RSA 暗号の数学的基礎 (2020 年度新入生用資料)

目標

- 高校段階で学んだ整数分野を復習する.(素因数分解・最大公約数・ユークリッドの互除法など)
- 整数の初等的な取り扱い方の中で高校段階から少し進んだ内容について学習する.(合同式の計算・フェルマーの小定理・中国剰余定理など)
- RSA 暗号と呼ばれる「公開鍵暗号」の数学的な基礎を概説する.上記のような整数の初等的な取り扱い方を学ぶだけで,現代暗号理論の最も初歩的な実例に触れることができる.

1 イントロダクション

「暗号」と聞くと,犯罪とかスパイのような危険な香りか,あるいは,巷に流行するクイズのようなものを連想するかもしれない.しかし,殊に現代は,個人情報はもとより他者に漏れては困る情報を送受信しなければならない時代であり,外部から解読されることなく機密情報をやり取りできる仕組みとしての「暗号」は情報技術の中でも重要な分野である.

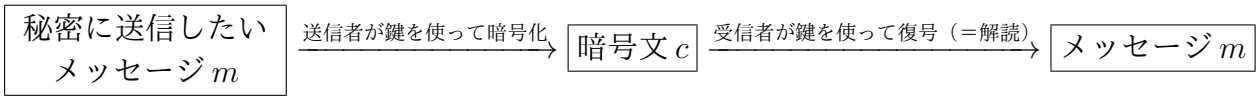
紀元前 6 世紀,古代ギリシャの都市国家スパルタでは,「**スキュタレー暗号**」と呼ばれる方式が用いられていたらしい.スキュタレーとは棒のことで,この棒に革紐を巻き付け,そこに文章を書く.ほどかれた革紐には,一見無意味な文字列が並んでいるように見えても,作成に使用した棒と同じ直径を持つ棒に巻き付ければ解読できるというものだ.同じ直径でなければ文章は意味をなさず解読できない.

また,紀元前 1 世紀,ユリウス・カエサルの使用した「**シーザー暗号**」は,文章のアルファベットを一定数だけずらして作成する暗号方式として有名である.これだけだと 26 文字しかないアルファベットを使う場合,26 通りずらして調べれば必ず元の文章が解読できてしまうので困るが,その後,文字の対応を単なるずらしではなく,26 文字のすべての入れ替え (26! 通り) を利用して作成する暗号が用いられた.このような方法を**換字式暗号**[1]などという.

例えば,コナン・ドイルの『踊る人形』では,踊る人形とアルファベットを対応させた暗号が登場する.この種の換字式暗号の解読は,9 世紀ごろにアラビア人によって初めて成功したらしい.その手法は,英文の場合,最も多く現れる文字が e,2 文字だと th であるなどという「頻度分析」だった.暗号文がたくさん入手できれば,この方法で解読できてしまう.『名探偵コナン』にも様々な暗号が登場するし,第二次世界大戦中にドイツ軍が使用した「エニグマ暗号機」のような機械式のものも有名だが,これらは換字の候補を膨大なものにするという工夫がなされている.こうした暗号方式は,当然のことながら暗号化や復元に使用する鍵を秘匿することが肝心な点であり,ここに様々なスパイが暗躍していた(かもしれない).戦争中は特に暗号表の奪取は重要な作戦のひとつであった.

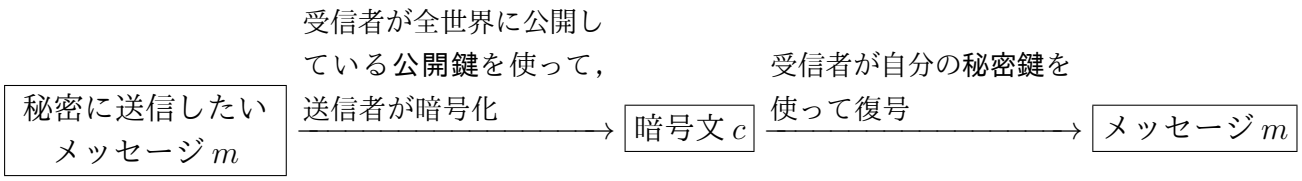
[1]「換字」の読み方は「かえじ」.

ここにあげた暗号の例は，どれも次のような仕組みになっている．



スキュタレー暗号における棒，シーザー暗号におけるずらしの数，換字式暗号における文字の対応表が鍵にあたる．この方式は，送信者と受信者が共通の鍵を使用しているという点で，**共通鍵暗号**と呼ばれる．これを利用する場合に最も重要になるのは「共通鍵を秘匿すること」である．例えば「頻度分析」によって名探偵が暗号文から実際に送信されている内容を読み取ってしまったり，スパイが文字の対応を記した暗号表を物理的に奪取してしまえば，情報が漏洩する．また，現代社会のように多数の相手へ様々な情報を送信する場合，情報を送信する相手ごとに別々の共通鍵を作っておく必要もあり，それらをすべて秘匿しておかなければならないから，作成や管理の面で実用上の負担も大きい．現代社会のセキュリティを考える上で,「暗号化や復号の操作は簡単にでき，逆に暗号化された文から暗号化や復号の操作を見抜くことが非常に困難である」という**一方向性**はより一層重要性を増している．

1976 年に，ディッフィー (Diffie) とヘルマン (Hellman) は，それまでの共通鍵暗号とは全く違う**公開鍵暗号**と呼ばれる方式を提案した．この方式は，送信者が暗号化に使う鍵と受信者が復号に使う鍵とが異なるという全く新しいアイデアである．アリスは，自分用の公開鍵と呼ばれる鍵を全世界に公開する．同時に，その公開鍵に応じて決まる別の鍵を秘密鍵として秘匿しておく．ボブがアリスに秘密のメッセージを送信したい場合，アリスの公開している公開鍵を用いて暗号化した暗号文をアリスに送る．送られた暗号文をアリスは自分の秘密鍵を用いて復号する．公開鍵暗号とはこのような暗号の仕組みである．



しかし，本当にこのような方式が実現可能なのだろうか．共通鍵方式に比べて，公開鍵方式は，具体的に公開鍵と秘密鍵をどうやって作るのか，全く非自明であるといってよい．メッセージを正しく復号できるためには，公開鍵と秘密鍵はもちろん無関係ではありえない．公開鍵を第三者が見て，秘密鍵を見抜かれないような一方向性をどうやれば獲得できるのだろうか．

