

# 「HPKIのPKIを支えるRSA暗号について -その2 冪剰余の周期性-

市立貝塚病院 顧問 放射線治療科 医師 兼

地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター  
放射線治療科 医師（在職出向）  
上杉 康夫



前回は、このHPKI(Healthcare Public Key Infrastructure：保健医療福祉分野の公開鍵基盤)の根本を支えるRSA(Rivest-Shamir-Adleman 以降RSA)暗号の特徴について述べました。その中でRSA暗号は一方方向性関数であるmodを使った冪剰余の周期性を利用していると記載いたしました。今回はRSA暗号の発想の大きな端緒となったこの点につき述べます※1、2、3、4、5。公開鍵や秘密鍵を中心にした話題は次号以後で記載したいと思います。

## 1. 冪剰余の周期性

RSA暗号は、巨大な素数の積を法N(除数：割る数)とする累乗剰余または冪剰余(以降 冪剰余)の周期性を利用することで、暗号化と復号化が可能となる仕組みでした

今回も前回説明したガウスが発明したmod演算※6を使用し冪剰余を検討します。

$C = m^x \bmod N$ とした時、C：冪剰余、 $m^x$ ：被

除数、m：底(冪乗演算で掛け合わせる元の数)、 $x$ ：累乗数(冪乗数)、N：法とします。

まず2の冪剰余Cの周期と法Nとの関係性について考えてみます※7。ここでは $x=0$ (すなわち $m^0=1$ )を周期の開始点とします。乗算の単位元である1に戻る周期を「純周期」と呼びます。一方、1には戻らないものの、それまでに計算したある数値に戻ってループを形成する状態は「混周期」と定義されます※8。

今回は法Nとして12,13,14,15,16,17の6つの値を取り上げて、 $C = 2^x \bmod N$ (表1)を検討します。底を2としたのは、最も基本的な数である2で法則性が見出せなければ、3以上で法則があっても汎用性に欠けると判断したためです。また、法Nにこの6つの数値を選んだ理由は、1桁では変化が乏しく特徴がつかみにくく、反対に大きすぎると計算が煩雑になるためです。この6つの数には、それぞれ特徴的な性質が現れます。

表1では、冪剰余Cが1になる箇所を無着色

|    | 数  | 数の特徴                       | 周期  | 周期の特徴              | 2の累乗X(被除数) |   |   |   |    |    |    |    |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----------------------------|-----|--------------------|------------|---|---|---|----|----|----|----|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|    |    |                            |     |                    | 0          | 1 | 2 | 3 | 4  | 5  | 6  | 7  | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 法N | 12 | $2^2 \times 3$             | 混周期 | 途中から<br>4 8の繰り返し   | 1          | 2 | 4 | 8 | 4  | 8  | 4  | 8  | 4 | 8 | 4  | 8  | 4  | 8  | 4  | 8  | 4  | 8  | 4  | 8  | 4  | 8  | 4  | 8  | 4  | 8  |
|    | 13 | 素数                         | 純周期 | $13-1=12$          | 1          | 2 | 4 | 8 | 3  | 6  | 12 | 11 | 9 | 5 | 10 | 7  | 1  | 2  | 4  | 8  | 3  | 6  | 12 | 11 | 9  | 5  | 10 | 7  | 1  | 2  |
|    | 14 | $2 \times 7$               | 混周期 | 途中から<br>2 4 8の繰り返し | 1          | 2 | 4 | 8 | 2  | 4  | 8  | 2  | 4 | 8 | 2  | 4  | 8  | 2  | 4  | 8  | 2  | 4  | 8  | 2  | 4  | 8  | 2  | 4  | 8  | 2  |
|    | 15 | $3 \times 5$ の相異なる2つの奇素数の積 | 純周期 | 4                  | 1          | 2 | 4 | 8 | 1  | 2  | 4  | 8  | 1 | 2 | 4  | 8  | 1  | 2  | 4  | 8  | 1  | 2  | 4  | 8  | 1  | 2  | 4  | 8  | 1  | 2  |
|    | 16 | $2^4$                      | 冪零  | 途中から<br>0が続く       | 1          | 2 | 4 | 8 | 0  | 0  | 0  | 0  | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
|    | 17 | 素数                         | 純周期 | 8<br>(17-1=16の約数)  | 1          | 2 | 4 | 8 | 16 | 15 | 13 | 9  | 1 | 2 | 4  | 8  | 16 | 15 | 13 | 9  | 1  | 2  | 4  | 8  | 16 | 15 | 13 | 9  | 1  | 2  |

