擬似素数と素数判定テスト

青山学院大学 理工学部 物理・数理学科
15108078 松隈 大輔

2012.02.22

1　プロローグ

この論文では素数判定テストを基に、整数の性質を探る。ある巨大な数が素数であるかどうかは、現在インターネットなどで広く使われているRSA暗号系で大変重要な役割を担っているので、このような整数の性質は応用面からも重要である。

この論文では$\mathbb{P} = \{2, 3, 5, 7, \cdots\}$で素数の集合を表す。以下に出てくる変数は特に断らない限り0以上の整数を表す。

ある数nが素数であるかどうかの判定法は様々あるが、本論文では次のフェルマーの小定理を用いた素数判定法について考える。

定理 1.1 (**フェルマーの小定理**)**.** p を素数とし、a を 整数とする。このとき任意のa に対して

$$a^p \equiv a \pmod{p} \tag{1.1}$$

が成り立つ。

この定理を利用したnの素数判定テストを紹介する。

定義 1.2. (**カーマイケル指数**) 正の整数nに対して

$$N(n) = \#\{0 \leq a < n : a^n \equiv a \pmod{n}\}$$

とおき、これをカーマイケル指数と呼ぶ。

定理 1.3. 正の整数nに対して

カーマイケル指数$N(n) \neq n$ならば$n \notin \mathbb{P}$である。

この定理はフェルマーの小定理から容易に従うが、後述するように逆は真でない。

定理 (1.3) を用いて$N(n)$計算する。$N(n) \neq n$ならnは素数ではないので、nの素数性を判定できる。これを仮に**素数判定テスト**と呼ぶ。この素数判定テストを徐々に大きな数nで試していくと、途中で合成数であるにもかかわらず、$N(n) = n$となる数が出てくる。このような数をカーマイケル数 (擬似素数) と定義する。つまりカーマイケル数は素数判定テストをパスするような数である。

定義 1.4. $n \geq 2$ が**カーマイケル数**とは次の条件を満たすときに言う。

1. $n \notin \mathbb{P}$ つまり n は合成数である。

2. $\forall a \in \mathbb{Z}$ に対して $a^n \equiv a \pmod{n}$ が成り立つ。

最小のカーマイケル数は 561 であることが知られている [1, p.122]。561 までの素数は 102 個あるので [1, p.409]、カーマイケル数は“ まれ ”にしか存在しないことが分かる。

カーマイケル数、つまりカーマイケル指数 $N(n)$ が n に一致する合成数は素数に非常によく似ている合成数である。$a = 0, 1$ の時 $a^n \equiv a \pmod{n}$ となるのは明らかだから、任意の整数 $n \geq 2$ に対して、カーマイケル指数 $N(n)$ は 2 以上である。したがって、$N(n) = 2$ となる数は最も合成数の性質が強く出ている数と言うことができる。卒業研究では、シルヴァーマン著「はじめての数論」を読み $N(n) = n - 1$(カーマイケル数になりかけた数) や $N(n) = 2$ となる数が存在するかどうかに興味をもった。そこで、数式処理ソフトの Mathematica を用い調べてみることにした。この論文では、その過程で発見した 4 つの数の性質について理論的に述べる。

例として特徴的な $a^n \pmod{n}$ の値を以下に表としてまとめておく。

a	0	1	2	3	4
$a^{15} \pmod{15}$	0	1	8	12	4
a	5	6	7	8	9
$a^{15} \pmod{15}$	5	6	13	2	9
a	10	11	12	13	14
$a^{15} \pmod{15}$	10	11	3	7	14

表 1: $n = 15$ のとき

表 1, 2 の他、多数の例を観察すると次のような予想が得られる。

予想 1. p を 3 以上の素数とし、$n = 3 \cdot p$ とする。このとき

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

となる a はすべて

$$a \equiv -1, 0, 1 \pmod{p}$$

を満たす。

a	0	1	2	3	4	5	6
$a^{21} \pmod{21}$	0	1	8	6	1	20	6
a	7	8	9	10	11	12	13
$a^{21} \pmod{21}$	7	8	15	13	8	6	13
a	14	15	16	17	18	19	20
$a^{21} \pmod{21}$	14	15	1	20	15	13	20

表 2: $n = 21$ のとき

a	0	1	2	3	4	5	6	7	8
$a^9 \pmod{9}$	0	1	8	0	1	8	0	1	8

表 3: $n = 9$ のとき周期 $T = 3$

a	0	1	2	3	4	5	6	7	8	9	10	11
$a^{12} \pmod{12}$	0	1	4	9	4	1	0	1	4	9	4	1

表 4: $n = 12$ のとき周期 $T = 6$

この予想はフェルマーの小定理、中国剰余定理を用いて証明することができる。正確な主張とその証明については第 5 章、定理 5.1 を参照して欲しい。

予想を $n = 3 \cdot p^k$ のときに一般化することもできるが、$k = 2$ のとき、オイラーの公式と中国剰余定理を用いて予想を証明することができる (定理 5.2)。

