自然数 a の約数の和を $\sigma(a)$ で表す.
a の関数と見て**ユークリッド関数**という.

$\sigma(a) - 2a = 0$ を満たす自然数を完全数という.

$\sigma(2^e)$ が素数のとき $2^e\sigma(2^e)$ は完全数になる.(ユークリッド)

完全数が偶数なら上の形になる.(オイラー)

目標 究極の完全数の探究

- 完全数の平行移動
- 底が3以上の素数について完全数を定義しまたその平行移動も研究する.
- 底が3以上の素数についてフェルマー完全数を定義し研究する.
- 概完全数の一般化
- 亜完全数
- 疑似完全数
- φ 完全数を導入しその平行移動,底の一般化を研究する.

原始根と平方剰余

1. 巡回群の性質

定理 1. 有限群 G の位数 *(*元の総数*)*が n のとき, その約数 m について方程式 $X^m = e$ を満たす群 G での根が常に m 個以下ならば, G は巡回群である.

proof

G の元 x についてその位数 m はn の約数である (ラグランジュの定理).

そこで集合 $G_m = \{x \in G \mid x \text{ の位数は } m\}$ を定義しよう.

G はn の約数 m について定まる集合 G_m の和集合になる. この和は共通部分の無い集合の和,いわゆる **disjoint sum** である.

集合 G_m の元の個数を ψ_m で表すと, $\sum_{m|n} \psi_m = n$ [1] となる.

一方, $G_m \neq \emptyset$ のとき, G_m の元 x を 1 つとる.

x の生成する部分群 $H = \{e, x, x^2, \cdots, x^{m-1}\}$ の位数はm.
H の元 x^j について $x^{jm} = e$ なのでx^j は$X^m = e$ の根でありこれらは丁度 m 個ある.

G の元について $X^m = e$ の根は m 個以下という仮定の下では, $X^m = e$ の根はすべて H の元である.

x に対して$G_m = \{x^j \mid x^j$ の位数は$m\}$.

x^j の元が位数 m になる条件はj と m は互いに素である.

x^j の位数を u とすると $x^{ju} = e$. よって $ju \equiv 0 \mod m$.
j, m の GCD を δ とおき $j = j'\delta, m = m'\delta$
とすると,
$j'u \equiv 0 \mod m'$. j', m' は互いに素なので $u \equiv 0 \mod m'$.
$u = m's$ と整数 s で書けるが, u 最小の正の整数なので,
$u = m'$. $m' = m/\delta$ なので
$u = m$ なら $\delta = 1$.

位数が m となるような x^j は $\varphi(m)$ 個ある. $\psi_m = \varphi(m)$.

- $G_m \neq \emptyset$ のとき, $\psi_m = \varphi(m)$.
- $G_m = \emptyset$ のとき,$\psi_m = 0 < \varphi(m)$.

よって

$$n = \sum_{m|n} \psi_m \leq \sum_{m|n} \varphi(m).$$

$\varphi(m)$ の定義から $\sum_{m|n} \varphi(m) = n$. これより, 上式で等号が成り立ち

$$\sum_{m|n} \psi_m = \sum_{m|n} \varphi(m).$$

よって,n の約数 m について $G_m \neq \emptyset$ になり $\psi_m = \varphi(m)$.

特に, $G_n \neq \emptyset$.

G_n の元 y は位数 n の部分群 H を生成する.H は巡回群である.

G と部分群 H とは 同じ位数の群になったので $H = G$.

2. 原始根

p を素数とし,p を法とする剰余環は有限体になり, これを $K_p = \mathbf{F}_p$ と書く.

一般に, 体 K における n 次方程式は n 個以下の根しか持たないから乗法群 $U(K)_p$ は巡回群になる.

その生成元を 1 つ決めて ξ と書くと整数 (p 以下の自然数) a によって $\xi = a \mod p$ と書かれる.

a は p を法としたときの **原始根** (primitive root) と呼ばれる.

$U(K)_p$ の元の個数は $p-1$ なので,$\xi^{p-1} = 1$. かつ $0 < r < p-1$ なら $\xi^r \neq 1$. これを合同の記号で書き換えると

$$a^{p-1} \equiv 1, a^r \not\equiv 1 \mod p$$

を満たす.

例として $p = 7$ の場合をとりあげる.

TABLE 1. $\mathbf{F}_7$ での累乗 a^s の表

$a \setminus s$	1	2	3	4	5	6	a の位数
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

この表によると 3 および 5 は6乗して初めて1になる. したがって, これらが7 を法としたときの原始根である.

一般に原始根は $\varphi(p-1)$ 個存在する.$p = 7$ のときは$\varphi(6) = 2$ なので丁度 2個ある.

指標.　$K = \mathbf{F}_p$ の元 $a \neq 0$ は,$U(K)$ の生成元 ξ により $a = \xi^j$ と整数 j で書けるが j は一通りに決まるわけではない. $\mathbf{F}_p$ の乗法群 $U(\mathbf{F}_p)$ は位数が $p-1$ なので$\xi^{p-1} = 1$ である.

$\xi^j = \xi^{j'}$ となる必要十分条件は $j-j'$ が $p-1$ の倍数となることである. このとき合同の記号を用いて $j \equiv j' \bmod (p-1)$ と書くことができる.

$a = \xi^j$ のとき,j は $p-1$ を法とすると一意に定まるので $j \equiv \mathrm{ind}_\xi(a)$ と書き,

p を法としたときの a の **指標**(index) という.

a, a' が p でわれないとき，対数の場合と類似した加法定理

$$\mathrm{ind}_\xi(aa') \equiv \mathrm{ind}_\xi(a) + \mathrm{ind}_\xi(a') \mod (p-1)$$

が成り立つ.

平方剰余.　　$X^2 = a$ が $\mathbf{F}_p$ で根 x を持つ必要十分条件は $\mathrm{ind}_\xi(a)$ が偶数になることである.

このとき a は整数 q を用いて $a = x^2 - qp$ と書ける.

$0 < a < p$ にとれば a は平方 x^2 を p で割った剰余になるので,**平方剰余**という.

そうならないとき**平方非剰余**と言う.

以下では, p は奇素数, すなわち $p > 2$ とする.

$0 < a < p$ に対して $\mathrm{ind}_\xi(a)$ が偶数になるときの a は丁度 $\dfrac{p-1}{2}$ 個あるので, 平方剰余になる a は $\dfrac{p-1}{2}$ 個ある.

5 を法とするとき, 1,4 は平方剰余. 2,3 は平方非剰余.