表1： $2^x \bmod N$   
1を強調するため無着色領域にしている。

領域として強調しています。この領域の現れ方に注目してみましょう。まず、法 $N$ が偶数である14と16(および12)について見てみます。法 $N=12$ では1回2を示した後は4,8を循環するだけで1に戻りません(混周期)。法 $N=14$ では最初から2,4,8を循環し、1に戻りません(混周期)。法 $N=16$ では $16=2^4$ なので、 $2^4 \bmod 16=0$ となるため、4乗以降はすべて0が繰り返されます(冪零)。このように、偶数を法 $N$ とした場合、純周期を示さず元の1に戻らないことが分かります。そのため、偶数を暗号システムに利用するのは不利です。

次に、法 $N$ が奇素数である13と17の場合を考えます。2の冪剰余 $C$ の周期は、 $N=13$ のとき12、 $N=17$ のとき8です。一見すると暗号に使いそうですが、フェルマーの小定理※9、10により法 $N$ に奇素数 $p$ を用いると周期は $p-1$ またはその約数となり、容易に割り出されてしまい、セキュリティ上好ましくありません。例えば $N=13$ では $13-1=12$ から周期12が、 $N=17$ では $17-1=16$ の約数から周期8が割り出されてしまいます。このことから、RSA暗号の法 $N$ に単一の奇素数を使うことは避けるべきだと判断できます。

そして第3に、法 $N$ が15の場合です。15は $3 \times 5$ という相異なる2つの奇素数の積であり、素数ではありません。このとき純周期は4を示します。この「4」という周期は、15という数値から直接割り出すことが困難な値です。

周期の算出にはオイラー関数(オイラーのφ関数、オイラーのトーシェント関数：Euler's totient function)※11を用います。この $\phi(p)$ は「 $p$ より小さい正の整数のうち、 $p$ と互いに素な数の個数」を表す関数です※12。 $p$ が素数のときは簡単です。 $p$ を素数とすると、 $\phi(p)=p-1$ が成り立ちます。なぜなら1から $p-1$ のうちに素数 $p$ の素因子である $p$ を因子として含むものは存在しないからです※11。法 $N$ が相異なる2つの素数 $p, q$ の積( $N=p \times q$ )である場合、周期は $\phi(p)=p-1$ と $\phi(q)=q-1$ の最小公倍数として求められます。また、カーマイケル関数 $\lambda(N)$

(Carmichael function)※13で一度に同計算をすることも可能です。 $N=15$ の場合は $15=3 \times 5$ ですので、 $3-1=2$ と $5-1=4$ の最小公倍数である4が周期 $\lambda$ (以降 $\lambda$ )となります。つまり $\lambda(15)=4$ です。

以上の観察から、相異なる2つの奇素数の積が持つ性質は暗号システムに非常に適していることが見えてきます。2つの奇素数が生み出す純周期を利用することで暗号化と復号化が可能になり、さらに法 $N$ を構成する2つの奇素数への素因数分解を困難にすれば、周期 $\lambda$ の解読を防いで高い秘匿性を維持できるからです。RSA暗号は、まさにこの数学的特性を活用して開発されたシステムだと推察されます※14。

## 2. 冪剰余 $C$ の周期 $\lambda$ と法 $N$ との関係

前章で相異なる2つの奇素数の積がRSA暗号の法 $N$ として使いそうであることを見出しました。さらに進めて、法 $N$ の候補として $15=3 \times 5$ のほか、 $21=3 \times 7$ 、 $33=3 \times 11$ 、 $35=5 \times 7$ 、 $55=5 \times 11$ について検討します。底 $m$ を素数のうち最小から順に2, 3, 5, 7を用い、累乗 $2^x, 3^x, 5^x, 7^x$ の冪剰余 $C$ に絞って法 $N$ の変化による周期 $\lambda$ の変化を観察してみましょう。

表2では、底 $m$ と同じ値の冪剰余 $C$ を強調するために無着色領域としています。無着色領域の縦の列の並びとして、冪剰余 $C$ の周期 $\lambda$ が観察されます(表2)。