1977 年，リベスト (Rivest)，シャミア (Shamir)，エーデルマン (Adleman) が，公開鍵暗号の具体的な方法を提案した．これが今日 **RSA 暗号**と呼ばれている最も基本的な公開鍵暗号の方式である．今回の資料では，この RSA 暗号という方式が具体的にどのような方法であるのかを説明し，その数学的な基礎付けを理解してもらうことを目標とする．この方式の「一方向性」は，次のことによって導かれる．一般的に，2 つの素数を掛け算するのは非常に容易だが，積だけを見て掛けられている 2 つの素数を見つけることは素数が大きくなればなるほど非常に難しくなる．**RSA 暗号における「一方向性」は，素数の積を計算することに比べて素因数分解することが非常に困難であることを利用している．**

それでは，本編に入ろう．

2　素因数分解・最大公約数・ユークリッドの互除法

2.1　素因数分解

1 より大きい整数で，1 と自分自身以外に正の約数を持たないものを**素数**という．小さいものから順に書き出してみると

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

となる．素数についての面白い話題は数多くある．例えば，**素数は無限個存在する**．このことは，紀元前 3 世紀ごろに書かれたとされるユークリッド (Euclid) の『原論』ですでに証明が述べられていた．現在では，この『原論』にある証明以外にも非常に多くのエレガントな証明が知られている．また，$2^n - 1$ の形で表される素数は**メルセンヌ素数**と呼ばれており，小さい方から順番に書き出してみると

$$3, 7, 31, 127, 8191, \ldots$$

となるが,「メルセンヌ素数が無限個存在する」かどうかは現在もなお未解決である．こうした素数に関する興味深い話題は，暗号や情報理論と深い関わりがあるが，ここでは詳しくは述べない．

RSA 暗号について述べるという観点からひとつ重要な注意として，**素数であることをどうやって判定するか**という点について触れておこう．下から順番に書き出していく方法は,「**エラトステネスの篩**」と呼ばれている．2 以上の整数の中から，まず 2 を素数のリストに加え，2 より大きい 2 の倍数をすべて消す．残っている最小の整数である 3 を素数のリストに加え，3 より大きい 3 の倍数をすべて消す．残っている最小の整数 5 を素数のリストに加え，5 より大きい 5 の倍数をすべて消す．これを順番に繰り返すことによって素数を小さい方から順番に列挙していくことができる．また，別の単純な方法は，$\sqrt{n}$ **以下の素数で割り切れるかどうかを調べる**という方法である[2]．

例 2.1. 例えば，269 が素数かどうか調べたければ，$\sqrt{269} = 16.4\cdots$ なので，16 以下の素数で割り切れるかどうか調べればよい．$2, 3, 5, 7, 11, 13$ のいずれでも割り切れないことから，269 は素数とわかる．

しかし，どちらの方法も非常に大きな素数を見つけたり，非常に大きな数が素数であるかどうかを判定する方法としては非実用的である．実は，RSA 暗号を使うためには，非常に大きな素数を用意しなければならないため，この問題は実は重要である．

さて，素数を使って述べられる性質として最も重要なものは**素因数分解**である．

定理 2.2. どんな正の整数 n も，素数の積としてただ一通りに表せる．これを n の素因数分解という.（ただし，1 の素因数分解は 1 と定めることにする.）

ここでは証明はしない．素因数分解がわかると計算できるものはいろいろある．その代表的なものが**最大公約数**である．

定義 2.3. 2 つの整数 n, m に対し，n, m をともに割り切るような整数の中で最大のものを，n と m の最大公約数といい，$\gcd(n, m)$ とかく．

[2] $\sqrt{n}$ までによい理由は，$n = pn'$ と積で書けるとすると，$p > \sqrt{n}$ なら $n' < \sqrt{n}$ であり，n' を割り切る素数は $\sqrt{n}$ 以下になるからである．

例 2.4. 24 と 36 の最大公約数を求めよ．答えは 12.

n, m が小さければわざわざ素因数分解などと言わなくても答えられる．しかし少し n, m が大きくなると面倒である．

例 2.5. 520 と 221 の最大公約数を求めよ．

$$520 = 2^3 \cdot 5^1 \cdot 13^1, \qquad 221 = 7^2 \cdot 13^1$$

だから答えは 13.

この方法を一般的な形に述べると次のようになる．

命題 2.6. $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$，$m = p_1^{e_1'} p_2^{e_2'} \cdots p_k^{e_k'}$ とおく．ここで，$p_1, p_2, \ldots, p_k$ は相異なる素数で，e_i, e_i' $(1 \leqq i \leqq k)$ は 0 以上の整数である．このとき，

$$\gcd(n, m) = p_1^{\min\{e_1, e_1'\}} p_2^{\min\{e_2, e_2'\}} \cdots p_k^{\min\{e_k, e_k'\}}$$

である．

つまり，**素因数分解して各素数ごとに指数の小さい方を選んで掛ければ，最大公約数になる．**さらに 2 つやってみよう．

例 2.7. $n = 9,789,395,616$ と $m = 45,173,700$ の最大公約数を求めよ．
$n = 2^5 \cdot 3^4 \cdot 5^0 \cdot 7^4 \cdot 11^2 \cdot 13^1$ と $m = 2^2 \cdot 3^5 \cdot 5^2 \cdot 11^1 \cdot 13^2$ より，$\gcd(n, m) = 2^2 \cdot 3^4 \cdot 5^0 \cdot 7^0 \cdot 11^1 \cdot 13^1 = 46,332$.

例 2.8. $n = 783,451$ と $m = 588,817$ の最大公約数を求めよ．
$783,451 = 983 \cdot 797$ と $588,817 = 983 \cdot 599$ より，$\gcd(n, m) = 983$.

この例からもわかるように，確かに上で述べた方法は最大公約数を求めるには方法としては正しいが，素因数分解を求める部分が実は非常に大変である．特に現れる素数が大きい場合は素因数分解を求めることが難しい．

実は，2 以上の整数 n が与えられたとき，n の素因数分解を求めることは，n が大きくなるにつれて飛躍的に計算しなければならない量が増える問題であり，計算量の増え方は n の多項式のオーダーでは押さえられないだろうと予想されている[3]．この予想が正しい限り，

$$f : \{ \text{素数 2 つの組} \} \ni (p, q) \mapsto pq \in \{ \text{素数 2 個の積で表される整数} \}$$

という関数は，一方向関数になっている．2 つの素数の積を求めることに比べて，2 個の素数の積で表される整数に対して，その素因数 2 個を実際に求めることは非常に大変（であろう）というわけである．RSA 暗号は，この一方向性を基盤とする暗号である．

2.2 ユークリッドの互除法

では最大公約数を求めることも素因数分解と同じように大変なのかというと，実はそうではない．素因数分解を求めることなく，最大公約数を決定するアルゴリズムがある．**ユークリッドの互除法**と呼ばれている．

[3] いわゆる「$P \neq NP$ 予想」.

