原始根と位数の関係

A Relationship between a Primitive Root and a Multiplicative Order

渋 田　昌 士　　Masashi Shibuta

はじめに

現在の暗号技術は, 桁数の多い数の素因数分解が比較的困難であることに基づいている. そこで, 素因数分解がどれほど困難であるのかを研究することにより, 現在の暗号技術の脆弱性を指摘できるほか, 新たな暗号技術の基礎が見えてくるものと思われる.

今研究では, フェルマー数の素因数分解についての研究の過程でみえてきた, 原始根と位数の間にある関係性を証明した内容となっている. 具体的には, ある素数 p の原始根の 1 つ r を利用することで r 以外の位数がわかるという内容となっている. また $a,\ k \in \mathbb{N}$ を, $1 \leq a,\ k \leq p-1$ の範囲で考えたとき,$a^k \equiv n \pmod{p}$ で表される n は, $1 \leq n \leq p-1$ の範囲で,$(p-1)^2$ 個作られる. よってこの n は同じ値を何度かとることとなり,n の重複数についても触れている.

フェルマー数の素因数分解について, 筆者は 2 の位数が関係していると予想を立てている. そのため今回の位数を算出する方法は非常に貴重なものであり, 今後の研究を進める上でかなり重要なものとなるはずである.

1　原始根と位数の関係について

1.1　原始根と位数の関係

ある素数 p の原始根の一つ r について考えるとき, $\{r^1,\ r^2,\ \ldots,\ r^{p-1}\} \pmod{p}$ は, $\{1,\ 2,\ \ldots,\ p-1\}$ に 1 対 1 の上への写像となる.

例えば $p = 13$ に対し, 2 は原始根の 1 つで, それの累乗と $\pmod{13}$ の関係は, 以下のようになる.

$$2^1 \equiv 2 \pmod{13}$$
$$2^2 \equiv 4 \pmod{13}$$

$$
\begin{aligned}
2^3 &\equiv 8 \pmod{13}\\
2^4 &\equiv 3 \pmod{13}\\
2^5 &\equiv 6 \pmod{13}\\
2^6 &\equiv 12 \pmod{13}\\
2^7 &\equiv 11 \pmod{13}\\
2^8 &\equiv 9 \pmod{13}\\
2^9 &\equiv 5 \pmod{13}\\
2^{10} &\equiv 10 \pmod{13}\\
2^{11} &\equiv 7 \pmod{13}\\
2^{12} &\equiv 1 \pmod{13}
\end{aligned}
$$

これをを $2^k \equiv n \pmod{13}$ としたとき, $k \longrightarrow n$ の写像を置換 $\sigma_{13(2)}$ とすると,

$$
\sigma_{13(2)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 4 & 8 & 3 & 6 & 12 & 11 & 9 & 5 & 10 & 7 & 1 \end{pmatrix}
$$

これは 1 対 1 の上への写像となるので, 逆写像を置換 $\sigma_{13(2)}^{-1}$ とすると,

$$
\sigma_{13(2)}^{-1} = \begin{pmatrix} 2 & 4 & 8 & 3 & 6 & 12 & 11 & 9 & 5 & 10 & 7 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{pmatrix}
$$

これを並べ替えて,

$$
\sigma_{13(2)}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 1 & 4 & 2 & 9 & 5 & 11 & 3 & 8 & 10 & 7 & 6 \end{pmatrix} \tag{1}
$$

さらに, $\sigma_{13(2)}^{-1}(k)$ と $p-1$ との最大公約数を求める写像, つまり $n \longrightarrow \gcd(p-1,\ k)$ は,

$$\tau_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 1 & 4 & 2 & 3 & 1 & 1 & 3 & 4 & 2 & 1 & 6 \end{pmatrix} \tag{2}$$