1章で述べた $\lambda(N)$ を用いますと法15では $\lambda(15)=4$ から冪剰余 $C$ の周期 $\lambda$ は4となります。他のものと併せて一覧表(表2)に示します。もっとも、底 $m$ の数値によっては、 $\lambda(N)$ より小さい周期を示す場合もあります。例えば法 $N=15$ における底5の冪剰余 $C$ の周期 $\lambda$ は $\lambda(15)=4$ より小さく2を示します。また法 $N=21$ における底7の冪剰余 $C$ はすべて7を示します。しかし、そのような例外があったとしても、全体としては無着色領域の縦列として周期性が観察できます(表2)。

|        | 数  | 素因数<br>分解 | オイラー<br>関数 | カーマイケル<br>関数 λ (N) | 周<br>期 | 被除<br>数の<br>底m | 累乗X              |                    |                     |                   |                  |                    |                     |                   |                  |                    |                     |                   |                  |                    |                     |                   |                  |                    |                     |                   |                  |                    |                     |                   |    |    |
|--------|----|-----------|------------|--------------------|--------|----------------|------------------|--------------------|---------------------|-------------------|------------------|--------------------|---------------------|-------------------|------------------|--------------------|---------------------|-------------------|------------------|--------------------|---------------------|-------------------|------------------|--------------------|---------------------|-------------------|------------------|--------------------|---------------------|-------------------|----|----|
|        |    |           |            |                    |        |                | 1                | 2                  | 3                   | 4                 | 5                | 6                  | 7                   | 8                 | 9                | 10                 | 11                  | 12                | 13               | 14                 | 15                  | 16                | 17               | 18                 | 19                  | 20                | 21               | 22                 | 23                  | 24                | 25 | 26 |
| 法<br>N | 15 | 3×5       | 2          | 4                  | 4      | 4              | 2<br>3<br>5      | 4<br>9<br>10       | 8<br>12<br>5        | 1<br>6<br>10      | 2<br>3<br>5      | 4<br>9<br>10       | 8<br>12<br>5        | 1<br>6<br>10      | 2<br>3<br>5      | 4<br>9<br>10       | 8<br>12<br>5        | 1<br>6<br>10      | 2<br>3<br>5      | 4<br>9<br>10       | 8<br>12<br>5        | 1<br>6<br>10      | 2<br>3<br>5      | 4<br>9<br>10       | 8<br>12<br>5        | 1<br>6<br>10      | 2<br>3<br>5      | 4<br>9<br>10       | 8<br>12<br>5        | 1<br>6<br>10      |    |    |
|        | 21 | 3×7       | 2          | 6                  | 6      | 6              | 2<br>3<br>5      | 4<br>9<br>16       | 8<br>18<br>12       | 1<br>6<br>15      | 2<br>3<br>5      | 4<br>9<br>16       | 8<br>18<br>12       | 1<br>6<br>15      | 2<br>3<br>5      | 4<br>9<br>16       | 8<br>18<br>12       | 1<br>6<br>15      | 2<br>3<br>5      | 4<br>9<br>16       | 8<br>18<br>12       | 1<br>6<br>15      | 2<br>3<br>5      | 4<br>9<br>16       | 8<br>18<br>12       | 1<br>6<br>15      | 2<br>3<br>5      | 4<br>9<br>16       | 8<br>18<br>12       | 1<br>6<br>15      |    |    |
|        | 33 | 3×11      | 2          | 10                 | 10     | 10             | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>16 | 8<br>18<br>26<br>13 | 1<br>6<br>14<br>4 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>16 | 8<br>18<br>26<br>13 | 1<br>6<br>14<br>4 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>16 | 8<br>18<br>26<br>13 | 1<br>6<br>14<br>4 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>16 | 8<br>18<br>26<br>13 | 1<br>6<br>14<br>4 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>16 | 8<br>18<br>26<br>13 | 1<br>6<br>14<br>4 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>16 | 8<br>18<br>26<br>13 | 1<br>6<br>14<br>4 |    |    |
|        | 35 | 5×7       | 4          | 6                  | 12     | 12             | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>14 | 8<br>18<br>25<br>7  | 1<br>6<br>15<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>14 | 8<br>18<br>25<br>7  | 1<br>6<br>15<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>14 | 8<br>18<br>25<br>7  | 1<br>6<br>15<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>14 | 8<br>18<br>25<br>7  | 1<br>6<br>15<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>14 | 8<br>18<br>25<br>7  | 1<br>6<br>15<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>14 | 8<br>18<br>25<br>7  | 1<br>6<br>15<br>5 |    |    |
|        | 55 | 5×11      | 4          | 10                 | 20     | 20             | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>49 | 8<br>18<br>36<br>13 | 1<br>6<br>20<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>49 | 8<br>18<br>36<br>13 | 1<br>6<br>20<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>49 | 8<br>18<br>36<br>13 | 1<br>6<br>20<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>49 | 8<br>18<br>36<br>13 | 1<br>6<br>20<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>49 | 8<br>18<br>36<br>13 | 1<br>6<br>20<br>5 | 2<br>3<br>5<br>7 | 4<br>9<br>25<br>49 | 8<br>18<br>36<br>13 | 1<br>6<br>20<br>5 |    |    |

