興味を持った。そこで、数をn進法で表記した場合も同様の性質があるか確かめたい、もしかしたら10進法からn進法に広げることで見えてくる規則性があるかもしれない、と思い研究することにした。

2　内容

特に指定がない場合、nをpの倍数でない2以上の自然数、pを素数とする。

まず、n進法での$\frac{1}{p}$の循環節の長さについて、視覚的に規則性を発見しやすいように、表計算ソフトを使って表を作成することにした。ここで、(p−1)÷($\frac{1}{p}$の循環節の長さ)は整数になるから、(p−1)÷($\frac{1}{p}$の循環節の長さ)を表に入れることにした。

(p−1)÷($\frac{1}{p}$の循環節の長さ)＝1 のとき、$\frac{1}{p}$の循環節はダイヤル数になるなど、(p−1)÷($\frac{1}{p}$の循環節の長さ)が同じならば、$\frac{1}{p}$の循環節は似た性質を持つと考えたからである。

つまり、(p−1)÷(n進法での$\frac{1}{p}$の循環節の長さ)を表にする。縦軸がn、横軸がp、表中の数は全て10進法で表記されている。###は$\frac{1}{p}$が有限小数であることを意味する。

また、ここでは、(p−1)÷(n進法での$\frac{1}{p}$の循環節の長さ)を〈n, p〉と表すことにする。

〈例〉 n=10, p=3のとき、10進法で $\frac{1}{3}=0.\dot{3}$ だから、

〈10, 3〉＝(3−1)÷(10進法での$\frac{1}{3}$の循環節の長さ)＝2÷1＝2

n=10, p=7のとき、10進法で $\frac{1}{7}=0.\dot{1}4285\dot{7}$ だから、

〈10, 7〉＝(7−1)÷(10進法での$\frac{1}{7}$の循環節の長さ)＝6÷6＝1

n=2, p=5のとき、2進法で $\frac{1}{101}=0.\dot{0}01\dot{1}$ だから、

〈2, 5〉＝(5−1)÷(2進法での$\frac{1}{5}$の循環節の長さ)＝4÷4＝1

n=4, p=13のとき、4進法で $\frac{1}{31}=0.\dot{0}1032\dot{3}$ だから、

〈4, 13〉＝(13−1)÷(4進法での$\frac{1}{13}$の循環節の長さ)＝12÷6＝2

同様に、〈5, 7〉＝1, 〈10, 11〉＝5, 〈13, 17〉＝4, 〈17, 29〉＝7

また、n進法で$\frac{1}{p}$の循環節の長さはp−1の約数だから、〈n, p〉はp−1の約数である。

n\p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137
2	###	1	1	2	1	1	2	1	2	1	6	1	2	3	2	1	1	1	1	2	8	2	1	8	2	1	2	1	3	4	18	1	2
3	1	###	1	1	2	4	1	1	2	1	1	2	5	1	2	1	2	6	3	2	6	1	2	1	2	1	3	2	4	1	1	2	1
4	###	2	2	2	2	2	4	2	2	2	6	2	4	6	2	2	2	2	2	2	8	2	2	8	4	2	2	2	6	8	18	2	4
5	1	1	###	1	2	3	1	2	1	2	10	1	2	1	1	1	2	2	3	14	1	2	1	2	1	4	1	1	4	1	3	2	1
6	###	###	4	3	1	1	1	2	2	2	5	9	1	14	2	2	1	1	2	2	2	1	1	1	8	10	1	1	1	1	1	1	1
7	1	2	1	###	1	1	1	6	1	4	2	4	1	7	2	2	2	1	1	1	3	1	2	1	1	1	2	1	4	8	1	2	2
8	###	1	1	6	1	3	2	3	2	1	6	3	2	3	2	1	1	3	3	2	24	6	1	8	6	1	6	1	9	4	18	1	2
9	1	###	2	2	2	4	2	2	2	2	2	4	10	2	2	2	2	12	6	2	12	2	2	2	4	2	6	2	4	2	2	2	2
10	###	2	###	1	5	2	1	1	1	1	2	12	8	2	1	4	1	1	2	2	9	6	2	2	1	25	3	2	1	1	3	1	17
11	1	1	4	2	###	1	1	6	1	1	1	6	1	6	1	2	1	15	1	1	1	2	2	4	2	1	1	2	1	2	2	2	2
12	###	###	1	1	10	6	1	3	2	7	1	4	1	1	2	1	2	4	1	2	2	3	2	11	6	1	1	2	2	1	1	2	1
13	1	2	1	3	1	###	4	1	2	2	1	1	1	2	1	4	1	20	1	1	1	2	1	1	1	2	6	2	1	2	2	2	1
14	###	1	2	###	2	12	1	1	1	1	2	3	5	2	2	1	1	10	6	7	1	3	1	1	1	10	6	2	1	4	1	1	4
15	1	###	###	6	2	1	2	1	1	1	3	1	1	2	1	4	2	4	6	2	1	3	1	1	1	1	2	1	4	28	2	2	4
16	###	2	4	2	2	4	8	2	2	4	6	4	8	6	2	4	2	4	2	2	8	2	2	8	8	4	2	2	12	16	18	2	8
17	1	1	1	1	1	2	###	2	1	7	1	1	1	2	2	2	2	1	2	7	3	3	2	2	1	10	2	1	3	1	2	1	2
18	###	###	1	2	1	3	16	9	2	1	2	1	8	1	2	1	1	1	1	2	4	6	1	2	6	1	2	1	1	14	2	5	4
19	1	2	2	1	1	1	2	###	1	1	2	1	1	1	1	1	2	2	2	2	2	2	1	1	3	4	2	2	3	1	42	5	2
20	###	1	###	3	2	1	1	18	1	4	2	1	2	1	1	1	2	12	1	10	1	2	1	2	3	2	1	1	2	1	21	2	1
21	1	###	4	###	5	3	4	1	1	1	1	2	2	6	2	1	2	5	2	1	3	6	2	2	1	2	1	1	4	1	2	2	1
22	###	2	1	6	###	4	1	1	11	2	1	1	1	3	1	1	2	4	6	1	9	6	1	4	24	2	3	1	4	2	14	1	4
23	1	1	1	2	10	2	1	2	###	4	3	3	4	2	1	13	1	3	2	5	2	26	2	1	1	2	6	2	3	1	1	1	1
24	###	###	2	1	1	1	1	2	22	4	1	1	1	2	2	4	1	3	6	2	6	13	1	1	4	4	3	1	1	1	7	5	1
25	1	2	###	2	2	6	2	2	2	4	10	2	4	2	2	2	2	4	6	14	2	2	2	4	2	4	2	2	4	2	6	2	2
26	###	1	4	1	2	###	2	6	2	1	5	12	1	1	1	1	2	1	2	5	1	2	2	1	1	1	2	1	4	2	2	1	1
27	1	###	1	3	2	12	1	3	2	1	3	6	5	3	2	1	2	6	3	2	18	3	2	1	6	1	3	2	12	1	3	2	1
28	###	2	1	###	1	1	1	2	1	14	2	2	1	1	2	4	2	3	1	1	1	1	2	1	3	1	2	1	2	16	7	2	2
29	1	1	2	6	1	4	1	1	2	###	3	3	1	1	1	2	2	5	22	2	1	1	2	1	1	1	2	2	2	1	1	1	1
30	###	###	###	2	1	2	4	6	1	28	15	2	1	1	1	13	1	1	11	10	3	1	2	1	3	2	6	2	1	16	2	1	2
31	1	2	4	1	2	3	1	3	2	1	###	9	4	2	1	1	1	1	1	1	1	2	2	1	2	4	3	1	2	2	2	1	1
32	###	1	1	2	5	1	2	1	2	1	30	1	10	3	2	1	1	5	1	10	8	2	1	8	2	5	2	1	3	4	18	5	2
33	1	###	1	1	###	1	8	1	1	2	6	4	2	1	1	1	1	3	2	1	1	3	2	1	12	2	2	2	27	1	3	2	1