命題 2.9. a, b, q, r を整数とし，$a = bq + r$ とする．このとき，a, b の公約数の全体と b, r の公約数の全体は一致する．従って特に，$\gcd(a, b) = \gcd(b, r)$ が成り立つ．

証明. c が a, b の公約数なら，$a - bq$ は c で割り切れるので，c は b, r の公約数である．逆に，c が b, r の公約数なら $bq + r$ は c で割り切れので，c は a, b の公約数である． □

使ってみよう．

例 2.10. (1) $n = 36, m = 24$ の最大公約数．$36 = 24 \times 1 + 12$．よって，$\gcd(36, 24) = \gcd(24, 12)$．次に，$24 = 12 \times 2 + 0$ だから，$\gcd(24, 12) = 12$．よって $\gcd(36, 24) = 12$.

(2) $n = 520, m = 221$ の最大公約数.

$$\begin{aligned} 520 &= 221 \times 2 + 78, \\ 221 &= 78 \times 2 + 65, \\ 78 &= 65 \times 1 + 13, \\ 65 &= 13 \times 5 + 0 \end{aligned}$$

より，
$$\begin{aligned} &\gcd(520, 221) \\ &= \gcd(221, 78) \\ &= \gcd(78, 65) \\ &= \gcd(65, 13) = 13. \end{aligned}$$

(3) $n = 783,451, m = 588,817$ の最大公約数.

$$\begin{aligned} 783451 &= 588817 \times 1 + 194634, \\ 588817 &= 194634 \times 3 + 4915, \\ 194634 &= 4915 \times 39 + 2949, \\ 4915 &= 2949 \times 1 + 1966, \\ 2949 &= 1966 \times 1 + 983, \\ 1966 &= 983 \times 2 \end{aligned}$$

より，
$$\begin{aligned} &\gcd(783451, 588817) \\ &= \gcd(588817, 194634) \\ &= \gcd(194634, 4915) \\ &= \gcd(4915, 2949) \\ &= \gcd(2949, 1966) \\ &= \gcd(1966, 983) = 983. \end{aligned}$$

(4) $n = 9,789,395,616, m = 45,173,700$ の最大公約数.

$$\begin{aligned} 9789395616 &= 45173700 \times 216 + 31876416, \\ 45173700 &= 31876416 \times 1 + 13297284, \\ 31876416 &= 13297284 \times 2 + 5281848, \\ 13297284 &= 5281848 \times 2 + 2733588, \\ 5281848 &= 2733588 \times 1 + 2548260, \\ 2733588 &= 2548260 \times 1 + 185328, \\ 2548260 &= 185328 \times 13 + 138996, \\ 185328 &= 138996 \times 1 + 46332, \\ 138996 &= 46332 \times 3 \end{aligned}$$

より，$\gcd(n, m) = 46332$.

最大公約数を求めるだけならこれで良いのだが，今後のために，ユークリッドの互除法をより精密なものにしておく方がよい．というのも，$nx + my = \gcd(n, m)$ という不定方程式の整数解を求められるようになっている必要があるからである．これを実行する次のアルゴリズムは「**拡張されたユークリッドの互除法**」と呼ばれている．

定理 2.11. n, m を正の整数とし，$n > m$ とする．

$a_0 = n, a_1 = m$ とおき，補助数列 $x_0 = 1, x_1 = 0, y_0 = 0, y_1 = 1$ を導入する[4]．

$a_2, a_3, \ldots$ と $x_2, x_3, \ldots, y_2, y_3, \ldots$ を以下のようにして帰納的に定める．

$a_i = x_i n + y_i m$ と $a_{i+1} = x_{i+1} n + y_{i+1} m$ が成り立っているとき，

$$a_i = a_{i+1} q_i + a_{i+2} \ (0 \leqq a_{i+2} < a_{i+1})$$

つまり，a_i を a_{i+1} で割った商を q_i，余りを a_{i+2} とおく．さらに，

$$x_{i+2} = x_i - x_{i+1} q_i, \qquad y_{i+2} = y_i - y_{i+1} q_i$$

とおく[5]．これを繰り返し，$a_{N+1} = 0$ となったとき，

$$\gcd(n, m) = a_N = x_N n + y_N m$$

が成り立つ．

例 2.12. $n = 520, m = 221$ の場合．

$$\begin{aligned} 520 &= 221 \times 2 + 78, \\ 221 &= 78 \times 2 + 65, \\ 78 &= 65 \times 1 + 13, \\ 65 &= 13 \times 5 + 0 \end{aligned}$$

i	a	x	y	q
0	520	1	0	
1	221	0	1	2
2	78	1	-2	2
3	65	-2	5	1
4	13	3	-7	5
5	0			

より，$\gcd(520, 221) = 13$ で，$520x + 221y = 13$ の整数解として $(x, y) = (3, -7)$ が得られる．

注意 2.13. なお，$520x+221y = 13$ のすべての整数解も求められる．$520 \cdot 3 + 221 \cdot (-7) = 13$ を引くと，$520(x-3)+221(y+7) = 0$．両辺を最大公約数 13 で割ると $40(x-3)+17(y+7) = 0$．$40, 17$ は互いに素であることに注意すると，$x - 3$ が 17 で割り切れるので，$x - 3 = 17k$ とおける．このとき $y+7 = -40k$．よって，$(x, y) = (3+17k, -7-40k)$ (k は整数) と解ける．

上のアルゴリズムから次の定理が示されたことになっている．

定理 2.14. a, b を正の整数とするとき，$ax + by = \gcd(a, b)$ は（無限個の）整数解を持つ．特に，a, b が互いに素（つまり最大公約数が 1）なら，$ax + by = 1$ となる整数 x, y が存在する．

練習問題 1 $n = 3107$，$m = 975$ とする．

(1) ユークリッドの互除法を用いて，n, m の最大公約数を求めよ．これを d とおく．

(2) 拡張されたユークリッドの互除法を用いて，$nx + my = d$ の整数解をひとつ求めよ．

---

[4] $n = a_0 = x_0 n + y_0 m, m = a_1 = x_1 n + y_1 m$ となっていることに注意．

[5] すると

$$a_{i+2} = a_i - a_{i+1} q_i = (x_i n + y_i m) - (x_{i+1} n + y_{i+1} m) q_i = (x_i - x_{i+1} q_i) n + (y_i - y_{i+1} q_i) m = x_{i+2} n + y_{i+2} m$$

となっている．

3　合同式の計算とフェルマーの小定理

3.1　合同式の計算

定義 3.1. 整数 m_1, m_2 を自然数 n で割った余りが等しいとき，$m_1 \equiv m_2 \pmod{n}$ とかいて，m_1, m_2 は n を法として合同であるという．

