公開鍵暗号を解読せよ!—君もスパイになれる?—

楫　元
早稲田大学理工学部

2004 年 12 月 25 日–26 日, 湘南国際村センターにおいて, 現代数学入門市民講座および湘南数学セミナーの講師をさせていただきました. 簡単にその報告をしたいと思います.

現代数学入門市民講座では「素数を見つけて百万長者になろう!?」というタイトルで 75 分間の講演をしました. 詳細は述べませんが,

1. 素数とは?
2. 素数はどれくらい存在するか?
3. 素数の展覧会
4. 巨大素数の世界記録
5. なぜ素数を探すのか?

が, そのとき用いたスライドの目次です. 素数の定義から始めて, 素数が無限に多く存在することのユークリッドによる証明や, 素数の分布を記述する素数定理を紹介しました. そして, これまでに発見されている様々な印象的形をした素数を多数, 鑑賞していただき, メルセンヌ素数、フェルマー素数などにまつわる歴史, そして, 巨大素数発見の歴史を解説しました. 大きな桁数 (たとえば 1 千万桁以上) の素数の発見に多額の賞金が懸けられているという事実をひとつの糸口として, 素数 (数学) のもつ魅力を伝えたいという思いで話しました. 時間的余裕がありましたので講演の途中, 何回か質疑応答の時間を設けたところ, 講演内容に関係のあることないこと, さまざまな質問をいただき, 結局, 聴衆の皆様に講演を大いに盛り上げていただいた形となりました.

湘南数学セミナーでは, 一泊二日の日程で公開鍵暗号の一つ, 『RSA 暗号』について講義・演習をしました. そのときのタイトルをそのまま本稿の標題としてあります. 湘南数学セミナーは高校生対象の企画ですが, 実際は中学 1 年生から社会人の方まで, 年齢幅が 60 歳以上という広い層の方々が参加されました. 名簿を見るとその半数は中学生ということで, 最初どうなることかと少々心配にもなりましたが, 蓋を開けてみれば私の予想をはるかに凌ぐ圧倒的パワーで, 全くの杞憂に終りました. 年齢など関係なく, いますぐにでも早稲田大学の学生にしたいと思うような方が何人もいました.

以下に添付したのは, 湘南数学セミナーで配布したテキストのうち, 実際に用いた部分の抜粋です. 25 日の午後から夕食を挟んで夜にかけて §§1–4 を, 翌日午前中に §§5,6 を講義し, その合間には, 参加者各自がテキストの練習問題を解く時間を設けました. 参加者のレベルからすると問題のほとんどは易しすぎたようで, あっと言う間に解いてしまった人が随分いました. また, 大きな数の計算では電卓を使ってもよい, としてあったのですが, 敢えて使わずに筆算でガンガンやっている人もいました. 大学では, 最近, 要領の良さばかり気にして自らの手で試行錯誤することを嫌う学生を多く眼にしますが, このセミナーの参加者の方々を見ていると何だかホッとした気持ちになりました. 第一日目の締めくく

りはグループ対抗で暗号解読 (問 **4.2.3**) に挑戦したのですが, 全員が自分の分担を解読することができました. 時間が余ると, 知ったばかりの RSA 暗号の仕組みを応用した何やら新しいゲームを考え出して友達どうしで遊び始める人たちまで現れて, ただただ, その豊かな独創性と思考の柔軟さにはびっくりさせられました. とにかく, 皆さんすごいやる気と集中力で, 大学の教壇に立っているだけでは到底味わえない非常に貴重な体験をさせて頂きました.

市民講座および数学セミナーの参加者の皆様, このような素晴らしい機会を与えてくださった日本数学会広報委員の方々, そして, 大変お世話になりました湘南国際村センターのスタッフの方々に, この場をお借りして御礼申し上げます. 特に, 広報委員の川崎徹郎先生には 2 日間にわたりとても親切にサポートしていただきました. また, 湘南国際村センターの渡辺聖司様には, 準備の段階から最後の最後まで, こまやかなご配慮をいただきました. どうもありがとうございました.

0　まえがき

‘暗号’と言うと, 戦争やスパイ小説などを連想するかも知れません. インターネットが広く普及した現代社会では, 実は, さまざまなところで暗号が使われています. そのひとつに『公開鍵暗号』があります. ‘暗号’に‘公開 (鍵)’なんて, 言葉の組合せとしてはちょっと奇妙ですよね. でも実際, 暗号に変換する手順やそのための鍵となる情報が秘密ではなく公開されている暗号なのです. それなのに, 変換したその本人でさえ元に戻すことが出来ないという不思議な暗号です. 今年の湘南数学セミナーでは, 公開鍵暗号のうち最も一般的である『RSA 暗号』に焦点を当て, そのアイディアやトリックについて種明かしをしてみようと思います. そして, RSA 暗号の理論的裏付けとなっている数学—初等整数論—の面白さを皆さんと一緒に味わいたいと思います.

このテキストでは, 要となる命題や目新しい命題には証明を付けましたが, よく知られているであろう命題については証明は載せませんでした. ここに書かれている命題や証明がよく解らなくても全く心配はありません. 例や問に挙げてある計算を自分の手を動かして少しずつやってみれば, RSA 暗号の仕組みはよく理解できるようになります. 問については無理に全部を解く必要はありません. 面白そうだな, と思ったものを解いてみてください.

付記: 市民講座「素数を見つけて百万長者になろう!?」と, その内容をセットにして考えておりましたので, 湘南数学セミナー「公開鍵暗号を解読せよ!—君もスパイになれる?—」(およびそのテキスト) では, 素数はかなり軽い扱いとなっていることを断わりしておきます.

1　RSA 暗号, I

1.1　公開鍵暗号と秘密鍵暗号

まず初めに, **暗号**とは, 送信者がメッセージを別の形にすることにより, 第三者には秘匿し, 意図した受信者だけが判読できるようにする秘密通信の手段のこと, となる. もとのメッセージそのものを**平文** (“ひらぶん” と読む), 第三者に秘匿する形にしたメッセージを

暗号文という. 平文を暗号文に変換する過程を**暗号化**といい, その逆の過程を**復号**, または, **復号化**という.

現在使われている多くの暗号では, 暗号化復号化のアルゴリズム自身は公開されている. そのアルゴリズムを適用する際に重要な役割を果たすのが**鍵**と呼ばれる情報である. これは, 一種のパスワード, または, 暗証番号のような情報である. この鍵情報を導入することにより, 暗号は, アルゴリズムが公開されてもその秘匿性を保つことができる. 暗号化の際に用いられる鍵を**暗号化鍵**といい, 復号化の際に用いられる鍵を**復号化鍵**という. 復号化鍵を知らされていない第三者が暗号文の内容を (不正に) 解明することを, 復号化と区別して, **解読**という.

暗号化鍵と復号化鍵とが一致している暗号を, **対称暗号**, または, **共通鍵暗号**といい, 暗号化鍵と復号化鍵とが異なる暗号を, **非対称暗号**という. 対称暗号ではその共通な鍵を秘密にする必要があるが, 非対称暗号では暗号化鍵は公開しても構わない (もちろん, 復号化鍵は秘密にする). そこで, 対称暗号, 非対称暗号を, それぞれ, **秘密鍵暗号**, **公開鍵暗号**とも呼ぶ. 秘密鍵暗号の発祥は, 紀元前にまで遡るが, 公開鍵暗号のアイディアは, ディフィー (Whitfield Diffie) とヘルマン (Martin Hellman) により, 1976 年に発表された (暗号理論一般については, [3, 第 3 章], [4], [5, 第 I 部], [6] 参照).

対称暗号に分類できる非常に単純な例を挙げよう.

例. 紀元前 100 年頃, ローマで生まれた武将, ジュリアス・シーザー (ユリウス・カエサル) は, 「3 個, アルファベットをずらす」という規則により, 平文の文字を置き換えるという暗号を通信に用いていたとのことである. つまり, 「A」→「D」, 「B」→「E」, . . . , 「W」→「Z」, さらに, 「X」→「A」, 「Y」→「B」, 「Z」→「C」と文字を置き換える. たとえば平文

「HAYAMA」

の暗号文は,

「KDBDPD」

となる. 受け取った暗号文を復号化は, 逆方向に「3 個, アルファベットをずらす」という規則で行えばよい. この場合, 大げさに言えば, アルゴリズムは「アルファベットをずらす」である. また, 暗号化および復号化における鍵は, 共に, 「3」ということになる. したがって, これは共通鍵暗号の一つである. この暗号は**シーザー暗号**と呼ばれる.

シーザー暗号は, 余りに単純な暗号ゆえ, アルゴリズムを知られたら, 簡単に解読されてしまう. たとえば, 鍵は (自明なものも含めて) 26 種類しかないので, 総当たりにすべての鍵を試せば, 解読が可能となる. □

さて, 公開鍵暗号においては, 暗号化鍵を知っても復号化鍵を求めること, そして, 暗号文を平文に戻すことが事実上不可能, ということであるが, これは, 非常に不思議な感じがするかもしれない.

このセミナーでは, 公開鍵暗号の原理を初めて実現した **RSA 暗号**とよばれる暗号について取上げる. RSA 暗号とは, MIT (マサチューセッツ工科大学) の計算機科学者, リヴェスト (Ronald L. Rivest), シャミア (Adi Shamir), アドルマン (Leonald Adleman) により発明され, 1977 年に発表された, 最も古くからある, 最も有名な公開鍵暗号であり, その信頼性は大きな数の素因数分解の困難さに基づいている. 発明者 3 人の名前の頭文字をとって, RSA 暗号と呼ばれる. 実際に計算してみることにより, その仕組みの巧妙さを味わっ

てみたい.