7 を法とするとき, 1,2,4 は平方剰余. 3,5,6 は平方非剰余.

a が p を法とするとき平方剰余なら $\left(\frac{a}{p}\right) = 1$ と書き,

平方非剰余なら $\left(\frac{a}{p}\right) = -1$ と書く. (ルジャンドルの平方剰余記号)

a, b がp で割れないとき

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$a \equiv a' \mod p$ なら

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).$$

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right). \tag{1}$$

これをオイラーの基準という

相異なる奇素数 p, q に対して

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{2}$$

平方剰余の相互法則という. これによって平方剰余記号の計算できる.

3. 平方剰余の定理の証明

$h = \frac{p-1}{2}$ とおくとき $\xi^{2h} = \xi^{p-1} \equiv 1 \bmod p$ なので $\xi^h \equiv -1 \bmod p$ を満たす.

p の倍数でない整数 a は $\bmod p$ においてξ のべきで表せる.すなわち整数 j があって

$$a \equiv \xi^j \bmod p$$

と書ける.

これを h 乗すると

$$a^h \equiv \xi^{jh} \equiv \xi^{hj} \equiv (-1)^j \bmod p.$$

そこで $\chi_p(a) = (-1)^j$ と定義する.すると

$$a^h \equiv (-1)^j = \chi_p(a) \bmod p. \tag{3}$$

$a \equiv a' \bmod p$ なら $\chi_p(a) = \chi_p(a')$ が成り立つ.

$$\chi_p(a) = \left(\frac{a}{p}\right)$$

となることを以下で証明する.

3.1. **準同型性.** p の倍数ではない整数 a, b について

$$\chi_p(ab) = \chi_p(a)\chi_p(b) \tag{4}$$

が成り立つ.

実際 $h = \frac{p-1}{2}$ について

$$(ab)^h \equiv \chi_p(ab) \mod p$$

と

$$(ab)^h = a^h b^h \equiv \chi_p(a)\chi_p(b) \mod p$$

とが成り立つので

$$\chi_p(ab) \equiv \chi_p(a)\chi_p(b) \mod p$$

をえる. よって $\chi_p(ab) - \chi_p(a)\chi_p(b)$ は p の倍数であるが $\chi_p(ab)$ と $\chi_p(a)\chi_p(b)$ はともに ± 1 なので等式 (4) が成立する.

いかえると写像 $\chi_p : \mathbb{Z}_p^* \to \{\pm 1\}$ は群の準同型である.

3.2. **平方剰余の意味.** a は p を法とするとき平方数 x^2 と合同とする. すなわち

$$a \equiv x^2 \bmod p \tag{5}$$

とすると $\chi_p(x) = \pm 1$ なので

$$\chi_p(a) = \chi_p(x^2) = \chi_p(x)^2 = 1.$$

式 (5) を書き換えると

$$a = x^2 - pk$$

となる. ここで $k \in \mathbb{Z}$.

$0 < x < p, 0 < a < p$ のときは 平方数 x^2 を p で割った余り (剰余) がa になる.

一般の場合も a はp を法として**平方剰余**(quadratic residue) であるという.

a が平方剰余であるとき $\chi_p(a) = 1$ が示されたがこの逆が成り立つ.

実際 $\chi_p(a) = 1$ とすると

$$1 = \chi_p(a) \equiv a^h \equiv (-1)^j \bmod p.$$

よって j は偶数になる. $j = 2m$ とすれば $x = \xi^m$ とおくと

$$a \equiv \xi^j = (\xi^m)^2 = x^2 \bmod p.$$

したがって a は平方剰余になった.

3.3. $a = p-1$ のとき． $a = p-1$ のとき $h = \dfrac{p-1}{2}$ について

$$a^h \equiv (-1)^h = \chi_p(a) \bmod p$$

が成り立つので

- $p = 4k+1$ なら $h = 2k$ より $\chi_p(-1) = 1$.
- $p = 4k-1$ なら $h = 2k-1$ より $\chi_p(-1) = -1$.

この結果は

$$\left(\frac{-1}{p}\right) = \chi_p(-1) = (-1)^{\frac{p-1}{2}}$$

とまとめられ, **平方剰余の第一補充法則** という.

$$\left(\frac{2}{p}\right) = \chi_p(2) = (-1)^{\frac{p^2-1}{8}}$$

平方剰余の第2補充法則 という.

- $\chi_p(2) = 1;\ p \equiv \pm 1 \bmod 8,$
- $\chi_p(2) = -1;\ p \equiv \pm 3 \bmod 8,$

と書ける.

$$\left(\frac{3}{p}\right) = \chi_p(3)$$

$$\left(\frac{5}{p}\right) = \chi_p(5)$$

の計算を行う.

- $\chi_p(5) = 1$; $p \equiv \pm 1 \bmod 5$,
- $\chi_p(5) = -1$; $p \equiv \pm 2 \bmod 5$.

例

- $p = 5$ のとき $-1 \equiv 4 = 2^2$.
- $p = 7$ のとき $-1 \equiv X^2 \bmod 7$ に解はない.

$h = \frac{p-1}{2}$ とおくと (オイラーの基準)

$$a^h \equiv \left(\frac{a}{p}\right) = \chi_p(a) \bmod p. \tag{6}$$

オイラーとフェルマーの古典的結果

4. 素数べきの約数の和

$\sigma(2^e) = 2^{e+1} - 1$ が素数になるとき, $e+1$ も素数である. ここでは $e+1$ が素数になる場合に限って ,$\sigma(2^e)$ の素因数分解をしている.

$\sigma(2^e)$ が素数になる場合は 7,31,127,8191, 131071,524287,$\cdots$ となって意外に多い.

これらを (2を底とする) **メルセンヌ素数**という. ($e+1$ は素数と限定した効果である)

TABLE 2. $\sigma(2^e) = 2^{e+1} - 1$, $e + 1$:素数

$2^e = a$	$\sigma(a)$	素因数分解
$2 = 2$	3	$[3]$
$2^2 = 4$	7	$[7]$
$2^4 = 16$	31	$[31]$
$2^6 = 64$	127	$[127]$
$2^{10} = 1024$	2047	$[23, 89]$
$2^{12} = 4096$	8191	$[8191]$
$2^{16} = 65536$	131071	$[131071]$
$2^{18} = 262144$	524287	$[524287]$
$2^{22} = 4194304$	8388607	$[47, 178481]$
$2^{30} = 1073741824$	2147483647	$[2147483647]$

$\sigma(2^e)$ が素数のとき $2^e\sigma(2^e)$ は完全数になる.

4.1. フェルマーとオイラーの結果.

補題 1. q が素数のとき 2^q-1 の素因数 p については $p-1=2Lq$ と書ける.

さらに $p \equiv \pm 1 \bmod 8$.

Proof.

条件より,

$$2^q \equiv 1 \mod p.$$

q は素数なので 2 の $\mathrm{mod}p$ での位数は q. ゆえに

フェルマーの小定理によると $2^{p-1} \equiv 1 \mod p$. よって, $p-1=kq$ と書ける. $p-1$ は偶数なので k も偶数. よって $k=2L$ と表せる.

