

Fermat 商
TRU 2026 8 月 28 日

飯高 茂

2026 年 8 月 8 日

Fermat 商 の定義から始めます.

素数 p と、 p と互いに素な整数 a に対して、

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ。

これが Fermat の小定理ですがこれを用いて Fermat 商は次のように定義されます.

$$Q_p(a) = \frac{a^{p-1} - 1}{p}$$

a を底, $Q_p(a)$ を法 p とする Fermat 商 と言います.

Fermat 商は対数関数と類似の性質を持っています.

$a^{p-1} - 1 = pQ_p(a)$ になるので $a^{p-1} - 1 \equiv pQ_p(a) \pmod{p^2}$ とおくと

$b^{p-1} - 1 \equiv pQ_p(b) \pmod{p^2}$, $(ab)^{p-1} - 1 \equiv pQ_p(ab) \pmod{p^2}$.

これより次の式ができます.

$$Q_p(a) + Q_p(b) \equiv Q_p(ab) \pmod{p}$$

$Q_p(a)$ を法 p として見るとき 対数関数と同じように 積を和に変換します.

$Q_p(a) = 1$ のとき a は対数関数の底と同様の性質を持っています.

Fermat 商 の性質を調べていろいろな例で調べたところ Fermat 商での 底が $p-1$ 個あるに違いないと思いました.

私は退職後 新宿の朝日カルチャーセンターで大学の数学を講義してきました.

素数の定理で Fermat の小定理を紹介しますがその応用として Fermat 商 を取り上げましたがこれは手触り感のある結果として Fermat 商 を扱うことにしました

Fermat 商 は一種の対数ですが底が複数個ある, 複合対数とでもいうべきものだと思います.

$p=5$ で試して下さい. Fermat 商 で遊ぶことができます.

表 1: $p = 5$ の fermat 商

a	$Q_p(a)$
1	0
2	3
3	1
4	1
6	4
7	0
8	4
9	2
11	3
12	2
13	2
14	3
16	2
17	4
18	0
19	4
21	1
22	1
23	3
24	0

最初は定義から. 以下 $p = 5$.

$Q_p(a) = (a^4 - 1)/5$ により以後は主に対数法則を使う.

$$Q_p(2) = (2^4 - 1)/5 = 3 \pmod{5}.$$

$$Q_p(4) = Q_p(2^2) = Q_p(2) + Q_p(2) = 3 + 3 = 6 \equiv 1 \pmod{5}.$$

$$Q_p(8) = Q_p(2 * 4) = Q_p(2) + Q_p(4) = 3 + 1 = 4$$

$$Q_p(16) = Q_p(2 * 8) = Q_p(2) + Q_p(8) = 3 + 4 = 7 \equiv 2 \pmod{5}.$$

$$Q_p(32) = Q_p(2 * 16) = Q_p(2) + Q_p(16) = 3 + 3 = 5 \equiv 0 \pmod{5}, Q_p(32) = Q_p(25 + 7) = Q_p(7).$$

$$Q_p(64) = Q_p(2 * 32) = Q_p(2) + Q_p(32) = 3 + 5 = 8 \equiv 3 \pmod{5}, Q_p(64) = Q_p(50 + 14) = Q_p(14).$$

$$Q_p(128) = Q_p(2 * 64) = Q_p(2) + Q_p(64) = 3 + 3 = 6 \equiv 1 \pmod{5},$$

$$Q_p(128) = Q_p(125 + 3) = Q_p(3).$$

$$Q_p(3) = 1 \text{ により } Q_p(3^2) = Q_p(9) = 2.$$

$$Q_p(27) = 2 + 1 = 3, Q_p(27) = Q_p(2).$$

$$Q_p(81) = 3 + 1 = 4, Q_p(81) = Q_p(75 + 6) = Q_p(6) = 4.$$

$$Q_p(243) = 4 + 1 = 5, Q_p(243) = Q_p(43) = Q_p(18).$$

1 指数関数と対数関数

$c = a^b$ のとき $\log_a c = b$ とおきこれを a を底とする 対数関数という.

$\log_a c = 1$ のとき定義によれば $c = a$.

$\log_a c = 1$ のとき $c = a$ でこれが底となる.

Fermat 商は対数の性質を持っているので $Q_p(a) = 1$ のときの a が底である.

$p = 5$ の Fermat 商の表を見ると, $a = 3, 4, 21, 22$ が $Q_p(a) = 1$ となる.