> [Ronald L. Rivest, Adi Shamir, Leonald Adleman: A Method of Obtaining Digital Signatures and Public-Key Cryptosystems, M. I. T. Laboratory for Computer Science, Technical Memo **82**, April 1977. Reprinted in Communications of the ACM **21**, February 1978, pp. 120–126]

1.2 RSA 暗号とは?

鍵生成: 自然数 n, e, d を次の条件を満たすようにとる:

- 相異なる素数 p, q により $n = pq$ となる n
- $\varphi(n) = (p-1)(q-1)$ と互いに素となる e
- $ed \equiv 1 \pmod{\varphi(n)}$ となる d

ただし, '$\varphi(n)$' はオイラーの関数であり, 等式 '$\varphi(pq) = (p-1)(q-1)$' はオイラーの公式の帰結である. また, '$ed \equiv 1 \pmod{\varphi(n)}$' は $\varphi(n)$ を法として e との積 ed が 1 と合同であることを意味する. 見知らぬ単語がいきなり出てきたが, 心配する必要はない. ここに現れる数学の術語や条件を満たす自然数の求め方については, すべて, 後に順々に説明してゆく:

- 素数 → §2.2
- オイラーの関数 $\varphi(n)$ → §5.1
- オイラーの公式 $\varphi(pq) = (p-1)(q-1)$ → §5.1
- 互いに素 → §2.1
- 合同 $\equiv$, 法 $\pmod{\ }$ → §3.1
- e の求め方 → 互いに素であることの判定 → ユークリッドの互除法 → §2.3
- d の求め方 → 一次合同式の解法 → §3.4

定義. n, e を**暗号化鍵**といい, d (または, p, q) を**復号化鍵**という.

暗号化鍵 n, e は公開しても構わないが, 復号化鍵 d (および, p, q) は秘密にしておく. これらは, それぞれ, **公開鍵**, **秘密鍵**とも呼ばれる.

簡単のために, 自然数を平文とする場合について考える. 平文 x が

$$x < n$$

を満たす自然数であるとする ($x \geq n$ の場合は, この条件を満たすように x を数字列として分割すればよい).

暗号化復号化のアルゴリズムは, 次で与えられる:

暗号化: 平文 x に対して

$$y \equiv x^e \pmod{n}, \quad 0 \leq y < n$$

となる y を求める.

ここでは, 無駄を省くため条件 $0 \leq y < n$ を課すが, 本質的ではない. この y が平文 x に対する暗号文である.

復号化: 暗号文 y に対して

$$z \equiv y^d \pmod{n}, \quad 0 \leq z < n$$

となる z を求める.

このとき, 次が成り立つ:

定理 1.2.1 (RSA 暗号).

$$x = z.$$

この定理 1.2.1 の基礎にあるのが 'フェルマーの小定理' と呼ばれる初等整数論の定理である. 実際には, フェルマーの小定理から導かれる系が RSA 暗号の定理 1.2.1 の証明で使われる. これらの命題やその証明は, 後に与える:

- フェルマーの小定理とその系 → §5.2
- RSA 暗号の定理 1.2.1 の証明 →§6.1

2 ユークリッドの互除法

2.1 最大公約数

定義. 整数 a, b に対して, $b \neq 0$ であり, かつ, ある整数 q により

$$a = qb$$

と表されるとき, a は b で**割り切れる**, そして, b は a を**整除する**という. また, a を b の**倍数**, そして, b を a の**約数**という. 約数を**因数**ともいう.

例. 6 の約数は, $-6, -3, -2, -1, 1, 2, 3, 6$ であり, 全部で 12 個ある. 一方, 6 の倍数は, $\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots$ と, 無限にある. とくに, 0 は 6 の倍数である. □

命題 2.1.1 (割り算). 整数 a と自然数 b に対して,

$$a = qb + r, \quad 0 \leq r < b \tag{2.1.1}$$

を満たす整数 q, r が存在し, しかも, ただ一組である.

定義. 命題 2.1.1 の q を, a の b による割り算の**商**, または, **整商**といい, r をその**余り**という.

例. 204 の 85 による割り算を考えると,

$$204 = 2 \times 85 + 34$$

となるので, 商は 2, 余りは 34 である. では, 85 の 204 による割り算はどうなるか?

$$85 = 0 \times 204 + 85$$

となり, 商は 0, 余りは 85 となる. □

定義. 整数 a, b に対して, $a \neq 0$ または $b \neq 0$ のとき, それらの共通の約数のうちで最大のものを**最大公約数**といい,

$$(a, b)$$

と書き表わす.

例. 12 と 18 の最大公約数は 6 である, ということは $(12, 18) = 6$ と表される. $(18, 12) = 6$ と書いても意味することは同じである. □

定義. 整数 a, b の最大公約数が 1 であるとき, すなわち, $(a, b) = 1$ のとき, a と b は**互いに素**であるという.

命題 2.1.2. 整数 a, b, n に対して, ab が n で割り切れるとき, a と n が互いに素ならば, b は n で割り切れる.

2.2 素数

定義. 自然数 n に対して, ± 1 と $\pm n$ 以外の n の約数を, n の**真の約数**という. 真の約数をもつ n を**合成数**といい, $n \neq 1$ かつ真の約数をもたない n を**素数**という.

つまり, 正の約数の数が三個以上ならば合成数, 二個ならば素数というわけである. 約数が一個しかない 1 は特別扱いして, 合成数とも素数とも考えない.

例. $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ は素数である. □

定理 2.2.1 (素因数分解). 合成数 n は, 素数の積に分解される. また, その分解の仕方は素数の順序を除いては一意的である. すなわち, 同じ素数の積を一つのべきにまとめれば, 次が成り立つ:

(1) 相異なる素数 p, q, r, $\dots$ と自然数 a, b, c, $\dots$ により, n は

$$n = p^a q^b r^c \cdots \tag{2.2.1}$$

と表される.

(2) 式 (2.2.1) に現れる素数 $p, q, r, \dots$, そして, 対応する指数 $a, b, c, \dots$ は, n により順序を除いて一意的に定まる.

定義. 自然数 n に対して, (2.2.1) を n の**素因数分解**といい, p, q, r, $\dots$ を n の**素因数**という. その場合, 特に断らない限り, p, q, r, $\dots$ は相異なる素数であり, a, b, c, $\dots$ は自然数であると仮定する.

系 2.2.2. 自然数 $m_1, m_2, \dots, m_k$ のどの二つも互いに素であるとき, 整数 a がこれらのいずれでも割り切れるならば, a は積 $M = m_1 m_2 \cdots m_k$ で割り切れる.

2.3 ユークリッドの互除法

ユークリッドの互除法とは, 二つの整数の最大公約数を求めるためのアルゴリズムのことである. そのミソは, 素因数分解しなくても, 一定の操作を繰り返すことにより二つの整数の最大公約数が簡単に求められる, というところにある. 大きな数の素因数分解は, 高性能の計算機を用いても, 特別な場合を除いては, 非常に困難であるが, 最大公約数については, ユークリッドの互除法により速く簡単に求めることができる. これは, 紀元前三百年の頃, ユークリッドにより著されたとされる “ストイケイア (原論)” [2] に述べられている.

定理 2.3.1 (ユークリッドの互除法). 自然数 a, b に対して, 次の操作を考える:
(ステップ 1) a の b による割り算の余りを r_1 とする;
(ステップ 2) b の r_1 による割り算の余りを r_2 とする;
(ステップ 3) r_1 の r_2 による割り算の余りを r_3 とする;
$\vdots$
以下, 同様にして, $r_{i-1} \neq 0$ である限り
(ステップ i) r_{i-2} の r_{i-1} による割り算の余りを r_i とする;
を, i の値を 1 ずつ増やしながら繰り返す. このとき, 次が成り立つ:

(1) ある有限回目のステップにおいて, 余り r_i は必ず 0 となる.

(2) $r_{n+1} = 0$ とすると

$$(a, b) = r_n$$

すなわち, r_n は a, b の最大公約数となる.

つまり, 式に書き下してみれば, 次のようになる. (ステップ i) での r_{i-2} の r_{i-1} による割り算の商を q_i とすれば,

$$\begin{aligned} a &= q_1 b + r_1, & b &> r_1, \\ b &= q_2 r_1 + r_2, & r_1 &> r_2, \\ r_1 &= q_3 r_2 + r_3, & r_2 &> r_3, \\ r_2 &= q_4 r_3 + r_4, & r_3 &> r_4, \\ &\vdots \\ r_{i-2} &= q_i r_{i-1} + r_i, & r_{i-1} &> r_i, \\ &\vdots \end{aligned} \tag{2.3.1}$$

と, 順々に割り算をしてゆき,

$$r_{n-1} = q_{n+1} r_n, \quad r_{n+1} = 0.$$

と, 余りが 0 になった時点での r_n が, a と b の最大公約数となる, ということである. なお, $a < b$ であっても構わない. その場合は, (ステップ 1) において, 商が 0, $r_1 = a$ となるだけである.

例. $85, 204$ の最大公約数を求めてみよう. ユークリッドの互除法 2.3.1 を実行すると

$$\begin{aligned} 85 &= 0 \times 204 + 85 \\ 204 &= 2 \times 85 + 34 \\ 85 &= 2 \times 34 + 17 \\ 34 &= 2 \times 17 + 0 \end{aligned}$$

となるので, 最大公約数は

$$(85, 204) = 17.$$

となる. □

以上のように, 有限回の計算の後に目的に達するあいまいさのない操作, 一連の手続きを**アルゴリズム**と呼ぶ. 昔は, 互除法のこと自身をアルゴリズムと呼んだそうである.

さて, ユークリッドの互除法のアルゴリズムを完了するのに, 何回の割り算が必要か考えてみると, 上の証明から, 最大 $b+1$ 回の割り算で完了することがわかる. 実は, もっと精密に次のことが知られている (証明については, [1, p. 15] 参照):

定理 2.3.2 (ラメの定理). 自然数 a, b に対して, $a > b$ とし b を 10 進数表示した際の桁数を s とする. このとき, a, b に対してユークリッドの互除法 2.3.1 を実行すると, 最大 $5s$ 回の割り算でアルゴリズムは完了する.

必要な割り算の回数が, a, b 自身でなく, その桁数に依存していることに注意しよう. これは, 大雑把に言うと, 計算機で実際にユークリッドの互除法を実行する際, 非常に速く計算できる, ということを意味する. たとえば, a, b が 10 進数表示で 10 桁の数の場合, 割り

算は, 何十億回も行う必要はなく, せいぜい 50 回も行えば, 最大公約数が求められるわけである.

例. 144, 89 の最大公約数求めてみよう. ユークリッドの互除法 2.3.1 を実行すると

$$\begin{aligned}
144 &= 1 \times 89 + 55 \\
89 &= 1 \times 55 + 34 \\
55 &= 1 \times 34 + 21 \\
34 &= 1 \times 21 + 13 \\
21 &= 1 \times 13 + 8 \\
13 &= 1 \times 8 + 5 \\
8 &= 1 \times 5 + 3 \\
5 &= 1 \times 3 + 2 \\
3 &= 1 \times 2 + 1 \\
2 &= 2 \times 1 + 0
\end{aligned}$$

となるので, 最大公約数は 1 となり, 144, 89 は互いに素である. □

この例では, アルゴリズムを完了するのに, 10 回の割り算が必要である. これは, 89 の桁数 2 のちょうど 5 倍であり, ラメの定理 2.3.2 での回数の評価に無駄の無いことがわかる.