例 3.2. $16 \equiv 11 \equiv 1 \equiv -4 \pmod{5}$．ここで，$-4 = 5 \times (-1) + 1$ だから -4 を 5 で割った余りは 1 と考える．

例えば，$m_1 \equiv m_2 \pmod{n}$ であることと $m_1 - m_2 \equiv 0 \pmod{n}$ であること，つまり $m_1 - m_2$ が n で割り切れることは同値である．なぜなら，$m_1 = nq_1 + r, m_2 = nq_2 + r$ と表せるので，$m_1 - m_2 = n(q_1 - q_2)$ だからである．これは，$m_1 \equiv m_2$ の両辺から m_2 を引いて $m_1 - m_2 \equiv 0$ とすることができる，ということに他ならない．このように合同式でも通常の等号と同じような演算が可能である．次のようにまとめておこう．

命題 3.3. $x_1 \equiv x_2$ かつ $y_1 \equiv y_2 \pmod{n}$ のとき，

$$(x_1 \pm y_1) \equiv (x_2 \pm y_2) \pmod{n}, \qquad x_1 y_1 \equiv x_2 y_2 \pmod{n}$$

が成り立つ．

証明. $x_i = nq_i + r, y_i = nq_i' + r'$ $(i = 1, 2)$ とおける．

このとき，$x_i \pm y_1 = n(q_i \pm q_i') + r + r'$ $(i = 1, 2)$ だから，$x_1 \pm y_1, x_2 \pm y_2$ を n で割った余りはいずれも $r + r'$ を n で割った余りに等しい．従って，$(x_1 \pm y_1) \equiv (x_2 \pm y_2) \pmod{n}$．

また，$x_i y_i = (nq_i + r)(nq_i' + r') = n(n + q_i + q_i') + rr'$ $(i = 1, 2)$ より，$x_1 y_1, x_2 y_2$ を n で割った余りはいずれも rr' を n で割った余りに等しい．従って，$x_1 y_1 \equiv x_2 y_2 \pmod{n}$． □

標語的に言うと,「和・差・積の余りは，それぞれ余りの和・差・積の余り」である．ここで単純に，例えば，積の余りは余りの積と誤解しないこと．$4 \cdot 4 \equiv 16 \equiv 1 \pmod{5}$ だから，余りの積は余りになるとは限らない．上で rr' が余りなのではなく，rr' を n で割った余りが $x_i y_i$ を n で割った余りであることに注意しよう．

さて，ここで合同式の取り扱いの例として次のような問題を考えてみよう．

例 3.4. 3^{520} を 521 で割った余りを求めよ．

$\log_{10}(3^{520}) = 520 \log_{10} 3 = 248.10\cdots$ なので，これを直接計算すると 248 桁程度の大きさになってしまう．それを求めてから 521 で割り算をするというのは手計算ではもちろん，計算機を使用する場合でも桁数を食ってしまい，実用的ではない．

例えば，$3^8 = 81 \cdot 81 = 6561 \equiv 309 \pmod{521}$ なので，

$$3^{16} = 3^8 \cdot 3^8 \equiv 309 \cdot 309 = 95481 \equiv 138 \pmod{521}$$

と計算することができる[6]．$3^{16} = 43046721$ と 8 桁の数を直接計算せずに 95481 という 5 桁の数で余りが計算できる．これなら手持ちの電卓で計算できる．

このように，$3^{2^m} \equiv r \pmod{521}$ を使って，$3^{2^{m+1}} = (3^{2^m})^2 \equiv r^2 \pmod{521}$ と順番に

[6] 丁寧に書けば，$x_1 = y_1 = 3^8, x_2 = y_2 = 309$ として上の命題の 2 つ目を使っている．

求めていくのである．実際にやってみると次のようになる．

まず，$520 = 512 + 8 = 2^9 + 2^3$ であることに注意する．以下，mod 521 は省略して書く．

$$
\begin{aligned}
&3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^4 \equiv 81,\\
&3^8 \equiv 81^2 = 6561 \equiv 309,\\
&3^{16} \equiv 309^2 = 95481 \equiv 138,\\
&3^{32} \equiv 138^2 = 19044 \equiv 288,\\
&3^{64} \equiv 288^2 = 82944 \equiv 105,\\
&3^{128} \equiv 105^2 = 11025 \equiv 84,\\
&3^{256} \equiv 84^2 = 7056 \equiv 283,\\
&3^{512} \equiv 283^2 = 80089 \equiv 376
\end{aligned}
$$

より，

$$
\begin{aligned}
3^{520} &= 3^{512} \times 3^8\\
&\equiv 376 \times 309\\
&= 116184\\
&\equiv 1 \pmod{521}
\end{aligned}
$$

3.2 mod n での「逆数」

整数の範囲では，$nx = 1$ となる x は $n \neq 0$ なら $\dfrac{1}{n}$ である．しかし，$n = \pm 1$ でない限り，n の逆数 x は整数にはならなかった．しかし，n を法とする合同式で考える場合は状況が変わってくる．この節ではこのことを見てみよう．前節の「拡張された Euclid の互除法」が重要な役割を果たす．

まず例を見てみよう．

例 3.5. n を法として，$0, 1, 2, \ldots, n-1$ の中から 2 個を選んで掛けることを考えてみる．

$n=3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$n=4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$n=5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

われわれが考えたい問題は，

$1 \leqq a \leqq n-1$ とするとき，$ab \equiv 1 \pmod{n}$ となる整数 b が存在するか？

ということである．上の例からすぐにわかるように，これはいつでも存在するわけではない．$n = 4, a = 2$ とすると，b は取れない．しかし，同じ $n = 4$ でも $a = 3$ なら $b = 3$ とすればよい．他の場合でも，$n = 3, a = 2$ なら $b = 2$，$n = 5, a = 2$ なら $b = 3$，$n = 5, a = 3$ なら $b = 2$，$n = 3, a = 4$ なら $b = 4$ という具合に存在する．しかも，存在している場合には，いずれも，$1 \leqq b \leqq n-1$ の範囲に，条件を満たすものはただ一つしかないこともわかる．

例 3.6. $n=6$ の場合も見ておくと規則が見えてくるかもしれない．

$n=6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$a=1,5$ 以外では条件を満たす b は存在しない．

一般に次のことが成り立つ．

定理 3.7. $1 \leqq a \leqq n-1$ とするとき，$ab \equiv 1 \pmod{n}$ となる整数 b が存在するための必要十分条件は，a と n が互いに素であることである．

さらに a と n が互いに素であるとき，$ab \equiv 1 \pmod{n}$ を満たす b は $1 \leqq b \leqq n-1$ の範囲にただ一つ存在する．