表2：法Nと冪剰余Cの周期λの関係  $m^x \bmod N$  画面のズームイン機能で拡大できます  
底mと同じ値の冪剰余Cを強調するために冪剰余Cの無着色領域にしている。無着色領域の縦の列の並びとして周期λが観察される。

| 累乗X    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|        | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |    |
| 底<br>m | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |    |
|        | 2  | 4  | 8  | 16 | 32 | 9  | 18 | 36 | 17 | 34 | 13 | 26 | 52 | 49 | 43 | 31 | 7  | 14 | 28 | 1  | 2  | 4  | 8  | 16 | 32 | 9  | 18 | 36 | 17 | 34 | 13 | 26 | 52 | 49 | 43 | 31 | 7  | 14 | 28 | 1  | 2  | 4  | 8  |
|        | 3  | 9  | 27 | 26 | 23 | 14 | 42 | 16 | 48 | 34 | 47 | 31 | 38 | 4  | 12 | 36 | 53 | 49 | 37 | 1  | 3  | 9  | 27 | 26 | 23 | 14 | 42 | 16 | 48 | 34 | 47 | 31 | 38 | 4  | 12 | 36 | 53 | 49 | 37 | 1  | 3  | 9  | 27 |
|        | 4  | 16 | 9  | 36 | 34 | 26 | 49 | 31 | 14 | 1  | 4  | 16 | 9  | 36 | 34 | 26 | 49 | 31 | 14 | 1  | 4  | 16 | 9  | 36 | 34 | 26 | 49 | 31 | 14 | 1  | 4  | 16 | 9  | 36 | 34 | 26 | 49 | 31 | 14 | 1  | 4  | 16 | 9  |
|        | 5  | 25 | 15 | 20 | 45 | 5  | 25 | 15 | 20 | 45 | 5  | 25 | 15 | 20 | 45 | 5  | 25 | 15 | 20 | 45 | 5  | 25 | 15 | 20 | 45 | 5  | 25 | 15 | 20 | 45 | 5  | 25 | 15 | 20 | 45 | 5  | 25 | 15 | 20 | 45 | 5  | 25 | 15 |
|        | 6  | 36 | 51 | 31 | 21 | 16 | 41 | 26 | 46 | 1  | 6  | 36 | 51 | 31 | 21 | 16 | 41 | 26 | 46 | 1  | 6  | 36 | 51 | 31 | 21 | 16 | 41 | 26 | 46 | 1  | 6  | 36 | 51 | 31 | 21 | 16 | 41 | 26 | 46 | 1  | 6  | 36 |    |
|        | 7  | 49 | 13 | 36 | 32 | 4  | 28 | 31 | 52 | 34 | 18 | 16 | 2  | 14 | 43 | 26 | 17 | 9  | 8  | 1  | 7  | 49 | 13 | 36 | 32 | 4  | 28 | 31 | 52 | 34 | 18 | 16 | 2  | 14 | 43 | 26 | 17 | 9  | 8  | 1  | 7  | 49 |    |
|        | 8  | 9  | 17 | 26 | 43 | 14 | 2  | 16 | 18 | 34 | 52 | 31 | 28 | 4  | 32 | 36 | 13 | 49 | 7  | 1  | 8  | 9  | 17 | 26 | 43 | 14 | 2  | 16 | 18 | 34 | 52 | 31 | 28 | 4  | 32 | 36 | 13 | 49 | 7  | 1  | 8  | 9  |    |
|        | 9  | 26 | 14 | 16 | 34 | 31 | 4  | 36 | 49 | 1  | 9  | 26 | 14 | 16 | 34 | 31 | 4  | 36 | 49 | 1  | 9  | 26 | 14 | 16 | 34 | 31 | 4  | 36 | 49 | 1  | 9  | 26 | 14 | 16 | 34 | 31 | 4  | 36 | 49 | 1  | 9  | 26 |    |
|        | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 | 10 | 45 |    |
|        | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 |    |    |
|        | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 | 23 | 1  | 12 | 34 |    |
|        | 13 | 4  | 52 | 16 | 43 | 9  | 7  | 36 | 28 | 34 | 2  | 26 | 8  | 49 | 32 | 31 | 18 | 14 | 17 | 1  | 13 | 4  | 52 | 16 | 43 | 9  | 7  | 36 | 28 | 34 | 2  | 26 | 8  | 49 | 32 | 31 | 18 | 14 | 17 | 1  | 13 | 4  |    |
|        | 14 | 31 | 49 | 26 | 34 | 36 | 9  | 16 | 4  | 1  | 14 | 31 | 49 | 26 | 34 | 36 | 9  | 16 | 4  | 1  | 14 | 31 | 49 | 26 | 34 | 36 | 9  | 16 | 4  | 1  | 14 | 31 | 49 | 26 | 34 | 36 | 9  | 16 | 4  | 1  | 14 |    |    |