問 2.3.3. 1960, 103 の最大公約数を求めよ.

3 合同式

3.1 合同

定義. 自然数 n と整数 a, b に対して, 差 $a - b$ が n の倍数であるとき, a と b とは n を**法**として**合同**であるといい,

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

と書き表す. つまり, n で割り算して余りが等しいとき, そして, そのときに限り, n を法として合同であるという.

例. $1 - 4 = -3 = (-1) \cdot 3$ は 3 の倍数なので,

$$1 \equiv 4 \pmod{3}$$

であり, $4 - (-5) = 9 = 3 \cdot 3$ も 3 の倍数なので,

$$4 \equiv -5 \pmod{3}$$

となる. また, 混乱が起きない場合は $\pmod 3$ を一つ省略して,

$$1 \equiv 4, \quad 4 \equiv -5 \pmod{3}$$

と書くこともある.

$$1 \equiv 4 \equiv -5 \pmod 3$$

と一本の式に書いてもよい. □

普通の等号 "=" と同じ概念のように思われるかもしれないが, 後に見るように, 全く異なる点があるので注意が必要である.

例. 条件

$$x \equiv 3 \pmod 5, \quad 14 \leq x \leq 19$$

を満たす整数 x を求めてみよう. $x \equiv 3 \pmod 5$ とは, $x-3$ が 5 の倍数, ということだから,

$$x = 3 + 5k, \quad k \in \mathbb{Z}$$

と表されることと同値である. したがって,

$$14 \leq 3 + 5k \leq 19$$

を満たす k を求めればよい. $k = 3$ となり答は, $\underline{x = 18}$ となる. □

問 3.1.1. ここに何本かの鉛筆がある. 1 ダースずつ箱に詰めてゆくと, 5 本余った. 200 本は無いとするとき, 鉛筆は最大で何本あるか? (ヒント: 1 ダースは 12 本)

問 3.1.2. 1 月 3 日が日曜日の年, 1 月最後の日曜日は何日か? (ヒント: 1 月は 31 日までである)

3.2 加減乗

命題 3.2.1 (加減乗). 自然数 n と整数 a, a', b, b' に対して, $a \equiv a', b \equiv b' \pmod n$ ならば, 次が成り立つ:

$$a + b \equiv a' + b' \pmod n$$
$$a - b \equiv a' - b' \pmod n$$
$$ab \equiv a'b' \pmod n$$

証明. 仮定により, $a - a', b - b'$ はいずれも n の倍数である. したがって, その和, 差, そして倍数の和である.

$$(a + b) - (a' + b') = (a - a') + (b - b')$$
$$(a - b) - (a' - b') = (a - a') - (b - b')$$
$$ab - a'b' = (a - a')b + a'(b - b')$$

はいずれも n の倍数である. すなわち, 求める式が成り立つ. ■

この命題の意味するところは, 等式の場合と全く同様に, 合同式について辺々の足し算, 引き算, そして, 掛け算ができる, ということである.

例. 条件

$$5 + x \equiv 1 \pmod 9, \quad 0 \leq x \leq 9$$

を満たす整数 x を求めてみよう. この合同式から, 恒等的に成り立つ合同式, $5 \equiv 5 \pmod 9$ を辺々引き算すると, 命題 3.2.1 により,

$$5 + x - 5 \equiv 1 - 5 \pmod 9$$

が成り立つ. 両辺をそれぞれ計算すると

$$x \equiv -4 \equiv 5 \pmod 9$$

となり, $0 \leq x \leq 9$ を満たすのは, $\underline{x = 5}$ となる. □

問 3.2.2. 次の条件を満たす整数 x を求めよ:

$$x + 2 \equiv 6 \pmod 9, \quad 0 \leq x \leq 9.$$

命題 3.2.1 から直ちに次が導かれる:

系 3.2.3 (べき). 自然数 n と整数 a, a' に対して $a \equiv a' \pmod n$ ならば, 任意の自然数 m に対して次が成り立つ:

$$a^m \equiv a'^m \pmod n.$$

これはつまり, 等式の場合と同様に, 合同式の両辺をべき乗することができる, ということを保証している.

例. 29^{1000} を 7 で割り算したときの余りを求めてみよう. 実際に 29^{1000} を計算して 7 で割り算してもよいが, 次のように考えるととても簡単に求められる. $29 = 4 \times 7 + 1$ だから,

$$29 \equiv 1 \pmod 7$$

である. したがって, 両辺を 1000 乗すると系 3.2.3 により

$$29^{1000} \equiv 1^{1000} = 1 \pmod 7$$

となる. すなわち $\underline{\text{余りは}\,1}$ である. □

上の説明から直ちにわかるように, 自然数 n で割り算して 1 余る整数 a は, 何乗しても n で割り算したときの余りは 1 である.

問 3.2.4. 10^{10000} を 13 で割り算したときの余りは幾つか? (ヒント: $1001 = 7 \times 11 \times 13$)

3.3 除

これまでは合同の世界での足し算引き算掛け算について考えてきたが, 割り算についてはどうか? このセクションでは割り算について考えよう.

たとえば, 整数 a を自然数 b で "割り算" して $a \equiv qb \pmod{n}$ となったとしよう. このとき命題 2.1.1 のように, この "商" q は, a, b により (n を法として) ただ一つに定まるだろうか?

また, $c \not\equiv 0 \pmod{n}$ となる整数 c については, 任意の整数 a, b に対して

$$ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{n} \tag{3.3.1}$$

は成り立つのだろうか? たとえば, 次の推論にはどこに誤りがあるか?

> $14 - 8 = 6$ は明らかに 6 の倍数なので, $14 \equiv 8 \pmod{6}$ である. したがって,
>
> $$7 \times 2 \equiv 4 \times 2 \pmod{6}$$
>
> である. 2 は 6 の倍数ではないから $2 \not\equiv 0 \pmod{6}$ となる. そこで, 両辺を 2 で割り算すると,
>
> $$7 \equiv 4 \pmod{6}$$
>
> となる?

もちろん, $7 - 4 = 3$ は 6 の倍数ではないので, これは正しくない.

普通の数の計算では, 詳しく考えると,

$$\begin{aligned} ac = bc \text{ かつ } c \neq 0 &\Rightarrow (a-b)c = 0 \text{ かつ } c \neq 0 \\ &\Rightarrow a - b = 0 \\ &\Rightarrow a = b \end{aligned}$$

と推論するところだが, 合同式に関しては, これは一般に正しくない. どこがうまく行かないかというと, 二番目の $\Rightarrow$ では,

$$xy = 0 \Rightarrow x = 0 \text{ または } y = 0$$

という性質を使っている. しかし, 合同式ではこれが成り立たない. 実際,

$$(7 - 4) \times 2 = 3 \times 2 = 6 \equiv 0 \pmod{6}$$

にもかかわらず, $7 - 4 = 3 \not\equiv 0 \pmod{6}$ であり, $2 \not\equiv 0 \pmod{6}$ である. 合同の世界では 0 について,

$$0 \equiv 2 \times 3 \pmod{6}$$

という奇妙な "因数分解" がなされる.

さて, このようにして, 合同式においては, 普通の数と同様に割り算はしてよいわけではなく, とても注意が必要であることが納得されたと思う. しかし, 次のことは成り立つ:

命題 3.3.1 (除). 自然数 n と整数 a, b, c に対して, $(c, n) = 1$ ならば次が成り立つ:

$$ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{n}$$

つまり, 整数 c に対して, 通常の等号の世界における割り算の条件は $c \neq 0$ であるが, **合同の世界における割り算の条件**は $(c, n) = 1$ であり, $c \not\equiv 0 \pmod{n}$ では不十分なわけである.

証明. 仮定により, $ac - bc = (a - b)c$ は n で割り切れる. 命題 2.1.2 により, $(c, n) = 1$ なので $a - b$ は n で割り切れる. すなわち, $a \equiv b \pmod{n}$ である. ■

3.4 一次合同式

定義. 自然数 n と整数 a, b に対して, x を未知数とする合同式

$$ax \equiv b, \quad a \not\equiv 0 \pmod{n} \tag{3.4.1}$$

の整数解を求める問題を考える. (3.4.1) を**一次合同式**という. 一次合同式に対して, **解**といったら整数解のことと約束する.

命題 3.4.1 (一次合同式の解). 一次合同式 (3.4.1) において, $d = (a, n)$ とおくとき, 次が成り立つ:

(1) 次は同値である:

  (a) (3.4.1) は解をもつ;

  (b) b が d の倍数である.

(2) $d = 1$ ならば, (3.4.1) の解は, n を法としてただ一つである.

整数 x に対して, x が一次合同式 (3.4.1) を満たすことと, 整数 y が存在して, x, y が

$$ax + ny = b \tag{3.4.2}$$

を満たすこととは同値であることに注意しよう. (3.4.2) は, **一次不定方程式**と呼ばれるものである.

証明. (1) (a) $\Rightarrow$ (b) (3.4.1) が解 x を持つとすれば, ある整数 y により

$$ax + ny = b$$

が成り立つ. a, n は共に d の倍数なので, b も d の倍数となる.

(a) $\Leftarrow$ (b) まず,

$$ax \equiv d \pmod{n} \tag{3.4.3}$$

が解を持つことを示そう. そのためには,

$$ax + ny = d \tag{3.4.4}$$

を満たす整数 x, y が存在することを示せばよい.