これは p の原始根ならば, 今回例にとった 2 に限らず全く同じ数列になる．よって τ の添え字を 13 のみにしている．

そして, $\tau_{13}(a)$ は, $a^k \equiv 1 \pmod{13}$（$a, k \in \mathbb{N}$, $1 \leq a$,$k \leq p-1$）を満たす k が何個存在するかを表している．つまり, a を 1 乗から $p-1$ 乗するまでに, 同じ剰余が何度現れるかを示している．したがって $p-1$ を $\tau_{13}(a)$ で割ると法 p に関しての a の位数を求めることができる．この置換を υ_{13} とすると,

$$\upsilon_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 12 & 3 & 6 & 4 & 12 & 12 & 4 & 3 & 6 & 12 & 2 \end{pmatrix} \tag{3}$$

また,13 を法としたときの余りの計算を下記の表 1 に表している．表 1 は横軸は底 (a), 縦軸は指数 (k) としてある．確認のため $\upsilon_{13}(a)$ を 2 行目に表示してあり, それぞれの列で最初に 1 となるところ (位数) には, 1 を○で囲んで表示してある．

$a =$	1	2	3	4	5	6	7	8	9	10	11	12
$\tau_{13}(a)$	1	12	3	6	4	12	12	4	3	6	12	2
$k =$ 1	①	2	3	4	5	6	7	8	9	10	11	12
2	1	4	9	3	12	10	10	12	3	9	4	①
3	1	8	①	12	8	8	5	5	①	12	5	12
4	1	3	3	9	①	9	9	①	9	3	3	1
5	1	6	9	10	5	2	11	8	3	4	7	12
6	1	12	1	①	12	12	12	12	1	①	12	1
7	1	11	3	4	8	7	6	5	9	10	2	12
8	1	9	9	3	1	3	3	1	3	9	9	1
9	1	5	1	12	5	5	8	8	1	12	8	12
10	1	10	3	9	12	4	4	12	9	3	10	1
11	1	7	9	10	8	11	2	5	3	4	6	12
12	1	①	1	1	1	①	①	1	1	1	①	1

表 1　13 を法とした場合の位数の確認

ここで一度まとめてみると, 法 p に関して, 底が a, 指数が k, 剰余が n でる. したがって,

$$a^k \equiv n \pmod{p}$$

であるが, 今 a の位数 $\mathrm{Ord}(a)$ を求めるときに, $a = n$ として位数を求めていることに気づく.
したがって, 以下の式では n を底として扱う説明となっていることに注意されたい.

ある p の原始根の 1 つ r を k 乗したときの剰余 n は,

$$r^k \equiv n \pmod{p}$$

となるが, これの対数を取って

$$k = \log_r n \pmod{p}$$

と表現することにする．剰余の世界では，対数を計算することができないが，ここでは原始根の 1 つがわかっていて，その原始根の累乗の剰余もわかっているものと仮定し，式 (1) のような置換を用いて計算ができるものとして話を進める．

そうすると，法 p に関して n の位数 $\mathrm{Ord}(n)$ を求める式は，

$$\mathrm{Ord}(n) = \frac{p-1}{\gcd(p-1,\ \log_r n)} \pmod{p} \tag{4}$$

のように表すことができる．そして $\mathrm{Ord}(n) = p-1$ となる n は p の原始根となる．

式 (4) から，$n \longrightarrow \mathrm{Ord}(n)$ を計算する置換 υ_{13} を求めると，

$$\upsilon_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 12 & 3 & 6 & 4 & 12 & 12 & 4 & 3 & 6 & 12 & 2 \end{pmatrix} \tag{5}$$

となり式 (3) と一致する．また $\mathrm{Ord}(n) \pmod{p}$ のとる値は $p-1$ の約数の値になっていることに気づく．

1.2 剰余の個数

ある素数 p を法として，$a,\ k \in \mathbb{N}$ を，$1 \leq a,\ k \leq p-1$ の範囲で考えたとき，

$$a^k \equiv n \pmod{p}$$

となる n がとりうる範囲は $1 \leq n \leq p-1$ であり最大 $p-1$ 種類の n が存在する．a が 1 から $p-1$ まで変化し，その間に k も 1 から $p-1$ まで変化するので，その組み合わせは，

$$(a,\ k) = \{(1,\ 1),\ (1,\ 2),\ \ldots,\ (p-1,\ p-1)\}$$

となり，$(p-1)^2$ 通りになるので，同じ n がいくつか重複して現れることがわかる．この重複数を O_n とおく．

ここで法 p に関して $\{n \in \mathbb{N} \mid 1 \leq n \leq p-1\}$ の位数 $d = \mathrm{Ord}(n)$ について，d の倍数でありかつ $p-1$ の約数でもあるものの集合を $\{t_1,\ t_2,\ \ldots,\ t_m\}$ とする．