34	###	2	2	3	10	3	###	1	1	2	1	4	1	1	2	1	1	12	1	5	1	1	1	22	3	1	6	2	6	1	2	2	8
35	1	1	###	###	1	4	16	2	2	2	6	1	1	6	1	1	2	1	2	1	2	1	1	1	32	1	1	2	4	7	2	2	1
36	###	###	4	6	2	2	2	2	2	4	10	18	2	14	2	4	2	2	2	2	4	2	2	2	16	20	2	2	2	2	2	2	2
37	1	2	1	2	2	1	1	9	1	1	5	###	8	7	2	2	1	3	22	10	8	1	2	11	1	4	3	2	1	1	14	1	34
38	###	1	1	1	2	6	4	###	1	2	2	36	5	2	1	2	1	3	11	2	2	6	2	1	1	1	2	1	12	1	6	2	8
39	1	###	2	2	1	###	1	18	2	1	6	1	2	3	1	1	1	2	2	5	1	1	1	8	1	5	3	2	1	1	1	10	2
40	###	2	###	1	1	12	1	1	1	1	2	2	20	2	1	2	1	5	6	2	1	2	2	2	1	1	1	2	1	7	3	1	1
41	1	1	4	3	1	1	1	1	2	7	2	2	###	6	1	1	2	6	1	5	4	3	2	1	1	5	2	2	9	2	2	2	17
42	###	###	1	###	2	4	2	2	1	2	1	1	40	21	2	4	1	4	3	1	1	2	1	2	3	1	3	2	1	7	2	13	1
43	1	2	1	6	5	2	2	2	1	1	1	9	2	###	1	2	1	1	3	2	3	1	1	1	4	2	1	1	6	1	1	2	1
44	###	1	2	2	###	3	1	2	1	1	1	4	5	42	1	4	1	1	1	1	1	2	2	4	2	5	1	2	1	14	2	2	2
45	1	###	###	1	10	1	1	6	11	4	2	3	4	3	1	1	2	2	3	10	1	2	1	8	3	2	1	1	36	1	1	10	1
46	###	2	4	2	1	1	1	3	###	7	3	4	2	1	23	4	2	2	1	7	18	6	1	1	3	1	34	1	18	1	1	2	1
47	1	1	1	1	2	3	4	2	22	1	6	12	1	6	###	4	1	20	2	1	1	1	1	2	12	2	17	2	1	1	6	5	1
48	###	###	1	3	2	4	1	1	2	1	1	6	1	1	46	1	2	10	1	10	2	1	2	1	2	1	1	2	4	7	1	2	1
49	1	2	2	###	2	2	2	6	2	4	2	4	2	14	2	4	2	2	2	2	6	2	2	2	2	2	2	2	4	16	2	2	4
50	###	1	###	6	1	1	8	3	2	1	2	1	10	7	2	1	1	15	1	2	2	2	1	4	12	1	2	1	1	2	6	1	8
51	1	###	4	2	1	6	###	1	1	2	2	3	8	3	2	1	2	1	1	5	9	2	2	1	3	1	1	1	1	2	3	5	1
52	###	2	1	1	1	###	16	1	2	4	1	1	1	2	1	26	1	6	3	1	3	6	1	11	3	4	2	2	1	2	14	10	1
53	1	1	1	2	2	12	2	1	1	4	1	4	1	2	2	###	2	3	3	1	1	1	1	2	2	1	1	2	1	4	1	26	1
54	###	###	2	1	5	1	1	2	2	4	3	1	1	6	2	52	1	1	2	14	2	1	1	1	4	4	1	1	3	1	3	1	1
55	1	2	###	3	###	4	4	2	2	1	1	1	5	1	2	1	1	1	2	1	8	26	1	22	3	1	2	1	3	1	1	2	1
56	###	1	4	###	10	2	1	9	1	1	10	1	1	2	2	1	1	4	2	1	3	13	1	1	1	4	34	2	1	4	1	1	8
57	1	###	1	6	1	3	1	###	1	14	5	1	8	2	1	2	2	4	1	14	4	3	1	4	1	5	17	2	1	4	1	1	1
58	###	2	1	2	2	1	1	18	2	###	3	2	1	2	1	1	29	12	3	2	1	3	1	1	1	4	2	1	1	1	1	26	1
59	1	1	2	1	2	1	2	1	2	28	2	1	8	6	2	2	###	1	6	1	1	1	2	1	1	1	2	1	1	1	7	2	8
60	###	###	###	2	2	3	2	1	1	1	3	3	1	2	1	2	58	30	2	2	1	1	1	1	1	5	2	1	2	4	2	10	8
61	1	2	4	1	1	4	1	2	1	1	15	1	2	1	2	1	1	###	1	1	2	3	2	1	32	1	6	2	2	2	6	26	2
62	###	1	1	3	1	2	1	2	2	2	###	2	2	1	1	2	2	60	6	1	1	6	1	1	16	5	1	2	1	2	2	10	1
63	1	###	1	###	1	1	1	2	1	2	30	12	1	1	2	4	2	1	1	1	9	1	2	1	3	1	2	1	36	2	9	10	4
64	###	2	2	6	2	6	4	6	2	2	6	6	4	6	2	2	2	6	6	2	24	6	2	8	12	2	6	2	18	8	18	2	4
65	1	1	###	2	5	###	1	3	1	4	1	2	1	3	2	1	1	2	2	1	12	6	2	1	2	10	1	1	1	7	1	2	4
66	###	###	4	1	###	12	2	2	1	1	6	3	4	2	1	4	2	2	33	7	3	1	1	1	2	1	6	1	12	1	3	1	1
67	1	2	1	2	10	1	8	1	1	2	10	2	1	2	1	1	1	1	###	1	2	6	1	8	3	1	1	1	1	1	1	1	1
68	###	1	1	1	1	4	###	6	11	1	5	9	5	2	2	4	2	1	66	1	1	1	2	2	1	4	2	1	9	1	14	5	2
69	1	###	2	3	2	2	16	3	###	1	2	1	1	1	1	4	1	3	1	1	4	3	2	2	3	5	3	2	1	14	2	5	2
70	###	2	###	###	2	3	2	1	22	7	6	4	1	3	1	2	1	12	3	35	6	1	2	1	6	2	1	1	1	1	2	13	1
71	1	1	4	6	2	1	1	1	2	2	2	4	1	1	2	1	2	1	2	###	4	3	1	2	1	4	1	1	6	7	2	5	1
72	###	###	1	2	1	1	4	1	2	1	2	1	4	1	2	1	1	15	3	70	36	2	1	2	2	1	6	1	1	2	2	1	8
73	1	2	1	1	1	3	1	2	2	1	1	18	10	1	1	1	1	4	2	2	###	2	1	4	4	1	3	1	4	7	6	13	8
74	###	1	2	2	1	4	1	2	1	4	1	###	2	2	2	1	2	20	1	2	72	1	1	1	1	1	1	1	2	1	2	2	8
75	1	###	###	1	2	2	1	9	2	7	1	36	1	3	2	1	2	10	3	2	8	1	2	1	24	1	1	2	12	1	7	2	1
76	###	2	4	3	5	1	2	###	1	1	2	1	1	1	1	13	2	4	6	14	6	2	1	1	1	2	6	2	27	1	6	1	2
77	1	1	1	###	###	6	2	18	2	1	3	2	2	1	1	4	1	4	2	2	8	1	2	11	3	2	1	1	3	2	3	2	4
78	###	###	1	6	10	###	1	1	2	4	6	2	8	6	1	2	2	1	1	1	1	39	2	8	3	4	1	1	4	7	1	13	4
79	1	2	2	2	1	12	1	1	1	1	1	1	5	14	2	1	2	1	1	2	2	###	1	2	6	4	6	2	1	1	2	5	1
	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137