この のとき Fermat 商の底 b は 4 個あります.

表 2: 底 $b = 3$ のとき Fermat 商

e	$b^e \bmod p^2$	$Q(b^e)$
1	3	1
2	9	2
3	2	3
4	6	4

表 3: 底 $b = 4$ のとき Fermat 商

e	$b^e \bmod p^2$	$Q(b^e)$
1	4	1
2	16	2
3	14	3
4	6	4

表 4: 底 $b = 21$ のときの Fermat 商

e	$b^e \bmod p^2$	$Q(b^e)$
1	21	1
2	16	2
3	11	3
4	6	4

2 底の探求

一般には p のときの 底 は次の式の解です

表 5: 底 $b = 22$ があるとき Fermat 商

e	$b^e \bmod p^2$	$Q(b^e)$
1	22	1
2	9	2
3	23	3
4	6	4

$$b^{p-1} - 1 - p \equiv 0 \pmod{p^2}$$

数値実験によると、 p のときの 底 の個数は $p - 1$ あるようです。

底の定義式は $p - 1$ 次の式ですから 解が $p - 1$ 個あるのは納得できます。

3 対数関数としての姿

すこしかんばれば証明できるに違いないと思いましたが時間がないので 助けを AI (gemini 3.0) に求めました。

gemini 様は直ちに助けて下さいました。

Fermat 商は $p - 1$ 個ある底 b によって 指数関数の逆としての 対数関数としての姿を現したのです。

4 AI 様のご教示

素数 p に対して、法 p^2 における方程式 $X^{p-1} - 1 - p \equiv 0 \pmod{p^2}$ が $p - 1$ 個の解を持つことの証明ですね。

この証明には、ヘンゼルの補題 (Hensel's Lemma) の考え方をを用いるのが最も効率的で明快です。

以下のステップで進めていきましょう。

1. 法 p における解の検討

まず、与えられた方程式を法 p で考えます。

$$f(X) = X^{p-1} - 1 - p$$

とおくと、法 p においては以下ようになります。

$$f(X) \equiv X^{p-1} - 1 \pmod{p}$$

フェルマーの小定理により、 p と互いに素な任意の整数 X に対して $X^{p-1} \equiv 1 \pmod{p}$ が成り立ちます。したがって、法 p における解は次のように定まります。

$$X \equiv 1, 2, \dots, p-1 \pmod{p}$$

これらはすべて p と互いに素であり、解の個数は $p-1$ 個 です。

2. 法 p^2 への持ち上げ (Lifting)

次に、法 p での各解 $x_0 \in \{1, 2, \dots, p-1\}$ が、法 p^2 においてどのように振る舞うかを調べます。

法 p^2 における解を $X = x_0 + kp$ (ただし $0 \leq k < p$) とおき、これを $f(X) \equiv 0 \pmod{p^2}$ に代入します。テーラー展開 (または二項展開) を用いると、以下のようになります。

$$f(x_0 + kp) \equiv f(x_0) + f'(x_0) \cdot kp \pmod{p^2}$$

ここで、 $f'(X)$ を計算すると：

$$f'(X) = (p-1)X^{p-2}$$

となります。

3. k の一意性の証明

$f(x_0 + kp) \equiv 0 \pmod{p^2}$ となるための条件は以下の通りです。

$$f(x_0) + (p-1)x_0^{p-2} \cdot kp \equiv 0 \pmod{p^2}$$

ステップ 1 より $f(x_0) \equiv 0 \pmod{p}$ なので、ある整数 m を用いて $f(x_0) = mp$ と書けます。これを代入して全体を p で割ると：

$$m + (p-1)x_0^{p-2} \cdot k \equiv 0 \pmod{p}$$

これを k について整理します。法 p において $p-1 \equiv -1$ ですから、

$$-x_0^{p-2} \cdot k \equiv -m \pmod{p}$$

$$x_0^{p-2} \cdot k \equiv m \pmod{p}$$

ここで、 x_0 は p と互いに素 ($1 \leq x_0 \leq p-1$) なので、そのべき乗である x_0^{p-2} もまた p と互いに素です。したがって、法 p において x_0^{p-2} の逆元が必ず存在します。これにより、任意の x_0 に対して、 k は法 p でただ一つに定まります。

$$a^{p-1} = 1 \equiv Q_p(a) \pmod{p^2}$$

において、 $Q_p(a) \equiv 0 \pmod{p^2}$ を満たす a は $p-1$ 個。

底 b は $p-1$ 個あり、 $a \equiv b^e \pmod{p^2}$ で得られる $a \pmod{p^2}$ は $p-1$ 個。そこで底も数えると $(p-1)^2 = p^2 - 2p + 1$ 。

