$a^n(mod\,q)$ の循環周期について

石原　諭

参考文献[1]では 2^n の末尾の循環周期について,以下の性質について触れられている.完全な証明は載っていなかったため,証明した.

【定理1】
2^n （ $n=1,2,3,\cdots$ ）の下 k 桁は循環する.それは次の性質をもつ.
(性質1) 2^n の下 k 桁は 2^k から循環し,循環周期は $4\cdot5^{k-1}$ である.
(性質2)循環部分の最小値は 2^k であり,循環部分は 2^k の整数倍である.
(性質3)下 $k-1$ 桁が 2^k の倍数でないときの 10^{k-1} の位は $1,3,5,7,9$ の 5 通りであり,
下 $k-1$ 桁が 2^k の倍数であるときの 10^{k-1} の位は $0,2,4,6,8$ の 5 通りである.

(証明)(性質1)について
次のことを証明すればよい.
$2^{l+M}\equiv2^l\ \ (mod\,10^k)$ が成り立つと仮定する.ただし $M\geq1$, $l,k\geq1$
(1) $M=4\cdot5^{k-1}$ である.
(2)このような l の中で最小のものは $l=k$ である.

(1)(2)より, 2^n は 2^k から循環が始まり,循環周期は $M=4\cdot5^{k-1}$ であることがわかる.
(証明)仮定より, $2^{l+M}-2^l=10^k\times N$ (N は整数)とおける.変形して
$2^l(2^M-1)=10^k\times N$ ・・・①
ここで, l は $l\geq k$ でなければならない.
なぜなら $l=1,2,3,\cdots,k-1$ であるとすると,両辺を 2^l で割り $2^M-1=5^l\cdot10^{k-l}\times N$ となるが,
このとき左辺は奇数であり,右辺は偶数であるので矛盾であるからである.
①において両辺を 2^k で割ると $2^{l-k}(2^M-1)=5^k\times N$
2^{l-k} は 5^k の倍数ではないから 2^M-1 は 5^k で割り切れる.
ここで 2^M の1の位に着目すると,2, 4, 8, 6, 2, 4, ・・・と「2, 4, 8, 6」が循環する.
よって 2^M-1 が 5^k で割り切れるためには $M=4m$ （ m は整数)でなければならない.

次に示すべきことはこの m が $m=5^{k-1}$ であるということである.
$m\geq1$ であるとする.
$2^{l+4m}\equiv2^l\ \ (mod\,10^k)$ が成り立つと仮定すると $m=5^{k-1}q$ と表されることを数学的帰納法により証明する.
$k=1$ のとき,仮定は $2^{l+4m}\equiv2^l\ \ (mod\,10)$ である.したがって $2^{l+4m}-2^l=10\times N$ すなわち
$2^l(2^{4m}-1)=10\times N$ である.
両辺を 2 で割って $2^{l-1}(2^{4m}-1)=5\times N$
よって $2^{4m}-1$ は 5 で割り切れる.
$2^{4m}-1=(4^m)^2-1=(4^m+1)(4^m-1)$
ここでここで 4^m の1の位に着目すると,4, 6, 4, 6, ・・・と 4, 6 が循環する.
したがって m は何でもよい.よって $m=5^{1-1}\times m$ と表されるので成り立つ.
k のとき成り立つと仮定して, $k+1$ のとき成り立つことを示す.
$2^{l+4m}\equiv2^l\ \ (mod\,10^{k+1})$ が成り立つと仮定する.
上と同様なやり方で変形していく.
$2^{l+4m}-2^l=10^{k+1}\times N$
$2^l(2^{4m}-1)=10^{k+1}\times N$