$p-1=2Lq$ により

$$2^{\frac{p-1}{2}} \equiv 2^{Lq} \equiv 1 \bmod q.$$

ルジャンドルの記号を用いるとオイラーの基準によって

ゆえに $p \equiv \pm 1 \bmod 8$.

例

$q = 11$ とする. $A = 2^{11} - 1$ の素因数分解は $23 * 89$. このとき

$$23 - 1 = 22 = 2 * 11 = 2q, 89 - 1 = 88 = 8 * 11 = 8q.$$

4.2. **ラグランジュの結果.** 次の結果はオイラーが予想し15年後ラグランジュが証明した.

補題 2. $p > 3$ が奇素数のとき, $M_p = 2^p - 1$ とおく.

$q = 2p + 1$ が素数, かつ $q \equiv \pm 1 \bmod 8$ のとき,

($q = 2p + 1$により $q = 1 + 8k'$ は起きない. By Mizutani)

$q = 2p + 1$ は M_p の約数. とくに M_p はメルセンヌ素数にならない.

逆に $q = 2p + 1$ が M_p の因子なら q は素数.

$q = 2p + 1$ が素数になる素数 p を **Sophie Germain の素数**という.

このとき $q = 2p + 1$ が平方剰余なら M_p の素因子になる.

TABLE 3. p : Sophie Germain の素数

p	$q=2p+1$	平方剰余	M_p
11	23	+	$23*89$
23	47	+	$47*178481$
29	59	−	$233*1103*2089$
41	83	−	$13367*164511353$
53	107	−	$6361*69431*20394401$
83	167	−	$167*57912614113275649087721$

$q=2p+1$ を法として 2 が 平方剰余のとき,q が M_p の因子になっている.

表

Table 4

$2/q$ のルジャンドル	p	$q=2p+1$	M_p の素因数分解
$(+)$	3	7	7
$(+)$	11	23	23*89
$(+)$	23	47	47*178481
$(+)$	83	167	167*5791261411327564908772
$(+)$	131	263	263*1035079443105516238671861923
$(-)$	5	11	31
$(-)$	29	59	233*1103*2089
$(-)$	41	83	13367*164511353
$(-)$	53	107	6361*69431*20394401
$(-)$	89	179	6.1897E+26
$(-)$	113	227	3391*23279*65993*1868569*1066818

5. 完全数の平行移動

$q = 2^{e+1} - 1$ が素数のとき $2^e q$ は完全数になる. 完全数の平行移動とは次の意味である.

別のパラメータ m に対して $q = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e q$ を m だけ**平行移動した完全数**という. ただし m は偶数の整数.

これは概念としては新しいと思う.

6. m だけ並行移動した場合の数表

6.1. $m = 2$. 2 だけ並行移動した場合を見てみよう. $q = 2^{e+1} + 1$ が素数の場合になる. このとき $e + 1 = 2^m$ と表せる.

一般に $e + 1 = 2^m$ のとき $2^{e+1} + 1$ をフェルマー数といい, 素数のときフェルマー素数という.

TABLE 5. $q = 2^{e+1} + 1$ が素数

e	$e+1$	$e \bmod 4$	$2^e * q$	a
0	1	0	3	3
1	2	1	$2 * 5$	10
3	4	3	$2^3 * 17$	136
7	8	3	$2^7 * 257$	32896
15	16	3	$2^{15} * 65537$	2147516416

$3,5,17,257,65537$ らは5個のフェルマー素数である．2だけ平行移動した $2^e q = 3,10,136,32896,2147516416$ をフェルマーの完全数と呼んでやりたい．

フェルマーは F_5 も素数であると思ったがオイラーが合成数であることを示した．

$e \geq 3$ のとき $q \equiv 7, a \equiv 6 \mod 10$.

とくに a の末尾の数は 6.

Proof. $e+1 = 2^r$ により $r \geq 2$ なら $e+1 = 4N$ と書けるので

$q = 2^{e+1}+1 \equiv 2 \bmod 5$. 一方, q は奇数なので $2^e \equiv 3 \times 2^{e+1}$ なので $q \equiv 7 \mod 10$.

$a = 2^e * q \equiv 3 * q \equiv 6 \bmod 5$, a は偶数なので $a \equiv 6 \mod 10$.

7. オイラーの反例

フェルマーの期待に反して, $m \geq 5$ のときフェルマー素数は発見されていない.

オイラーは,次の結果を証明しこれを用いて F_5 の素因数 641 を発見した.

補題 3. F_m の素因数 Q は $1 + 2^{m+1}K$ と書ける.

Proof

$2^{2^m} + 1 \equiv 0 \mod Q$ なので $2^{2^m} \equiv -1 \mod Q$.

$\mod Q$ での 2の位数 u は 2^{m+1} の約数である.

$u = 2^s$ とおくと $s \leq 2^{m+1}$ だが $2^{2^m} \equiv -1$ により $s = 2^{m+1}$.

$2^{Q-1} \equiv 1 \mod Q$ によれば $Q - 1$ は 2^{m+1} の倍数なので $Q = 1 + 2^{m+1}k$.

補題 **4.** $Q = 1 + 2^{m+1}k$ において k は偶数である.

$Q = 1 + 2^{m+2}k'$ と書ける.

$2^{\frac{Q-1}{2}} = 2^{2^m k}$ となりオイラーの基準によって

$$2^{\frac{Q-1}{2}} \equiv \left(\frac{2}{Q}\right) \mod Q.$$

$$2^{\frac{Q-1}{2}} = 2^{2^m k} \equiv (-1)^k \mod Q.$$

k: 偶数 $k = 2k'$.

k: 奇数. $\left(\frac{2}{Q}\right) = -1$ になり $Q \equiv \pm 3 \mod 8$.

$Q = 1 + 2^m k, Q = \pm 3 + 8L$ のとき $2^m k = -1 + \pm 3 + 8L$.

$(+)$ なら $2^m k = 2 + 8L$. $2^{m-1}k = 1 + 4L$.$m > 1$ なら矛盾.

$(-)$ なら $2^m k = -4 + 8L$. $2^{m-1}k = -2 + 4L$.$m > 1$ なら矛盾.

7.1. **例.** $m = 5$ なら $Q = 1 + 128$. $k = 5$ のとき $Q = 641$.

$F_5 = 4294967297 = 641 * 6700417$ が素因数分解.

$641 - 1 = 640 = 2^7 * 5$; $2^7 = 2^{5+2}$.

$6700417 - 1 = 6700416 = 2^7 * 3 * 17449$

$F_6 = 18446744073709551617 = 274177 * 67280421310721$ が素因数分解.