|        | 15 | 5  | 20 | 25 | 45 | 15 | 5  | 20 | 25 | 45 | 15 | 5  | 20 | 25 | 45 | 15 | 5  | 20 | 25 | 45 | 15 | 5  | 20 | 25 | 45 | 15 | 5  | 20 | 25 | 45 | 15 | 5  | 20 | 25 | 45 | 15 | 5  | 20 | 25 | 45 | 15 | 5  |    |
|        | 16 | 36 | 26 | 31 | 1  | 16 | 36 | 26 | 31 | 1  | 16 | 36 | 26 | 31 | 1  | 16 | 36 | 26 | 31 | 1  | 16 | 36 | 26 | 31 | 1  | 16 | 36 | 26 | 31 | 1  | 16 | 36 | 26 | 31 | 1  | 16 | 36 | 26 | 31 | 1  | 16 |    |    |
|        | 17 | 14 | 18 | 31 | 32 | 49 | 8  | 26 | 2  | 34 | 28 | 36 | 7  | 9  | 43 | 16 | 52 | 4  | 13 | 1  | 17 | 14 | 18 | 31 | 32 | 49 | 8  | 26 | 2  | 34 | 28 | 36 | 7  | 9  | 43 | 16 | 52 | 4  | 13 | 1  | 17 |    |    |
|        | 18 | 49 | 2  | 36 | 43 | 4  | 17 | 31 | 8  | 34 | 7  | 16 | 13 | 14 | 32 | 26 | 28 | 9  | 52 | 1  | 18 | 49 | 2  | 36 | 43 | 4  | 17 | 31 | 8  | 34 | 7  | 16 | 13 | 14 | 32 | 26 | 28 | 9  | 52 | 1  | 18 |    |    |
|        | 19 | 31 | 39 | 26 | 54 | 36 | 14 | 26 | 19 | 1  | 19 | 31 | 39 | 26 | 54 | 36 | 14 | 26 | 19 | 1  | 19 | 31 | 39 | 26 | 54 | 36 | 14 | 26 | 19 | 1  | 19 | 31 | 39 | 26 | 54 | 36 | 14 | 26 | 19 | 1  | 19 |    |    |
|        | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 | 15 | 25 | 5  | 20 |    |    |
|        | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 | 1  | 21 |    |    |
|        | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 | 44 | 33 | 11 | 22 |    |    |
|        | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 | 34 | 12 | 1  | 23 |    |    |
|        | 24 | 26 | 19 | 16 | 54 | 31 | 29 | 36 | 39 | 1  | 24 | 26 | 19 | 16 | 54 | 31 | 29 | 36 | 39 | 1  | 24 | 26 | 19 | 16 | 54 | 31 | 29 | 36 | 39 | 1  | 24 | 26 | 19 | 16 | 54 | 31 | 29 | 36 | 39 | 1  | 24 |    |    |
|        | 25 | 20 | 5  | 15 | 45 | 20 | 5  | 15 | 45 | 20 | 5  | 15 | 45 | 20 | 5  | 15 | 45 | 20 | 5  | 15 | 45 | 20 | 5  | 15 | 45 | 20 | 5  | 15 | 45 | 20 | 5  | 15 | 45 | 20 | 5  | 15 | 45 | 20 | 5  | 15 |    |    |    |
|        | 26 | 16 | 31 | 36 | 1  | 26 | 16 | 31 | 36 | 1  | 26 | 16 | 31 | 36 | 1  | 26 | 16 | 31 | 36 | 1  | 26 | 16 | 31 | 36 | 1  | 26 | 16 | 31 | 36 | 1  | 26 | 16 | 31 | 36 | 1  | 26 | 16 | 31 | 36 | 1  | 26 |    |    |
|        | 27 | 14 | 48 | 31 | 12 | 49 | 3  | 26 | 42 | 34 | 28 | 36 | 37 | 9  | 23 | 16 | 47 | 4  | 53 | 1  | 27 | 14 | 48 | 31 | 12 | 49 | 3  | 26 | 42 | 34 | 28 | 36 | 37 | 9  | 23 | 16 | 47 | 4  | 53 | 1  | 27 |    |    |
|        | 28 | 14 | 7  | 31 | 43 | 49 | 52 | 26 | 13 | 34 | 17 | 16 | 28 | 8  | 32 | 16 | 8  | 4  | 2  | 1  | 28 | 14 | 7  | 31 | 43 | 49 | 52 | 26 | 13 | 34 | 17 | 16 | 28 | 8  | 32 | 16 | 8  | 4  | 2  | 1  | 28 |    |    |
|        | 29 | 16 | 24 | 36 | 54 | 26 | 39 | 31 | 19 | 1  | 29 | 16 | 24 | 36 | 54 | 26 | 39 | 31 | 19 | 1  | 29 | 16 | 24 | 36 | 54 | 26 | 39 | 31 | 19 | 1  | 29 | 16 | 24 | 36 | 54 | 26 | 39 | 31 | 19 | 1  | 29 |    |    |