$(a,\ k) = \{(1,\ 1),\ (1,\ 2),\ \ldots,\ (p-1,\ p-1)\}$ を取るときに $a^k \equiv n \pmod p$ となる $(a,\ k)$ の組み合わせの数 O_n は,

$$O_n = \sum_{i=1}^{m} \phi(t_i) \frac{p-1}{t_i}$$

と表せる. [*1]

例えば, 法 13 に関して, $(a,\ k) = \{(1,\ 1),\ (1,\ 2),\ \ldots,\ (12,\ 12)\}$ で $a^k \equiv n \pmod p$ を計算した場合, $n = 3$ となる $(a,\ k)$ の組み合わせの数 O_3 を計算する.

まず式 (3) より法 13 に関する 3 の位数 $\mathrm{Ord}(3)$ を求める.

$$\mathrm{Ord}(3) = 3$$

さらに, $p - 1 = 12$ の約数は $\{1,\ 2,\ 3,\ 4,\ 6,\ 12\}$ であり, この中で 3 の倍数となるのは $t_m = \{3,\ 6,\ 12\}$ なので,

$$O_3 = \sum_{i=1}^{3} \phi(t_i) \frac{13-1}{t_i}$$

$$O_3 = (3-1) \cdot \frac{12}{3} + (3-1) \cdot (2-1) \cdot \frac{12}{6} + (3-1) \cdot (2^2-2) \cdot \frac{12}{12} = 16$$

16 個現れる. 実際の計算を以下の表 2 で確認する. なお横軸は底 (a), 縦軸は指数 (k) としている. また確認しやすいよう 3 は ③ と○付きで表示してある.

[*1] $\phi(n)$ は, オイラーのトーシェント関数を現す

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	③	4	5	6	7	8	9	10	11	12
2	1	4	9	③	12	10	10	12	③	9	4	1
3	1	8	1	12	8	8	5	5	1	12	5	12
4	1	③	③	9	1	9	9	1	9	③	③	1
5	1	6	9	10	5	2	11	8	③	4	7	12
6	1	12	1	1	12	12	12	12	1	1	12	1
7	1	11	③	4	8	7	6	5	9	10	2	12
8	1	9	9	③	1	③	③	1	③	9	9	1
9	1	5	1	12	5	5	8	8	1	12	8	12
10	1	10	③	9	12	4	4	12	9	③	10	1
11	1	7	9	10	8	11	2	5	③	4	6	12
12	1	1	1	1	1	1	1	1	1	1	1	1

表 2　13 を法とした場合の剰余

2　フェルマー数の素因数分解の考察

2.1　フェルマー数の素因数

まずフェルマー数 F_n が素因数分解できるとき，その素因数は n を用いて

$$k \cdot 2^{n+1} + 1 \quad (k \in \mathbb{N})$$

の形をとることがオイラーによって明かされた．以下に証明をする．

証明． p が $F_n = 2^{2^n} + 1$ の約数であると仮定して，

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

両辺 2 乗して

$$2^{2^{n+1}} \equiv 1 \pmod{p}$$

ここで，$2^x \equiv -1 \pmod{p}$ を満たす x で最小のものを g とすると，x は g の奇数倍となる．

そうすると，もし 2^n 以外に $2^x \equiv -1 \pmod{p}$ を満たす x で最小となる値 g が存在すると仮定すると，2^n が g の奇数倍になることはない．したがって g が最小の値であるという仮定は矛盾する．