3 考察

3.1 n進法で$\frac{1}{p}$の循環節の長さがdであることと、dが$n^d \equiv 1 \pmod{p}$を満たす最小の自然数であることは同値

(証明)

(i) n進法で$\frac{1}{p}$の循環節の長さをdとする。
dは$n^d \cdot \frac{1}{p}$と$\frac{1}{p}$の小数点以下が一致する最小の自然数だから、
$(n^d \cdot \frac{1}{p} - \frac{1}{p}) =$(整数)
両辺にpをかけて、$(n^d - 1) =$(pの倍数) つまり、$n^d \equiv 1 \pmod{p}$
よって、dは$n^d \equiv 1$を満たす最小の自然数.

(ii) dが$n^d \equiv 1 \pmod{p}$を満たす最小の自然数であるとき、
$n^d \equiv 1 \pmod{p}$より、$(n^d - 1) =$(pの倍数)
両辺をpで割って、$(n^d \cdot \frac{1}{p} - \frac{1}{p}) =$(整数)
よって、dは$n^d \cdot \frac{1}{p}$と$\frac{1}{p}$の小数点以下が一致する最小の自然数だから、
$\frac{1}{p}$の循環節の長さはdである。

(i)・(ii)より、n進法で$\frac{1}{p}$の循環節の長さがdであることと、
dが$n^d \equiv 1 \pmod{p}$を満たす最小の自然数であることは同値. ■

3.2.1 $\langle n, p \rangle = a$ならば、$n^{\frac{p-1}{a}} \equiv 1 \pmod{p}$

(証明)

$\langle n, p \rangle = a$のとき、$\langle n, p \rangle$の定義より、n進法での$\frac{1}{p}$の循環節の長さは$\frac{p-1}{a}$だから、$n^{\frac{p-1}{a}} \equiv 1 \pmod{p}$ ■

3.2.2 $n^{\frac{p-1}{a}} \equiv 1 \pmod{p}$ならば、$\langle n, p \rangle$はaの倍数.

(証明)

$n^{\frac{p-1}{a}} \equiv 1 \pmod{p}$より、$(n^{\frac{p-1}{a}} - 1) =$(pの倍数)
両辺をpで割って、$(n^{\frac{p-1}{a}} \cdot \frac{1}{p} - \frac{1}{p}) =$(整数)
よって、$n^{\frac{p-1}{a}} \cdot \frac{1}{p}$と$\frac{1}{p}$の小数点以下は一致するから、$\frac{1}{p}$の循環節の長さは$\frac{p-1}{a}$の約数であるから、
$\langle n, p \rangle = (p-1) \div (\frac{p-1}{a}$の約数$) =$(aの倍数)
したがって、$n^{\frac{p-1}{a}} \equiv 1 \pmod{p}$ならば、$\langle n, p \rangle$はaの倍数。 ■

3.3 $n_1 \equiv n_2 \pmod{p}$ならば、$\langle n_1, p \rangle = \langle n_2, p \rangle$

(n_1, n_2はpの倍数でない2以上の自然数)

〈例〉$p=2$のとき、$\langle 3, 2 \rangle = \langle 5, 2 \rangle = \langle 7, 2 \rangle = \langle 9, 2 \rangle = \cdots$
$p=7$のとき、$\langle 4, 7 \rangle = \langle 11, 7 \rangle = \langle 18, 7 \rangle = \langle 25, 7 \rangle = \cdots$
$p=17$のとき、$\langle 12, 17 \rangle = \langle 29, 17 \rangle = \langle 46, 17 \rangle = \langle 63, 17 \rangle = \cdots$

(証明)
mod p で考える。a, r を自然数とする。
$\langle n_1, p\rangle = a$ のとき、n_1 進法での $\frac{1}{p}$ の循環節の長さは $\frac{p-1}{a}$ だから、$\frac{p-1}{a}$ は $n_1^{\frac{p-1}{a}} \equiv 1$ を満たす最小の自然数 ―①
また、$n_1 \equiv n_2$ より、$n_1^r \equiv n_2^r$ ―② (∵ 3.1)
①・②より、$\frac{p-1}{a}$ は $n_2^{\frac{p-1}{a}} \equiv 1$ を満たす最小の自然数。
よって、n_2 進法での $\frac{1}{p}$ の循環節の長さは $\frac{p-1}{a}$ だから、$\langle n_2, p\rangle = (p-1) \div \frac{p-1}{a} = a$ (∵ 3.1)
したがって、$\langle n_1, p\rangle = \langle n_2, p\rangle$ ■