証明. まず a と n が互いに素であるとする．このとき，a, n の最大公約数は 1 だから，前回の定理 2.14 やったように $nx+ay=1$ となる整数 x, y が存在する．つまり $ay=-nx+1 \equiv \pmod{n}$ が成り立つので，この y を b とすればよい．

逆に，a, n の最大公約数が $d>1$ であるとする．$a=a'd, n=n'd$ とおくと，$ab=nq+1$ のとき，$a'db=n'bq+1$ だから $d(a'b-n'q)=1$ になる．d も $a'b-n'q$ も整数であり，d が 2 以上の整数だとすると，これは矛盾である．よって a, n が互いに素でないときには，条件を満たす b は存在しない．

後半の主張を示す．もし $ab_1 \equiv 1, ab_2 \equiv 1 \pmod{n}$ とすると，$ab_1 - ab_2 \equiv 0 \pmod{n}$ だから，$a(b_1-b_2)=nq$ とおける．a, n が互いに素なので b_1-b_2 が n で割り切れる．従って，$ay \equiv 1 \pmod{n}$ となる整数 y がひとつ見つかると，$b=y+nq$ (q は整数) が条件を満たす整数のすべてである．これは n 個おきに現れ，しかも $y=0$ は条件を満たさないのだから，$1 \leqq b \leqq n-1$ の範囲に入るものがただ一つ存在する． □

定義 3.8. a と n が互いに素であるとき，$ab \equiv 1 \pmod{n}$ を満たす b は $1 \leqq b \leqq n-1$ の範囲にただ一つ存在する．これを **n を法とする a の逆数**と呼び，a^{-1} とかく．

上の証明の最初の部分を見れば明らかなように，逆数を求めるには「拡張されたユークリッドの互除法」を用いて $ax+ny=1$ となる整数 x, y を見つければよい．具体例でやってみよう．

例 3.9. $n=29$ を法として 13 の逆数を求める．

$29x+13y=1$ となる整数 x, y を見つける．拡張されたユークリッドの互除法を使う．$29=13\times 2+3$，$13=3\times 4+1$ であることに注意すると，$a_0=29, a_1=13, (x_0, y_0)=(1,0), (x_1, y_1)=(0,1)$ から始めて，$a_2=3, q_1=2, (x_2, y_2)=(1,-2)$．$a_3=1, q_2=4, (x_3, y_3)=(-4,9)$．よって $29x+13y=1$ の整数解のひとつは $(x, y)=(-4,9)$．つまり，$29\times(-4)+13\times 9=1$．よって，$13\times 9 \equiv 1 \pmod{29}$ となり，29 を法として 13 の逆数は 9 となる．

例 3.10. $n = 24$ を法として 13 の逆数を求める．

$24x + 13y = 1$ となる整数 x, y を見つける．拡張されたユークリッドの互除法を使う．$24 = 13 \times 1 + 11$，$13 = 11 \times 1 + 2$，$11 = 2 \times 5 + 1$ なので，$a_0 = 24, a_1 = 13, (x_0, y_0) = (1, 0), (x_1, y_1) = (0, 1)$ から始めて，$a_2 = 11, q_1 = 1, (x_2, y_2) = (1, -1)$．$a_3 = 2, q_2 = 1, (x_3, y_3) = (-1, 2)$．$a_4 = 1, q_3 = 5, (x_4, y_4) = (6, -11)$．よって $24x+13y = 1$ の整数解のひとつは $(x, y) = (6, -11)$．つまり，$24\times6+13\times(-11) = 1$．よって，$13\times(-11) \equiv 1 \pmod{29}$．$-11 \equiv 13 \pmod{24}$ なので，29 を法として 13 の逆数は 13 自身となる．

逆数を求めることで，次のような一次の合同方程式が解けることにも注意しておこう．

例 3.11. $13x + 7 \equiv y \pmod{29}$ を考える．これは $13x \equiv y - 7 \pmod{29}$ だから，$x \equiv 13^{-1}(y-7) \equiv 9(y-7) = 9y-63 \equiv 9y-5 \pmod{29}$ と解ける．同様に，$13x+7 \equiv y \pmod{24}$ は，$x \equiv 13^{-1}(y-7) \equiv 13y - 91 \equiv 13y + 5 \pmod{24}$ と解ける．

3.3 フェルマーの小定理

先ほど例 3.5 と例 3.6 で見た表をもう少し詳しく見てみる．すると a, n が互いに素のとき，ai $(1 \leqq i \leqq n-1)$ には，$1, 2, \ldots, n-1$ が丁度 1 回ずつ現れていることが見て取れる．これは簡単に証明できる．

命題 3.12. a, n が互いに素のとき，$a, 2a, 3a, \ldots, (n-1)a$ ををを n で割った余りは，$1, 2, 3, \ldots, n-1$ が丁度 1 回ずつ現れる．

証明. もし $ia \equiv ja \pmod{n}$ だとすると，$ia - ja = (i-j)a$ が n で割り切れる．いま n, a は互いに素なので，$i-j$ が n で割り切れる．ところが $1 \leqq i, j \leqq n-1$ のとき，$|i-j| < n$ である．従って，$i-j$ が n で割り切れるためには $i-j = 0$ つまり $i = j$ でなければならない．このことから，$a, 2a, 3a, \ldots, (n-1)a$ ををを n で割った余りはすべて異なる．また，この余りが 0 になることもない．なぜなら ia が n で割り切れると a, n が互いに素より i が n で割り切れ，$1 \leqq i \leqq n-1$ に矛盾するからである．

$a, 2a, 3a, \ldots, (n-1)a$ ををを n で割った余りは，1 以上 $n-1$ 以下の整数でしかもすべて相異なるのだから，$1, 2, \ldots, n-1$ が丁度 1 回ずつ現れるしかない． □

この命題は，前節で証明した定理の主張「a と n が互いに素であるとき，$ab \equiv 1 \pmod{n}$ を満たす b は $1 \leqq b \leqq n-1$ の範囲にただ一つ存在する.」の別証明を与えている．しかしこの証明の通りにやろうとすると $n = 29, a = 13$ のとき，$\{13, 2 \cdot 13, 3 \cdot 13, \ldots, 28 \cdot 13\}$ を 29 で割った余りをひとつずつ調べていかなければならないので，13 の逆数を求める計算は大変になる．前節でやったように「拡張されたユークリッドの互除法」を使う方が大きい a, n に対しても早く計算できる．

注意 3.13. なお，$ab \equiv 1$ となる $1 \leqq b \leqq n-1$ が見つかってしまえば，$ax \equiv j$ となる x は $bj \pmod{n}$ と求められる．従って，本質的に $ax \equiv 1$ が解ければ，$ax \equiv j$ も解ける．