まず, $a > 0$ の場合に考えよう. 自然数 a, n に対してユークリッドの互除法 2.3.1 を適用し,

$$r_m = d, \quad r_{m+1} = 0$$

となったとする. その際に現れる式 $r_{m-2} = q_m r_{m-1} + r_m$ から,

$$d = r_{m-2} - q_m r_{m-1}$$

となる. これに, 一つ前のステップに現れる式を r_{m-1} について解いた式

$$r_{m-1} = r_{m-3} - q_{m-1} r_{m-2}$$

を代入すると,

$$\begin{aligned} d &= r_{m-2} - q_m r_{m-1} \\ &= r_{m-2} - q_m (r_{m-3} - q_{m-1} r_{m-2}) \\ &= -q_m r_{m-3} + (1 + q_m q_{m-1}) r_{m-2} \end{aligned}$$

を得る. さらに, 一つ前のステップに現れる式を r_{m-2} について解いた式

$$r_{m-2} = r_{m-4} - q_{m-2} r_{m-3}$$

を代入すると,

$$\begin{aligned} d &= -q_m r_{m-3} + (1 + q_m q_{m-1}) r_{m-2} \\ &= -q_m r_{m-3} + (1 + q_m q_{m-1})(r_{m-4} - q_{m-2} r_{m-3}) \\ &= (1 + q_m q_{m-1}) r_{m-4} - (q_m + (1 + q_m q_{m-1}) q_{m-2}) r_{m-3} \end{aligned}$$

を得る. $r_{-1} = a, r_0 = n$ とおけば, $i = 0, 1, \ldots, m-1$ について

$$r_{i+1} = r_{i-1} - q_{i+1} r_i$$

が成り立っているので, 上の式変形を繰り返すことにより (厳密には, 数学的帰納法を用いると), $i = 0, 1, \ldots, m-1$ について, d はある整数 c_{i-1}, c_i を用いて,

$$d = c_{i-1} r_{i-1} + c_i r_i$$

と表される. したがって, とくに, $i = 0$ のとき,

$$ac_{-1} + nc_0 = d$$

となり,

$$x = c_{-1}, \quad y = c_0$$

は一次不定方程式 (3.4.4) の解である.

$a < 0$ の場合については, (3.4.4) のかわりに

$$(-a)x + by = d \tag{3.4.5}$$

に対して上の証明を適用すると, 解が一つ得られる. その (3.4.5) の解を $x = c_{-1}$, $y = c_0$ とすれば,

$$x = -c_{-1}, \quad y = c_0$$

が (3.4.4) の解となることは明かだろう.

さて, こうして (3.4.3) は解を持つことが解った. 解をあらためて $x = x_0$ と書くことにしよう.

$$ax_0 \equiv d \pmod{n}$$

となる. $b' = b/d$ とおいて, この両辺を b' 倍すると

$$a(b'x_0) \equiv b'd = b \pmod{n}$$

を得るので, $x = b'x_0$ は (3.4.1) の解となることがわかる.

(2) $x = x_1, x_2$ が (3.4.1) の解ならば,

$$ax_1 \equiv b \equiv ax_2 \pmod{n}$$

となる. $(a, n) = d = 1$ なので, 命題 3.3.1 により

$$x_1 \equiv x_2 \pmod{n}$$

を得る. ■

一次合同式の解法 (その 1): 一次合同式

$$ax \equiv b \pmod{n} \tag{3.4.1}$$

は次の手順で解けばよい:

(1) ユークリッドの互除法 2.3.1 により $d = (a, n)$ を求める.

(2) b を d により割り算する.

(a) b が d で割り切れない場合は, 解は存在しない.

(b) b が d で割り切れる場合は, $b' = b/d$ とおく. そして,

i. 一次合同式

$$ax_0 \equiv d \pmod{n} \tag{3.4.3}$$

を満たす x_0 を, (1) でユークリッドの互除法 2.3.1 を行う際に現れた式から逆算して求める.

ii. (3.4.3) の解を b' 倍すれば, (3.4.1) の解が一つ得られる. すなわち, $x = b'x_0$ は (3.4.1) の解の一つである.

例. 上の解法の手順にしたがって, 一次合同式

$$85x \equiv 34 \pmod{204} \tag{3.4.6}$$

を解いてみよう.

(1) ユークリッドの互除法 2.3.1 により $d = (85, 204) = 17$ となる.

(2) $b = 34$ は $d = 17$ で割り切れる. $b' = 34/17 = 2$ とおく.

(b-i) 一次合同式

$$85x_0 \equiv 17 \pmod{204} \tag{3.4.7}$$

を満たす x_0 を求めよう. ユークリッドの互除法 2.3.1 を実行した際の式, $204 = 2\times 85+34$, $85 = 2 \times 34 + 17$ を用いて, $85 \times 5 - 2 \times 204 = 17$ が得られていたので,

$$85 \times 5 \equiv 17 \pmod{204}$$

である. したがって, $x_0 = 5$ は (3.4.7) を満たす.

(b-ii) $x_0 = 5$ を $b' = 2$ 倍すれば (3.4.6) の解の一つ, $x = 2 \times 5 = 10$ が得られる. □

一次合同式 (3.4.1) において, 係数 a と法 n とが互いに素である場合には, ユークリッドの互除法 2.3.1 で現れる式を用いて, 合同式のまま直接解くこともできる. 例で見てみよう.

例. 一次合同式

$$7x \equiv 1 \pmod{18} \tag{3.4.8}$$

を解いてみよう. ユークリッドの互除法 2.3.1 により $(7, 18) = 1$ となり, 命題 3.4.1 によりただ一つの解が存在する. ユークリッドの互除法 2.3.1 を実行した際に現れた式

$$\begin{aligned} 18 &= 2 \times 7 + 4 \\ 7 &= 1 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \end{aligned}$$

を利用して, (3.4.8) の x の係数が 1 となるように変形しよう.

まず, $18 = \underline{2} \times 7 + 4$ にならって, 恒等的に成り立つ式

$$18x \equiv 0 \pmod{18}$$

から (3.4.8) の $\underline{2}$ 倍:

$$14x \equiv 2 \pmod{18}$$

を引き算すると,

$$4x \equiv -2 \pmod{18} \tag{3.4.9}$$

を得る. 次に, $7 = \underline{1} \times 4 + 3$ にならって, (3.4.8) から (3.4.9) の $\underline{1}$ 倍を引き算すると,

$$3x \equiv 3 \pmod{18} \tag{3.4.10}$$

を得る.

ここで, 思わず両辺を 3 で割り算して,

$$x \equiv 1 \pmod{18}$$

と変形したくなるところだが, 明らかに $x = 1$ は (3.4.8) を満たさない. $(3, 18) = 3 \neq 1$ であり, **合同の世界における割り算の条件が満たされていないこと**に注意. ここは非常に間違えやすいところ. 正しくは, 次のようにする:

$4 = \underline{1} \times 3 + 1$ にならって, (3.4.9) から (3.4.10) の $\underline{1}$ 倍を引き算すると,

$$x \equiv -5 \equiv 13 \pmod{18}$$

となる. したがって, 解が存在するならば, それは $x \equiv 13 \pmod{18}$ でなければならないが, 解がただ一つ存在することはわかっているので, これがそのただ一つの解である. また, 以上の計算では, 命題 3.2.1 を繰り返し使っていることに注意しよう. □

以上の手順をまとめると, 次を得る:

一次合同式の解法 (その 2): 一次合同式

$$ax \equiv b \pmod{n} \tag{3.4.1}$$

において, $(a, n) = 1$ の場合, 解は次の手順で求められる:

(1) 恒等的に成り立つ一次合同式,

$$nx \equiv 0 \pmod{n} \tag{3.4.11}$$

を考える.

(2) (3.4.1) の x の係数 a と(3.4.11) の x の係数 n に対して, ユークリッドの互除法 2.3.1 を適用し, x の係数が 1 となる一次合同式を求める.

(3) (2) で得られた一次合同式を

$$x \equiv x_0 \pmod{n}$$

とすれば, (3.4.1) の解は n を法としてただ一つ存在し, $x = x_0$ で与えられる.

問 3.4.2. 次の一次合同式を解け:

$$103x \equiv 3 \pmod{1960}. \tag{3.4.12}$$

問 3.4.3. 次の一次合同式を解け:

(1) $17x \equiv 1 \pmod{24}$

(2) $13x \equiv 2 \pmod{36}$

問 3.4.4. 某研究室の 1999 年忘年会では, 350cc の缶ビールを何ケースか開けて, 参加者全員が仲よく 7 本ずつ飲んだところ, 最後に 1 本だけ残った. この研究室の所属メンバーは 25 名であるが, 忘年会に参加したのはそのうち何名か? (ヒント: 缶ビールは通常, 1 ケースに 24 本入っている)

4 RSA 暗号, II

4.1 計算の実際

例. まず鍵を選ぶ. 相異なる素数として $p = 2$, $q = 17$ をとり, $n = 2 \times 17 = 34$ とする. オイラーの公式 5.1.1 を用いると

$$\varphi(n) = (2-1)(17-1) = 16 = 2^4$$

だから, 2^4 と互いに素となる e として $e = 3$ と選んでみる. 暗号化鍵は $n = 34$, $e = 3$ である. これをひとまとめにして,

$$(n, e) = (34, 3)$$

と書くことにしよう.

次に, 復号化鍵 d を求める. $e = 3, \varphi(n) = 16$ だから, 一次合同式

$$3d \equiv 1 \pmod{16} \tag{4.1.1}$$

を満たす d を求めればよい. 一次合同式の解法, その 2 (p. 17) にしたがって, (4.1.1) を解いてみよう. 16 と 3 にユークリッドの互除法 2.3.1 を適用したと考えて, 恒等的に成り立つ式,

$$16d \equiv 0 \pmod{16}$$

から (4.1.1) の 5 倍, $15d \equiv 5 \pmod{16}$ を引き算すればよい. すると,

$$d \equiv -5 \equiv 11 \pmod{16}$$

を得る. したがって, たとえば,

$$d = 11$$

が復号化鍵である.

さて, $0 \leq x < n = 34$ を満たす平文として,

$$x = 26$$

を暗号化してみよう.

$$x^e = 26^3 \equiv (-8)^3 = (-8)^2 \cdot (-8) \equiv (-4) \cdot (-8) \equiv 32 \pmod{34}$$

となるので

$$y = 32$$

が暗号文である.

次に, これを復号化してみよう.

$$y^d = 32^{11} \equiv (-2)^{11} = ((-2)^5)^2 \cdot (-2) \equiv 2^2 \cdot (-2) = -8 \equiv 26 \pmod{34}$$

となり, 確かにもとの平文 $x = 26$ が復号化された. □

例. 相異なる素数として $p = 3$, $q = 13$ をとり, $n = 3 \times 13 = 39$ とする. オイラーの公式 5.1.1 を用いると

$$\varphi(n) = (3-1)(13-1) = 24 = 2^3 \cdot 3$$

だから, $2^3 \cdot 3$ と互いに素となる e として $e = 5$ と選んでみる. 暗号化鍵は,

$$(n, e) = (39, 5)$$

である. 次に, 復号化鍵を求める. $e = 5$, $\varphi(n) = 24$ だから, 一次合同式

$$5d \equiv 1 \pmod{24} \tag{4.1.2}$$

を満たす d を求めればよい. (4.1.2) を解いてみよう. 一次合同式の解法, その 2 (p. 17) にしたがって, 24 と 5 にユークリッドの互除法 2.3.1 を適用して考えてもよいが, (4.1.2) の 5 倍, $25d \equiv 5 \pmod{24}$ から恒等的に成り立つ式,

$$24d \equiv 0 \pmod{24}$$

を引き算する方がより簡単である (これは, 余りに負の数を許した “ユークリッドの互除法” である). すると,

$$d \equiv 5 \pmod{24}$$

を得るので, たとえば,

$$d = 5$$

が復号化鍵である.