$F_7 = 340282366920938463463374607431768211457$

$= 59649589127497217 * 5704689200685129054721$ が素因数分解.

各素因子について, フェルマーの結果を確認する.

```
 m=6 8=m+2
 ?- A=274177, B is A-1,factorize(B,C),exps(C,D),write(B),put
274176  [2^8,3^2,7,17] ;2^8=2^{6+2}.
A = 274177,
B = 274176,
D = [2^8, 3^2, 7, 17].

 ?- A=67280421310721, B is A-1,factorize(B,C),exps(C,D),writ
67280421310720  [2^8,5,47,373,2998279]
A = 67280421310721,
B = 67280421310720,
D = [2^8, 5, 47, 373, 2998279].

 ?- A=5964958912749721 7, B is A-1,factorize(B,C),exps(C,D),w
5964958912749721 6       [2^9,116503103764643]
A = 5964958912749721 7,
```

8. 3のべきとそのユークリッド関数の値

3のべき 3^e について $e+1$ が素数の場合 $\sigma(a)$ の素因数分解を行う.

TABLE 6. $3^e = a$

$3^e = a$	$\sigma(a)$	の素因数分解
$3^2 = 9$	13	$[13]$
$3^4 = 81$	121	$[11^2]$
$3^6 = 729$	1093	$[1093]$
$3^{10} = 59049$	88573	$[23, 3851]$
$3^{12} = 531441$	797161	$[797161]$
$3^{16} = 43046721$	64570081	$[1871, 34511]$
$3^{18} = 387420489$	581130733	$[1597, 363889]$
$3^{22} = 31381059609$	47071589413	$[47, 1001523179]$
$3^{28} = 22876792454961$	34315188682441	$[59, 28537, 20381027]$
$3^{30} = 205891132094649$	308836698141973	$[683, 102673, 4404047]$

$\sigma(3^e)$ が素数になるのは 13,1093, 797161であり数少ない. これらを **3を底としたメルセンヌ素数**という.

8.1. **フェルマーとオイラーの結果.** 3を底としたメルセンヌ数についてもフェルマーとオイラーの結果は成立する. New Result

補題 5. q が素数のとき $\frac{3^q-1}{2}$ の奇数素因数 p については $p-1=2Lq$ と書ける.

さらに $p \equiv \pm 1 \bmod 12$ を満たす.

Proof.
条件より,

$$3^q \equiv 1 \mod p.$$

q は素数なので 3 の $\mathrm{mod}p$ での位数は q.
フェルマーの小定理によると $3^{p-1} \equiv 1 \mod p$.

よって, $p-1=kq$ と書ける. $p-1$ は偶数なので k も偶数. $k=2L$ と表せるから$p-1=2Lq$.

$$3^{\frac{p-1}{2}} \equiv 3^{Lq} \equiv 1 \bmod p.$$

オイラーの基準によって

$$3^{\frac{p-1}{2}} \equiv \left(\frac{3}{p}\right)$$

$3^{\frac{p-1}{2}} \equiv 1$ なので $\left(\frac{3}{p}\right)=1$.

平方剰余の法則から $p \equiv \pm 1 \bmod 12$.

例$q=17$ のとき $A=3^{17}-1=129140162$. この 素因子分解 $[2, 1871, 34511]$.

$p_1=1871$ とおくと p_1-1 の 素因子分解 $[2, 5, 11, 17]$.

$p_2=34511$ とおくと p_2-1 の 素因子分解 $[2, 5, 7, 17, 29]$.

8.2. **オイラーとラグランジュの結果.** オイラーとラグランジュの結果は底が3でも成り立つ. しかも具体例で計算すると, 底が2のときより結果が断然良い. これは驚くべき結果であった.

補題 6. p を素数とし, $q = 2p + 1$ も素数とする.
$N_p = 3^p - 1$ とおくとき, q を法として 3 が平方剰余とする.
このとき q は N_p の素因子である.

Proof.

仮定から$3 \equiv n^2 \mod q$ を満たす整数 n がある. フェルマーの小定理を用いて

$$3^p \equiv n^{2p} \equiv n^{q-1} \equiv 1 \mod q$$

ゆえに $N_p = 3^p - 1 = qk$ と書けるので, q はN_p の素因子.

注意

q を法として3 が平方剰余とするとき (平方剰余の相互法則から)

$q \equiv \pm 1 \mod 12$.

この逆も成立する.

補題 **7.** p を素数とし, $q = 2p + 1$ が N_p の因子とする.
このとき $q = 2p + 1$ も素数.

Proof.

$q = 2p + 1$ は素数でないとする. その最小の素因子をとり q_0 とする. $2p + 1 \geq q_0^2$ を満たす. q_0 も N_p の素因子なので $q_0 \neq 3$.

$$3^p = N_p + 1 \equiv 1 \mod q_0.$$

p は素数なので q_0 を法とした3の位数である. フェルマーの小定理を用いて

$$3^{q_0-1} \equiv 1 \mod q_0.$$

ゆえに, $q_0 - 1$ は p の倍数. とくに $q_0 - 1 > p$ になり

$$2p + 1 \geq q_0^2 > p^2 + 2p + 1 > 2(p + 1) + 1.$$

これで矛盾した.

p : Sophie Germain 素数について, q はすべて $q+1=12L$ を満たし結果としてすべて q は N_p の因子となっていた. これは感動の結果である.

TABLE 7. $q=2p+1$: 素数

p	$q=2p+1$	$q+1$	$q+1 \bmod 12$	N_p 素因数分解
5	11	12	0	$2*11^2$
11	23	24	0	$2*23*3851$
23	47	48	0	$2*47*1001523179$
29	59	60	0	$2*59*28537*20381027$
41	83	84	0	$2*83*2526913*86950696619$
53	107	108	0	$2*107*24169*3747607031112307667$
83	167	168	0	A
89	179	180	0	B
113	227	228	0	C
131	263	264	0	D
173	347	348	0	E
178	359	360	0	F
190	383	384	0	G

$$A = 2 * 167 * 12119 * 1036745531 * 9509960596272108979433 51$$

$$B = 2 * 179 * 16114798915198 07 * 5042939439565996049162197$$

$$C = 2*227*1583*2172539*526256453012063980796131127321354599535039$$

$$D = 2*263*60519958859114400310088130657440685166028842774039488582 8171$$

$$E = 2*347*762239*2125048865543*309854287003880455089590180543928107620331492 8$$

$$F = 2*359*56207*100957*19510643*2910660661304 51*67799636437851381 1*$$
$$16186866474449165570585896359433 1$$

$$G = 2*383*311713*9593931911*589086859176036543433200507492971040054890918146 8$$

8.3. **証明.** 参加者の水谷氏の指摘により, 次の結果を証明する.