実は，上の定理はもっとエレガントな利用法がある．
「$a, 2a, 3a, \ldots, (n-1)a$ ををを n で割った余りは，$1, 2, 3, \ldots, n-1$ が丁度 1 回ずつ現れる.」ということは，それらを互いにすべて掛けても合同だから，

$$a^{n-1}(n-1)! \equiv (n-1)! \pmod{n}$$

ということにほかならない．これは，$(a^{n-1}-1)\times(n-1)!$ が n で割り切れることを意味している．一般には，$(n-1)!$ と n は互いに素とは限らない．しかし，もし n が素数だとすると，素数 p は $p-1, p-2, \ldots, 1$ のすべてと互いに素なので，p と $(p-1)!$ は互いに素である．従って，a が素数 p と互いに素なら，$a^{p-1}-1$ が p で割り切れる．つまり次が成り立つ．

定理 3.14 (フェルマーの小定理)**.** a が素数 p の倍数でない（つまり a と p が互いに素の）とき，$a^{p-1}\equiv 1 \pmod{p}$ が成り立つ．

例 3.15. $p=521$ は素数である．（例えば $\sqrt{521}=22.8\ldots$ なので，22 以下の素数で割り切れないことをチェックすれば良い．）

フェルマーの小定理は，a が 521 の倍数でない限り，$a^{520}\equiv 1 \pmod{521}$ であることを主張している．例えば，$a=3$ のとき，$3^{520}\equiv 1 \pmod{521}$ であることは例 3.4 でチェックしていた．

練習問題 2

(1) $7^{430} \pmod{23}$ を求めよ．

(2) 173 を法として，2 および 17 の逆数をそれぞれ求めよ．

(3) $16x\equiv 19 \pmod{41}$ を解け．

4　中国剰余定理と大きな素数の見つけ方

4.1　中国剰余定理

中国の南北朝時代（439-589）に編纂されたと言われている算術書『孫子算経』に登場し，後に日本の和算の中でも取り上げられている「百五減算」と呼ばれる問題（とその解法）がある．有名な形としては「年齢当て」の形で述べられる．

あなたの年齢を 3,5,7 で割った余りをそれぞれ教えてください．

と問い，その答えから年齢をあてるものである．『孫子算経』でも次のような解法が与えられていた．つまり，余りをそれぞれ a, b, c としたとき，$a \times 70 + b \times 21 + c \times 15$ を計算し，$3 \times 5 \times 7 = 105$ を引いて行って年齢として妥当な値を見つける，というものである．例えば，$a = 1, b = 4, c = 5$ なら，$1 \times 70 + 4 \times 21 + 5 \times 15 = 229$ から 105 を 2 回引いて，19 歳となる．もちろん 124 歳や 229 歳の可能性もあるが，目の前の人が若い姿を保っている仙人でもない限り，通常は 19 歳であろう．このように $3, 5, 7$ の最小公倍数である 105 を引いて行くので，和算では「百五減算」と呼ばれている．

この問題は，次のような連立形の合同方程式を解くことに他ならない．

$$x \equiv a \pmod 3, \qquad x \equiv b \pmod 5, \qquad x \equiv c \pmod 7$$

まず 2 個の連立合同方程式の場合から考えよう．

命題 4.1. m_1, m_2 は互いに素な正の整数とする．このとき，整数 a, b に対して，

$$x \equiv a \pmod{m_1}, \qquad x \equiv b \pmod{m_2}$$

を満たす整数 x が $0 \leqq x \leqq m_1 m_2 - 1$ の範囲にただ一つ存在する．（あるいは $m_1 m_2$ を法としてただ一つ存在する，と言ってもよい．）

証明. m_1, m_2 は互いに素なので，$m_1 u + m_2 v = 1$ となる整数 u, v が存在する．両辺を m_1，m_2 を法としてみると，$m_1 u \equiv 1 \pmod{m_2}$ かつ $m_2 v \equiv 1 \pmod{m_1}$ が成り立っている．そこで，$x = a(m_2 v) + b(m_1 u)$ を考えると，$x \equiv a \pmod{m_1}$ かつ $x \equiv b \pmod{m_2}$ を満たす．

次に，もし $x \equiv a \pmod{m_1}, x \equiv b \pmod{m_2}$ と $y \equiv a \pmod{m_1}, y \equiv b \pmod{m_2}$ が成り立っていたとすると，$x - y \equiv 0$ が $\bmod m_1$ でも $\bmod m_2$ でも成り立つ．つまり $x - y$ は m_1 の倍数かつ m_2 の倍数になる．m_1, m_2 は互いに素だから，$x - y$ は $m_1 m_2$ の公倍数である．逆に，$x \equiv a \pmod{m_1}, x \equiv b \pmod{m_2}$ なら $x + m_1 m_2$ も条件を満たすことは明らかなので，連立合同方程式の解は $m_1 m_2$ おきに 1 個現れることがわかる．従って，$0 \leqq x \leqq m_1 m_2 - 1$ の範囲に解がただ一つ存在する．　□

例 4.2. $x \equiv 3 \pmod{13}$ かつ $x \equiv 2 \pmod{17}$ を満たす x を見つけよう．

上の証明の通りに考える．

まず $13u + 17v = 1$ となる u, v を見つける．前回も使ったように「拡張されたユークリッドの互除法」を使う．$17 = 13 \times 1 + 4$，$13 = 4 \times 3 + 1$ に注意し，$a_0 = 17, a_1 = 13, (v_0, u_0) = (1, 0), (v_1, u_1) = (0, 1)$ から始めると，$a_2 = 4, q_1 = 1$，$(v_2, u_2) = (1, -1)$．$a_3 = 1, q_2 = 3$，$(v_3, u_3) = (-3, 4)$．よって，$13 \times 4 + 17 \times (-3) = 1$ が見つかる．

そこで $x = 3 \times 17 \times (-3) + 2 \times (13 \times 4) = -49 \equiv 172 \pmod{13 \cdot 17 (= 221)}$ とわかる．

一般に k 個の場合も考えよう．これを**中国剰余定理** (Chinese remainder theorem) と呼んでいる[7]．

定理 4.3 (中国剰余定理)．$m_1, m_2, \ldots, m_k$ をどの 2 つをとっても互いに素な正の整数とする．$m = m_1 m_2 \cdots m_k$ とおく．このとき，整数 $a_1, a_2, \ldots, a_k$ に対して，

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_k \pmod{m_k},$$

を満たす整数 x が $0 \leqq x \leqq m-1$ の範囲にただ一つ存在する．(あるいは m を法としてただ一つ存在する，と言ってもよい．)