さて, $0 \leq x < n = 39$ を満たす平文として,

$$x = 37$$

を暗号化してみよう.

$$x^e = 37^5 \equiv (-2)^5 = -32 \equiv 7 \pmod{39}$$

となるので

$$y = 7$$

が暗号文である.

次に, これを復号化してみよう.

$$y^d = 7^5 = (7^2)^2 \cdot 7 \equiv 10^2 \cdot 7 = 10 \cdot 70 \equiv 10 \cdot (-8) \equiv -2 \equiv 37 \pmod{39}$$

となり, 確かにもとの平文 $x = 37$ が復元された. □

問 4.1.1. 次の暗号化鍵 (n, e) をもつ暗号文 y を解読せよ. すなわち, 暗号化鍵 (n, e) から復号化鍵 d を求め, 暗号文 y を復号化し, もとの平文 x を求めよ.

(1) $(n, e) = (38, 5), y = 2$.

(2) $(n, e) = (33, 3), y = 28$.

4.2 文字列の暗号化·復号化

実際に文字を送ることを考えよう. ここでは, 簡単のために, アルファベットと幾つかの記号のみを考え, 次の表により数字列化する:

十の位 \ 一の位	0	1	2	3	4	5	6	7	8	9
1	□	!	"	#	$	%	&	’	(	)
2	*	+	,	-	.	/	0	1	2	3
3	4	5	6	7	8	9	:	;	<	=
4	>	?	@	A	B	C	D	E	F	G
5	H	I	J	K	L	M	N	O	P	Q
6	R	S	T	U	V	W	X	Y	Z	[
7	¥	]	z	_	`	a	b	c	d	e
8	f	g	h	i	j	k	l	m	n	o
9	p	q	r	s	t	u	v	w	x	y

ただし,「□」は, 四角形でなく, 空白のことである. 表の見方は, たとえば,「a」は 75,「H」は 50 である.「z」は 72 としてある. これらは,「z」以外については, 半角文字に対応するアスキーコードから 22 を引き算した数で決めてある. 文章を数字列化するには, 一文字一文字数字化して, それをつないで一つの数字とする (パソコンなどで変換用のプログラムを組む場合には, たとえば, [8, p. 375] 参照).

例. 平文

「Mathematics」

をメッセージとして送信することを考えよう. まず, これを一文字一文字, 数字に直すと,

M	a	t	h	e	m	a	t	i	c	s
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
55	75	94	82	79	87	75	94	83	77	93

となる. これら 2 桁の数字を繋ぎ合わせて得られる自然数

$$x = 55759482798775948377 93$$

を数字列化された平文としよう. そして, 次の暗号化鍵

$$\begin{aligned} n =& 1427247692705959880439315947500961989719490561 \\ e =& 1999 \end{aligned}$$

が公開されていると仮定して, x を暗号化してみよう. 見づらいので, n は 4 桁ずつ区切って,

$$\begin{aligned} n = \quad & 14 \quad 2724 \quad 7692 \quad 7059 \quad 5988 \quad 0439 \\ & 3159 \quad 4750 \quad 0961 \quad 9897 \quad 1949 \quad 0561 \end{aligned}$$

と表そう. 暗号化するには,

$$y \equiv x^e \pmod{n}, \quad 0 \leq y < n$$

となる y を求めればよい. 実際に, パソコンで計算してみると,

$$\begin{aligned} y &= 557594827987759483779 3^{1999} \\ &\equiv 12165911580189596489217007732478795723997099 96 \\ &\quad \pmod{14272476927059598804393159475009619897194 90561} \end{aligned}$$

となり,

$$\begin{array}{rcccccc} y = & 12 & 1659 & 1158 & 0189 & 5964 & 8921 \\ & 7007 & 7324 & 7879 & 5723 & 9970 & 9996 \end{array}$$

が x に対する暗号文となる. □

さて, これまでのところ, 暗号化鍵 n, e は公開されているが, 我々はまだ復号化鍵 d を知らないわけである. n, e の情報からこの暗号文 y を解読できるだろうか? たとえば, 法 n をパソコンなどで素因数分解できるか? 興味のある方は是非, 挑戦してみていただきたい. そして, 素因数分解の難しさを味わって欲しい.

問 4.2.1. 上の例と同じ暗号化鍵 (n, e) を用いて暗号化された暗号文

$$\begin{array}{rcccccc} y = & 5 & 7156 & 3177 & 5305 & 5926 & 2523 \\ & 2821 & 4836 & 3898 & 3159 & 3244 & 0640 \end{array}$$

を解読して, x を求めよ. さらに, それを文字列に戻し, 平文を求めよ. (Hint: パソコンなどを用いて, n の素因数分解を求めよ)

例. 暗号化鍵 $(145, 75)$ による暗号文 $y = 7$ を解読してみよう. ただし, 文字の数字化は上の表を用いているとする. まず, $n = 145 = 5 \cdot 29$ と分解し, $\varphi(n) = (5-1)(29-1) = 112$ となる. $75d \equiv 1 \pmod{112}$ を解くと, $d = 3$ は解であることがわかる. ゆえに

$$x \equiv y^3 = 7^3 = 343 \equiv 53 \pmod{145}$$

となり, 上の表によれば, もとの文字は「K」である. □

問 4.2.2. 次の暗号化鍵 (n, e) による暗号文 y を, 上の表を用いて解読せよ. すなわち, 暗号化鍵 (n, e) から復号化鍵 d を求め, 暗号文 y を復号化し, 数字列化されたもとの平文 x を求め, 上の表によりもとの文字を求めよ. (Hint: ベキ乗の計算には電卓を用いてよい)

(1) $(n, e) = (111, 29), y = 61.$

(2) $(n, e) = (319, 187), y = 10.$

問 4.2.3. ある組織で使われている秘密のパスワードは, 4 文字からなるという. 入手したそのパスワードの暗号文は,

$$(y_1, y_2, y_3, y_4) = (99, 348, 410, 60)$$

であるが, これは, パスワードの文字の順序をデタラメに並べ替えてから一文字ずつ上の表で数字列化し, 鍵

$$(n, e) = (493, 299)$$

を用いて暗号化されているという. この暗号を解読せよ. すなわち,

(1) 暗号化鍵 $(n, e) = (493, 299)$ に対する復号化鍵 d を求めよ.

(2) 各暗号文 $y_1, \ldots, y_4$ から, それぞれ対応する平文 $x_1, \ldots, x_4$ を求めよ. (Hint: 計算には電卓を用いてよい)

(3) $x_1, \ldots, x_4$ の一つ一つを, 表を用いて文字に変換し, パスワードを構成する 4 文字を求めよ.

(4) 秘密のパスワードを推測せよ.

5 フェルマーの小定理

5.1 オイラーの関数

定義. 自然数 n に対して, $\{1, 2, 3, \ldots, n\}$ の中で n と互いに素となる数の個数を

$$\varphi(n)$$

で表す. この φ を**オイラーの関数**という.

例. $\varphi(1) = 1$ である. というのは, 1 は 1 と互いに素だからである. □

例. $\varphi(12)$ を求めてみよう. まず, 12 と互いに素とならない整数は, 12 の素因数の倍数と一致することに注意する. ここで, 12 の素因数は 2, 3 であり, これらの倍数となるのは, $\{1, 2, 3, \ldots, 12\}$ の中で

$$\{2, 3, 4, 6, 8, 9, 10, 12\}$$

の 8 個. したがって, $\{1, 2, 3, \ldots, 12\}$ の中で 12 と互いに素となる数の個数は, $\varphi(12) = 12 - 8 = 4$ となる. □

例. 素数 p に対しては, $\varphi(p) = p - 1$ が成り立つ. $\{1, 2, 3, \ldots, p\}$ のうちで p と互いに素となる数は, $1, 2, \ldots, p-1$ の $p-1$ 個だからである. □

例. $\varphi(60)$ を求めてみよう. 素因数分解は

$$60 = 2^2 \times 3 \times 5$$

となるゆえ, 素因数は, 2, 3, 5 の 3 個である. $\{1, 2, \ldots, 60\}$ のうち, これらの倍数ではない数の個数を数えればよい. まず, 2, 3, 5 の倍数の個数は, それぞれ,

$$\frac{60}{2} = 30, \quad \frac{60}{3} = 20, \quad \frac{60}{5} = 12$$

である. 次に, 重複している分について考える. 3×5, 2×5, 2×3 の倍数の個数は, それぞれ,

$$\frac{60}{3 \cdot 5} = 4, \quad \frac{60}{2 \cdot 5} = 6, \quad \frac{60}{2 \cdot 3} = 10$$

であり, また, $2 \times 3 \times 5$ の倍数の個数は

$$\frac{60}{2 \cdot 3 \cdot 5} = 2$$

である. したがって, 重複を打ち消せば, 求める個数は,

$$\varphi(60) = 60 - 30 - 20 - 12 + 4 + 6 + 10 - 2 = 16$$

となる. これは, “因数分解” をして, 次のようにも計算できる:

$$\begin{aligned}
\varphi(60) &= 60 - \frac{60}{2} - \frac{60}{3} - \frac{60}{5} + \frac{60}{3 \cdot 5} + \frac{60}{2 \cdot 5} + \frac{60}{2 \cdot 3} - \frac{60}{2 \cdot 3 \cdot 5} \\
&= 60 \left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{3 \cdot 5} + \frac{1}{2 \cdot 5} + \frac{1}{2 \cdot 3} - \frac{1}{2 \cdot 3 \cdot 5}\right) \\
&= 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \\
&= 16
\end{aligned}$$

□

上の例における計算を一般化すると, 次の公式が得られる (厳密な証明は, たとえば [10] 参照):

定理 5.1.1 (オイラーの公式). 自然数 n の素因数分解を

$$n = p^a q^b r^c \cdots$$

とすれば, 次が成り立つ:

$$\varphi(n) = n \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{r}\right) \cdots .$$

問 5.1.2. $\varphi(36)$, $\varphi(42)$, $\varphi(90)$ を求めよ.

