ウィルソンの定理の初等的証明

Wikipedia によると一般に「ウィルソンの定理」と呼ばれるこの性質は、ウィルソンではなく、ラグランジュが最初に証明を与えた。したがって本来はウィルソン予想（ラグランジュの定理）と呼ぶべきであろうが、ここでは通称に従うこととする。

なお、やはり Wikipedia にあるように、既に十世紀の数学者イブン・アル・ハイサムがこの性質を発見していたとすれば、予想についても「ハイサム予想」とするべきなのであろうか。

（ウィルソンの定理）

素数 p について $(p-1)! \equiv -1 \pmod{p}$

注 1）$n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$ （念のため。）

注 2）$a \equiv b \pmod{p}$ とは $a - b$ が p の倍数であることを示す表現である。

したがって $(p-1)! \equiv -1 \pmod{p}$ は $(p-1)! + 1$ が p の倍数であることに他ならない。これはまたある整数 q が存在して $(p-1)! + 1 = pq$ すなわち $(p-1)! = pq - 1$ となることでもある。

具体例の考察

以下ではアルファベットの右下に小さな番号を付けた記号(a_1, q_2 など)が頻繁に現れる。高校生が数学 B の一分野「数列」で習う内容であり、この表現にはそれなりに深い意味がある。しかしここでは単純に、ある数を表すのに用いられていると考えれば十分である。この表現の一つの長所は数が何個あっても扱いに困らないことである。例えば 100 個の数を表現するために a, b, c, $\cdots$ などとすると、次をどの文字にするかはちょっとした悩みにもなる。ところがこれを a_1, a_2, a_3, $\cdots$, a_{100} と表すと、実にスマートな表現であって何番目に何があるのかもわかりやすい。x の 100 次式も

$$a_{100}x^{100} + a_{99}x^{99} + a_{98}x^{98} + \cdots + a_1 x + a_0$$

とすれば x^k の係数は a_k で、構造が直感的になっている。

$p = 2$ ならば $(p-1)! = 1$ であり $1 \equiv -1 \pmod{2}$ より $(p-1)! \equiv -1 \pmod{p}$ である。また $p = 3$ ならば $(p-1)! = 2$ かつ $2 \equiv -1 \pmod{3}$ より、$p = 5$ ならば $(p-1)! = 24$ かつ $24 \equiv -1 \pmod{5}$ より、さらに $p = 7$ ならば $(p-1)! = 720$ かつ $720 \equiv -1 \pmod{7}$ より、それぞれの p について $(p-1)! \equiv -1 \pmod{p}$ である。

次に $p = 11$ の場合を例に挙げて証明の指針を確認する。

$p = 11$ のとき $(p-1)! = 10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$ であるがこの右辺の積を

$$1 \times 10,\ 2 \times 6,\ 3 \times 4,\ 5 \times 9,\ 7 \times 8$$

の 5 組に分けて考える。すると最初の積のみ $11q_1 - 1$ であり、それ以外は $11q_2 + 1$, $11q_3 + 1$, $11q_4 + 1$, $11q_5 + 1$ の形になる。この 5 つを掛け合わせて

$$(11q_1-1)(11q_2+1)(11q_3+1)(11q_4+1)(11q_5+1)=11Q-1$$

となることは容易にわかるであろう。実は 5 以上のすべての素数 p について同様のことが出来てそれが証明の核であるのだが、問題となるのは $2, 3, 4, \cdots, p-3, p-2$ の $p-3$（偶数）個が、それぞれの 2 数の積が $pq+1$ となるような $\frac{1}{2}(p-3)$ 組に綺麗に分かれるのかという部分である。

$$2\cdot3\cdot4\cdot\cdots\cdot10\cdot11=(2\cdot7)(3\cdot9)(4\cdot10)(5\cdot8)(6\cdot11)$$

$$2\cdot3\cdot4\cdot\cdots\cdot14\cdot15=(2\cdot9)(3\cdot6)(4\cdot13)(5\cdot7)(8\cdot15)(10\cdot12)(11\cdot14)$$

であり、$p=13, 17$ についてもうまく分けられることがわかる。しかしこのような具体例はいくつ並べても、すべての素数 p について同様の組分けが可能という論証にはならない。

証明で使われる性質の確認

とはいえ、具体的なものの考察は問題の仕組みと本質をつかむために重要である。ここでは $p=11$ の場合を例として、証明で用いられる性質(のほとんど)を確かめておく。

(A – 2 数の積の表)

	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	12	14	16	18	20	22
3	3	6	9	12	15	18	21	24	27	30	33
4	4	8	12	16	20	24	28	32	36	40	44
5	5	10	15	20	25	30	35	40	45	50	55
6	6	12	18	24	30	36	42	48	54	60	66
7	7	14	21	28	35	42	49	56	63	70	77
8	8	16	24	32	40	48	56	64	72	80	88
9	9	18	27	36	45	54	63	72	81	90	99
10	10	20	30	40	50	60	70	80	90	100	110
11	11	22	33	44	55	66	77	88	99	110	121