証明．$m = m_i M_i$ $(1 \leqq i \leqq k)$ とおく．$m_1, m_2, \ldots, m_k$ はどの 2 つをとっても互いに素なので，m_i と M_i は互いに素である．よって，$M_i u_i \equiv 1 \pmod{m_i}$ となる u_i が取れる[8]．すると

$$x = a_1 M_1 u_1 + a_2 M_2 u_2 + \cdots + a_k M_k u_k$$

とおけば，$x \equiv a_i \pmod{m_i}$ が成り立つ．なぜなら，M_j $(j \neq i)$ はすべて m_i を因子に持つので m_i で割り切れ，上の u_i の作り方から $a_i M_i u_i \equiv a_i \pmod{m_i}$ であるから．

また，もし x, y がいずれも条件を満たすと $x - y \equiv 0 \pmod{m_i}$ が $1 \leqq i \leqq k$ で成り立つ．$m_1, m_2, \ldots, m_k$ はどの 2 つをとっても互いに素だから，最小公倍数は $m = m_1 m_2 \cdots m_k$ であることに注意すれば，$x \equiv y \pmod{m}$．逆に，x が解のとき $x + m$ も条件を満たすことは明らかだから，$0 \leqq x \leqq m-1$ の範囲に解がただ一つ存在する． □

例 4.4. $x \equiv 1 \pmod 3, x \equiv 4 \pmod 5, x \equiv 5 \pmod 7$ を満たす x を求めよう．上の証明をなぞりながら考える．

$m_1 = 3$，$M_1 = 5 \times 7 = 35$ である．$35u_1 + 3v_1 = 1$ となる u_1 を求める．$35 = 3 \times 11 + 2$，$3 = 2 \times 1 + 1$ だから，$a_0 = 35, a_1 = 3, (x_0, y_0) = (1, 0), (x_1, y_1) = (0, 1)$ から始めて $a_2 = 2, q_1 = 11$，$(x_2, y_2) = (1, -11)$．$a_3 = 1, q_2 = 1$，$(x_3, y_3) = (-1, 12)$．つまり，$35 \times (-1) + 3 \times 12 = 1$ が見つかったので，$u_1 = -1$．

$m_2 = 5$，$M_2 = 3 \times 7 = 21$ である．$21u_2 + 5v_2 = 1$ となる u_2 を求める．$21 = 5 \times 4 + 1$ だから，$a_0 = 21, a_1 = 5, (x_0, y_0) = (1, 0), (x_1, y_1) = (0, 1)$ から始めて $a_2 = 1, q_1 = 4$，$(x_2, y_2) = (1, -4)$．つまり，$21 \times 1 + 5 \times (-4) = 1$ が見つかったので，$u_2 = 1$．

$m_3 = 7$，$M_3 = 3 \times 5 = 15$ である．$15u_3 + 7v_3 = 1$ となる u_3 を求める．$15 = 7 \times 2 + 1$ だから，$a_0 = 15, a_1 = 7, (x_0, y_0) = (1, 0), (x_1, y_1) = (0, 1)$ から始めて $a_2 = 1, q_1 = 2$，$(x_2, y_2) = (1, -2)$．つまり，$15 \times 1 + 7 \times (-2) = 1$ が見つかったので，$u_3 = 1$．

よって，$x = 1 \times (35 \times (-1)) + 4 \times (21 \times 1) + 5 \times (15 \times 1) = 124 \equiv 19 \pmod{3 \cdot 5 \cdot 7 = 105}$．

注意 4.5. 上の証明で本質的なことは $M_i u_i \equiv 1 \pmod{m_i}$ となる u_i を見つけることである．これは一般には上で述べたような「拡張されたユークリッドの互除法」を用いることになるが，M_i, m_i が小さければそこまでしなくてもすぐにわかる．

例えば，$35u_1 \equiv 1 \pmod 3$ は，$2u_1 \equiv 1 \pmod 3$ なので，$u_1 = -1, 2$ などと見つかる．$21u_2 \equiv 1 \pmod 5$ は，$u_2 \equiv 1 \pmod 5$ となるから，$u_2 = 1$．$15u_3 \equiv 1 \pmod 7$ も，$u_3 \equiv 1 \pmod 7$ となるから，$u_3 = 1$．

最初の「百五減算」の解法で出てきた $70, 21, 15$ は，$u_1 = 2, u_2 = 1, u_3 = 1$ としたときの $M_1 u_1 = 70, M_2 u_2 = 21, M_3 u_3 = 15$ に他ならない．

[7] 英訳通り訳すと「中国の剰余定理」とか「中国人の剰余定理」となる．また「孫子定理」などと呼ばれることもある．

[8] $M_i u_i + m_i v_i = 1$ となる u_i, v_i を各 i ごとに取る．

4.2 大きな素数の見つけ方

次回，RSA 暗号と呼ばれる公開鍵暗号のひとつについて紹介するが，その際，非常に大きな素数を用意する必要がある．しかし，第 1 回で述べたように，素数を小さいほうから順番に列挙していったり，$\sqrt{n}$ 以下のすべての素数で割り切れるか調べるという方法は現実的ではない．また，与えられた整数の素因数分解を求めることは非常に困難である．他方，2002 年に発表された”PRIMES is in P”という論文において，Agarmal-Kayal-Saxena は，大きな奇数が与えられたとき，それが素数であるか否かを判定することは，多項式時間で可能である[9]ことを示した．これは AKS アルゴリズムと呼ばれている．このことは，素数判定は素因数分解に比べると速く判定できる（だろう[10]）ということを意味している．しかしこの場合も，多項式時間とはいえ，その判定には非常に長い時間がかかるため，現実的ではない．このように，大きな奇数 n が素数であるか否かを決定しようとする方法を確定的素数判定法と呼ぶ．しかし現状では，確定的素数判定法で実用的なものは見つかっていない．多くの場合，合成数である確率が非常に小さいかどうかを判定する**確率的素数判定法**が用いられている．ここではそのもっとも簡単な一例として「フェルマー・テスト」と呼ばれる方法を紹介する．

フェルマーの小定理（定理 3.14）を思い出そう．この定理は，

「p が素数」$\Rightarrow$「p と互いに素なすべての整数 a に対して，$a^{p-1} \equiv 1 \pmod{p}$」

ということを主張していた．ということは，上の命題の対偶を取ると，奇数 n に対して，

「n と互いに素な整数 a で $a^{n-1} \not\equiv 1$ となるものが存在する.」$\Rightarrow$「n は合成数」

という主張が導かれる．

定義 4.6. 奇数 n に対し，整数 a を $1 < a < n$ の範囲から 1 つ選ぶ．

(i) a と n が互いに素でなければ「n は合成数」と出力する．

(ii) a と n が互いに素のとき，

- $a^{n-1} \not\equiv 1 \pmod{n}$ ならば,「n は合成数」と出力．
- $a^{n-1} \equiv 1 \pmod{n}$ ならば,「n は素数の可能性がある」と出力．