5.2 フェルマーの小定理

RSA 暗号のマジックの種がここに述べる初等整数論の一命題である.

補題 5.2.1. 素数 p と $0 < r < p$ である整数 r に対して次が成り立つ:

$$\frac{p!}{r!(p-r)!} \equiv 0 \pmod{p}$$

証明. 分子が p で割り切れることは明らかなので, 分母が p で割り切れないことを示せば十分である. もしも, $r!(p-r)!$ が素数 p で割り切れたとすると, この積のいずれかの項が p で割り切れるはずだが, それらはすべて p よりも小さい自然数なので矛盾である. ■

例. $p=7, r=3$ で考えてみると,

$$\frac{7!}{3!(7-3)!}=\frac{7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{3\cdot 2\cdot 1\cdot 4\cdot 3\cdot 2\cdot 1}=7\cdot 5\equiv 0 \pmod 7$$

となる. 約分して計算すると, 分子の $p=7$ が最後まで生き残ることがよくわかるであろう. □

命題 5.2.2. 素数 p と整数 a, b に対して次が成り立つ:

$$(a+b)^p\equiv a^p+b^p \pmod p.$$

証明. 左辺を二項展開して補題 5.2.1 を使うと,

$$(a+b)^p=\sum_{r=0}^{p}\frac{p!}{r!(p-r)!}a^r b^{p-r}\equiv a^p+b^p \pmod p$$

を得る. ■

この命題を用いると次の有名な定理が得られる:

定理 5.2.3 (フェルマーの小定理). 素数 p と整数 a に対しては

$$a^p\equiv a \pmod p. \tag{5.2.1}$$

さらに, 次が成り立つ:

$$(a,p)=1\Rightarrow a^{p-1}\equiv 1 \pmod p. \tag{5.2.2}$$

証明. $a>0$ の場合に, (5.2.1) を a についての数学的帰納法で示そう. まず, 明らかに

$$1^p=1$$

である. つぎに, 命題 5.2.2 と帰納法の仮定を使うと

$$(a+1)^p\equiv a^p+1^p\equiv a+1 \pmod p$$

となる. これで $a>0$ の場合に (5.2.1) が示された.

$a<0$ の場合には, 上で示したことにより $-a>0$ に対して

$$(-1)^p a^p=(-a)^p\equiv -a \pmod p$$

が成り立つ. ここで, $p=2$ の場合には $-1\equiv 1 \pmod 2$ であり, p が奇素数の場合には $(-1)^p=-1$ となるので, いずれにしろ, (5.2.1) が成り立つことがわかる. $a=0$ の場合に (5.2.1) が成り立つことは明らかである.

さて, (5.2.2) については, 命題 3.3.1 を用いて (5.2.1) の両辺を a により割り算すればよい. ■

例. 10^{100} を 17 で割り算したときの余りを求めてみよう. 素数 17 についてフェルマーの小定理 5.2.3 を用いると, $(10, 17) = 1$ なので

$$10^{16} \equiv 1 \pmod{17}$$

を得る. 100 を 16 で割り算すると $100 = 6 \times 16 + 4$ だから,

$$10^{100} = (10^{16})^6 \cdot 10^4 \equiv 10^4 \pmod{17}$$

ここで $102 = 6 \times 17$ を 利用すると, $100 \equiv -2 \pmod{17}$ となるので,

$$10^4 \equiv (-2)^2 = 4 \pmod{17}$$

となり, 余りは 4 となる. □

問 5.2.4. $3^{100} + 4^{100}$ を 7 で割り算したときの余りを求めよ.

問 5.2.5. $2^{70} + 3^{70}$ を 13 で割り算したときの余りを求めよ.

問 5.2.6. $39^{50!}$ を 2251 で割り算したときの余りを求めよ. (ヒント: 2251 は素数)

さて, 次が, RSA 暗号において使われている命題である:

系 5.2.7. 自然数 n, t に対して, n が平方因子を持たないとき, すなわち, どんな素数の 2 乗も約数にもたないとき, 次が成り立つ:

(1) もしも n の任意の素因数 p について

$$t \equiv 1 \pmod{p-1}$$

となるならば, 任意の整数 a に対して次が成り立つ:

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

(2) 任意の整数 a に対して次が成り立つ:

$$t \equiv 1 \pmod{\varphi(n)} \Rightarrow a^t \equiv a \pmod{n}.$$

証明. (1) n が平方因子をもたないので, 系 2.2.2 により, n の任意の素因数 p に対して

$$a^t \equiv a \pmod{p}$$

を示せばよいことがわかる. ここに, 仮定から t は, $k \geq 0$ となる整数 k により

$$t = k(p-1)+1$$

と表される. ゆえに, n の任意の素因数 p に対して

$$a \cdot (a^{p-1})^k \equiv a \pmod{p} \tag{5.2.3}$$

となることを示せば十分である.

a が p と互いに素の場合には, フェルマーの小定理 5.2.3 により $a^{p-1} \equiv 1 \pmod{p}$ となるので, 両辺を k 乗して a を掛け算すれば (5.2.3) が得られる. a が p と互いに素ではない場合は, $a \equiv 0 \pmod{p}$ となるので, (5.2.3) は明らかに成立する. いずれにしろ, (5.2.3) が成り立つことが示された.

(2) (1) から導かれることを示そう. $t \equiv 1 \pmod{\varphi(n)}$ とすると, $t-1$ は $\varphi(n)$ の倍数であるが, 一方, n の任意の素因数 p について, 定理 5.1.1 により $\varphi(n)$ は $p-1$ の倍数である. したがって, $t-1$ は $p-1$ の倍数となり, t についての (1) の仮定が満たされていることが示された. ■

例. 任意の整数 a に対して,

$$a^7 \equiv a \pmod{42}$$

となる. というのは, $n = 42$, $t = 7$ について系 5.2.7 の仮定が満たされるからである. 実際, $n = 42 = 2 \cdot 3 \cdot 7$ は平方因子をもたず, 各素因数, 2, 3, 7 についてそれぞれ, $t-1 = 6$ は $2-1 = 1$, $3-1 = 2$, $7-1 = 6$ の倍数である. □

問 5.2.8. 197^{157} を 35 で割り算したときの余りを求めよ.

RSA 暗号とは, 直接関係ないが, フェルマーの小定理 5.2.3 の一般化として, 次の定理がある:

定理 5.2.9 (オイラーの定理). 自然数 n と整数 a に対して次が成り立つ:

$$(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}.$$

例. 7^{100} を 12 で割り算したときの余りを求めてみよう. $(7, 12) = 1$ だからオイラーの定理 5.2.9 が適用できる. それによると, $\varphi(12) = 4$ より,

$$7^4 \equiv 1 \pmod{12}$$

となるので,

$$7^{100} = (7^4)^{25} \equiv 1 \pmod{12}$$

となり, 余りは 1 となる. □

問 5.2.10. 13^{100} を 16 で割り算したときの余りを求めよ.

6　RSA 暗号, III

6.1　復号化の仕組み

定理 1.2.1 の証明をしよう.

証明. $y \equiv x^e \pmod{n}$ の両辺を d 乗すると,

$$y^d \equiv x^{ed} \pmod{n}$$

となる. $ed \equiv 1 \pmod{\varphi(n)}$ なので, 系 5.2.7 により

$$x^{ed} \equiv x \pmod{n}$$

である. したがって,

$$z \equiv y^d \equiv x^{ed} \equiv x \pmod{n}$$

となる. ここで $0 < x < n$ かつ $0 \leq z < n$ なので $x = z$ である. ■

6.2　暗号として機能することの根拠

RSA 暗号では, 公開鍵を (n, e), 秘密鍵を d とすれば, 平文 x を n を法として e 乗を計算することにより暗号化し, 暗号文 y を n を法として d 乗を計算することにより復号化するわけだが, こんな簡単なことで, 暗号になるのか? と思われるかもしれない.

それは, なぜか? つまり, 暗号文 y と暗号化鍵 n, e を既知としても, なぜ暗号文 y から平文 x を得ることが困難なのか?

現在のところ, 復号化鍵 d を求めずに y から x を得る一般的方法, そして, 素因数分解 $n = pq$ を知らずに d を求める一般的方法が知られていない. したがって, y から x を得るには d を求めることが必要で, そのためには $\varphi(n)$ を求める必要があり, さらに, そのためには素因数分解 $n = pq$ が必要となる. 結局, 暗号文 y から平文 x を得るためには, 暗号化鍵の法 n の素因数分解 $n = pq$ が必要となるわけであるが, ネックは, この素因数分解にある. すなわち, 暗号化鍵の法 n として選ばれるような巨大な数の素因数分解が, 最大公約数などを求めるのとは異なり, 非常に難しい, という点にある.

これは, 巨大な数の素因数分解が理論的に不可能という意味ではない. 実際, 小さな素数から始めて順々に割り算をして行けば, どんなに大きな数に対しても必ず素因数分解は可能である. しかし, たとえば 10 進数表示で 300 桁以上の, 非常に大きい数の場合, 現実的な (暗号化された情報が価値をもつ) 時間内でその素因数を見つけることは, 現在の数学の水準, 計算機の能力では不可能に等しい, ということなのである. したがって, 事実上, n の素因数分解を知っている者のみが y から x を得ることできる, ということになる.

例.　100 桁くらい大きさの数 n の因数を見つけるために, 単純に小さい数から順に割っていったとしよう. すると, 最悪の場合には $\sqrt{n} = 10^{50}$ 程度の回数の割り算が必要となる. 毎秒 10^{10} 回の割り算ができる計算機に実行させると, $10^{50}/10^{10} = 10^{40}$ 秒かかる. 1 年は $3.15 \cdot 10^7$ 秒程度ゆえ, 少なくとも 10^{32} 年かかること計算になる. 一方, 宇宙の始まりであるビッグバンは, $2 \cdot 10^{10}$ 年くらい前に起こったとされている. □

さて, ここで, 少々矛盾している感じがするかもしれない. 暗号として機能することの根拠は, 鍵である大きな数 n の素因数分解の困難さにある. 一方, 鍵 n を生成するために大きな素数 p, q を必要とするということは, 大きな数 p, q が素数であることを確かめなければならない. 素数であることを確かめるために素因数分解しなければならないとしたら, たしかに, これは矛盾である. 実は, 自然数に対しては, 素因数分解を求めなくとも, つまり, 分解してみなくとも素数であるかどうかの効率的な判定方法が知られている. だから, 暗号化鍵の法 n の素因数 p, q を選ぶことは易しい. したがって, RSA 暗号では, 大きな数の素数が効率的に判定できること, そして, 大きな数の素因数分解に時間がかかることが重要となる.