両辺を 2^{k+1} で割って，$2^{l-k-1}(2^{4m}-1)=5^{k+1}\times N$
よって，$2^{4m}-1$ は 5^{k+1} で割り切れる.
したがって $2^{4m}\equiv 1 \pmod{5^{k+1}}$
ここで $m=5^k q+r$ と表す.（ $r=1,2,3,\cdots,5^k-1$ ）
このとき $2^{4(5^k q+r)}\equiv 1 \pmod{5^{k+1}}$
指数部分は $4(5^k q+r)=4\cdot 5^k q+4r$ である.
ここで簡単な計算により，$2^{4\cdot 5^{k-1}}-1$ は 5^k で割り切れることがわかる･･･①から
$2^{4\cdot 5^{k-1}}-1=5^k\times A$ と表される.すなわち $2^{4\cdot 5^{k-1}}=5^k\times A+1$
したがって $2^{4(5^k q+r)}=2^{4\cdot 5^k q+4r}=2^{4\cdot 5^k q}\times 2^{4r}=2^{4\cdot 5^{k-1}\cdot 5q}\times 2^{4r}=(2^{4\cdot 5^{k-1}})^{5q}\times 2^{4r}=(5^k A+1)^{5q}\times 2^{4r}$
ここで $(5^k A+1)^5=(5^k A)^5+5^{k+1}B+1=5^{k+1}C+1$ の形をしていることは,パスカルの三角形などからわかる.
また，$(5^{k+1}A+1)(5^{k+1}B+1)=5^{k+1}C+1$ であることより,帰納的に $(5^{k+1}C+1)^q=5^{k+1}D+1$ が成り立つから，$(5^k A+1)^{5q}\equiv 1 \pmod{5^{k+1}}$ となる.（A,B,C,D は適当な整数）
したがって $2^{4(5^k q+r)}=(5^k\times A+1)^{5q}\times 2^{4r}\equiv 1\times 2^{4r}\equiv 2^{4r}\equiv 16^r \pmod{5^{k+1}}$

ここで 16^r の下2桁は $16,56,96,36,76,16,\cdots$ であるので
$2^{4(5^k q+r)}\equiv 16^r\equiv 1 \pmod{5^{k+1}}$ より $r=0$ でなければならない.
すなわち $m=5^k q$ となる.
よって数学的帰納法により
$2^{l+4m}\equiv 2^l \pmod{10^k}$ が成り立つと仮定すると $m=5^{k-1}q$ と表される.
よって $M=4\cdot 5^{k-1}q$ である.
ここでMは最小の数であったから，$M=4\cdot 5^{k-1}$ である.
また証明中より，$l\geq k$ であったから,（2）も成り立つ.

指数r	16^r
1	16
2	256
3	4096
4	65536
5	1048576
6	16777216

（①の証明について）
$2^{4\cdot 5^{k-1}}-1$ は 5^k で割り切れること
（証明）
$L=5^{k-1}$ とおく.
$2^{4\cdot 5^{k-1}}-1=2^{4L}-1=4^{2L}-1=(4^L+1)(4^L-1)$
Lは奇数であるから，$4^L-1\equiv(-1)^L-1=-2 \pmod{5}$ となるので 4^L-1 は5で割り切れない.
したがって $4^L+1=4^{5^{k-1}}+1$ が 5^k で割り切れることを証明すればよい.数学的帰納法による.
$k=1$ のとき $4^{5^{1-1}}+1=4+1=5$ なので成り立つ.
$k=i$ のとき成り立つと仮定すると，$4^{5^{i-1}}+1\equiv 0 \pmod{5^i}$ ゆえに $4^{5^{i-1}}=5^i N-1$ と表せる.
$k=i+1$ のとき，$4^{5^i}+1\equiv(4^{5^{i-1}})^5+1=(5^i N-1)^5+1=(5^{i+1}M-1)+1=5^{i+1}M\equiv 0 \pmod{5^{k+1}}$
ゆえに成り立つ.よって数学的帰納法により成り立つ.（終）

