$X^Q \equiv A \mod N$ の解の数
Numbers of Solutions of Equation

学習院大学理学部数学科
presented by H.Tamaki

2010 年 11 月 25 日

目 次

1　目的

$X^Q \equiv A\ modN$ の解の個数について調べる。今回は N を素数とし
① $X^Q \equiv 1 \bmod P$
② $X^Q \equiv -1 \bmod P$（P は素数）
の 2 つを調べる.

2　方法

N が素数より $X^{P-1} = 1$.(フェルマーの小定理)
よって $Q \geq P$ の時 $X^Q = X^Q \cdot X^P - 1 = X$ となるので, 今回は $Q < P$ について調べる.

prolog で作ったプログラムを用いてデータを集め, 以下の点に着目する.
① $X^Q \equiv 1 \mod P$(P は素数)

1. 与えられた Q に対して解の数はどんな数があるか.
2. 解が 1 つしかない場合、Q と P の関係.
3. 解が $P-1$ 個の時、どんな P と Q か.
4. 解が Q 個（Q と同じ数）の時、どんな P と Q か.

② $X^Q \equiv -1 \mod P$(P は素数)

1. 与えられた Q に対して解の数はどんな数があるか.
2. 解が 1 つしかない場合、Q と P の関係.
3. 解がない時の Q と P の関係.
4. 解が $\frac{P-1}{2}$ 個の時、どんな P と Q か.
5. 解が Q 個の時、どんな P と Q か.

～使ったプログラム～

$X^Q \equiv 1 \mod P$ の解の数を出すプログラム

```
tama(N,Q,C):-ctr_set(0),
xpqs(X^Q=1 mod N),
ctr_inc(_),
fail.
tama(_,_,C):-ctr_is(C).
```

$X^Q \equiv 1 \mod P$ の P を定めた時,Q の値毎の解の個数を出すプログラム

```
tamaq(N):-N1 is N-1,
for(2=<N1,Q),
tama(N,Q,C),
euler(N,F),
write([N,Q,F,C]),
nl,
fail.
tamaq(_).
```

$X^Q \equiv -1 \mod P$ の解の数を出すプログラム

```
tama2(N,Q,C):-ctr_set(0),
N1 is N-1,
xpqs(X^Q=N1 mod N),
ctr_inc(_),
fail.
tama2(_,_,C):-ctr_is(C).
```

$X^Q \equiv -1 \mod P$ の P を定めた時,Q の値毎の解の個数を出すプログラム

```
tamaq2(N):-N2 is N-1,
for(2=<N2,Q),
tama2(N,Q,C),
euler(N,F),
write([N,Q,F,C]),
nl,
fail.
tamaq2(_).
```

オイラー数を出すプログラム

```
factor(P/2):-Q is P//2,P =:= 2*Q,!.
factor(P/I):-P1 is floor(sqrt(P)),
for(1 =<P1,J),
J1 is 2*J+1,
Q is P//J1,
```

```
P =:= J1*Q,I=J1,!.
factor(P/P):-!.

euler(N,F):-factor(N/P),(
P==N ->F is P-1;
        M is N//P,euler(M,F1),
        (M mod P =:=0 ->(F is P*F1); F is (P-1)*F1)
).
```

3　結果

表 1: $X^Q \equiv 1 \mod P$ の解の数と Q と P の関係

P	$P-1$	$P-1$ の約数	解が 1 つの時の Q
3	2	1,2	なし
5	4	1,2,4	3
7	6	1,2,3,6	5
11	10	1,2,5,10	3,7,9
13	12	1,2,3,4,6,12	5,7,11
17	16	1,2,4,8,16	3,5,7,9,11,13,15
19	18	1,2,3,6,9,18	5,7,11,13,17
23	22	1,2,11,22	3,5,7,9,13,15,17,19,21
29	28	1,2,4,7,14,28	3,5,9,11,13,15,17,19,23,25,27
31	30	1,2,3,5,6,10,15,30	7,11,13,17,19,23,29
37	36	1,2,3,4,6,9,12,18,36	5,7,11,13,17,19,23,25,29,31,35
41	40	1,2,4,5,8,10,20,40	3,7,9,11,13,17,19,21,23,27,29,31,33,37,39
43	42	1,2,3,6,7,14,21,42	5,11,13,17,19,23,25,29,31,37,41
47	46	1,2,23,46	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45