3.4.1 $n \equiv 1 \pmod p$ のとき、$\langle n, p\rangle = p-1$
〈例〉 $\langle 3,2\rangle = 1$, $\langle 4,3\rangle = 2$, $\langle 6,5\rangle = 4$, $\langle 8,7\rangle = 6$, $\langle 12,11\rangle = 10$
(証明) $n \equiv 1 \pmod p$ より、$\frac{1}{p}$ の循環節の長さは1だから、$\langle n, p\rangle = (p-1) \div 1 = p-1$ ■

3.4.2 $n \equiv -1 \pmod p$ のとき、$\langle n, p\rangle = \frac{p-1}{2}$ (pは奇素数)
〈例〉 $\langle 2,3\rangle = 1$, $\langle 4,5\rangle = 2$, $\langle 6,7\rangle = 3$, $\langle 10,11\rangle = 5$
(証明) $n \not\equiv 1 \pmod p$, $n^2 \equiv 1 \pmod p$ より、$\frac{1}{p}$ の循環節の長さは2だから、$\langle n, p\rangle = (p-1) \div 2 = \frac{p-1}{2}$ ■

3.5 g が p を法とする原始根であることと、$\langle g, p\rangle = 1$ は同値 ($g \geqq 2$)
〈例〉 $\langle 2,5\rangle = 1$ mod 5で、$2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$, $2^4 \equiv 1$ より、2は5を法とする原始根
$\langle 3,7\rangle = 1$ mod 7で、$3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1$ より、3は7を法とする原始根
(証明) (i) g が p を法とする原始根であるとき、
$p-1$ は $g^{p-1} \equiv 1 \pmod p$ を満たす最小の自然数だから、g 進法での $\frac{1}{p}$ の循環節の長さは $p-1$
よって、$\langle g, p\rangle = (p-1) \div (p-1) = 1$ (∵ 3.1)
(ii) $\langle g, p\rangle = 1$ であるとき、g 進法の $\frac{1}{p}$ の循環節の長さは $p-1$ であるから、
$p-1$ は $g^{p-1} \equiv 1 \pmod p$ を満たす最小の自然数だから、g は p を法とする原始根 (∵ 3.1)
(i)・(ii)より、g が p を法とする原始根であることと、$\langle g, p\rangle = 1$ は同値。 ■

3.6 $\langle g, p\rangle = 1$ のとき、$\langle g^a, p\rangle = \gcd(a, p-1)$
$\langle n, p\rangle = k$ のとき、$\langle n^a, p\rangle = \gcd(a, \frac{p-1}{k}) \cdot k$ ($g \geqq 2$, g, a, k は自然数)
〈例〉 $g=2$, $p=5$ のとき、$\langle 2,5\rangle = 1$ であるから、
$\langle 2,5\rangle = \gcd(1,4) = 1$, $\langle 2^2,5\rangle = \gcd(2,4) = 2$,
$\langle 2^3,5\rangle = \gcd(3,4) = 1$, $\langle 2^4,5\rangle = \gcd(4,4) = 4$
$g=3$, $p=7$ のとき、$\langle 3,7\rangle = 1$ であるから、
$\langle 3,7\rangle = \gcd(1,6) = 1$, $\langle 3^2,7\rangle = \gcd(2,6) = 2$,
$\langle 3^3,7\rangle = \gcd(3,6) = 3$, $\langle 3^4,7\rangle = \gcd(4,6) = 2$,
$\langle 3^5,7\rangle = \gcd(5,6) = 1$, $\langle 3^6,7\rangle = \gcd(6,6) = 6$

$n=3$, $p=11$ のとき、$\langle 3,11\rangle=2$ であるから、
$\langle 3,11\rangle=\gcd(1,5)\cdot 2=2$, $\langle 3^2,11\rangle=\gcd(2,5)\cdot 2=2$,
$\langle 3^3,11\rangle=\gcd(3,5)\cdot 2=2$, $\langle 3^4,11\rangle=\gcd(4,5)\cdot 2=2$
$\langle 3^5,11\rangle=\gcd(5,5)\cdot 2=10$
$n=5$, $p=13$ のとき、$\langle 5,13\rangle=3$ であるから、
$\langle 5,13\rangle=\gcd(1,4)\cdot 3=3$, $\langle 5^2,13\rangle=\gcd(2,4)\cdot 3=6$,
$\langle 5^3,13\rangle=\gcd(3,4)\cdot 3=3$, $\langle 5^4,13\rangle=\gcd(4,4)\cdot 3=12$

(証明) mod p で考える。
$\langle g,p\rangle=1$, a,r を自然数, $d=\gcd(a,p-1)$, m は $\frac{p-1}{d}$ の約数とする。
フェルマーの小定理より, $g^{p-1}\equiv 1$ —①
$\frac{a}{d}$ は整数だから、①より, $g^{(p-1)\cdot\frac{a}{d}}=g^{a\cdot\frac{p-1}{d}}=(g^a)^{\frac{p-1}{d}}\equiv 1$
よって、$\langle g^a,p\rangle$ は d の倍数. (∵ 3.2.2)
また、$\langle g^a,p\rangle$ は $p-1$ の約数だから, m を $\frac{p-1}{d}$ の約数として、
$\langle g^a,p\rangle=dm$ とおける。—②
②より, $(g^a)^{\frac{p-1}{dm}}=g^{a\frac{(p-1)}{dm}}\equiv 1$ —③ (∵ 3.2.1)
ここで, $\langle g,p\rangle=1$ より, $g^r\equiv 1$ を満たす最小の自然数が $p-1$ だから, (∵ 3.1)
③より, $\frac{a(p-1)}{dm}$ は $p-1$ の倍数であるから, $\frac{a}{dm}$ は整数。よって、m は $\frac{a}{d}$ の約数。
仮定より, m は $\frac{p-1}{d}$ の約数でもあるから, m は $\frac{a}{d}$ と $\frac{p-1}{d}$ の公約数。
ここで, $d=\gcd(a,p-1)$ より, $\frac{a}{d}$ と $\frac{p-1}{d}$ は互いに素だから, $m=1$
$m=1$ を②に代入して, $\langle g^a,p\rangle=d$
したがって, $\langle g,p\rangle=1$ のとき, $\langle g^a,p\rangle=\gcd(a,p-1)$ が成り立つ. ■