(B – 2 数の積を 11 で割った余りの表)

	1	2	3	4	5	6	7	8	9	10	11
1	①	2	3	4	5	6	7	8	9	10	0
2	2	4	6	8	10	①	3	5	7	9	0
3	3	6	9	①	4	7	10	2	5	8	0
4	4	8	①	5	8	2	6	10	3	7	0
5	5	10	4	9	3	8	2	7	①	6	0
6	6	①	7	2	8	3	9	4	10	5	0
7	7	3	10	6	2	9	5	①	8	4	0
8	8	5	2	10	7	4	①	9	6	3	0
9	9	7	5	3	①	10	8	6	4	2	0
10	10	9	8	7	6	5	4	3	2	①	0
11	0	0	0	0	0	0	0	0	0	0	0

表 A は 1 から 11 までの 2 数の積を表にしたものである。問題なのは 11 で割った余りであり、その積について 11 で割った余りを記したのが表 B である。なお余り 1 については強調するために丸で囲んで①としてある。

まず表 B について以下のことが成り立っている。

(a) 一番下の行(横の並び)と一番右の列(縦の並び)以外についてはどの行もどの列も、余りとして 0 から 10 までの数がそれぞれ 1 回ずつ現れる。特に①が 2 回現れる行も列もない。

さて、考えるべきは 2 から 9 までの組合せであった。表 B からその部分を抜き出したものが右の表 C である。表 B の余りの並びについて 2 行目から 9 行目のいずれもが、一番左(×1 の余り)は①でなく、また右の 2 つ(×10, ×11 の余り)も①ではなかったため、やはり表 C において以下が成り立つことになる。

(b) 表 C の余りの並びについて、どの行においても①はちょうど 1 回現れる。(列についても同様のことが起こっている。)

(C – 表 B の一部)

	2	3	4	5	6	7	8	9
2	4	6	8	10	①	3	5	7
3	6	9	①	4	7	10	2	5
4	8	①	5	8	2	6	10	3
5	10	4	9	3	8	2	7	①
6	①	7	2	8	3	9	4	10
7	3	10	6	2	9	5	①	8
8	5	2	10	7	4	①	9	6
9	7	5	3	①	10	8	6	4

さらに、やはり説明は抜きに事実だけを述べておくが、表 C での余りのつくる正方形において左上から右下への対角線を考えると

(c) この対角線上に①は現れない。

すなわち(b)(c)より 2 から 9 のそれぞれについて、積が 11 で割って余り 1 となるような 2 以上 9 以下の自分自身でない数がただ一つ決まることがわかる。実際この場合は表 C の上の行から順にみて $2 \leftrightarrow 6$, $3 \leftrightarrow 4$, $5 \leftrightarrow 9$, $7 \leftrightarrow 8$ がその対応で、8 個の数は条件に合う 4 組に確かに分かれることになる。

ここでは $p = 11$ の場合を考えたが、実はより大きな素数 p についても表 C をつくると同様に(b)(c)が起こる。(疑わしいと思う人には $p = 13, 17$ などについて確認してみることをお勧めする。) 必ずそうなることが論理的に示されれば、定理の証明はほぼ終わりである。

証明の核となる性質の証明

(補助定理)

p は 5 以上の素数で、a は整数かつ $2 \leqq a \leqq p-2$ とする。このとき以下の(i)～(iv)が成り立つ。

(i) $a \times 1$, $a \times 2$, $a \times 3$, $\cdots$, $a \times p$ のそれぞれを p で割った余りはすべて異なる。

(ii) $a \times 1$, $a \times 2$, $a \times 3$, $\cdots$, $a \times p$ の p 個の積の中に p で割った余りが 1 であるものがただ 1 つ存在する。

(iii) $a \times 1$, $a \times (p-1)$, $a \times p$ はいずれも p で割って 1 余る数でない。

(iv) $a \times a$ を p で割った余りは 1 でない。

(証明)

(i) 2 数 m, n を p で割った余りが等しいことと $m-n$ が p の倍数であることは同じ条件である(2 つの条件は同値)。すなわち異なる 2 組の積の差が p の倍数でないことをいえばよい。いま整数 b, c について $1 \leqq b < c \leqq p$ とすると $1 \leqq c-b \leqq p-1$ であり、p が素数であることから $\dfrac{a(c-b)}{p}$ は p が約分されず整数でない。よって条件を満たすすべての b, c について $ac-ab$ は p の倍数でなく、(i)が示された。

(ii) 整数を p で割った余りとして現れる数は $0, 1, 2, \cdots, p-1$ の p 通りである。これと(i)から(ii)が成り立つ。(いわゆる鳩の巣原理からの帰結。)