次に表 3, 4 を観察すると次のような予想を得る。

予想 2. p と q を素数、k を 1 以上の整数とする。

1. $n = p^k$ のとき、数列 $\{a^n \pmod{n} : a = 0, 1, 2, \ldots, n-1\}$ は周期 p を持つ
2. $n = p^k \cdot q$ のとき、数列 $\{a^n \pmod{n} : a = 0, 1, 2, \ldots, n-1\}$ は周期 pq を持つ

この予想も二項定理と中国剰余定理を利用して証明することができた (第 6 章の定理 6.1,6.2 参照)。

本論文の構成は次のようになっている。

§2 では素数の実用例として RSA 暗号について述べる。§3 ではカーマイケル数とその性質を紹介する。§4 では素数判定に用いた Mathematica のプログラムについて解説する。§5 では予想 1 とその一般化の証明をする。§6 では予想 2 を証明する。§7 はまとめである。

2 RSA 暗号

この章では「はじめての数論」[1] に基づいて RSA 暗号の概略を解説する。RSA 暗号の理論をこの後の章で直接扱うわけではないが、この章で紹介する整数の性質は後の章でも必要である。また、研究のきっかけをこの暗号理論を学ぶ過程で得たものである。

2.1 RSA 暗号とは?

RSA 暗号とは、大きい数同士の積を計算することは簡単でも、極めて大きい数の素因数分解は困難であることを根拠とした暗号理論である。

$$p, q : \text{素数} \quad \overset{\text{積:簡単}}{\underset{\text{因数分解:困難}}{\rightleftarrows}} \quad n = p \cdot q$$

この暗号理論は現在インターネットの電子証明書での標準的な公開鍵暗号として利用されている [3, 64 ページ]。以下に RSA 暗号系の手順を簡単に紹介する。

2.2 RSA 暗号のしくみ

暗号には、情報の送り手 (**送信者**) と受け手 (**受信者**) が存在する。情報を解読されることなく、秘密裏に送るためには古来、暗号を解く鍵となる情報を秘密にするのが普通であった (**秘密鍵**)。しかし RSA 暗号においてはこの暗号解読のための鍵を公開するのが特色である。これを**公開鍵**と呼ぶ。

ここで、RSA 暗号を使用するにあたり、フェルマーの小定理を一般化したオイラーの公式、並びにオイラー関数を紹介する [1, p.65,66,70]

定義 2.1. (**オイラー関数**)1 から n の間で n と互いに素な整数の個数を

$$\phi(n) = \#\{a : 1 \leq a \leq n, \gcd(a, n) = 1\} \tag{2.1}$$

と書いて、$\phi(n)$ をオイラー関数と呼ぶ。

定理 2.2 (オイラー関数の性質)**.**

1. $\gcd(m, n) = 1$ のとき

$$\phi(mn) = \phi(m)\phi(n) \tag{2.2}$$

が成り立つ。

2. p が素数であり $k \geq 1$ とするとき

$$\phi(p^k) = p^k - p^{k-1} \tag{2.3}$$

が成り立つ。

上のような性質を持つ関数を数論的関数という。オイラー関数は重要な数論的関数の一つである。

定理 2.3 (**オイラーの公式**)**.** $\gcd(a, n) = 1$ のとき

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{2.4}$$

が成り立つ。但し、$\gcd(a, n)$ は a と n の最大公約数を表す。

これはフェルマーの小定理の一般化になっている。実際、$\phi(p) = p - 1$ だから a と p が互いに素であれば

$$a^{p-1} \equiv 1 \pmod{p} \Leftrightarrow a^p \equiv a \pmod{p} \tag{2.5}$$

である。

2.2.1 公開鍵作成

まず、メッセージ受信者は公開鍵を作成する。2 つの極めて大きな素数 p と q をとり、これらを掛け合わせて数

$$n = p \cdot q \tag{2.6}$$

を得る。コンピュータ・ソフトウェアにおける完装では、極めて大きな素数 p, q を生成する方法として、適当な巨大な数 p を用意し $N(p) = p$ となれば素数であるとみなすことが多い[1]。このとき、p がカーマイケル数である可能性も否定できないのだが、そのような確率は低いので無視してしまうのである。

このように n を定めると、オイラー関数の性質より

$$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) \tag{2.7}$$

を得る。次に、$\phi(n)$ と互いに素な数 k を選ぶ。受信者はこの 2 つの数の組 (n, k) を公開鍵として公表する。p と q は公開してはならない。メッセージ送信者は、この公開鍵をもとにメッセージを作成することになる。