(証明) mod p で考える。
$\langle n,p\rangle=k$, a,r を自然数, $d=\gcd(a,\frac{p-1}{k})$, m は $\frac{p-1}{dk}$ の約数とする。
$\langle n,p\rangle=k$ より, $n^{\frac{p-1}{k}}\equiv 1$ —① (∵ 3.2.1)
$\frac{a}{d}$ は整数だから, ①より, $n^{\frac{p-1}{k}\cdot\frac{a}{d}}=n^{a\cdot\frac{p-1}{dk}}=(n^a)^{\frac{p-1}{dk}}\equiv 1$
よって, $\langle n^a,p\rangle$ は dk の倍数. (∵ 3.2.2)
また, $\langle n^a,p\rangle$ は $p-1$ の約数だから, m を $\frac{p-1}{dk}$ の約数として、
$\langle n^a,p\rangle=dkm$ とおける. —②
②より, $(n^a)^{\frac{p-1}{dkm}}=n^{\frac{a(p-1)}{dkm}}\equiv 1$ —③ (∵ 3.2.1)
ここで, $\langle n,p\rangle=k$ より, $n^r\equiv 1$ を満たす最小の自然数が $\frac{p-1}{k}$ だから, (∵ 3.1)
③より, $\frac{a(p-1)}{dkm}$ は $\frac{p-1}{k}$ の倍数であるから, $\frac{a}{dm}$ は整数. よって, m は $\frac{a}{d}$ の約数.
仮定より, m は $\frac{p-1}{dk}$ の約数でもあるから, m は $\frac{a}{d}$ と $\frac{p-1}{dk}$ の公約数.
ここで, $d=\gcd(a,\frac{p-1}{k})$ より, $\frac{a}{d}$ と $\frac{p-1}{dk}$ は互いに素だから, $m=1$
$m=1$ を②に代入して, $\langle n^a,p\rangle=dk$
したがって, $\langle n,p\rangle=k$ のとき, $\langle n^a,p\rangle=\gcd(a,\frac{p-1}{k})\cdot k$ が成り立つ. ■

3.7 $\langle n_1, p\rangle$ と $\langle n_2, p\rangle$ の偶奇が一致するならば、$\langle n_1 n_2, p\rangle$ は偶数。
$\langle n_1, p\rangle$ と $\langle n_2, p\rangle$ の偶奇が一致しないならば、$\langle n_1 n_2, p\rangle$ は奇数。
(n_1, n_2 は p の倍数でない2以上の自然数, p は奇素数)

〈例〉$n_1=2, n_2=3, p=5$ のとき、$\langle 2,5\rangle=1, \langle 3,5\rangle=1, \langle 6,5\rangle=4$　$n_1=4, n_2=12, p=13$ のとき、$\langle 4,13\rangle=2, \langle 12,13\rangle=6, \langle 48,13\rangle=4$
$n_1=2, n_2=4, p=3$ のとき、$\langle 2,3\rangle=1, \langle 4,3\rangle=2, \langle 8,3\rangle=1$　$n_1=4, n_2=5, p=7$ のとき、$\langle 4,7\rangle=2, \langle 5,7\rangle=1, \langle 20,7\rangle=3$

(証明) mod p で考える。a, k_1, k_2, m_1, m_2 を自然数、$\langle g, p\rangle=1$ とする。

(i) $\langle n_1, p\rangle=2k_1, \langle n_2, p\rangle=2k_2$ のとき、$n_1 \equiv g^a$ とおくと、$\langle n_1, p\rangle=\langle g^a, p\rangle=\gcd(a, p-1)=2k_1$ より
$n_1 \equiv g^{2m_1}$ とおける。同様に、$n_2 \equiv g^{2m_2}$ とおけるから、$\langle n_1 n_2, p\rangle=\langle g^{2(m_1+m_2)}, p\rangle=\gcd(2(m_1+m_2), p-1)=$(偶数)

(ii) $\langle n_1, p\rangle=2k_1-1, \langle n_2, p\rangle=2k_2-1$ のとき、$n_1 \equiv g^a$ とおくと、$\langle n_1, p\rangle=\langle g^a, p\rangle=\gcd(a, p-1)=2k_1-1$ より
$n_1 \equiv g^{2m_1-1}$ とおける。同様に、$n_2 \equiv g^{2m_2-1}$ とおけるから、$\langle n_1 n_2, p\rangle=\langle g^{2(m_1+m_2-1)}, p\rangle=\gcd(2(m_1+m_2-1), p-1)=$(偶数)

(iii) $\langle n_1, p\rangle=2k_1-1, \langle n_2, p\rangle=2k_2$ のとき、(i)・(ii)と同様に、$n_1 \equiv g^{2m_1-1}, n_2 \equiv g^{2m_2}$ とおけるから、
$\langle n_1 n_2, p\rangle=\langle g^{2(m_1+m_2)-1}, p\rangle=\gcd(2(m_1+m_2)-1, p-1)=$(奇数)

(i)・(ii)より、$\langle n_1, p\rangle$ と $\langle n_2, p\rangle$ の偶奇が一致するならば、$\langle n_1 n_2, p\rangle$ は偶数。
(iii)より、$\langle n_1, p\rangle$ と $\langle n_2, p\rangle$ の偶奇が一致しないならば、$\langle n_1 n_2, p\rangle$ は奇数。 ■

3.8 $\langle p+1, p\rangle, \langle p+2, p\rangle, \cdots, \langle p+(p-1), p\rangle$ の種類と個数は、
$\gcd(1, p-1), \gcd(2, p-1), \cdots, \gcd(p-1, p-1)$ の種類と個数に等しい。

〈例〉$p=13$ のとき、$\langle 14,13\rangle, \langle 15,13\rangle, \cdots, \langle 25,13\rangle$ と
$\gcd(1,12), \gcd(2,12), \cdots, \gcd(12,12)$ の種類と個数は、それぞれ、
1が4個 …$\langle 15,13\rangle, \langle 19,13\rangle, \langle 20,13\rangle, \langle 24,13\rangle, \gcd(1,12), \gcd(5,12), \gcd(7,12), \gcd(11,12)$
2が2個 …$\langle 17,13\rangle, \langle 23,13\rangle, \gcd(2,12), \gcd(10,12)$
3が2個 …$\langle 18,13\rangle, \langle 21,13\rangle, \gcd(3,12), \gcd(9,12)$
4が2個 …$\langle 16,13\rangle, \langle 22,13\rangle, \gcd(4,12), \gcd(8,12)$
6が1個 …$\langle 25,13\rangle, \gcd(6,12)$
12が1個 …$\langle 14,13\rangle, \gcd(12,12)$

(証明) mod p で考える。
p を法とする原始根の1つを g, a, m は $1 \leqq a, m \leqq p-1$ を満たす自然数とする。
g は p を法とする原始根であるから、
任意の m に対して $p+m \equiv m \equiv g^a$ を満たす a がただ1つ存在し、
任意の a に対して $p+m \equiv m \equiv g^a$ を満たす m がただ1つ存在する。
よって、$\langle p+1, p\rangle, \langle p+2, p\rangle, \cdots, \langle p+(p-1), p\rangle$ の種類と個数は、$\langle g, p\rangle, \langle g^2, p\rangle, \cdots, \langle g^{p-1}, p\rangle$ の種類と個数に等しい。—①
また、$\langle g^a, p\rangle=\gcd(a, p-1)$ より、
$\langle g, p\rangle, \langle g^2, p\rangle, \cdots, \langle g^{p-1}, p\rangle=\gcd(1, p-1), \gcd(2, p-1), \cdots, \gcd(p-1, p-1)$ —②
①・②より、$\langle p+1, p\rangle, \langle p+2, p\rangle, \cdots, \langle p+(p-1), p\rangle$ の種類と個数は、
$\gcd(1, p-1), \gcd(2, p-1), \cdots, \gcd(p-1, p-1)$ の種類と個数に等しい。 ■