(iii) $a \times 1 = p \cdot 0 + a$, $a \times (p-1) = p(a-1) + (p-a)$ で、それぞれを p で割った余りは a, $p-a$ であり 1 ではない(どちらも $2 \leqq a \leqq p-2$ より)。また $a \times p$ は p の倍数で p で割り切れる。

(iv) a^2 を p で割った余りが 1 とは a^2-1 が p の倍数であることで、さらに $\dfrac{a^2-1}{p}$ が整数であることに他ならない。よって $\dfrac{a^2-1}{p}$ が整数でないことをいえばよい。いま $2 \leqq a \leqq p-2$ より $1 \leqq a-1 \leqq p-3$, $3 \leqq a+1 \leqq p-1$ であって $\dfrac{a^2-1}{p} = \dfrac{(a+1)(a-1)}{p}$ は素数 p が約分されず、整数でない。よって題意は示された。

ウィルソンの定理の証明

準備が整ったので、ウィルソンの定理を証明する。$p=2\,,3\,,5\,,7$ については具体的に計算して確認できるので、以下では $p\geqq 11$ とする。

$$(p-1)!=1\cdot(p-1)\{2\cdot 3\cdot 4\cdot\cdots\cdot(p-3)\cdot(p-2)\}$$

であり、上式右辺の { } の中にある $p-3$(偶数)個の数の積が p で割ると 1 余る数であることを示せばよい。

集合 $A_0=\{2\,,\ 3\,,\ 4\,,\ \cdots\,,\ p-3\,,\ p-2\}$ とする。補助定理(ii)(iii)(iv)より A_0 の要素で $2\times b$ を p で割った余りが 1 であるような 2 と異なる整数 b が存在する。この b を b_0 として、次に集合 A_0 から 2 数 $2\,,b_0$ を除いた集合 A_1 を考える。A_1 は $p-5$ 個の要素からなるが、そのうちの最小の数を a_1 とおく。($\to A_1=\{\not{2}\,,\ a_1,\cdots,\not{b_0}\,,\cdots,\ p-2\}$（$\not{x}$ は x を除くの意味。）) すると補助定理(ii)より $2\times a_1$ も $a_1\times b_0$ も p で割って 1 余る数ではなく($2\times b_0$ を p で割った余りが 1 であって、仮に $2\times a_1$ または $a_1\times b_0$ が p で割って 1 余る数とすると、どちらの場合も補助定理(ii)に反することになる。)、さらに(ii)(iii)(iv)から a_1 と異なる A_1 のある要素 b_1 が存在して $a_1\times b_1$ は p で割ると 1 余る数になる。

以下同様で A_0 から $2\,,b_0\,,a_1\,,b_1$ の 4 数を除いた集合を A_2 とすると $a_2\times b_2$ が p で割って 1 余る数であるような A_2 の異なる要素 $a_2\,,b_2$ が存在する。この操作は $A_0\to A_1\to A_2\to\cdots$ として順に得られる集合の要素の個数が 0 になるまで続けられるので、$2\,,3\,,\cdots\,,p-2$ の $p-3$ 個の数は、それぞれの 2 数の積がすべて p で割ると 1 余る数となるような $\dfrac{1}{2}(p-3)$ 組

$$(2\,,b_0)\,,(a_1\,,b_1)\,,\cdots\,,(a_{\frac{1}{2}(p-5)}\,,b_{\frac{1}{2}(p-5)})$$

に重複なく分けられることがわかる。よって

$$2\cdot 3\cdot\cdots\cdot(p-2)=(2\times b_0)(a_1\times b_1)\cdots(a_{\frac{1}{2}(p-5)}\times b_{\frac{1}{2}(p-5)})$$

であり $2\cdot 3\cdot\cdots\cdot(p-2)$ は p で割ると 1 余る数である。これを $pq+1$ として

$$(p-1)!=1\cdot(pq+1)\cdot(p-1)=p(pq+1-q)-1,\ (p-1)!-(-1)=p(pq+1-q)$$

$$\therefore\ (p-1)!\equiv -1\ (\mathrm{mod}\,p)$$

□◿

(補足)

本来、A_1 以降の集合の定め方については A_k から $a_k\times b_k$ の p で割った余りが 1 であるような異なる 2 数 $a_k\,,b_k$ を除いた集合を A_{k+1} として(空集合になるまで)$A_1\,,A_2\,,A_3\,,\cdots$ を考える、とすべきであろう。しかしこの帰納的定義は「数列」についての知識で中学生向けではないので、上のような(やや曖昧な)表現にした。なお上の証明から以下の成立も容易にわかる。

（ウィルソンの定理の系）素数 p について $(p-2)!\equiv 1\ (\mathrm{mod}\,p)$

2009.12/8（最終更新日 2009.12/13）