2.2.2 暗号作成

暗号作成の最初のステップはメッセージを数の列に変換して暗号化することである。例えばアルファベットに数字を当てはめて

$$\text{A=11, B=12, } \ldots \text{, Z=36}$$

とおく。例として

$$\text{“ To be or not to be ”}$$

というメッセージを暗号化してみよう。“ To be or not to be ”は数字に変換すると

T	O	B	E	O	R	N	O	T	T	O	B	E
30	25	12	15	25	28	24	25	30	30	25	12	15

となる[2]。よってメッセージは数の列

$$\text{“ 3025121525282425303025 1215 ”}$$

に変換される。このような単純な符号化は、一種の暗号と呼べないこともないが、このような暗号では数分もあれば解けてしまう。そこで、この数のメッセージを RSA 暗号理論に基づき、さらに暗号化する。

まず、数の列を n 未満になるように区切る。例えば n が百万くらいの数であれば 6 桁ごとに区切る。このときメッセージは数のリスト $a_1, a_2, a_3, \cdots, a_r$ となる。次に**繰り返し乗法** [1, p.105] を使い

[1] 実際には簡単に推測されないような素数を選ぶためにさらに工夫が必要である。
[2] ここでは大文字、小文字を区別しない。また、空白は省いて考えることにする。

$$a_1^k \pmod n, \quad a_2^k \pmod n, \quad \cdots, \quad a_r^k \pmod n$$

を計算する。得られた値を $b_1, b_2, \cdots, b_r$ とし新たな数の列 $b_1, b_2, \cdots, b_r$ を得る。これにて暗号化は完了。

2.2.3 暗号の復号化

メッセージ受信者は受け取った数の列

$$b_1, b_2, \cdots, b_r$$

をもとの数の列

$$a_1, a_2, \cdots, a_r$$

に複号化する。

$$b_i \equiv a_i^k \pmod n \quad (i = 1, 2, \cdots, r)$$

であった。この b_i から a_i を複号するためには

$$b_i^u = (a_i^k)^u \equiv a_i \pmod n$$

となるような u が見つけられれば良いが、このような u はユークリッドの互除法を用いて計算できる。以下に計算アルゴリズムを書く。ここで、**$\phi(n)$ の値が必要になる。**

復号化の計算アルゴリズム まず

$$\gcd(k, \phi(n)) = 1$$

であることに注意する。

$$b \equiv a^k \pmod n$$

とする。

1. ユークリッドの互除法 [1, p.30] を用いて 方程式 $ku - \phi(n)v = 1$ を満たす正の整数解 u, v を見つける。
2. $b^u \pmod n$ を繰り返し自乗法で計算する。
3. $b^u = (a^k)^u = a^{ku} = a^{\phi(n)v+1} \equiv a \pmod n$ となって、b^u は n を法として a と一致する。

このようにして、b_iから b_i^u を計算することで a_i を復号化できる。

2.3 RSA 暗号の安全性

法 n と数 k は公開されているので、誰でも知ることができる。しかし、暗号化されたメッセージが第三者の手に渡ったとしても、今のところ、RSA 暗号を復号する唯一の方法は **$\phi(n)$ の値を計算することのみ**である。しかし、n の値だけから $\phi(n)$ を計算することは非常に難しい。それを説明しよう。

n が 2 つの素数 p と q の積であるとき

$$\begin{aligned}\phi(n) =& \phi(p)\phi(q) = (p-1)(q-1)\\ =& pq - p - q - 1 = n - p - q - 1\end{aligned}$$

であった。

n の値はすでに分かっているので、$p+q$ の値が分かれば $\phi(n)$ がわかってしまう。ここで
X の二次方程式

$$X^2 - (p+q)X + n = 0 \qquad (n = p \cdot q)$$

について考える。この式の解は $X = p, q$ であり、$(p+q)$ の値が分かれば比較的簡単に p と q の値も計算でき、p と q の値が計算出来れば $(p+q)$ の値が計算できる。このことは **$\phi(n)$ を計算することと n を素因数分解することがほぼ同程度の困難さを持つことを示す。**よって暗号を復号するためには n を素因数分解しなければならない。

n がそんなに大きな数でなく 5〜10 桁ならばコンピュータは直ちに素因数を見つける。数論を活用した高度な方法を使えば 50〜100 桁の数でも素因数分解が可能である。例えば 1977 年に 2 進数で 129 桁の鍵を使った RSA 方式で暗号化された懸賞金問題が、出題から 17 年たって解読された (引用：wikipedia)。素因数分解よって、素数 p と q を 50 桁より小さくとると、その暗号は安全ではない。しかし、p と q を 2 進数で 200 桁を超える素数をとれば、選んだ p と q を明らかにしない限り、素因数分解を実行することは容易ではなく、その暗号は安全である。