補題 8. p を素数とし, $q = 2p + 1$ も素数とする. このとき q を法として 3 は平方剰余である.

素数 q を mod12 で分類すると $q \equiv 1, 5, 7, 11 \mod 12$ である.

(1).$q \equiv 1 \mod 12$ とすると $q = 1 + 12k$. $q = 2p + 1$ なので $1 + 12k = 2p + 1$. よって $p = 6k$. 矛盾.

(3). $q \equiv 5 \mod 12$ とすると $q = 5 + 12k = 2p + 1$. よって $p = 4 + 6k$. 矛盾.

(3). $q \equiv 7 \mod 12$ とすると $q = 7 + 12k = 2p + 1$. よって $p = 3 + 6k$. 矛盾.

$q \equiv 11 \mod 12$ のみ生き残り, このとき q を法として 3 は平方剰余.

TABLE 8. $e+1$: prime, $q=2p+1$: prime

e	$(2e+3)$ =factor	$(Q=(3^{e+1}-1)/2)$=fct
2	(7)=7	(13)=13
4	(11)=11	$(121)=11^2$
10	(23)=23	(88573)=23*3851
22	(47)=47	(47071589413)=47*1001523179
28	(59)=59	(34315188682441)=59*28537*20381027
40	(83)=83	(1823649188585393201)=83*2526913*86950696619
52	(107)=107	(9691622833840009948398361)=107*24169*374760703111230766
82	(167)=167	(19954191970936699647671233377861745176
88	(179)=179	(14546605946812854043152329132461212233

9. $\sigma(5^e)$ が素数になる場合

TABLE 9. $5^e a$ の $\sigma(a)$

$5^e = a$	$\sigma(a)$	素因数分解
$5^2 = 25$	31	[31]
$5^4 = 625$	781	[11, 71]
$5^6 = 15625$	19531	[19531]
$5^{10} = 9765625$	12207031	[12207031]
$5^{12} = 244140625$	305175781	[305175781]
$5^{16} = 152587890625$	190734863281	[409, 466344409]
$5^{18} = 3814697265625$	4768371582031	[191, 6271, 3981071]
$5^{22} = 238418579101562 5$	298023223876953 1	[8971, 332207361361]
$5^{28} = 372529029846191406 25$	465661287307739257 81	[59, 35671, 221259964

$q = \sigma(5^e)$ が素数になるのは $q = 31, 19531, 12207031, 305175781$ であり少ない.

9.1. フェルマーとオイラーの結果(一般の場合).

補題 **9.** $q, k > 1$ が 奇数のとき $q^k - 1 = \overline{q}L$ と書ける. ここで L は奇数

Proof.

$$\frac{q^k - 1}{\overline{q}} = 1 + q + \cdots + q^{k-1} \equiv k \equiv 1 \mod 2.$$

奇素数 P を底としたメルセンヌ数についてもフェルマーとオイラーの結果は成立する.

補題 10. q が素数のとき $\frac{P^q-1}{P}$ の素因数 p は $p-1=2Lq$ と書ける.

$\left(\frac{P}{p}\right)=1.$

さらに $P=5$ なら $p\equiv\pm1 \bmod P.$

Proof.

条件より,

$$P^q \equiv 1 \mod p.$$

q は素数なので P の $\mathrm{mod}p$ での位数は q.

フェルマーの小定理によると $P^{p-1} \equiv 1 \mod p.$ よって, $p-1=kq$ と書ける. $p-1$ は偶数なので k も偶数. よって $k=2L$ と表せることによって$p-1=2Lq$ と書ける.

$$P^{\frac{p-1}{2}} \equiv P^{Lq} \equiv (P^q)^L \equiv 1 \bmod q.$$

10. オイラーとラグランジュの結果(一般の場合)

オイラーとラグランジュの結果は底が P でも成り立つ.

補題 11. p を素数とし, $q = 2p+1$ も素数とする. $L_p = P^p - 1, P \neq p$ とおくとき, q を法として P が平方剰余とする. このとき q は L_p の素因子である.

Proof.

仮定から $P \equiv n^2 \mod q$ を満たす整数 n がある. フェルマーの小定理を用いて

$$P^p \equiv n^{2p} \equiv n^{q-1} \equiv 1 \mod q$$

ゆえに $L_p = P^p - 1 = qk$ と書けるので, q は L_p の素因子.

(平方剰余の相互法則から $q \equiv \pm 1 \mod P$)

この逆も成立する.

補題 12. p を素数とし, $q = 2p + 1$ が $L_p = P^p - 1$ の因子とする. このとき $q = 2p + 1$ も素数.

Proof.

$q = 2p + 1$ は素数でないとする. その最小の素因子をとり q_0 とする. $2p + 1 \geq q_0^2$ を満たす. q_0 も N_p の素因子なので $q_0 \neq P$.

$$P^p - 1 = N_p \equiv 0 \mod q_0.$$

p は素数なので q_0 を法としたPの位数である. フェルマーの小定理を用いて

$$P^{q_0 - 1} \equiv 1 \mod q_0.$$

ゆえに, $q_0 - 1$ は p の倍数. とくに $q_0 - 1 > p$ になり

$$2p + 1 \geq q_0^2 > p^2 + 2p + 1 > 2(p + 1) + 1.$$

TABLE 10. q : 素数

p	$q=2p+1$	$q-1$	$q+1$	L_p 素因数分解
11	23	22	24	$2^2 * 12207031$
23	47	46	48	$2^2 * 8971 * 332207361361$
29	59	58	60	$2^2 * 59 * 35671 * 2212599644432962555250847358847 1$
41	83	82	84	A
53	107	106	108	$2^2 * 5960555749 * 17154094481 * 2714536505262944 9$
89	179	108	180	$2^2 * B$

$A = 2238236249 * 50793046432166879 69$

$B = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 * 2316696543636831300950 95909$

$p = 89, q = 179 \equiv +1 \mod 5$ なので q を法として 5 は平方剰余.

$q = 179$ は L_p の素因子.

11. オイラーとラグランジュの結果の例

以下では素数 P に対してその素数べき P^p について $N_p = \frac{P^p-1}{P-1}$ が素数にならない場合を扱う. $q = 2p+1$ も素数になる場合に限定した.

TABLE 11. $P = 3, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p)=素因数分解
2	5	$(4) = 2^2$
3	7	(13)=13
5	11	$(121) = 11^2$
11	23	(88573)=23*3851
23	47	(47071589413)=47*1001523179
29	59	(343151886824 41)=59*28537*20381027
41	83	(18236498188585393201)=83*2526913*86950696619
53	107	(96916228338400099483 98361)=107*24169*374760703111230
83	167	$A = B$
89	179	$C = D$

11.1. $P = 3$.