表 2: $X^Q \equiv 1 \mod P$ の解の数と Q と P の関係

P	$P-1$	$P-1$ の約数	解が Q 個（Q と同じ数）の時の Q
3	2	1,2	2
5	4	1,2,4	2,4
7	6	1,2,3,6	2,3,6
11	10	1,2,5,10	2,5,10
13	12	1,2,3,4,6,12	2,3,4,6,12
17	16	1,2,4,8,16	2,4,8,16
19	18	1,2,3,6,9,18	2,3,6,9,18
23	22	1,2,11,22	2,11,22
29	28	1,2,4,7,14,28	2,4,7,14,28
31	30	1,2,3,5,6,10,15,30	2,3,5,6,10,15,30
37	36	1,2,3,4,6,9,12,18,36	2,3,4,6,9,12,18,36
41	40	1,2,4,5,8,10,20,40	2,4,5,8,10,20,40
43	42	1,2,3,6,7,14,21,42	2,3,6,7,14,21,42
47	46	1,2,23,46	2,23,46

表 3: $X^Q \equiv 1 \mod P$ の解の数と Q と P の関係

Q	Q と同じ数の解を持つ P
2	3,4,5,6,9,10,11,13,14,17,18,19,22,23,25,26,27,29,31,34,37,38,41,43,46,47
3	7,9,13,14,18,19,21,26,27,28,31,35,36,37,38,39,42,43,45
4	5,8,10,12,13,17,21,25,26,28,29,33,34,36,37,41,42,44
5	11,22,25,31,33,41,44
6	7,9,13,14,18,19,26,27,31,37,38,43
7	29,43
8	15,16,17,20,24,30,34,35,39,41,45
9	19,27,37,38,39
10	11,22,25,31,41
11	23,46
12	13,21,26,28,36,37,42
14	29,43
15	31
16	17,32,34,40,48
18	19,27,37,38
20	25,33,41,44
21	43
22	23
23	47
28	29
30	31
36	37
40	41
42	43
46	47

表 4: $X^Q \equiv -1 \mod N$ の解の数と Q と P の関係

P	$\frac{P-1}{2}$	$\frac{P-1}{2}$ の約数	解がない時の Q
3	1	1	2
5	2	1,2	4
7	3	1,3	2,4,6
11	5	1,5	2,4,6,8,10
13	6	1,2,3	4,8,12
17	8	1,2,4,8	16
19	9	1,3,9	2,4,6,8,10,12,14,16,18
23	11	1,11	2,4,6,8,10,12,14,16,18,20,22
29	14	1,7,14	2,4,6,8,10,12,14,16,18,20,22,24,26,28
31	15	1,3,5,15	2,4,6,8,10,12,14,16,18,20,22,24,26,28,30
37	13	1,13	2,4,6,8,10,22,24,26,28,30,32,34,36
41	20	1,2,4,5,10,20	8,16,24,32,40
43	21	1,3,7,21	2,4,6,8,10,22,24,26,28,30,32,34,36,38,40,42
47	23	1,23	2,4,6,8,10,22,24,26,28,30,32,34,36,38,40,42,44,46
257	128	1,2,4,8,16,32,64,128	256

表 5: $X^Q \equiv -1 \mod N$ の解の数と Q と P の関係

P	$\frac{P-1}{2}$	$\frac{P-1}{2}$ の約数	解が 1 つの時の Q
3	1	1	なし
5	2	1,2	3
7	3	1,3	5
11	5	1,5	3,7,9
13	6	1,2,3	5,7,11
17	8	1,2,4,8	3,5,7,9,11,13,15
19	9	1,3,9	5,7,11,13,17
23	11	1,11	3,5,7,9,13,15,17,19,21
29	14	1,7,14	3,5,9,11,13,15,17,19,23,25,27
31	15	1,3,5,15	7,11,13,17,19,23,29
37	18	1,2,3,6,9,18	5,7,11,13,17,19,23,25,29,31,35
41	20	1,2,4,5,10,20	3,7,9,11,13,17,19,21,23,27,29,31,33,37,39
43	21	1,3,7,21	5,11,13,,17,19,23,25,29,31,37,41
47	23	1,23	5,7,9,11,13,15,17,19,21,25,27,29,31,33,35,37,39,41,43,45