よって，2^n は $2^x \equiv -1 \pmod{p}$ を満たす x の中で最小の値である．

したがって，2^{n+1} は法 p に関する 2 の位数となる．

またフェルマーの小定理より，

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

よって，$p-1$ は位数の整数倍となるので，

$$p - 1 = k \cdot 2^{n+1}$$
$$p = k \cdot 2^{n+1} + 1 \tag{6}$$

□

このことにより，比較的フェルマー数の番号が大きい数であっても，k が小さい素因数であれば，かなり早い時代に素因数がわかっているものもある．

2.2　フェルマー数の素因数分解の考察

RSA など現代の暗号技術には, 多くの整数論が用いられている．そしてその核となっている部分が, 大きな数は素因数分解することが困難, というところに起因している．

しかし現代のコンピュータの進歩には目覚ましいものがあり, 俗に言う「力技」でどんどんこの困難な素因数分解を可能なものとしている．そうなれば今度は現在の「力技」では解決できないほど大きい数字に変えていく．この繰り返しのように思える．

そもそも, 素因数分解が多項式時間で行えるようなアルゴリズムが存在すれば, RSA など公開鍵暗号の脆弱性を指摘することができ, より強固な暗号技術の開発が進むと考えられる．

現段階では, フェルマー数に限って素因数分解の新しいアルゴリズムを研究中であり．

まずフェルマー数 F_n が素因数分解できるとき, その素因数は n を用いて

$$k \cdot 2^{n+1} + 1 \qquad (k \in \mathbb{N})$$

の形をとることがオイラーによって明かされた．

筆者もフェルマー数の素因数分解には素因数 p を法とした 2 の位数 e が判ればよいという予想を立てたが, では位数 e はどのように求められるのであろうか．それについても, 本論文の 1.1 節の『原始根と位数の関係』の中で触れている．

その内容は, 法 p に関する原始根の 1 つ r を利用し,

$$\mathrm{Ord}(2) = \frac{p-1}{\gcd(p-1,\ \log_r 2)} \qquad (\mathrm{mod}\ p)$$

で求められる．ただし, 剰余の世界では対数を計算することは, 現在不可能であるので, ここは置換数列を用いてクリアすることを提案する．

これであとは, 原始根を求められれば, フェルマー数 F_n の素因数であるかどうかの確認ができる, というのが本論文の提案である．

途中数学的証明が追い付かないところや, 少々無理のある証明をせざるを得ないのが現状ではあるが, ある程度の数で確認してあることなので, 相当の自信をもって提案している．

ただ整数論では, 相当大きな数で矛盾や反例が出てくることはしばしばあるので, 今後は数学的に証明していきこの提案を確実な定義と変えていきたいと考えている．

参考文献

1) Paulo Ribenboim :『素数の世界－その探索と発見（第 2 版)』(吾郷　孝視訳)、共立出版、2001
2) 小林　昭七 :『なっとくするオイラーとフェルマー』、講談社、2003
3) 結城　浩 :『新版暗号技術入門－秘密の国のアリス』、ソフトバンク　クリエイティブ株式会社、2008
4) 遠山　啓 :『初等整数論』、日本評論社、1972
5) 新妻　弘 :『演習群・環・体入門』、共立出版、2000
6) イアン・スチュアート :『解明ガロア理論（原著第 3 版)』(並木　雅俊・鈴木　治郎訳)、講談社サイエンティフィク、2008
7) 永原　賢・本瀬　香 :『代数的整数論入門』、学術図書出版社、1998
8) S.C. コウチーニョ :『暗号の数学的基礎－数論と RSA 暗号入門』(林　彬訳)、シュプリンガー・フェアラーク東京、2001
9) 井田　哲雄・浜名　誠 :『計算モデル論入門－チューリング機械からラムダ計算へ』、サイエンス社、2006
10) 米田　政明・広瀬　貞樹・大里　延康・大川　知 :『オートマトン・言語理論の基礎』米田政明監修、近代科学社、2003
11) 奥村　浩士 :『電気電子情報のための線形代数』、朝倉書店、2015
12) 佐藤　泰介・高橋　篤司・伊東　利哉・上野　修一 :『情報基礎数学』、オーム社、2014
13) 陳　慰・和田　幸一 :『情報工学レクチャーシリーズ離散数学』、森北出版、2014
14) 「Fermat factoring status」<http://www.maths.dur.ac.uk/users/dzmitry.badziahin/Fermat% 20factoring% 20status.html>