|        | 30 | 20 | 50 | 15 | 10 | 25 | 35 | 5  | 40 | 45 | 30 | 20 | 50 | 15 | 10 | 25 | 35 | 5  | 40 | 45 | 30 | 20 | 50 | 15 | 10 | 25 | 35 | 5  | 40 | 45 | 30 | 20 | 50 | 15 | 10 | 25 | 35 | 5  | 40 |    |    |    |    |
|        | 31 | 26 | 36 | 16 | 1  | 31 | 26 | 36 | 16 | 1  | 31 | 26 | 36 | 16 | 1  | 31 | 26 | 36 | 16 | 1  | 31 | 26 | 36 | 16 | 1  | 31 | 26 | 36 | 16 | 1  | 31 | 26 | 36 | 16 | 1  | 31 | 26 | 36 | 16 | 1  | 31 |    |    |
|        | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 | 34 | 43 | 1  | 32 |    |    |
| 33     | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 | 44 | 22 | 11 | 33 |    |    |    |
| 34     | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 | 1  | 34 |    |    |    |    |
| 35     | 15 | 30 | 5  | 10 | 20 | 40 | 25 | 50 | 45 | 35 | 15 | 30 | 5  | 10 | 20 | 40 | 25 | 50 | 45 | 35 | 15 | 30 | 5  | 10 | 20 | 40 | 25 | 50 | 45 | 35 | 15 | 30 | 5  | 10 | 20 | 40 | 25 | 50 | 45 | 35 |    |    |    |
| 36     | 31 | 16 | 26 | 1  | 36 | 31 | 16 | 26 | 1  | 36 | 31 | 16 | 26 | 1  | 36 | 31 | 16 | 26 | 1  | 36 | 31 | 16 | 26 | 1  | 36 | 31 | 16 | 26 | 1  | 36 | 31 | 16 | 26 | 1  | 36 | 31 | 16 | 26 | 1  | 36 |    |    |    |
| 37     | 49 | 53 | 36 | 12 | 4  | 38 | 31 | 47 | 34 | 48 | 16 | 42 | 14 | 23 | 26 | 27 | 9  | 3  | 1  | 37 | 49 | 53 | 36 | 12 | 4  | 38 | 31 | 47 | 34 | 48 | 16 | 42 | 14 | 23 | 26 | 27 | 9  | 3  | 1  | 37 |    |    |    |
| 38     | 14 | 37 | 31 | 23 | 49 | 47 | 26 | 53 | 34 | 27 | 36 | 48 | 9  | 12 | 16 | 3  | 4  | 42 | 1  | 38 | 14 | 37 | 31 | 23 | 49 | 47 | 26 | 53 | 34 | 27 | 36 | 48 | 9  | 12 | 16 | 3  | 4  | 42 | 1  | 38 |    |    |    |
| 39     | 36 | 29 | 31 | 54 | 16 | 19 | 26 | 24 | 1  | 39 | 36 | 29 | 31 | 54 | 16 | 19 | 26 | 24 | 1  | 39 | 36 | 29 | 31 | 54 | 16 | 19 | 26 | 24 | 1  | 39 | 36 | 29 | 31 | 54 | 16 | 19 | 26 | 24 | 1  | 39 |    |    |    |
| 40     | 5  | 35 | 25 | 10 | 15 | 50 | 20 | 30 | 45 | 40 | 5  | 35 | 25 | 10 | 15 | 50 | 20 | 30 | 45 | 40 | 5  | 35 | 25 | 10 | 15 | 50 | 20 | 30 | 45 | 40 | 5  | 35 | 25 | 10 | 15 | 50 | 20 | 30 | 45 | 40 |    |    |    |
| 41     | 31 | 6  | 26 | 21 | 36 | 46 | 16 | 51 | 1  | 41 | 31 | 6  | 26 | 21 | 36 | 46 | 16 | 51 | 1  | 41 | 31 | 6  | 26 | 21 | 36 | 46 | 16 | 51 | 1  | 41 | 31 | 6  | 26 | 21 | 36 | 46 | 16 | 51 | 1  | 41 |    |    |    |
| 42     | 4  | 3  | 16 | 12 | 9  | 48 | 36 | 27 | 34 | 53 | 26 | 47 | 29 | 33 | 31 | 37 | 14 | 38 | 1  | 42 | 4  | 3  | 16 | 12 | 9  | 48 | 36 | 27 | 34 | 53 | 26 | 47 | 29 | 33 | 31 | 37 | 14 | 38 | 1  | 42 |    |    |    |
| 43     | 34 | 32 | 1  | 43 | 34 | 32 | 1  | 43 | 34 | 32 | 1  | 43 | 34 | 32 | 1  | 43 | 34 | 32 | 1  | 43 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