表 6: $X^Q \equiv -1 \mod N$ の解の数と Q と P の関係

P	$\frac{P-1}{2}$	$\frac{P-1}{2}$ の約数	解が Q 個（Q と同じ数）の時の Q
3	1	1	なし
5	2	1,2	2
7	3	1,3	3
11	5	1,5	5
13	6	1,2,3,6	2,3,6
17	8	1,2,4,8	2,4,8
19	9	1,3,9	3,9
23	11	1,11	11
29	14	1,2,7,14	2,7,14
31	15	1,3,5,15	3,5,15
37	18	1,2,3,6,9,18	2,3,6,9,18
41	20	1,2,4,5,10,20	2,4,5,10,20
43	21	1,3,7,21	3,7,21
47	23	1,23	23

表 7: $X^Q \equiv -1 \mod P$ の解の数と Q と P の関係

Q	Q と同じ数の解を持つ P
2	5,13,17,29,37,41
3	7,13,19,31,37,43
4	17,41
5	11,31,41
6	13,37
8	17
9	19,37
10	41
14	29
15	31
18	37
20	41
21	43
23	47

表 8: $P = 5$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	1	0
4	3	2	0

表 9: $P = 7$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	5	0
5	4	6	2
6	5	9	0

表 10: $P = 11$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	1	0
5	4	9	0
6	5	8	0
7	6	9	0
8	7	1	0
9	8	6	0
10	9	2	0

表 11: $P = 13$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	2
5	4	7	0
6	5	4	0
7	6	3	0
8	7	4	0
9	8	7	0
10	9	12	2
11	10	6	0
12	11	2	0

表 12: $X = 17$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	3	0
6	5	13	0
7	6	8	0
8	7	5	0
9	8	4	0
10	9	5	0
11	10	8	0
12	11	13	0
13	12	3	0
14	13	12	0
15	14	6	0
16	15	2	0

表 13: $X = 19$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	1	0
6	5	11	0
7	6	4	0
8	7	18	2
9	8	15	0
10	9	14	0
11	10	15	0
12	11	18	2
13	12	4	0
14	13	11	0
15	14	1	0
16	15	12	0
17	16	6	0
18	17	2	0

表 14: $X = 23$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	20	0
6	5	7	0
7	6	19	0
8	7	10	0
9	8	3	0
10	9	21	0
11	10	18	0
12	11	17	0
13	12	18	0
14	13	21	0
15	14	3	0
16	15	10	0
17	16	19	0
18	17	7	0
19	18	20	0
20	19	12	0
21	20	6	0
22	21	2	0

表 15: $X = 29$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	20	0
6	5	1	0
7	6	13	0
8	7	27	0
9	8	14	0
10	9	3	0
11	10	23	0
12	11	15	0
13	12	11	0
14	13	8	0
15	14	7	0
16	15	8	0
17	16	11	0
18	17	15	0
19	18	23	0
20	19	3	0
21	20	14	0
22	21	27	0
23	22	13	0
24	23	1	0
25	24	20	0
26	25	12	0
27	26	6	0
28	27	2	0

表 16: $X = 31$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	20	0
6	5	30	2
7	6	11	0
8	7	25	0
9	8	10	0
10	9	26	0
11	10	17	0
12	11	8	0
13	12	1	0
14	13	27	0
15	14	24	0
16	15	23	0
17	16	24	0
18	17	27	0
19	18	1	0
20	19	8	0
21	20	17	0
22	21	26	0
23	22	10	0
24	23	25	0
25	24	11	0
26	25	30	2
27	26	20	0
28	27	12	0
29	28	6	0
30	29	2	0