（性質2）の前半について
循環部分は $2^k \pmod{10^k}$ ，$2^{k+1} \pmod{10^k}$ ，$2^{k+2} \pmod{10^k}$,･･･，$2^{k+4\cdot 5^{k-1}-1} \pmod{10^k}$
である.
ここである l に対して，$2^{k+l} \pmod{10^k}<2^k \pmod{10^k}$ であるとする.（ $l=1,2,\cdots,4\cdot 5^{k-1}-1$ ）
このときmodなしで考えれば,ある c が存在して，$0<2^{k+l}-c\cdot 10^k<2^k$ が成り立っている.
この両辺を 2^k で割れば，$0<2^l-c\cdot 5^k<1$ であるが,これを満たすような整数 l,k は存在しない.
したがって矛盾である.
すなわち循環部分の最小値は $2^k \pmod{10^k}$ である.

（性質2）の後半については,今の証明から循環部分は,ある c が存在して，$2^{k+l}-c\cdot 10^k$ と表せたが,
変形すると $2^{k+l}-c\cdot 10^k=2^k(2^l-c\cdot 5^k)$ となり,これは 2^k の整数倍となっている.ゆえに成り立つ.

(性質3)について

性質2の結果から, 2^n の下 k 桁は 2^k の倍数であった.このことと, $2^k \cdot 5^{k-1} = 2 \cdot 10^{k-1}$ (これは 200･･･00 :0 が k-1 個の形)が 2^k の倍数であることにより,次のことがしたがう.

(1) 下 $k-1$ 桁が 2^k の倍数であるときの k 桁目の数(10^{k-1} の位)は $0,2,4,6,8$ のいずれかでなければならない.

(2) 下 $k-1$ 桁が 2^k の倍数でないときの k 桁目の数(10^{k-1} の位)は $1,3,5,7,9$ のいずれかでなければならない.

以上により成り立つ.(終)

2^nの下k桁

累乗n ↓	下1桁	下2桁	下3桁	累乗n ↓	下1桁	下2桁	下3桁
1	2	2	2	53	2	92	992
2	4	4	4	54	4	84	984
3	8	8	8	55	8	68	968
4	6	16	16	56	6	36	936
5	2	32	32	57	2	72	872
6	4	64	64	58	4	44	744
7	8	28	128	59	8	88	488
8	6	56	256	60	6	76	976
9	2	12	512	61	2	52	952
10	4	24	24	62	4	4	904
11	8	48	48	63	8	8	808
12	6	96	96	64	6	16	616
13	2	92	192	65	2	32	232
14	4	84	384	66	4	64	464
15	8	68	768	67	8	28	928
16	6	36	536	68	6	56	856
17	2	72	72	69	2	12	712
18	4	44	144	70	4	24	424
19	8	88	288	71	8	48	848
20	6	76	576	72	6	96	696
21	2	52	152	73	2	92	392
22	4	4	304	74	4	84	784
23	8	8	608	75	8	68	568
24	6	16	216	76	6	36	136
25	2	32	432	77	2	72	272
26	4	64	864	78	4	44	544
27	8	28	728	79	8	88	88
28	6	56	456	80	6	76	176
29	2	12	912	81	2	52	352
30	4	24	824	82	4	4	704
31	8	48	648	83	8	8	408
32	6	96	296	84	6	16	816
33	2	92	592	85	2	32	632
34	4	84	184	86	4	64	264
35	8	68	368	87	8	28	528
36	6	36	736	88	6	56	56
37	2	72	472	89	2	12	112
38	4	44	944	90	4	24	224
39	8	88	888	91	8	48	448
40	6	76	776	92	6	96	896
41	2	52	552	93	2	92	792
42	4	4	104	94	4	84	584
43	8	8	208	95	8	68	168
44	6	16	416	96	6	36	336
45	2	32	832	97	2	72	672
46	4	64	664	98	4	44	344
47	8	28	328	99	8	88	688
48	6	56	656	100	6	76	376
49	2	12	312	101	2	52	752
50	4	24	624	102	4	4	504
51	8	48	248	103	8	8	8
52	6	96	496	104	6	16	16

これらの性質に興味をもったため,Excel を用いて計算したところ,さらに次のような性質を見つけることができた.