### 3. 法Nを55とした冪剰余Cのモデル

表3は、 $m \times \text{mod } 55$ の冪剰余Cの表で、底mと同じ数値の冪剰余Cを強調するために無着色領域で表現しています。検討したのは、 $m=1 \sim 55$ 、 $X=1 \sim 42$ です。無着色領域の縦の列は、1,21,41乗で認められ、20乗の周期が認められます(表3)。

本モデルでは $\lambda(55)=20$ であるため(表2)、すなわち $(k \times 20 + 1) = (k \times \lambda(55) + 1)$ 乗 [ $k$ は自然数：以降同]の時に、冪剰余Cは周期性を示して元の底mに戻ります。

### 4. 暗号への利用

それではこの規則性を暗号に利用するにはどうすればよいでしょうか。

冪剰余モデルの $m \times \text{mod } N$ で記載すれば、冪剰余Cの周期は $\lambda(N)$ になりますから、 $(k \times \lambda(N) + 1)$ 乗の時に冪剰余Cは周期性を示して元の底mに戻ります。この周期性と累乗指数とが持つ関係を暗号に利用します。

すなわち、暗号システムでは平文Mの要素である底mを指数eで累乗して、法Nに対する冪剰余Cを算出し、これを暗号文 $C_1$ の要素である数値 $c_1$ にします。これが暗号化です。そしてその暗号文 $C_1$ の要素である数値 $c_1$ を

$(k \times \lambda(N) + 1)$ 乗に合うような適切な指数dで累乗して、法Nで冪剰余Cを算出すれば、元の平文Mの要素である数値mが現れるはずです。これが復号化です(図1)。