3.9 $\langle p+n, p\rangle$ と $\langle p+(p-n)\rangle, p\rangle$ の関係 （nは$1 \leqq n \leqq p-1$を満たす自然数, pは奇素数）

〈例〉$p=13$のとき, $\langle 14,13\rangle, \langle 15,13\rangle, \cdots, \langle 25,13\rangle$を左から書き出すと,

12, 1, 4, 2, 3, 1 , 1, 3, 4, 2, 1, 6

$\langle 13+n,13\rangle=1$のとき, $\langle 13+(13-n),13\rangle=1$, $\langle 13+n,13\rangle=2$のとき, $\langle 13+(13-n),13\rangle=4$, $\langle 13+n,13\rangle=3$のとき, $\langle 13+(13-n),13\rangle=3$

$\langle 13+n,13\rangle=4$のとき, $\langle 13+(13-n),13\rangle=2$, $\langle 13+n,13\rangle=6$のとき, $\langle 13+(13-n),13\rangle=12$, $\langle 13+n,13\rangle=12$のとき, $\langle 13+(13-n),13\rangle=6$

$p=17$のとき, $\langle 18,17\rangle, \langle 19,17\rangle, \cdots, \langle 33,17\rangle$を左から書き出すと,

16, 2, 1, 4, 1, 1, 1, 2 , 2, 1, 1, 1, 4, 1, 2, 8

$\langle 17+n,17\rangle=1$のとき, $\langle 17+(17-n),17\rangle=1$, $\langle 17+n,17\rangle=2$のとき, $\langle 17+(17-n),17\rangle=2$, $\langle 17+n,17\rangle=4$のとき, $\langle 17+(17-n),17\rangle=4$

$\langle 17+n,17\rangle=8$のとき, $\langle 17+(17-n),17\rangle=16$, $\langle 17+n,17\rangle=16$のとき, $\langle 17+(17-n),17\rangle=8$

これらから, rは自然数, kとlは奇数, $p-1=2^r\cdot k$とすると,

$\langle p+n,p\rangle=2^r\cdot l$ のとき, $\langle p+(p-n),p\rangle=2^{r-1}\cdot l$

$\langle p+n,p\rangle=2^{r-1}\cdot l$ のとき, $\langle p+(p-n),p\rangle=2^r\cdot l$

$\langle p+n,p\rangle \neq 2^r\cdot l, 2^{r-1}\cdot l$のとき, $\langle p+(p-n),p\rangle=\langle p+n,p\rangle$ が成り立つと予想できる。

また, $\langle n,p\rangle=(p-1)\div$（$n$進法での$p$の循環節の長さ）

$=(p-1)\div$（$n^d\equiv 1 \pmod p$となる最小の自然数d） （$\because$ 3.1）

$=(p-1)\div$（pを法とするnの位数） だから,

$\langle p+n,p\rangle=2^r\cdot k\div$（$p$を法とする$p+n$の位数）$=2^r\cdot k\div$（$p$を法とする$n$の位数）

$\langle p+(p-n),p\rangle=2^r\cdot k\div$（$p$を法とする$p+(p-n)$の位数）$=2^r\cdot k\div$（$p$を法とする$p-n$の位数）

よって, 上記の予想は, Lを奇数, Mを自然数として,

（pを法とするnの位数）$=L$のとき, （pを法とする$p-n$の位数）$=2L$

（pを法とするnの位数）$=2L$のとき, （pを法とする$p-n$の位数）$=L$

（pを法とするnの位数）$=4M$のとき, （pを法とする$p-n$の位数）$=4M$ と言い替えられる。

（証明） mod p で考える.

pは素数だから, $ab\equiv 0$ ならば, $a\equiv 0$ または $b\equiv 0$ が成り立つ.

(i) （pを法とするnの位数）$=L$のとき, $n, n^2, \cdots, n^{L-1}, n^{L+1}, \cdots, n^{2L-1}\not\equiv \pm 1$, $n^L\equiv 1$ だから,

$(p-n), (p-n)^2, \cdots, (p-n)^{L-1}, (p-n)^{L+1}, \cdots, (p-n)^{2L-1}\not\equiv \pm 1$, $(p-n)^L\equiv -1$, $(p-n)^{2L}\equiv 1$

よって, （pを法とする$p-n$の位数）$=2L$

(ii) （pを法とするnの位数）$=2L$のとき, $n, n^2, \cdots, n^{L-1}\not\equiv \pm 1$, $(n^L-1)(n^L+1)\equiv 0$より$n^L\equiv -1$だから,

$(p-n), (p-n)^2, \cdots, (p-n)^{L-1}\not\equiv \pm 1$, $(p-n)^L\equiv 1$

よって, （pを法とする$p-n$の位数）$=L$

(iii) （pを法とするnの位数）$=4M$のとき, $n, n^2, \cdots, n^{2M-1}, n^{2M+1}, \cdots, n^{4M-1}\not\equiv \pm 1$,

$(n^{2M}-1)(n^{2M}+1)\equiv 0$より, $n^{2M}\equiv -1$, $n^{4M}\equiv 1$ だから,

$(p-n), (p-n)^2, \cdots, (p-n)^{2M-1}, (p-n)^{2M+1}, \cdots, (p-n)^{4M-1}\not\equiv \pm 1$, $(p-n)^{2M}\equiv -1$, $(p-n)^{4M}\equiv 1$

よって, （pを法とする$p-n$の位数）$=4M$

(i)〜(iii)より, 題意は満たされた。 ■

3.10 $\langle \frac{p-1}{4k-1}, p \rangle$ は2の倍数（kは自然数，pは$p \equiv 1 \pmod{4k-1}$を満たす奇素数）

〈例〉 $k=1$のとき，$4k-1=3$　$\langle 2,7\rangle=2, \langle 4,13\rangle=2, \langle 6,19\rangle=2, \langle 10,31\rangle=2$

$k=2$のとき，$4k-1=7$　$\langle 4,29\rangle=2, \langle 6,43\rangle=14, \langle 10,71\rangle=2, \langle 16,113\rangle=16$

$k=3$のとき，$4k-1=11$　$\langle 2,23\rangle=2, \langle 6,67\rangle=2, \langle 8,89\rangle=8, \langle 18,199\rangle=18$

$k=4$のとき，$4k-1=15$　$\langle 2,31\rangle=6, \langle 4,61\rangle=2, \langle 10,151\rangle=2, \langle 12,181\rangle=2$