さらには, ユークリッドの互除法 2.3.1 など用いれば, 指数 e を選ぶことも易しい. そして, n が大きくても, 計算機など用いれば, 復号化鍵 d を求めることや, 平文の暗号化はたやすく計算できる.

例. 10 進数表示で 4933 桁の数, $F_{14} = 2^{2^{14}} + 1$ は, 素数ではないことは証明されているが, その約数は, 2004 年 9 月現在, 一つも知られていない. □

6.3 解読するには?

RSA 暗号のミソは, $n = pq$ において, 二つの素数 p, q から n を得るのは簡単だが, n から p, q を得るのが非常に困難であること, つまり, 掛け算は簡単だが, 逆にそれを素因数分解するのは非常に困難である, という一方向性にある. ただし, 素因数分解が困難であるというのは, 単なる予想 (または期待) に過ぎず, いつの日か, 素因数分解を効率的に行なうアルゴリズムが発見されれば, RSA 暗号は, 暗号として機能しなくなる. また, 厳密には, RSA 暗号を解読することは n を素因数分解をすることと同程度難しいらしい, としかいえない. というのも, 現在のところ, 復号化鍵 d を求めずに y から x を得る簡単な方法が存在しないことも, そして, 素因数分解 $n = pq$ を知らずに d を求める方法が存在しないことも証明されていないからである.

問 6.3.1. 暗号化鍵 (n, e) が与えられているとき, 復号化鍵 d を求めずに暗号文 y からもとの平文 x を得る一般的方法を求めよ.

問 6.3.2. 暗号化鍵 (n, e) が与えられているとき, 素因数分解 $n = pq$ を求めずに復号化鍵 d を得る一般的方法を求めよ.

一方, 素因数分解 $n = pq$ を知ることと, オイラー関数の値 $\varphi(n)$ を知ることが同値であることは, 次のようにしてわかる. オイラーの公式 5.1.1 により, n の素因数分解 $n = pq$ を既知とすれば, $\varphi(n) = (p-1)(q-1)$ として, $\varphi(n)$ が得られる. 逆に,

$$\varphi(n) = (p-1)(q-1) = n + 1 - (p+q), \quad (p+q)^2 - 4n = (p-q)^2$$

なので,

$$\begin{aligned} p + q &= n + 1 - \varphi(n) \\ p - q &= \pm\sqrt{(n + 1 - \varphi(n))^2 - 4n} \end{aligned}$$

となる (複号は p, q の大小で定まる). ゆえに, p, q についてこれを解けば, p, q を n, $\varphi(n)$ で表す式が得られ, $\varphi(n)$ を既知とすれば n の素因数, p, q が得られることになる.

問 6.3.3. 素因数分解を効率的に行なうアルゴリズムを発見せよ.

6.4 鍵の選び方

暗号化鍵の指数 e については, 暗号化速度向上のため, $e = 2^{16} + 1 = 65537$ が用いられることが多い.

暗号化鍵の法 n を与える素数 p, q の選び方については, たとえば, $p \pm 1$ と $q \pm 1$ とが大きな素数を含んでいることが推奨されている. $p - 1$, $p + 1$ が小さな素数の積に分解されるような素因数 p をもつ合成数に対して威力する素因数分解アルゴリズム, **$p - 1$ 法**, および, **$p + 1$ 法**が知られているからである. また, **フェルマー法**により容易に分解されないように, 差 $|p - q|$ が極端に小さくないことが推奨されている.

一方, 法 n のサイズについては, 年々, 素因数分解のアルゴリズムが進歩し, そして, 計算機の能力が向上しているため, 1980 年代前半には鍵 n として 150 桁程 (2 進数表示で 512 桁) で安全とされたが, 現在では, 300 桁以上 (2 進数表示で 1024 桁) が推奨されている (詳しくは, [3, §4.2], [6, §7.3] 参照).

6.5 懸賞問題

現在のところ, RSA 暗号を解読するには, 復号化鍵の法 n を素因数分解することになるが, RSA 暗号に限らず, 巨大な数の素因数分解をいかにして速く効率的に行うかは, 非常に重要な問題である. 現在, RSA Security 社の RSA 研究所 [7] により, 合成数の素因数分解に対して賞金が懸けられている. 研究促進を主旨としたこのコンテストは, RSA Factoring Challenge と呼ばれている. 賞金の懸けられた合成数は, ランダムに選ばれたほぼ同じサイズの素数二つの積であり, 現在は, 2 進表示の桁数を用いて, RSA-140, RSA-155, ..., などと名づけられている. その幾つかはすでに素因数分解されているが, 少しずつ, 新しい賞金の懸けられた合成数も付け加えられている. RSA 研究所のサイト

`http://www.rsasecurity.com/rsalabs/`

に入り, → Challenges → The New RSA Factoring Challenge と辿れば, その詳細が見られる. 2004 年 11 月末日現在では, RSA-140, RSA-155, RSA-160, RSA-576 が既に分解されている一方, RSA-640 はまだ分解が知られてなく, 2 万ドルの賞金が懸けられている. 因みに, その数を引用すると,

$$\begin{aligned}\text{RSA-640} = 3 \quad & 1074\ 1824\ 0490\ 0437\ 2135\ 0750\ 0358\ 8856 \\ & 7930\ 0373\ 4602\ 2842\ 7275\ 4572\ 0161\ 9488 \\ & 2320\ 6440\ 5180\ 8150\ 4556\ 3468\ 2967\ 1723 \\ & 2867\ 8243\ 7916\ 2728\ 3803\ 3415\ 4710\ 7310 \\ & 8501\ 9195\ 4852\ 9007\ 3377\ 2482\ 2783\ 5257 \\ & 4238\ 6454\ 0146\ 9173\ 6602\ 4776\ 5234\ 6609\end{aligned}$$

という, 10 進表示で 193 桁の数である. 他にも, RSA-704 には 3 万ドル, RSA-768 には 5 万ドル, ... となっており, RSA-2048 に至っては, 20 万ドルの賞金が懸けられている. これらの賞金の懸けられた合成数のリストは, 上記サイトから誰でも簡単にダウンロードできる.

問 6.5.1. RSA-640 を分解せよ.

参考文献

[1] 一松 信: 代数学入門第一課, 近代科学社 (1992)

[2] ユークリッド (I. L. Heiberg 編集; 池田美恵, 寺阪英孝, 中村幸四郎, 伊藤俊太郎訳): 原論, 共立出版 (1971)

[3] N. Koblitz (櫻井幸一訳): 数論アルゴリズムと楕円暗号理論入門, シュプリンガー東京 (1997)

[4] A. Menezes, P. van Oorschot, S. Vanstone: *Handbook of Applied Cryptography*, CRC Press (1996)
`http://cacr.math.uwaterloo.ca/hac/`

[5] 情報処理学会監修, 岡本龍明, 太田和夫共編: 暗号・ゼロ知識証明・数論, 共立出版 (1995)

[6] 岡本龍明, 山本博資: 現代暗号, 産業図書 (1997)

[7] RSA Laboratories, RSA Security, Inc.
`http://www.rsa.com/rsalabs/`

[8] S. Wagon (長岡亮介監訳): *Mathematica* で見える現代数学, ブレーン出版 (1992)

[9] S. C. コウチーニョ (林 彬訳): 暗号の数学的基礎, スプリンガーフェアラーク東京 (2001)

[10] 楫 元: 工科系のための初等整数論入門—公開鍵暗号をめざして—, 培風館 (2000)

解答

2.3.3. ユークリッドの互除法 2.3.1 を実行すると

$$1960 = 19 \times 103 + 3$$
$$103 = 34 \times 3 + 1$$
$$3 = 3 \times 1 + 0$$

となるので, 最大公約数は 1 となる. とくに, 1960, 103 は互いに素である. ■

3.1.1. 鉛筆の本数を x とする. 条件を式に表すと,

$$x \equiv 5 \pmod{12}, \quad x < 200$$

である. $x = 5 + 12k$ $(k \in \mathbb{Z})$ と表されるので,

$$5 + 12k < 200$$

を満たす k の最大を求めればよい. $k = 16$ となり, $x = 197$ となる. したがって答は, 197 本 となる. ■

3.1.2. 1 月最後の日曜日の日付を x とする. 条件を式に表すと,

$$x \equiv 3 \pmod{7}, \quad x \leq 31$$

である. $x = 3 + 7k$ $(k \in \mathbb{Z})$ と表されるので,

$$3 + 7k \leq 31$$

を満たす k の最大を求めればよい. $k = 4$ となり, $x = 31$ となる. したがって答は, 31 日 となる. ■

3.2.2. この合同式から, 恒等的に成り立つ合同式, $2 \equiv 2 \pmod 9$ を辺々引き算すると, 命題 3.2.1 により,

$$x - 2 + 2 \equiv 6 - 2 \pmod 9$$

が成り立つ. 両辺をそれぞれ計算すると

$$x \equiv 4 \pmod 9$$

となり, $0 \leq x \leq 9$ を満たすのは, $x = 4$ となる. ■

3.2.4. $1001 = 7 \times 11 \times 13$ より $10^3 \equiv -1 \pmod{13}$ となる. $10000 = 3333 \times 3 + 1$ だから

$$10^{10000} = (10^3)^{3333} \cdot 10 \equiv (-1)^{3333} \cdot 10$$
$$= -10 \equiv 3 \pmod{13}$$

となり, 余りは 3 である. ■

3.4.2. $(103, 1960) = 1$ となることは, ユークリッドの互除法 2.3.1 を使ってすでに前の問で確かめてあるので, 一次合同式の解法 (その 2) の手順にしたがって, (3.4.12) を解いてみよう.

(1) 恒等的に成り立つ式

$$1960x \equiv 0 \pmod{1960} \tag{6.5.1}$$

を考える.