この時大切なのは平文Mと暗号文 $C_1$ の間で暗号化用の指数eと復号化用の指数dをそれぞれ適切に定めることです。

今回はRSA暗号の発想の大きな端緒となった冪剰余の周期性が利用された背景について解説しました。

※なお、本稿では、慣習に従い累乗と冪乗の表記が混在していますが、両者を同じ意味として用いています。また、自然数に0を含めるとしています。

#### 参考文献

- ※1：ホームページの広場：第46回「HPKIのPKIを支えるRSA暗号について-その1 特徴-」  
上杉康夫 大阪医科大学医師会会報 (65) 38-45 (ISSN 2436-5424) 2026年3月  
[https://www.omp.ac.jp/u-deps/ompuda/report/pdf/report\\_65\\_p38-45.pdf](https://www.omp.ac.jp/u-deps/ompuda/report/pdf/report_65_p38-45.pdf)
- ※2：公開鍵暗号 - Wikipedia  
<https://ja.wikipedia.org/wiki/公開鍵暗号>
- ※3：RSA暗号の仕組み  
<https://kobayashi.hub.hit-u.ac.jp/topics/rsa.pdf>
- ※4：公開鍵暗号(RSA暗号)解説その2 仕組みについて  
[https://ndk.co.jp/wp-content/uploads/2023/11/tp\\_20231102-2.pdf](https://ndk.co.jp/wp-content/uploads/2023/11/tp_20231102-2.pdf)
- ※5：基礎から学ぶ整数論-RSA暗号入門 長嶋 祐二, 福田 一帆, P5 コロナ社 (2020/9/25)
- ※6：剰余演算 - Wikipedia  
<https://ja.wikipedia.org/wiki/剰余演算>
- ※7：【図解】素数とRSA暗号/署名の仕組み ~わかりやすい計算例とシーケンス, アルゴリズム~ | SEの道標  
<https://milestone-of-se.nesuke.com/nw-basic/tls/rsa-summary/>
- ※8：Periodicities of a Class of Infinite Integer Sequences Modulo  $n/r$   
[https://www.sciencedirect.com/science/article/pii/S0022314X89900528?ref=pdf\\_download&fr=RR-2&rr=a1b9d5d69d42fcb1](https://www.sciencedirect.com/science/article/pii/S0022314X89900528?ref=pdf_download&fr=RR-2&rr=a1b9d5d69d42fcb1)
- ※9：フェルマーの小定理 - Wikipedia  
<https://ja.wikipedia.org/wiki/フェルマーの小定理>
- ※10：原始根の定義と具体例(高校生向け) | 高校数学の美しい物語  
<https://manabitimes.jp/math/842>
- ※11：オイラーのφ関数 - Wikipedia  
<https://ja.wikipedia.org/wiki/オイラーのφ関数>
- ※12：RSA 暗号がようやく分かった気がしたのでまとめてみる  
<https://tsujimotter.hatenablog.com/entry/rsa>
- ※13：Carmichael function - Wikipedia  
[https://en.wikipedia.org/wiki/Carmichael\\_function](https://en.wikipedia.org/wiki/Carmichael_function)
- ※14：暗号解説(下) (新潮文庫) Kindle版 サイモン・シン(著), 青木薫(翻訳) 新潮社 (2007/7/1) 第VI章 アリスとボブは鍵を公開する PP149-175

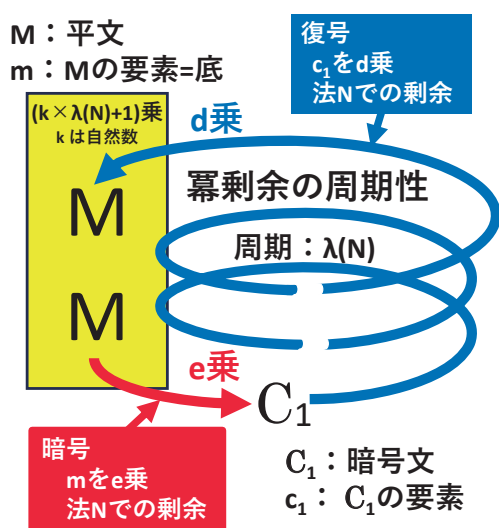


図1：暗号への利用