$A = (19954191970936699647671233377861745176 13)$
$B = 167 * 12119 * 1036745531 * 95099605962721089794335 1$
$C = (14546605946812854043152329132461212233 40241)$
$D = 179 * 1611479891519807 * 50429394395659960491621 97$

$q = 2p + 1$ が N_p の最小素因子となる.

TABLE 12. $P = 5, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p)=素因数分解
2	5	(6)=2*3
5	11	(781)=11*71
23	47	(2980232238769531)=8971*332207361361
29	59	A
41	83	B
53	107	C
83	167	$D = E$
89	179	$F = G$
113	(227)=227	$H = I$
131	(263)=263	$J = K$

11.2. $P = 5$.

$$A = (46566128730773925781) = 59 * 35671 * 22125996444329$$

$$B = (113686837721616029739379882 81) = 2238236249*5079304643216687$$

$$C = (27755575615628913510590791702270 50781) = 960555749*$$

$$17154094481 * 2714536505262944 9$$

$$D = (25849394142282114839731521627186339173931628465652465820 31)$$

$$E = 20515111*1431185706701868962383741*880400959451038346273767 8$$

$$F = (40389678347315804437080502542478654959268169477581977844238 2$$

$$G = 179 * 9807089 * 14597959 * 834019001 * 8157179360521 *$$

$$23166965436368313009590 9$$

$$H = (24074124304840448163199724282311591481726270602692352440499$$

$$I = 2939*6329*129499*308491*304247586761*2084303944451$$

$$- *620216264269531 * 8237123176890810696379$$

$$J = 91835496157991211560057541970487943579583246622819 3-$$

$$37617871227053001348394900560379028320 31)$$

$$K = 2621 * 23928199 * 34720241 * 16815642611861* -$$

$q = 2p + 1$ が N_p の最小素因子となるのは$q = 11, 179,$

$p = 23$ での (N_p) の素因数分解 $8971 * 332207361361$ について

```
 ?-  A=8971,B is A-1, factorize(B,BB),exps(BB,J).
A = 8971,
B = 8970,
BB = J, J = [2, 3, 5, 13, 23].

3 ?- A=332207361361,B is A-1, factorize(B,BB),exps(BB,J).
A = 332207361361,
B = 332207361360,
BB = [2, 2, 2, 2, 3, 3, 5, 7, 23|...],
J = [2^4, 3^2, 5, 7, 23, 293, 9781].
```

B がどれも 2×23 を因数に持つ.

$p = 29$ での (N_p) の素因数分解 $59 * 35671 * 22125996444329$ について

```
4 ?- A=59,B is A-1, factorize(B,BB),exps(BB,J).
A = 59,
B = 58,
BB = J, J = [2, 29].

5 ?- A=35671,B is A-1, factorize(B,BB),exps(BB,J).
A = 35671,
B = 35670,
BB = J, J = [2, 3, 5, 29, 41].

6 ?- A=22125996444329,B is A-1, factorize(B,BB),exps(BB,J).
A = 22125996444329,
B = 22125996444328,
BB = [2, 2, 2, 7, 29, 13624382047],
```

TABLE 13. $P = 7, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p)=素因数分解
2	5	$(8)=2^3$
3	7	$(57)=3*19$
11	23	$(329554457)=1123*293459$
23	47	$(45614578900134860 57)=47*3083*3147982339 6757$
29	59	$(53665095930219662 1139601)=59*127540261*7131692298499$
41	83	A
53	107	$B = C$
83	167	$D = E$

11.3. $P = 7$.

$A = (74279400543938659833650076624280 01) = 83*20515909*$
$436213933622906865609478 3$
$B = (10281225160467706104845935946923162113219640 1)$
$C = 8269 * 319591 * 89042760170351880563720518398412 19$
$D = (23173203249700874472330986792321198522833668720161907874906$
$E = 167 * 66733 * 76066181 * 7685542369 * 6291113047752 1 *$
$303567967057423 * 18624275418445601$
$q = 2p+1$ が N_p の最小素因子となるのは$q = 47, 59, 83, 167.$

TABLE 14. $P = 11, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p)=素因数分解
2	5	$(12)=2^2 * 3$
3	7	(133)=7*19
5	11	(16105)=5*3221
11	23	(28531167061)=15797*1806113
23	47	(895430243255237372246 53)=829*28878847*37402219
29	59	(158630929717149157441443670489)=523*3033096170499983
41	83	$X = Y$
53	107	$A = B$
83	167	$C = D$

11.4. $P = 11$.

$X = (4978518112499354698647829163838661251242 41)$

$Y = 83 * 1231 * 27061 * 509221 * 14092193 * 29866451 * 840139875599$

$A = (156247225182874466270373106163166923838785226992003 1433)$

$B = 107*351497*6005113*691808237490131385512539766532597713 5579$

$C = (272642068561325511040414333102035297723974312150221630961592$

$D = 167*12119*178057577*52447614013*144252522599698103459589490 1$

$q = 2p+1$ が N_p の最小素因子となるのは $q = 7, 83, 107, 167$

TABLE 15. $P = 13, q = 2p + 1$ も素数

p	$q = 2p + 1$	(N_p)=素因数分解
2	5	$(8)=2^3$
3	7	$(57)=3*19$
11	23	$(329554457)=1123*293459$
23	47	$(45614578900134860 57)=47*3083*3147982339 6757$
29	59	$(53665095930219662113 9601)=59*127540261*7131692298499$
41	83	A
53	107	$B = C$
83	167	$D = E$
89	179	$F = G$

11.5. $P = 13$.

$A = (74279400543938659833650076624280 01) = 83*20515909*$
$436213933622906865609478 3$
$B = (10281225160467706104845935946923162113219640 1)$
$C = 8269 * 319591 * 389042760170351880563720518398412 19$
$D = (23173203249700874472330986792321198522833668720161907874906$
$E = 167 * 66733 * 76066181 * 7685542369 * 6291113047752 1 *$
$303567967057423 * 18624275418445601$
$F = (27263041891240581807952682651297966850128582912583282995748$
$G = 1805633*184896053147409877659 13*816614687584787676285911901 5$
$q = 2p+1$ が N_p の最小素因子となるのは$q = 47, 59, 83, 167$

$p = 89$ のときの$G = 1805633 * 184896053147409877659 13 * 816614687584787676285911901514700476265645056 9$ の各素因数について

```
?- A=1805633,B is A-1, factorize(B,BB),exps(BB,J).
A = 1805633,
B = 1805632,
J = [2^6, 89, 317].

?- A=184896053147409877659 13,B is A-1, factorize(B,BB),exps(
A = 184896053147409877659 13,
B = 184896053147409877659 12,
J = [2^3, 3, 7, 89, 89839, 13764595178129].
```

B はどちらも 2×89 を因数に持つ.