$k=5$のとき，$4k-1=19$　$\langle 10,191\rangle=2, \langle 12,229\rangle=2, \langle 24,457\rangle=8, \langle 30,571\rangle=2$

ここから，$\langle \frac{p-1}{4k-1}, p \rangle$は2の倍数であると予想できる。

3.10.1 nがpを法とする平方剰余であることと，$\langle n,p\rangle$が2の倍数であることは同値（pは奇素数）

（証明） mod pで考える。

xはpの倍数でない自然数，aとmは自然数，pを法とする原始根の1つをgとする。

(i) nがpを法とする平方剰余であるとき，$x^2 \equiv n$を満たすxが存在する。

$x \not\equiv 0$だから，$g^m \equiv x$を満たすg, mが存在する。

このとき，$n \equiv g^{2m}$だから，$\langle n,p\rangle = \langle g^{2m},p\rangle = \gcd(2m, p-1) =$（2の倍数）（∵ 3.6）

(ii) $\langle n,p\rangle$が2の倍数であるとき，$n \equiv g^a$とおくと，$\langle n,p\rangle = \langle g^a,p\rangle = \gcd(a,p-1) =$（2の倍数）より，（∵ 3.6）

$a=2m$とおける。このとき，$(g^m)^2 \equiv n$だから，nはpを法とする平方剰余。

(i)・(ii)より，nがpを法とする平方剰余であることと，$\langle n,p\rangle$が2の倍数であることは同値。■

3.10.2 $\langle n,p\rangle$がlの倍数ならば，nはpを法とするl次剰余（lは自然数）

（証明） mod pで考える。

aとmは自然数，pを法とする原始根の1つをgとする。

$n \equiv g^a$とおくと，$\langle n,p\rangle = \langle g^a,p\rangle = \gcd(a,p-1) =$（lの倍数）より，（∵ 3.6）

$a=lm$とおける。このとき，$(g^m)^l \equiv n$だから，nはpを法とするl次剰余。■

3.10.3 $\langle \frac{p-1}{4k-1}, p \rangle$は2の倍数（kは自然数，pは$p \equiv 1 \pmod{4k-1}$を満たす奇素数）

（証明）

$4k-1 = a_1 a_2 a_3 \cdots a_r$と素因数分解されているとする。

（ただし，a_i $(i=1,2,3,\cdots,r)$には同じものがあってもよい。）

$p \equiv 1 \pmod{4k-1}$より，$p \equiv 1 \pmod{a_i}$だから，

pはa_iの平方剰余 ―― ⊛

(i) $p \equiv 1 \pmod 4$のとき，平方剰余の相互法則と⊛より，a_iはpの平方剰余であるから，

$\langle a_1,p\rangle, \langle a_2,p\rangle, \cdots, \langle a_r,p\rangle$は全て2の倍数だから，（∵ 3.10.1）

$\langle a_1 a_2 a_3 \cdots a_r, p\rangle = \langle 4k-1,p\rangle$も2の倍数。（∵ 3.7）

よって，$(4k-1)^{\frac{p-1}{2}} \equiv 1 \equiv (-1)^{\frac{p-1}{2}} \pmod p$　（∵ 3.2.1）

したがって，$(p-1)^{\frac{p-1}{2}} \equiv (4k-1)^{\frac{p-1}{2}} \pmod p$

(ii) $p \equiv -1 \pmod 4$ のとき、平方剰余の相互法則と㊙より、
$a_i \equiv 1 \pmod 4$ のとき、a_i は p の平方剰余であるから、$\langle a_i, p\rangle$ は 2 の倍数 ―① (∵3.10.1)
$a_i \equiv -1 \pmod 4$ のとき、a_i は p の平方非剰余であるから、$\langle a_i, p\rangle$ は 2 の倍数ではない ―②
また、$4k-1 = a_1 a_2 a_3 \cdots a_r \equiv -1 \pmod 4$ だから、
$a_1, a_2, \cdots, a_r$ の中で、$a_i \equiv -1 \pmod 4$ となるような a_i は奇数個ある。―③
①〜③より、$\langle a_1 a_2 a_3 \cdots a_r, p\rangle = \langle 4k-1, p\rangle$ は 2 の倍数ではない。(∵ 3.7)
フェルマーの小定理より、$(4k-1)^{p-1} - 1 = \{(4k-1)^{\frac{p-1}{2}} - 1\}\{(4k-1)^{\frac{p-1}{2}} + 1\} \equiv 0 \pmod p$ だから、$(4k-1)^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$
$\langle 4k-1, p\rangle$ は奇数だから、$(4k-1)^{\frac{p-1}{2}} \not\equiv 1 \pmod p$ より、$(4k-1)^{\frac{p-1}{2}} \equiv -1 \equiv (-1)^{\frac{p-1}{2}} \pmod p$ (∵3.2.2)
よって、$(p-1)^{\frac{p-1}{2}} \equiv (4k-1)^{\frac{p-1}{2}} \pmod p$
(i)・(ii)より、$(p-1)^{\frac{p-1}{2}} \equiv (4k-1)^{\frac{p-1}{2}} \pmod p$
$(4k-1)^{\frac{p-1}{2}}$ と p は互いに素だから、両辺を $(4k-1)^{\frac{p-1}{2}}$ で割って、$\left(\frac{p-1}{4k-1}\right)^{\frac{p-1}{2}} \equiv 1 \pmod p$
したがって、$\langle \frac{p-1}{4k-1}, p\rangle$ は 2 の倍数。(∵3.2.2) ■

3.11 $\langle \frac{p-1}{2^r}, p\rangle$ は 2^{m+1} の倍数

(r は 2 以上の自然数、k は奇数、m は $r = 2^m \cdot k$ を満たす非負整数、p は $p \equiv 1 \pmod{2^r}$ を満たす奇素数)