$Q_p(a) \equiv 0 \pmod{p^2}$ を満たす a は $p-1$ 個を加えると $(p-1)^2 + p - 1 = p^2 - p = p(p-1) = \varphi(p^2)$ 。

4. 結論

法 p における解 x_0 は $\{1, 2, \dots, p-1\}$ の $p-1$ 個 存在する。それぞれの x_0 に対して、法 p^2 における解 $X = x_0 + kp$ を与える $k \in \{0, 1, \dots, p-1\}$ がただ一つ 存在する。

以上のことから、方程式 $X^{p-1} - 1 - p \equiv 0 \pmod{p^2}$ の解は、整数として $p-1$ 個 存在することが証明されました。

補足：この証明は、一般の $X^{p-1} \equiv a \pmod{p^2}$ (ただし $a \equiv 1 \pmod{p}$) の形の解の構造を示しています。今回のケースは $a = 1 + p$ の特別な場合ですね。

5 Eisenstein の結果

Dikson の数論 I の 105 ページの Eisenstein (Berlin Berichte, 1850) に対数関数の性質を見いだしかつ $r < p$ について

$$Q_p(a + rp) \equiv Q_p(a) - r/a \pmod{p}$$

も書かれています。

Proof

$$(a + rp)^{p-1} \equiv a^{p-1} + a^{p-2}rp \pmod{p^2}$$

$$a^{p-1} - 1 = pQ_p(a) \text{ に } a \text{ の代りに } a+rp \text{ を入れると, } (a+rp)^{p-1} \equiv 1 + Q_p(a+rp)p \pmod{p^2}.$$

$$1 + Q_p(a + rp)p = (a + rp)^{p-1} \equiv a^{p-1} + a^{p-2}rp(p-1) \equiv a^{p-1}a^{p-2}rp \pmod{p^2}.$$

$$a^{p-1} \equiv 1 + pQ_p(a) \pmod{p^2} \text{ によれば}$$

$$Q_p(a + rp) = (a + rp)^{p-1} \equiv a^{p-1} + a^{p-2}rp(p-1) \pmod{p^2}.$$

$$Q_p(a + rp)p = Q_p(a)p + a^{p-2}rp(p-1) \pmod{p^2}.$$

$$Q_p(a + rp) = Q_p(a) - a^{p-2}r \pmod{p}.$$

$$\text{Fermat の小定理 により } a * a^{p-2} \equiv 1 \pmod{p}$$

$$Q_p(a + rp) = Q_p(a) - r/a \pmod{p}.$$

宇都宮潔さんに注意を受け証明を修正しました (2026/6/9). 感謝

q.e.d.

$Q_7(a) = 1$ になる a は底です. 順に探してみます.

表 6: $p = 7$, フェルマ商の表

a	$Q_7(a)$	a	$Q_7(a)$	a	$Q_7(a)$
1	0	8	6	15	5
2	2	9	5	16	1*
3	6	10	1*	17	3
4	4	11	2	18	0
5	6	12	3	19	0
6	1*	13	2	20	3
a	$Q_7(a)$	a	$Q_7(a)$	a	$Q_7(a)$
22	4	29	3	36	2
23	4	30	0	37	3
24	5	31	0	38	2
25	5	32	3	39	1
26	4	33	1	40	5
27	4	34	5	41	6
a	$Q_7(a)$	a	$Q_7(a)$	a	$Q_7(a)$
43	1				
44	6				
45	4				
46	6				
47	2				
48	0				

表 7: $p = 17$, フェルマ商の表

a	$Q_{17}(a)$	a	$Q_{17}(a)$
1	0	34	—
2	13	35	15
3	10	36	12
4	9	37	15
5	12	38	0
6	6	39	15
7	3	40	0
8	5	41	10
9	3	42	9
10	8	43	16
11	9	44	1
12	2	45	15
13	5	46	16
14	16	47	14
15	5	48	11
16	1	49	6
17	—	50	3
18	16	51	—
19	4	52	14
20	4	53	3
21	13	54	9
22	5	55	4
23	3	56	8
24	15	57	14
25	7	58	5
26	1	59	11
27	13	60	14
28	12	61	6
29	9	62	1
30	1	63	6
31	5	64	10
32	14	65	0
33	2	66	15