3 カーマイケル数の性質

前章より、極めて大きな素数を知ることは実用面からも RSA 暗号系を使う時に重要な役割を担っていることが明らかとなった。また、実用的

な素数の判定も定理 (1.3) を基にしている。しかし、カーマイケル数もこの判定法をパスしてしまうのであった。そこで、この章ではカーマイケル数の性質とその判定法について紹介する。

まず、カーマイケル数の簡単な性質を述べよう [1, p.123]。

定理 3.1 (カーマイケル数の性質)**.**

1. 全てのカーマイケル数は奇数である。
2. 全てのカーマイケル数は相異なる素数の積である。

逆にある数 n がカーマイケル数であることを判定するには次の定理を使えばよい。

定理 3.2 (カーマイケル数に対する**コルセルトの判定法**)**.** 合成数 n がカーマイケル数である必要十分条件は、n が奇数であって、かつ n を割る素数 p は全て以下の 2 条件を満たすことである。

1. p^2は n を割らない。つまり n は無平方数である。
2. p を n の素因数とすると、$p-1$ は $n-1$ を割 り切る。

カーマイケル数の理論的な判定法は上のように与えられるが、これを実行するためには n を因数分解しなければならず、これは計算量的にみて困難であることを注意しておく。

4 Mathematicaのプログラム

ここでは素数判定法における整数の性質を調べるために数式処理ソフト Mathematica[3]で自分が作ったプログラミングを紹介する。

4.1 求める数値

正の整数 n が与えられたとする。Mathematica を使い

$$a^n \pmod{n} \tag{4.1}$$

[3]http://www.wolfram.com/index.ja.html

$$N(n) = \#\{0 \leq a < n : a^n \equiv a \pmod{n}\} \tag{4.2}$$

$$a^n \equiv a \pmod{n} \tag{4.3}$$

$$\phi(n) \tag{4.4}$$

$$a^n \equiv a \pmod{n} \text{となる割合}(\%) = \frac{N(n)}{n} \times 100$$

を計算する。

4.2 プログラミング例

例として $n = 77$ のとき、Mathematica のプログラムを紹介する。

$$b = 77 \tag{4.5}$$

$$f[a] := (\mathbf{PowerMod}[a, b, b] == a) \tag{4.6}$$

$$\mathbf{PowerMod}[\mathbf{Range}[b], b, b] \tag{4.7}$$

$$\mathbf{EulerPhi}[b] \tag{4.8}$$

$$\mathbf{Position}[\mathbf{Table}[f[a], a, 1, b], \mathbf{True}] \tag{4.9}$$

$$\mathbf{Length}[\mathbf{Position}[\mathbf{Table}[f[a], a, 1, b], \mathbf{True}]] + 1 \tag{4.10}$$

$$(\mathbf{Length}[\mathbf{Position}[\mathbf{Table}[f[a], a, 1, b], \mathbf{True}]] + 1) * 100/(\mathrm{b}) \tag{4.11}$$

上で太字立体で表わされた **PowerMod** などは Mathematica のコマンドを表わしている。これを実行すると

$$n = 77$$

$$\{a^{77} \pmod{77}\} =$$

{1, 18, 75, 16, 3, 41, 28, 57, 4, 54, 44, 45, 62, 42, 71, 25,
19, 72, 24, 48, 21, 22, 67, 40, 9, 38, 69, 63, 50, 46, 26,
65, 66, 34, 7, 64, 60, 47, 30, 17, 13, 70, 43, 11, 12, 51,
31, 27, 14, 8, 39, 68, 37, 10, 55, 56,29, 53, 5, 58, 52, 6,
35, 15, 32, 33, 23, 73, 20, 49, 36, 74, 61, 2, 59, 76, 0}

$$\begin{aligned}\phi(77) =& 60\\ \{a^{77} \equiv a \pmod{77}\} =& \{1, 21, 22, 34, 43, 55, 56, 76\}\\ N(77) =& 9\\ 100 \times \frac{N(77)}{77}(\%) =& 11.6883\end{aligned}$$

が得られる。

5　3の倍数のカーマイケル指数

この章ではnが3の倍数の時の数列$a^n \pmod n \quad (a = 0, 1, 2, \dots)$の性質について述べる。

5.1　$n = 3 \cdot p$の時$(p \in \mathbb{P}_{\geq 5})$

$n = 3 \cdot p$のときの計算例を挙げよう。

a	0	1	2	3	4
$a^{15} \pmod{15}$	0	1	8	12	4
a	5	6	7	8	9
$a^{15} \pmod{15}$	5	6	13	2	9
a	10	11	12	13	14
$a^{15} \pmod{15}$	10	11	3	7	14