P を底とするフェルマーの完全数

P を奇素数とし $E > 0$ について $Q = P^E + 1$ とおく. これは偶数なので $L_E = \frac{Q}{2}$ とする. L_E を素数とすると, E は 2 のべきになるので $E = 2^m, m > 0$ とかける.

そこで一般に $E = 2^m$ とかけるとき L_E は奇数であることが証明できる.

実際,$L_E = \frac{Q}{2} = 2L'$ とすると$Q = 4L'$ なので

$$Q = P^E + 1 = 4L' \equiv 0 \mod 4.$$

ゆえに, $P^E \equiv -1$.

一方, $P = 2k + 1$ とおくとき

$$P^E = (2k+1)^{2^m} \equiv 1 \mod 4.$$

これで前の式に矛盾した.

$E = 2^m$ のとき $L_m = \frac{P^E+1}{2}$ とおく.

L_m は奇数であり, P を底とするフェルマー数と理解する.

素数ならP を底とするフェルマー素数といいこのとき$P^{E-1}L_E$ はP を底とするフェルマー完全数と理解する.

ただし,$P = 2$ のとき$L_m = F_m = P^E + 1, E = 2^m$ とおく.

12. オイラーの結果の一般化

L_E は奇数なのでその素因子を Q とおくと

$$P^E + 1 = 2L_E \equiv 0 \mod Q.$$

$E = 2^m$ によって

$$P^E = P^{2^m} \equiv -1 \mod Q.$$

ゆえに

$$(P^E)^2 = P^{2^{m+1}} \equiv 1 \mod Q.$$

Q を法とすると P の位数は 2^{m+1} 以下であるが $P^E = P^{2^m} \equiv -1$ によって 2^m より大なので, P の位数は 2^{m+1}.

$P^E = P^{2^m} \equiv -1 \mod Q$ により $Q \neq P$. フェルマーの小定理によって

$P^{Q-1} \equiv 1 \mod Q$. $Q - 1$ は位数 2^{m+1} の倍数なので, $Q - 1 = 2^{m+1}K$.

この結果は $P = 2$ のときオイラーによる.

13. 例

TABLE 16. $P = 2$

m	2^m	$2^{2^m}+1$	素因数分解
0	1	3	3
1	2	5	5
2	4	17	17
3	8	257	257
4	16	65537	65537
5	32	4294967297	$641 * 6700417$
6	64	18446744073709551617	$274177 * 67280421310721$
7	128	A	B
8	256	$--$	C

13.1. $P = 2$. $A = 340282366920938463463374607431768211457$

$B = 59649589127497217 * 5704689200685129054721$

$C = 1238926361552897*93461639715357977769163558199606896584051237$

$m = 5, 6, 7, 8$ について, F_m の各素因子 Q について $Q - 1$ の素因子分解を行う.

Table 17. 素因子 Q

m	Q	$Q-1$	素因数分解
5	641	640	$[2^7, 5]$
5	6700417	6700416	$[2^7, 3, 17449]$
6	274177	274176	$[2^8, 3^2, 7, 17]$
6	67280421310721	67280421310720	$[2^8, 5, 47, 373, 2998279]$
7	59649589127497217	59649589127497216	A

$A = [2^9, 116503103764643]$

$m = 0, 1, 2, 3, 4$ のときのみ素数(フェルマー素数)という予想がある.

TABLE 18. $P = 3$

m	2^m	$2L_E$	素因数分解
1	2	10	$2 * 5$
2	4	82	$2 * 41$
3	8	6562	$2 * 17 * 193$
4	16	43046722	$2 * 21523361$
5	32	1853020188851842	$2 * 926510094425921$
6	64	3433683820292512484657849089282	$2 * 1716841910146256242328924$
7	128	A	B

13.2. $P = 3$. $A = 11790184577738583171520872861412518665678211592275$

$B = 2*257*275201*1384246188687 37*391378628151452492 9*1538498348539$

$P=3$を底とするフェルマー素数は
5,41,21523361,92651009442592 1,1716841910146256242328924544641.
とりあえず5個あるのが不思議.
５を除くと末尾は1.

```
?- A is 17,B is A-1,factorize(B,C),exps(C,D).
A = 17,
D = [2^4].

?- A is 193,B is A-1,factorize(B,C),exps(C,D).
A = 193,
D = [2^6, 3].
?- A is 257-1,factorize(A,B), exps(B,C).
A = 256,
C = [2^8].

 ?- A is 275201-1,factorize(A,B), exps(B,C).
A = 275200,
C = [2^8, 5^2, 43].

 ?- A is 138424618868737-1,factorize(A,B), exps(B,C).
```

```
?- A is 39137862815145249291,factorize(A,B), exps(B,C).
A = 3913786281514524928,
C = [2^8, 31, 787, 3919, 159898891].

?- A is 153849834853910661121-1,factorize(A,B), exps(B,C).
A = 153849834853910661120,
C = [2^11, 3, 5, 433, 19801, 584118287].
```

これらは数値例とはいえ,実に見事な美しい結果である.

TABLE 19. $P = 5$

m	2^m	$2L_E$	素因数分解
1	2	26	$2 * 13$
2	4	626	$2 * 313$
3	8	390626	$2 * 17 * 11489$
4	16	152587890626	$2 * 2593 * 29423041$
5	32	23283064365386962890626	$2 * 641 * 75068993 * 2419310016 01$
6	64	A	$2 * B$

13.3. $P = 5$. $A = 542101086242752217003726400434970855712890626$

$B = 769 * 3666499598977 * 96132956782643741951225664001$

$P = 5$を底とするフェルマー素数は 13,313.

$m = 3, m + 1 = 4, 2^4 = 16.$

```
13 ?- A is 17,B is A-1,factorize(B,C),exps(C,D),write((A,B,D
17,16,[2^4]
A = 17,
B = 16,
D = [2^4].

8 ?- A is 11489,B is A-1,factorize(B,C),exps(C,D),write((A,B
11489,11488,[2^5,359]
A = 11489,
B = 11488,
D = [2^5, 359].

9 ?- A is 2593,B is A-1,factorize(B,C),exps(C,D),write((A,B,
2593,2592,[2^5,3^4]
A = 2593,
```

```
10 ?- A is 641,B is A-1,factorize(B,C),exps(C,D),write((A,B,
641,640,[2^7,5]
A = 641,
B = 640,
C = [2, 2, 2, 2, 2, 2, 2, 5],
D = [2^7, 5].

11 ?- A is 75068993,B is A-1,factorize(B,C),exps(C,D),write(
75068993,75068992,[2^6,1172953]
A = 75068993,
B = 75068992,
C = [2, 2, 2, 2, 2, 2, 1172953],
D = [2^6, 1172953].

12 ?- A is 241931001601,B is A-1,factorize(B,C),exps(C,D),wr
241931001601,241931001600,[2^8,3^2,5^2,23,182617]
```