表 17: $X = 37$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	20	0
6	5	30	0
7	6	5	0
8	7	19	0
9	8	35	0
10	9	16	0
11	10	36	0
12	11	21	0
13	12	8	0
14	13	34	0
15	14	25	0
16	15	18	0
17	16	13	0
18	17	10	0
19	18	9	0
20	19	10	0
21	20	13	0
22	21	18	0
23	22	25	0
24	23	34	0
25	24	8	0
26	25	21	0
27	26	36	0
28	27	16	0
29	28	35	0
30	29	19	0
31	30	5	0
32	31	30	0
33	32	20	0
34	33	12	0
35	34	6	0
36	35	2	0

表 18: $X = 41$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	20	0
6	5	30	0
7	6	1	0
8	7	15	0
9	8	31	0
10	9	8	0
11	10	28	0
12	11	9	0
13	12	33	0
14	13	18	0
15	14	5	0
16	15	35	0
17	16	26	0
18	17	19	0
19	18	14	0
20	19	11	0
21	20	10	0
22	21	11	0
23	22	14	0
24	23	19	0
25	24	26	0
26	25	35	0
27	26	5	0
28	27	18	0
29	28	33	0
30	29	9	0
31	30	28	0
32	31	8	0
33	32	31	0
34	33	15	0
35	34	1	0
36	35	30	0
37	36	20	0
38	37	12	0
39	38	6	0
40	39	2	0

表 19: $X = 43$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	20	0
6	5	30	0
7	6	42	2
8	7	13	0
9	8	29	0
10	9	4	0
11	10	24	0
12	11	3	0
13	12	27	0
14	13	10	0
15	14	38	0
16	15	25	0
17	16	14	0
18	17	5	0
19	18	41	0
20	19	36	0
21	20	33	0
22	21	32	0
23	22	33	0
24	23	36	0
25	24	41	0
26	25	5	0
27	26	14	0
28	27	25	0
29	28	38	0
30	29	10	0
31	30	27	0
32	31	3	0
33	32	24	0
34	33	4	0
35	34	29	0
36	35	13	0
37	36	42	2
38	37	30	0
39	38	20	0
40	39	12	0
41	40	6	0
42	41	2	0

表 20: $X = 47$ の解の数

x	x-1	x(x-1)	解の数
2	1	2	0
3	2	6	0
4	3	12	0
5	4	20	0
6	5	30	0
7	6	42	0
8	7	9	0
9	8	25	0
10	9	43	0
11	10	16	0
12	11	38	0
13	12	15	0
14	13	41	0
15	14	22	0
16	15	5	0
17	16	37	0
18	17	24	0
19	18	13	0
20	19	4	0
21	20	44	0
22	21	39	0
23	22	36	0
24	23	35	0
25	24	36	0
26	25	39	0
27	26	44	0
28	27	4	0
29	28	13	0
30	29	24	0
31	30	37	0
32	31	5	0
33	32	22	0
34	33	41	0
35	34	15	0
36	35	38	0
37	36	16	0
38	37	43	0
39	38	25	0
40	39	9	0
41	40	42	0
42	41	30	0
43	42	20	0
44	43	12	0
45	44	6	0
46	45	2	0

3.1 $X^Q \equiv 1 \mod N$ についての観察結果

①与えられた Q に対して得られる解の数は $P-1$ の約数, と予想される.

（例）P =17 の時、$P-1$ =16 であり約数は 1,2,4,8,16. 得られる解も 1,2,4,8,16 となっている. $P=37$ の時、$P-1$ =36 であり約数は 1,2,3,4,6,9,12,18,36. 得られる解も 1,2,3,4,6,9,12,18,36 となっている.

②解が最大個数である $P-1$ 個の時の Q は $P-1$, と予想される.

（例）P =23 の時 $P-1$ =22 となる為,Q =22 の時,22 個の最大個数の解がある.

③解が 1 つしかない場合,Q と $P-1$ は互いに素 (GCD(Q,$P-1$)=1)、と予想される.

（例）Q =9,$P-1$ =17 の時 Q と $P-1$ は互いに素 (GCD(9,17)=1) なので解は 1 つ.

3.2 $X^Q \equiv -1 \mod N$ についての観察結果

①解を 1 つも持たない時 Q は必ず偶数となる, と予想される. 特に $P=1+2^E (E=2^e)$ であれば $Q=2^E$ の時解を持たない.

(例)P =17 の時 $P=1+2^4$ と表現できる (E =4).