表 5: $n = 3 \cdot 5 = 15$のとき

卒業研究のセミナーでは、この表より、次の予想をした。

予想 3. pを5以上の素数とし、$n = 3 \cdot p$とする。このとき

$$a^n \equiv a \pmod n$$

となるaはすべて

$$a \equiv -1, 0, 1 \pmod p$$

で表せる。

a	0	1	2	3	4	5	6
$a^{21} \pmod{21}$	0	1	8	6	1	20	6
a	7	8	9	10	11	12	13
$a^{21} \pmod{21}$	7	8	15	13	8	6	13
a	14	15	16	17	18	19	20
$a^{21} \pmod{21}$	14	15	1	20	15	13	20

表 6: $n = 3 \cdot 7 = 21$ のとき

この予想を、より詳しく、次の定理の形で証明する。

定理 5.1. $p > 3$ を素数とし、$n = 3 \cdot p$ とする。このとき

$$a^n \equiv a \pmod{n} \tag{5.1}$$

が成り立つことと

$$a \equiv -1, 0, 1 \pmod{p} \tag{5.2}$$

は同値である。

Proof. $p \in \mathbb{P}, p > 3$ として $n = 3 \cdot p$ とおく。中国剰余定理 [1, p.72] より法 $p \cdot q$ で考えることと法 p, 法 q 別々で考えることは同値である。よって

$$a^n \equiv a \pmod{n} \Longleftrightarrow \begin{cases} a \equiv a^n \pmod{3} & \cdots (1) \\ a \equiv a^n \pmod{p} & \cdots (2) \end{cases}$$

を得る。まず (1) について考える。フェルマーの小定理より

$$a^3 \equiv a \pmod{3} \tag{5.3}$$

が成り立つ。従って

$$a^n \equiv a^{3 \cdot p} \equiv (a^3)^p \equiv a^p \pmod{3} \tag{5.4}$$

であるが、素数 p は 5 以上なので奇数である。このとき $a \equiv 0 \pm 1$ ならば $a^p \equiv a \pmod{3}$ が成り立つことは明らかである。よって $a^n \equiv a \pmod{3}$ は常に成り立っている。(従って実質的には (1) の条件はあってもなくても同じであることに注意する。)

次に (2) を考える。まず (2) が成り立つとしよう。フェルマーの小定理より

$$a^p \equiv a \pmod{p} \tag{5.5}$$

が成り立つ。従って、$n = 3 \cdot p$ なので

$$a^n \equiv a^{3 \cdot p} \equiv (a^p)^3 \equiv a^3 \pmod{p} \tag{5.6}$$

そこで (5.6) を (2) 式に代入して

$$a^3 \equiv a \pmod{p} \tag{5.7}$$

を得る。これを a の方程式として解く。右辺を左辺に移項して因数分解すると

$$a(a+1)(a-1) \equiv 0 \pmod{p} \tag{5.8}$$

よって (5.8) 式を満たす a は

$$a \equiv -1, 0, 1 \pmod{p} \tag{5.9}$$

であることがわかる。

逆に $a \equiv -1, 0, 1 \pmod{p}$ なら (2) の式 $a \equiv a^n \pmod{p}$ が成り立つことは明らかである。

(1),(2) が証明されたので、これは $a^n \equiv a \pmod{n}$ と同値である。 □

系 1. $p > 3$ を素数とし、$n = 3 \cdot p$ とおく。このときカーマイケル指数 $N(n)$ は

$$N(n) = 9 \tag{5.10}$$

で与えられる。

5.2 $n = 3 \cdot p^2$の時 $(p \in \mathbb{P}_{\geq 5})$

次に、$n = 3 \cdot p^2$ についても考えよう。

定理 5.2. $p > 3$ を素数とし、$n = 3 \cdot p^2$とする。このとき

$$a^n \equiv a \pmod{n} \tag{5.11}$$

が成り立つことと

$$a \equiv -1, 0, 1 \pmod{p^2} \tag{5.12}$$

は同値である。

定理 5.1 と同じ方針で説明する。

Proof. $(p \in \mathbb{P}, p > 3)$ $n = 3 \cdot p^2$ とおく。中国剰余定理より

$$a^n \equiv a \pmod{n} \Longleftrightarrow \begin{cases} a \equiv a^n \pmod{3} & \cdots (1) \\ a \equiv a^n \pmod{p^2} & \cdots (2) \end{cases}$$

である。まず (1) は定理 (5.1) の証明より任意の a に対して常に成り立つことに注意する。そこで (2) について場合分けして考えよう。

(i) a が p^2 の倍数のとき。$a \equiv 0 \pmod{p^2}$ より $a \equiv a^n \pmod{p^2}$ が成り立つのは明らか。