〈例〉$r=2$ のとき、$m=1$、$\langle \frac{p-1}{4}, p\rangle$ は $2^2=4$ の倍数　$\langle 3,13\rangle=4, \langle 4,17\rangle=4, \langle 7,29\rangle=4, \langle 9,37\rangle=4, \langle 10,41\rangle=8$
$r=3$ のとき、$m=0$、$\langle \frac{p-1}{8}, p\rangle$ は $2^1=2$ の倍数　$\langle 2,17\rangle=2, \langle 5,41\rangle=2, \langle 9,73\rangle=12, \langle 11,89\rangle=4, \langle 12,97\rangle=6$
$r=4$ のとき、$m=2$、$\langle \frac{p-1}{16}, p\rangle$ は $2^3=8$ の倍数　$\langle 6,97\rangle=8, \langle 7,113\rangle=8, \langle 12,193\rangle=8, \langle 15,241\rangle=80, \langle 16,257\rangle=64$
$r=5$ のとき、$m=0$、$\langle \frac{p-1}{32}, p\rangle$ は $2^1=2$ の倍数　$\langle 3,97\rangle=2, \langle 6,193\rangle=2, \langle 8,257\rangle=16, \langle 11,353\rangle=4, \langle 14,449\rangle=2$
$r=6$ のとき、$m=1$、$\langle \frac{p-1}{64}, p\rangle$ は $2^2=4$ の倍数　$\langle 3,193\rangle=12, \langle 4,257\rangle=32, \langle 7,449\rangle=4, \langle 9,577\rangle=24, \langle 10,641\rangle=20$
$r=7$ のとき、$m=0$、$\langle \frac{p-1}{128}, p\rangle$ は $2^1=2$ の倍数　$\langle 2,257\rangle=16, \langle 5,641\rangle=10, \langle 6,769\rangle=2, \langle 9,1153\rangle=4, \langle 11,1409\rangle=2$
$r=8$ のとき、$m=3$、$\langle \frac{p-1}{256}, p\rangle$ は $2^4=16$ の倍数　$\langle 3,769\rangle=16, \langle 13,3329\rangle=16, \langle 30,7681\rangle=16, \langle 31,7937\rangle=16$
$r=10$ のとき、$m=1$、$\langle \frac{p-1}{1024}, p\rangle$ は $2^2=4$ の倍数
$\langle 12,12289\rangle=4, \langle 13,13313\rangle=4, \langle 15,15361\rangle=40, \langle 18,18433\rangle=16, \langle 19,19457\rangle=8$
$r=12$ のとき、$m=2$、$\langle \frac{p-1}{4096}, p\rangle$ は $2^3=8$ の倍数
$\langle 3,12289\rangle=24, \langle 10,40961\rangle=16, \langle 15,61441\rangle=48, \langle 16,65537\rangle=8192, \langle 21,86017\rangle=24$
$r=16$ のとき、$m=4$、$\langle \frac{p-1}{65536}, p\rangle$ は $2^5=32$ の倍数
$\langle 12,786433\rangle=32, \langle 18,1179649\rangle=64, \langle 21,1376257\rangle=2048, \langle 27,1769473\rangle=96$
ここでは、$r=2$ の場合と $r \geqq 3$ の場合に分けて証明する。

3.11.1 $\langle \frac{p-1}{4}, p\rangle$ は 4 の倍数　(p は $p \equiv 1 \pmod 4$ を満たす奇素数)

(証明) mod p で考える。
(i) $p \equiv 1 \pmod 8$ のとき、平方剰余の第2補充法則より、
2 は p の平方剰余であるから、$2^{\frac{p-1}{2}} \equiv 1 \equiv (-1)^{\frac{p-1}{4}}$ (∵ 3.10.1, 3.2.1)
$2^{\frac{p-1}{2}} = 4^{\frac{p-1}{4}}$ より、$(p-1)^{\frac{p-1}{4}} \equiv 4^{\frac{p-1}{4}}$

(ii) $p \equiv 5 \pmod 8$ のとき、平方剰余の第2補充法則より、
2はpの平方非剰余であるから、$2^{\frac{p-1}{2}} \not\equiv 1$ （∵ 3.10.1, 3.2.2）
また、フェルマーの小定理より、$2^{p-1}-1=(2^{\frac{p-1}{2}}-1)(2^{\frac{p-1}{2}}+1) \equiv 0$ だから、
$2^{\frac{p-1}{2}} \equiv -1 \equiv (-1)^{\frac{p-1}{4}}$
$2^{\frac{p-1}{2}} = 4^{\frac{p-1}{4}}$ より、$(p-1)^{\frac{p-1}{4}} \equiv 4^{\frac{p-1}{4}}$
(i)・(ii)より、$(p-1)^{\frac{p-1}{4}} \equiv 4^{\frac{p-1}{4}}$
$4^{\frac{p-1}{4}}$ とpは互いに素だから、両辺を $4^{\frac{p-1}{4}}$ で割って、$\left(\frac{p-1}{4}\right)^{\frac{p-1}{4}} \equiv 1$
したがって、$\langle \frac{p-1}{4}, p \rangle$ は4の倍数。（∵ 3.2.2）■

3.11.2 $\langle \frac{p-1}{2^r}, p \rangle$ は 2^{m+1} の倍数

（rは3以上の自然数、kは奇数、mは $r=2^m \cdot k$ を満たす非負整数、pは $p \equiv 1 \pmod{2^r}$ を満たす奇素数）

（証明）
$r \geqq 3$ より、$r \geqq m+2$ が成り立つから、2^{m+2} は 2^r の約数である。
$p \equiv 1 \pmod{2^r}$ で、2^{m+2} は 2^r の約数だから、$p \equiv 1 \pmod{2^{m+2}}$
よって、$(-1)^{\frac{p-1}{2^{m+1}}} = 1$ —①
また、$r \geqq 3$ より、$2^3=8$ は 2^r の約数である。
$p \equiv 1 \pmod{2^r}$ で、8は 2^r の約数だから、$p \equiv 1 \pmod 8$
よって、平方剰余の第2補充法則より、
2はpの平方剰余であるから、$2^{\frac{p-1}{2}} \equiv 1 \pmod p$ —② （∵ 3.10.1, 3.2.1）
また、$(2^r)^{\frac{p-1}{2^{m+1}}} = 2^{2^m \cdot k \cdot \frac{p-1}{2^{m+1}}} = 2^{\frac{k(p-1)}{2}}$ —③
②・③より、$(2^r)^{\frac{p-1}{2^{m+1}}} \equiv 1 \pmod p$ —④
①・④より、$(2^r)^{\frac{p-1}{2^{m+1}}} \equiv (-1)^{\frac{p-1}{2^{m+1}}} \pmod p$
よって、$(p-1)^{\frac{p-1}{2^{m+1}}} \equiv (2^r)^{\frac{p-1}{2^{m+1}}} \pmod p$
$(2^r)^{\frac{p-1}{2^{m+1}}}$ とpは互いに素だから、両辺を $(2^r)^{\frac{p-1}{2^{m+1}}}$ で割って、$\left(\frac{p-1}{2^r}\right)^{\frac{p-1}{2^{m+1}}} \equiv 1 \pmod p$
したがって、$\langle \frac{p-1}{2^r}, p \rangle$ は 2^{m+1} の倍数。（∵ 3.2.2）■

4 感想

証明を考えるのが一番楽しくて、文章にするのと10枚に収めるのが大変だった。
自分で予想を立て証明を考えることで、より本の内容を深く理解できたと思う。
今後は、n進法で $\frac{1}{p}$ の循環節に現れる数字について考えたい。

5 参考文献

・西来路 文朗　清水 健一、『素数はめぐる 循環小数で語る数論の世界』、講談社、2017年
・平方剰余の相互法則の意味と応用 | 高校数学の美しい物語
https://manabitimes.jp/math/1017　2021/08/26 閲覧