(2) 103 と 1960 に, 直接ユークリッドの互除法 2.3.1 を適用する. まず, $103 = 0 \times 1960 + 103$ となるが, これは, 103 と 1960 の順序を入れ換えるだけである. 次に, $1960 = 19 \times 103 + 3$ となるので, (6.5.1) から (3.4.12) の 19 倍:

$$19 \cdot 103x \equiv 19 \cdot 3 \pmod{1960}$$

を引き算すると,

$$3x \equiv -19 \cdot 3 \pmod{1960} \tag{6.5.2}$$

を得る. 次に, $103 = 34 \times 3 + 1$ となるので, (3.4.12) から (6.5.2) の 34 倍:

$$34 \cdot 3x \equiv -34 \cdot 19 \cdot 3 \pmod{1960}$$

を引き算すると,

$$x \equiv 3 + 34 \cdot 19 \cdot 3 \pmod{1960}$$

となり, 計算すると

$$x \equiv 1941 \pmod{1960}$$

を得る.

(3) $(103, 1960) = 1$ なので, 命題 3.4.1 により (3.4.12) の解は, 1960 を法としてただ一つであり, $x = 1941$ で与えられる. ■

3.4.3. 問 3.4.2 と同様に計算できる: (1) $x \equiv 17 \pmod{24}$; (2) $x \equiv 14 \pmod{36}$ ■

3.4.4. 参加者数を x とすれば, $7x + 1 \equiv 0 \pmod{24}$ すなわち,

$$7x \equiv -1 \pmod{24} \tag{6.5.3}$$

となる. 7 は素数で 24 は 7 の倍数ではないから, $(7, 24) = 1$ である. (6.5.3) の係数 7 と恒等的に成り立つ式

$$24x \equiv 0 \pmod{24} \tag{6.5.4}$$

の係数 24 にユークリッドの互除法 2.3.1 を適用する. まず, $24 = \underline{3} \times 7 + 3$ なので, (6.5.4) から (6.5.3) の $\underline{3}$ 倍を引き算すると,

$$3x \equiv 3 \pmod{24} \qquad (6.5.5)$$

となる (ここで, 両辺を 3 では割り算できない. $(3, 24) = 3 \neq 1$ となり, 合同の世界における割り算の条件が満たされていないからである). 次に, $7 = \underline{2} \times 3 + 1$ なので, (6.5.3) から (6.5.5) の $\underline{2}$ 倍を引き算すると,

$$x \equiv -7 \pmod{24}$$

つまり,

$$x = -7 + 24k, \quad k \in \mathbb{Z}$$

となる. $0 \leq x \leq 25$ だから, $x \equiv -7 \equiv 17 \pmod{24}$ の 17 が求める答である. したがって, $\underline{\text{参加したのは 17 名}}$ である. ■

4.1.1. (1) $n = 38 = 2 \times 19$ と分解するので $\varphi(n) = (2-1)(19-1) = 18$ であり, $e = 5$ なので, 復号化鍵 d は一次合同式

$$5d \equiv 1 \pmod{18} \qquad (6.5.6)$$

を満たす. 恒等的に成り立つ式,

$$18d \equiv 0 \pmod{18}$$

から (6.5.6) の 3 倍, $15d \equiv 3 \pmod{18}$ を引き算して,

$$3d \equiv -3 \pmod{18} \qquad (6.5.7)$$

を得る. ここで, 思わず両辺を 3 で割り算して $d \equiv -1 \pmod{18}$ としたくなるところだが, 割り算は**できない**. $(3, 18) = 3 \neq 1$ となり, 合同の世界における割り算の条件が満たされていないからである (詳しくは, §3.3 参照). 実際, 明らかに $d = -1$ は (6.5.6) を満たさない. 正しくは次のようにする: ユークリッドの互除法 2.3.1 を続けて, (6.5.6) から (6.5.7) を引き算して,

$$2d \equiv 4 \pmod{18}$$

を得る (ここでも 2 で割り算はできない). さらに, これを (6.5.7) から引き算して,

$$d \equiv -7 \equiv 11 \pmod{18}$$

を得る. たとえば

$$d = 11$$

が復号化鍵である. したがって, もとの平文は,

$$x \equiv y^d = 2^{11} \pmod{38}, \quad 0 \leq x < 38$$

を満たす. 実際, 計算すると,

$$\begin{aligned} 2^{11} &= (2^5)^2 \cdot 2 \equiv (-6)^2 \cdot 2 \\ &\equiv (-2) \cdot 2 = -4 \equiv 34 \pmod{38} \end{aligned}$$

となり, $\underline{x = 34}$ がもとの平文である.

(2) $n = 33 = 3 \times 11$ と分解するので $\varphi(n) = (3-1)(11-1) = 20$ であり, $e = 3$ なので, 復号化鍵 d は一次合同式

$$3d \equiv 1 \pmod{20}$$

を満たす. この式の 7 倍から恒等的に成り立つ式,

$$20d \equiv 0 \pmod{20}$$

を引き算して,

$$d \equiv 7 \pmod{20}$$

を得るので, たとえば $d = 11$ が復号化鍵である. したがって, もとの平文は,

$$x \equiv y^d = 28^7 \pmod{33}, \quad 0 \leq x < 33$$

を満たす. 実際, 計算すると, $28^2 \equiv (-5)^2 = 25 \equiv -8 \pmod{33}$ となり, $28^4 \equiv (-8)^2 = 64 \equiv -2 \pmod{33}$ となるから,

$$\begin{aligned} 28^7 &= 28^4 \cdot 28^2 \cdot 28^1 \equiv (-8)(-2)(-5) \\ &= -80 \equiv 19 \pmod{33} \end{aligned}$$

となり, $\underline{x = 19}$ がもとの平文である. ■

4.2.1. 解読できたら `kaji@waseda.jp` までご一報下さい. ■

4.2.2. (1) $n = 3 \cdot 37$ と分解し, $\varphi(n) = (3-1)(37-1) = 72$ となる. $29d \equiv 1 \pmod{72}$ を解くと, $d = 5$ は解であることがわかる. ゆえに

$$x \equiv y^d = 61^5 \equiv 76 \pmod{111}$$

となり, もとの文字は, $\underline{\text{「b」}}$ である.

(2) $n = 11 \cdot 29$ と分解し, $\varphi(n) = (11-1)(29-1) = 280$ となる. $187d \equiv 1 \pmod{280}$ を解くと, $d = 3$ は解であることがわかる. ゆえに

$$x \equiv y^d = 10^3 \equiv 43 \pmod{319}$$

となり, もとの文字は, $\underline{\text{「A」}}$ である. ■

4.2.3. $n = 493 = 17 \cdot 29$ と分解し, したがって, $\varphi(n) = (17-1)(29-1) = 16 \cdot 28 = 448$ となる. $e = 299$ より $299d \equiv 1 \pmod{448}$ を解くと, $d = 3$ は解であることが解る. 493 を法として

$$y_1^e = 99^3 \equiv 75, \quad y_2^e = 348^3 \equiv 87,$$
$$y_3^e = 410^3 \equiv 93, \quad y_4^e = 60^3 \equiv 66$$

となるので,

$$(x_1, x_2, x_3, x_4) = (75, 87, 93, 66)$$

となり, 表より, パスワードの 4 文字は,

「a」, 「m」, 「s」, 「X」

となる. さて, 秘密のパスワードは? ■

5.1.2. $36 = 2^2 \times 3^2, 42 = 2 \times 3 \times 7, 90 = 2 \times 3^2 \times 5$ から次を得る:

$$\varphi(36) = 36\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 12$$
$$\varphi(42) = 42\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right) = 12$$
$$\varphi(90) = 90\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 24$$

■

5.2.4. 素数 7 についてフェルマーの小定理 5.2.3 を用いると, $(3,7) = (4,7) = 1$ なので

$$3^6 \equiv 4^6 \equiv 1 \pmod{7}$$

を得る. $100 = 16 \times 6 + 4$ だから, 7 を法として

$$3^{100} = (3^6)^{16} \cdot 3^4 \equiv 3^4 = (3^2)^2 = 9^2 \equiv 2^2 = 4$$
$$4^{100} \equiv (-3)^{100} = 3^{100} \equiv 4$$

となるので,

$$3^{100} + 4^{100} \equiv 4 + 4 = 8 \equiv 1 \pmod{7}$$

となり, 余りは 1 となる. ■

5.2.5. 前問と同様に計算できる. フェルマーの小定理 5.2.3 を用いても良いが, $2^6 \equiv -1 \pmod{13}$, $3^3 \equiv 1 \pmod{13}$ を用いると楽.

$$2^{70} \equiv 2^4 \equiv -3, \quad 3^{70} \equiv 3 \pmod{13}$$

となり, $2^{70} + 3^{70} \equiv 0 \pmod{13}$ となる. したがって, 余りは 0, つまり, $2^{70} + 3^{70}$ は 13 で割りきれる. ■

5.2.6. 素数 2251 についてフェルマーの小定理 5.2.3 を用いると, $(2251, 39) = 1$ より

$$39^{2250} \equiv 1 \pmod{2251}$$

となる. ここで, たとえば, $2250 = 2 \cdot 3^2 \cdot 5^3 = 9 \cdot 10 \cdot 25$ と分解され, 50 の階乗の中に $9, 10, 25$ は現れるので, 2250 は 50! を割りきる. ゆえに, $39^{50!} \equiv 1 \pmod{2251}$, すなわち, 余りは 1 となる. ■

5.2.8. $n = 35 = 5 \cdot 7$ は平方因子をもたず, $t = 157$ とすると $t - 1 = 156$ は $5 - 1 = 4$, $7 - 1 = 6$ の倍数となるので, 系 5.2.7 により,

$$197^{157} \equiv 197 \pmod{35}$$

を得る. さらに, 実際に割り算すると $197 = 5 \times 35 + 22$ となるので, 余りは 22 となる. ■

5.2.10. $(13, 16) = 1$ だからオイラーの定理 5.2.9 が適用できる. それによると, $\varphi(16) = 8$ より,

$$13^8 \equiv 1 \pmod{16}$$

となるので, $100 = 12 \times 8 + 4$ より, 16 を法として

$$13^{100} = (13^8)^{12} \cdot 13^4 \equiv 13^4 \equiv (-3)^4 = 81 \equiv 1$$

となり, 余りは 1 となる. ■

6.3.1. 解けたら kaji@waseda.jp までご一報下さい. ■

6.3.2. 解けたら kaji@waseda.jp までご一報下さい. ■

6.3.3. 発見できたら kaji@waseda.jp までご一報下さい. ■

6.5.1. 分解できたら RSA 研究所のホームページ [7] を訪れ, → Challenges → The New RSA Factoring Challenge → The RSA Factoring Challenge FAQ と辿り, "How do I submit a completed factorization?" の項を参照のこと. ■