(ii) a と p が互いに素のとき。オイラーの公式より

$$a^{p^2-p} \equiv 1 \pmod{p^2} \tag{5.13}$$

両辺に a^p をかけて

$$a^{p^2} \equiv a^p \pmod{p^2} \tag{5.14}$$

従って

$$a^n \equiv a^{3 \cdot p^2} \equiv (a^{p^2})^3 \equiv a^{3 \cdot p} \pmod{p^2} \tag{5.15}$$

(5.17) 式を (2) 式に代入して

$$a^{3p} \equiv a \pmod{p^2} \tag{5.16}$$

両辺を a で割って

$$a^{3p-1} \equiv 1 \pmod{p^2} \tag{5.17}$$

両辺を p 乗して

$$a^{3p^2-p} \equiv 1^p \pmod{p^2} \tag{5.18}$$

$$a^{3p^2-3p+2p} \equiv 1 \pmod{p^2} \tag{5.19}$$

$$a^{3(p^2-p)+2p} \equiv 1 \pmod{p^2} \tag{5.20}$$

オイラーの公式 ($a^{p^2-p} \equiv 1 \pmod{p^2}$) より

$$a^{2p} \equiv 1 \pmod{p^2} \tag{5.21}$$

右辺を移項して

$$(a^p - 1)(a^p + 1) \equiv 0 \pmod{p^2} \tag{5.22}$$

(5.24) より

$$a^p \equiv \pm 1 \pmod{p^2} \text{ または} \tag{5.23}$$

$$a^p \equiv 1 \pmod{p} \text{ かつ } a^p \equiv -1 \pmod{p} \tag{5.24}$$

が分かった。ここで $p > 2$ より (5.26) 式は成り立たない。従って、(5.25) 式を両辺 3 乗して

$$a^{3p} \equiv \pm 1 \pmod{p^2} \tag{5.25}$$

(5.18) 式より

$$a \equiv a^3 \equiv \pm 1 \pmod{p^2} \tag{5.26}$$

(i),(ii) より $a^n \equiv a \pmod{n} \Rightarrow a \equiv 0, \pm 1 \pmod{p^2}$ が示された。

逆に $a \equiv 0, \pm 1 \pmod{p^2}$ ならば n が奇数なので $a \equiv a^n \pmod{p^2}$ が成り立つことは自明。

以上より $a \equiv 0 \pm 1 \pmod{p^2}$ と $a^n \equiv a \pmod{n}$ は同値であることを示せた。 □

系 2. $p > 3$ を素数とし、$n = 3 \cdot p^2$とする。このときカーマイケル指数 $N(n)$ は

$$N(n) = 9 \tag{5.27}$$

である。

6 周期Tはいくつか?

Mathematica のプログラムによって計算してみると、$a^n \pmod{n}$ で与えられる数列 $\{a^n \pmod{n} : a = 0, 1, 2, \dots\}$ に周期 T をもつものを発見した。以下に例をあげる。

この表より次の予想をした。

a	0	1	2	3	4	5	6	7	8
$a^9 \pmod 9$	0	1	8	0	1	8	0	1	8

表 7: $n = 9$ のとき周期 $T = 3$

a	0	1	2	3	4	5	6	7	8	9	10	11
$a^{12} \pmod{12}$	0	1	4	9	4	1	0	1	4	9	4	1

表 8: $n = 12$ のとき周期 $T = 6$

予想 4. p と q を素数、k を 1 以上の整数とする。

1. $n = p^k$ のとき、数列 $\{a^n \pmod n : a = 0, 1, 2, \dots\}$ は周期 p を持つ。
2. $n = p^k \cdot q$ のとき、数列 $\{a^n \pmod n : a = 0, 1, 2, \dots\}$ は周期 pq を持つ。

この予想を次の定理の形で証明する。

定理 6.1. *p と q を素数とし、k を 1以上の整数とする。このとき $n = p^k$ ならば*

$$a^n \equiv (a + p)^n \pmod n \tag{6.1}$$

である。

定理 6.2. *p と q を素数とし、k を 1以上の整数とする。このとき $n = p^k \cdot q$ ならば*

$$a^n \equiv (a + pq)^n \pmod n \tag{6.2}$$

である。

Proof. 定理 6.1 の証明
$n = p^k, \quad p \in \mathbb{P}, \quad k \in \mathbb{Z}_{\geq 1}$ のとき $a^n \equiv (a+p)^n \pmod n$ であることを示す。

まず $(a + p)^n$ を二項展開して

$$(a+p)^n = a^n + \binom{n}{1}a^{n-1}p + \binom{n}{2}a^{n-2}p^2 + \cdots + \binom{n}{k}a^{n-k}p^k + \cdots \tag{6.3}$$

$$\equiv a^n + \binom{n}{1}a^{n-1}p + \binom{n}{2}a^{n-2}p^2 + \cdots + \binom{n}{k}a^{n-k}p^k \pmod{p^k} \tag{6.4}$$