よって $Q=2^4=16$ の時解を持たない.

②解が 1 つの時の Q は必ず奇数, と予想される.

③ $Q=P$-2 の時,$x=-1$ しか解がない, と予想される.

④ $Q=P-4$ の時,$x=-1$ を必ず解に持ち, 場合によってその他 2 つの解を持つと予想される.

4 考察

4.1 $X^Q \equiv 1 \bmod N$ の観察結果の証明

①

②解が最大個数である $P-1$ 個の時の Q は $P-1$ となっている。これはフェルマーの小定理より明らか.

③ GCD$(Q, P-1)=\alpha$ とすると,$X^Q=1$ なる X は α 個ある.

証)

$P-1=\alpha$

$mQ=\alpha k$

と書ける.(m と k は互いに素)

$X^Q=1$ なら $X^\alpha=1$ になる. これを示す.

ユークリッドの補題より $am+bk=1$.

α を掛けると,

$\alpha am+\alpha bk=\alpha$

$a(P-1)+bQ=\alpha$

$X^{a(P-1)+bQ}=X^\alpha$

$X^{a(P-1)} \cdot X^{bQ}=X^\alpha$

よって $X^\alpha=1$

$X^\alpha=1$ の解を β_1,β_2 とすると

$\beta_1^Q=(\beta_1^\alpha)^k=1^k$

よって $X^Q=1$ なる X は α 個ある.(証明終わり)

4.2 $X^Q \equiv -1 \bmod P$ の観察結果の証明

① $X^Q \equiv -1 \bmod P$,$P=2^E(E=2^e)$ に解がないとする.

Q が奇数だと $X=-1$ が解となるので,Q を偶数とし $Q=X^{2^m \cdot S}(S$ は奇数) と置く.

$X^{2^m} \equiv -1$ に解があれば $X^{2^m \cdot S}$ は解がある.

よって $X^{2^m}=-1$ に解がなければよい.

フェルマーの小定理より $X^{P-1}=1$.

$P-1=2^E$ なので,$X^{2^E}=-1$ には解がない.

よって $m=E$ なら解がないので,$m<E$ なら解がある事を示せばよい.

α を原始根とする.

$m=E-1$ の時

$x^{2^m}=x^{(\frac{P-1}{2})}$.

これを 2 乗すると $x^{(\frac{P-1}{2})^2}=x^{P-1}=1$

よって $x^{(\frac{P-1}{2})}$=-1 となり $x=$ で解を持つ.

$m=E-2$ の時

$x^{2^m}=\alpha^{(\frac{P-1}{4})}$.

これを 4 乗すると $\alpha^{(\frac{P-1}{4})^4}=\alpha^{P-1}=1$

よって

②

③ $Q = P - 2$ とする.

$x^Q = -1$. 両辺に x を掛けると,

$x^{Q+1} = -x$

ここで $x^{Q+1} = x^{P-1} = 1$ となるので $x = -1$.

よって $Q = P - 2$ は $x = -1$ しか解を持たない.（証明終わり）

④ $Q = P - 4$ とする.

$x^Q = -1$. 両辺に x^3 を掛けると,

$x^{Q+3} = -x^3$

ここで $x^{Q+3} = x^{P-1} = 1$ となるので $x^3 = -1$

$x^3 + 1 = (x + 1)(x^2 - x + 1) = 0$

$x = -1$ が解となるのは明らかなので,$x^2 - x + 1 \equiv 0 \mod P$ を調べる.

表 8〜20 より $x^2 - x + 1 \equiv 0 \mod P$ は $X - 1$ が 3 の倍数の時,$X = -1$ を含めた 3 つの解を持つ時がある.

5　今後の課題

$X^Q \equiv 1 \mod P$,$X^Q \equiv -1 \mod P$ の一般的な解の個数については解明できなかった。
N=P(素数) の考え方を軸に,N が偶数, 奇数の場合も考える必要がある。

6　感想

当初の予定では, ③ $X^{2Q} + X^Q + 1 \equiv 0 \mod N$ についても研究する予定でしたが, 自分の力量不足により③については調べる事ができずに終わってしまいました。是非とも有能な後輩達に研究して貰えたら嬉しいです。