TABLE 20. $P = 7$

m	2^m	$2L_E$	素因数分解
1	2	50	$2 * 5^2$
2	4	2402	$2 * 1201$
3	8	5764802	$2 * 17 * 169553$
4	16	33232930569602	$2 * 353 * 47072139617$
5	32	1104427674243920646305299202	$2 * 7699649 * 134818753 * 53196866$
6	64	A	$2 * B$

13.4. $P = 7$. $A = 12197604876358357001385738625629718207556152941312$
$B = 35969*1110623386241*1526684819679355609808500033288863436 9$

```
14 ?- A is 353,B is A-1,factorize(B,C),exps(C,D),write((A,B,
353,352,[2^5,11]
A = 353,
B = 352,
D = [2^5, 11].

15 ?- A is 47072139617,B is A-1,factorize(B,C),exps(C,D),wri
47072139617,47072139616,[2^5,67,1847,11887]
A = 47072139617,
B = 47072139616,
D = [2^5, 67, 1847, 11887].

16 ?- A is 7699649,B is A-1,factorize(B,C),exps(C,D),write(C
7699649,7699648,[2^6,11,10937]
A = 7699649,
B = 7699648,
```

TABLE 21. $P = 11$

m	2^m	$2L_E$	素因数分解
1	2	122	$2 * 61$
2	4	14642	$2 * 7321$
3	8	214358882	$2 * 17 * 6304673$
4	16	459497298635721 62	$2 * 51329 * 447600088289$

13.5. $P = 11$.

```
17 ?- A is 6304673,B is A-1,factorize(B,C),exps(C,D),write(
6304673,6304672,[2^5,11,17911]
A = 6304673,
B = 6304672,
D = [2^5, 11, 17911].

18 ?- A is 51329,B is A-1,factorize(B,C),exps(C,D),write((A,
51329,51328,[2^7,401]
```

```
A = 447600088289,
B = 447600088288,
D = [2^5, 127, 110137817].
```

14. フェルマーの完全数の方程式

$e = 2^m - 1$ とおき, $q = \frac{P^{e+1}+1}{2}$ は素数とする. $a = P^e q$ は P を底とするフェルマーの完全数である.

これの満たす方程式を求める.

$e = 2^m - 1$ とおき, $q = \frac{P^{e+1}+1}{2}$ は素数とする. $a = P^e q$ は P を底とするフェルマーの完全数である.

これの満たす方程式を求める.

$P^{e+1} + 1 = 2q$ により,$2q + 2 = P^{e+1} + 3$. さらに $\sigma(a) = \frac{P^{e+1}-1}{\overline{P}}(q+1)$ によって

$$\begin{aligned}
\overline{P}\sigma(a) &= (P^{e+1} - 1)(q+1) \\
&= (2q-2)(q+1) \\
&= 2q(q+1) - 2(q+1) \\
&= q(P^{e+1} + 3) - 2(q+1) \\
&= qP^{e+1} + q - 2
\end{aligned}$$

よって,

$$\overline{P}\sigma(a) - aP = q - 2.$$

$\overline{P}\sigma(a) - aP = Maxp(a) - 2$ がP を底とするフェルマーの完全数の方程式である.

14.1. **例.**

14.2. $P=3$ **のとき.** $P=3$ のとき$2\sigma(a)-3P=Maxp(a)-2$ が3 を底とするフェルマーの完全数の方程式である.

この方程式の完全な解を得たい. これは無理な願望であろう.

TABLE 22. $P=3$

a	素因数分解
15	$3*5$
741	$3*13*19$
1107	3^3*41
14883	$3*11^2*41$
38781	$3^2*31*139$

$s(a)=2$ に限ると, $a=15=3*5$,$a=1107=3^3*41$ の 2 例のみ.

さらに多くの解を得るため$a=3^eqr$ の解を探すことが策

$a = 3^e qr, (3 < q, r)$ とおくと

$$(3^{e+1} - 1)(qr + \Delta + 1) - 3^e qr = r - 2.$$

$\Delta = q + r, \Gamma = 3^{e+1} - 1, D = \Gamma^2 + 2$

TABLE 23. $p = 3; 3^e qr$

a	素因数分解	$\sigma(a)$
741	$3^1 * 13 * 19$	1120
38781	$3^2 * 31 * 139$	58240
4954286665155815901	$3^{11} * 536917 * 52088299$	7431429997759768000

14.3. $P=5$ のとき. $P=5$ のとき $4\sigma(a)-5P=Maxp(a)-2$ が3 を底とするフェルマーの完全数の方程式である.

TABLE 24. $p=5$

a	素因数分解
65	$5*13$
14861	$7*11*193$
39125	5^3*313

$s(a)=2$ に限ると, $a=65=5*13$,$a=39125=5^3*313$ の２例のみ.

TABLE 25. $p=7$

a	素因数分解
411943	7^3*1201

14.4. $P=7$ のとき.

TABLE 26. $P = 11$

a	素因数分解
671	$11 * 61$
861773	$11 * 157 * 499$

14.5. $P = 11$ のとき.

TABLE 27. $p = 19$

a	素因数分解
3439	$19 * 181$

14.6. $P = 19$ のとき.

15. $a = P^e qr$ の解

$\overline{P}\sigma(a) - aP = Maxp(a) - 2$ の解$a = P^e qr$ があるとする.

$$(P^{e+1} - 1)\widetilde{qr} - P^{e+1}qr = r - 2$$

を得るので $\Gamma = P^{e+1} - 1, \Delta = q + r$ を用いると

$$\Gamma(qr + \Delta + 1) - (\Gamma + 1)qr = r - 2.$$

これより, $\Delta' = \widetilde{q} + r = \Delta + 1$ によって

$$\Gamma\Delta' = \widetilde{q}r - 2.$$

$\widetilde{q}_0 = \widetilde{q} - \Gamma, r_0 = r - \Gamma, D = \Gamma^2 + 2$ によれば

$$\widetilde{q}_0 r_0 = D.$$

これによって, 与えられた $\Gamma = P^{e+1} - 1$ について, D の因子分解 $\widetilde{q}_0 r_0$ を求め $q = \widetilde{q}_0 - 1 + \Gamma, r = r_0 + \Gamma$ がともに素数なら $a = P^e qr$ が解である.

その結果,得られた解は $P = 3$ のときの と

TABLE 28. $P = 3$

a	素因数分解
741	$3^1 * 13 * 19$
38781	$3^2 * 31 * 139$
49542866651558159 01	$3^{11} * 536917 * 52088299$

$P = 11$ のとき

TABLE 29. $P = 11$

a	素因数分解
861773	$11^1 * 157 * 499$
18850718310561181	$11^4 * 164431 * 7830211$

だけだった.少し残念である.