次に $m \leq k$ のとき $\binom{n}{m}p^m \equiv 0 \pmod{p^k}$ を示そう。

$$\binom{n}{m}p^m = p^m \cdot \frac{n!}{m!(n-m)!} = p^m \cdot \frac{p^k!}{m!(p^k-m)!} \tag{6.5}$$

$$= p^m \cdot \frac{p^k(p^k-1)(p^k-2)\cdots(p^k-m+1)}{m(m-1)(m-2)\ldots 1} \tag{6.6}$$

ここで $p^l \leq m < p^{l+1}$ として分母と分子に現れる因数 p の個数を調べる。まず分母と分子に現れる p の倍数の個数を比べよう。

$m \equiv 0 \pmod{p}$ ならば分母と分子に現れる p の倍数の個数は一致する。
$m \not\equiv 0 \pmod{p^2}$ ならば分母と分子に現れる p の倍数の個数は分子が一つ多い。

同様に p^2 の倍数が現れる回数は

$m \equiv 0 \pmod{p^2}$ ならば分母と分子に現れる p^2 の倍数の個数は一致する。
$m \not\equiv 0 \pmod{p^2}$ ならば分母と分子に現れる p^2 の倍数の個数は分子が一つ多い。

以下 p^l まで続けていくと、

$m \equiv 0 \pmod{p^l}$ ならば分母と分子に現れる p^l の倍数の個数は一致する。
$m \not\equiv 0 \pmod{p^l}$ ならば分母と分子に現れる p^l の倍数の個数は分子が一つ多い。従って

$$(\text{分子の因数 } p \text{ の個数}) \geq (\text{分母の因数 } p \text{ の個数}) \tag{6.7}$$

がわかる。上の議論では, p^k は p^l であれば十分であり、分子には少なくとも因数 p^{k-l} の余裕がある。よって、p^m と合わせて

$$k - l + m \geq k \tag{6.8}$$

であればよい。従って

$$m - l \geq 0 \tag{6.9}$$

を示せば証明は完了する。

$m \geq p^l$ より両辺の対数をとって

$$\log_p m \geq \log_p p^l = l \tag{6.10}$$

ここで $x > 0$ において $x > \log x$ に注意すると、$p \geq 3$ ならば $\log p > 1$ なので

$$m \geq \log m \geq \frac{\log m}{\log p} = \log_p m \tag{6.11}$$

が成り立つ。(6.10) と (6.11) より $p \geq 3$ のとき

$$m - l \geq 0 \tag{6.12}$$

が示された。

次に $p = 2$ のときを場合分けをして証明する。つまり、

$n = 2^k \quad (k \geq \mathbb{Z}_{\geq 1})$ のとき $a^n \equiv (a+2)^n \pmod{n}$ であることを示す。

(i) a が 偶数のとき。

a を

$$a = 2m \quad (m \in \mathbb{Z}_{\geq 1}) \tag{6.13}$$

とおく。従って

$$\begin{aligned} (a+p)^n &= (2m+2)^n && (6.14)\\ &\equiv 2^n(m+1)^n && (6.15)\\ &\equiv 2^{2^k}(m+1)^{2^k} \pmod{2^k} && (6.16) \end{aligned}$$

である。

ここで、$k \geq 0$ に対して、$2^{2^k} \geq 2^k$ が成り立つ。従って

$$(a+p)^n \equiv 2^{2^k}(m+1)^{2k} \equiv 0 \pmod{2^k} \tag{6.17}$$

を得る。よって a が偶数のとき $a^n \equiv 0 \pmod{n}$ が示せた。

(ii)　a が奇数のとき。$a \equiv 0 \pmod 2$ として a の代わりに $a+1$ を用いて $(a+1)^n = 1 \pmod n$ を示す。(i) の証明より

$$a^n \equiv 0 \pmod n \tag{6.18}$$

が成り立っている。一方 $\gcd(a+1, n) = 1$ だからオイラーの公式より

$$(a+1)^{\phi(n)} = 1 \pmod n \tag{6.19}$$

オイラー関数の性質より

$$\phi(n) = 2^k - 2^{k-1} = 2^{k-1} \tag{6.20}$$

よって

$$(a+1)^{2^{k-1}} = 1 \pmod n \tag{6.21}$$

両辺を 2 乗して

$$(a+1)^{2^k} \equiv 1 \pmod n \tag{6.22}$$
$$(a+1)^n \equiv 1 \pmod n \tag{6.23}$$

よって a が奇数のとき、$a^n \equiv 1 \pmod n$ が示せた。

(i),(ii) より $p = 2$ のとき数列は

$\{a^n \pmod n : a = 0, 1, 2, \dots\} = \{0, 1, 0, 1, 0, 1, \dots\}$

となり、$a^n \equiv (a+2)^k$ を示せた。以上によって定理 6.1 を証明した。 □

Proof. 定理 6.2 の証明 $n = p^k \cdot q \quad (p, q \in \mathbb{P}, \quad k \in \mathbb{Z}_{\geq 1})$ のとき $a^n \equiv (a+pq)^n \pmod n$ であることを示す。

$$p, q \in \mathbb{P} \text{ だから } \gcd(p^k, q) = 1$$

従って、中国剰余定理を使って

$$a^n \equiv (a+pq)^n \pmod n \Longleftrightarrow \begin{cases} a^n \equiv (a+pq)^n \pmod{p^k} & \cdots (1) \\ a^n \equiv (a+pq)^n \pmod q & \cdots (2) \end{cases}$$

を得る。$a + pq \equiv a \pmod q$ だから (2) は明らかに成り立つ。次に (1) を示す。まず $\gcd(p^k, q) = 1$ だから

$$xq \equiv 1 \pmod{p^k} \tag{6.24}$$

となる x が存在する。この x の n 乗を (1) 式の右辺にかけて

$$x^n(a+pq)^n = (xa+pxq)^n \tag{6.25}$$

$xq \equiv 1 \pmod{p^2}$ だから

$$\begin{aligned}(6.21) \equiv &(xa+p)^n && (6.26)\\ \equiv &\{(xa+p)^{p^k}\}^q \pmod{p^k} && (6.27)\end{aligned}$$

定理 (6.1) の証明より

$$\begin{aligned}(6.23) &\equiv \{(xa)^{p^k}\}^q \equiv (xa)^n && (6.28)\\ &\equiv x^n a^n \pmod{p^k} && (6.29)\end{aligned}$$

よって

$$x^n(a+pq)^n \equiv x^n a^n \pmod{p^k} \tag{6.30}$$

を得た。この式の両辺に q^n をかけて

$$q^n x^n (a+pq)^n \equiv q^n x^n a^n \pmod{p^k} \tag{6.31}$$

$qx \equiv 1 \pmod{p^k}$ だから

$$(a+pq)^n \equiv a^n \pmod{p^k} \tag{6.32}$$

が成り立つ。よって (1),(2) が示せたので $n = p^k q \quad (p, q \in \mathbb{P}, \quad k \geq 1)$ のとき $a^n \equiv (a+pq)^n \pmod{n}$ を示せた。

□

7 まとめ

当初の目的であったカーマイケル指数 $N(n) = 2$ または $n-1$ となる数は $n = 2^k$ のとき $N(n) = 2$ となり、片方は発見することができた。しかし、もう一方の $N(n) = n-1$ となる数は発見にはいたらなかった。100 までの数で $\frac{N(n)}{n} \cdot 100$ (%) を求めたが、最大でも $n = 6$ のときの 66.7(%) であり、6,15,91 を除いては、全ての数が 40%にも満たないものであることと、様々な数で N を求めたところ $N(555549) = 169$ が最大だったので、たぶん $N(n) = n-1$ となる数はないと思う。

他に、できなかったこととして、任意の数に対して N の値を求める定理が導き出せればよかったのだが、それにはいたらなかった。理論的に証明はできなかったが、Mathematica を使って実験的に求めた数列では、カーマイケル指数は $N = p^k \cdot q^k$ のかたちで全て表せたので、こちらの法則を導き出せれば任意の数に対しての N の値が分かるかもしれない。これができたら、本研究の目標であった $N(n) = n - 1$ となる数に出会えるかもしれない。他に、任意の n と a に対して $a^n \equiv a^k \pmod{n}$ となる数 k が発見されたので、こちらの法則も発見したかった。もし似たようなテーマで卒業論文を書く後輩がいたら、ぜひ私ができなかったこの 2 つのことを証明してもらいたい。

卒業研究を通して、今年は人生で最も数学をやった 1 年間になった。大学に入り、なかば勉強というものに諦めを持っていた私が、最近では時間があるときに、ネットで暗号の仕組みなどを調べ、楽しんでいたことに、自分自身驚きを隠せない。非常に辛かったけど、数学の楽しさを教えてくれた担当教官の西山享教授に感謝を述べてこの論文を閉じさせていただきます。1 年間ありがとうございました。

参考文献

[1] ジョセフ H シルヴァーマン著　鈴木 治郎訳『はじめての数論』ピアソン桐原

[2] 小林昭七著『なっとくするオイラーとフェルマー』講談社

[3] 岩田 彰監修　鈴木 春洋/奥野 琢人/若山 公威/高須 紀樹/杉江 修/村瀬 晋二著『インターネット暗号化技術〜PKI,RSA,SSA,S/MIME,etc〜』ソフト・リサーチ・センター

[4] サイモン・シン著 (青木薫訳)『フェルマーの最終定理』 (新潮文庫) 新潮社