この方法を**フェルマー・テスト**と呼ぶ．

例 4.7. 例えば，$n = 91$ としよう．

$a = 3$ を選んだ場合，$90 = 2^6 + 2^4 + 2^3 + 2$．$81^2 = 6561 \equiv 9 \pmod{91}$ に注意すると，$3^{90} = 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3^2 \equiv 81 \cdot 81 \cdot 9 \cdot 9 \equiv 729 \equiv 1 \pmod{91}$．となるので，91 は「素数の可能性がある」と出力される．

しかし，$a = 2$ を選んだ場合，$2^8 = 16^2 = 256 \equiv 74$ と $74^2 = 5476 \equiv 16$ から，$2^{90} = 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^2 \equiv 16 \cdot 16 \cdot 74 \cdot 464 \pmod{91}$．よって「91 は合成数」と出力される．

[9] 奇数 n を大きくしていったとき，素数であるか否かを判定するのにかかる時間が n の多項式のオーダーで抑えられる．

[10] $P \neq NP$ 予想が正しいなら．

フェルマー・テストにおいて，もしある a で「n は合成数」と出力された場合，n は必ず合成数である．これが上で述べたフェルマーの小定理の対偶である．つまり上の例で 91 は合成数とわかる．一方で，フェルマー・テストにおいて，ある a で「n は素数の可能性がある」と出力されたとしても，上の例のように必ずしも n が素数であるとは言い切れない．

一見するとフェルマー・テストが素数判定に使えるようには見えないかもしれない．しかし，実はこれだけでも比較的強力な「確率的素数判定法」を構築できる．その理由を考えてみよう．

補題 4.8. 奇数 n と互いに素な 2 つの整数 a_1, a_2 に対して $a_1^{n-1} \equiv 1 \pmod{n}$ かつ $a_2^{n-1} \equiv 1 \pmod{n}$ がともに成り立っているとする．このとき，$(a_1 a_2^{-1})^{n-1} \equiv 1 \pmod{n}$ が成り立つ．ここで a_2^{-1} とは n を法とする a_2 の逆数である[11]．

証明. 合同式の計算から明らかである．$a_2^{n-1} \equiv 1 \pmod{n}$ の両辺に $(a_2^{-1})^{n-1}$ を掛けると，$(a_2^{-1})^{n-1} \equiv 1$．この両辺に a_1^{n-1} を掛けると，$(a_1 a_2^{-1})^{n-1} \equiv a_1^{n-1} \equiv 1 \pmod{n}$． □

定理 4.9. n を奇数の合成数とするとき，n と互いに素な整数 $1 < a_0 < n$ で「n は合成数」と出力されたとする．このとき，$\{a \mid \gcd(a, n) = 1, 1 < a < n\}$ の中で，「n は合成数」と主力するものは半分以上ある．

証明. $\{a \mid \gcd(a, n) = 1, 1 < a < n\}$ の中で $a^{n-1} \equiv 1 \pmod{n}$ となっているものすべてを $a_1, a_2, \ldots, a_s$ とする．このとき，$a_0 a_i \pmod{n}$ $(1 \leqq i \leqq s)$ を考えてみる．これらはすべて相異なり，$1 < a_0 a_i < n$ を満たす．なぜなら，$a_0 a_i \equiv a_0 a_j$ なら両辺に a_0^{-1} を掛けて $a_i \equiv a_j$ となり $i = j$．また $a_0 a_i \equiv 1$ だと $a_i^{-1} = a_0$ となる．$a_0^{n-1} = (a_i^{-1})^{n-1} \equiv 1$ となって a_0 の取り方に反する．

もし $(a_0 a_i)^{n-1} \equiv 1$ なら，前の補題から $1 \equiv ((a_0 a_i) a_i^{-1})^{n-1} \equiv a_0^{n-1}$ となる．しかしこれは a_0 の取り方に矛盾している．よって $(a_0 a_i)^{n-1} \not\equiv 1$ なら，

以上のことから，$a_0 a_i \pmod{n}$ は $\{a \mid \gcd(a, n) = 1, 1 < a < n\}$ の中で「n は合成数である」と出力する．このことは，$\{a \mid \gcd(a, n) = 1, 1 < a < n\}$ の中に「n は素数の可能性がある」と出力するものと同数以上「n は合成数である」と出力するものが存在することを意味している． □

この定理は，$1 < a < n$ をランダムに選んだとき，フェルマー・テストにおいて，

奇数の合成数 n が「素数の可能性がある」と判定される確率は$\frac{1}{2}$より小さい．

ということを主張している．とすれば，フェルマー・テストを k 回行っていずれの a でも「素数の可能性がある」と判定されたにも拘わらず n が合成数であるという確率はたかだか $\dfrac{1}{2^k}$ 程度であり，これは試行回数を増やせば指数的に減少していく．n は非常に大きい奇数（例えば，10 進法で 300 桁以上）であることを想定しており，100 回フェルマーテストを行うことに支障はなく，素数でないのに素数であるとミスをする確率は $\dfrac{1}{2^{100}}$ 程度で非常に小さくなる．

ところが，実際には，フェルマー・テストには落とし穴もある．

「n と互いに素な整数 a で $a^{n-1} \not\equiv 1$ となるものが存在する.」$\Rightarrow$「n は合成数」

[11] a_2, n は互いに素だから n を法として a_2 に逆数が取れることに注意せよ．

の逆向きが正しくないのである．つまり，n が合成数であるにも関わらず，n と互いに素なすべての a に対して，$a^{n-1} \equiv 1 \pmod{n}$ となってしまうものが存在する．このような n を**カーマイケル数**という．運悪く n がカーマイケル数だと $\{a \mid \gcd(a,n) = 1, 1 < a < n\}$ のどれをとってフェルマー・テストをしても「n は素数の可能性がある」と判定されてしまう．このようなカーマイケル数は無限個存在することがわかっており，最小のカーマイケル数は 561 である．従って，現実的には，フェルマー・テストよりもさらに強力な確率的素数判定法が用いられている．代表的なもののひとつに**ミラー・ラビン法**と呼ばれている方法があり，この場合は，n がカーマイケル数であろうとなかろうと 1 回のテストでミスする確率は $\dfrac{1}{4}$ 以下になる．今回は述べる余裕がないので，興味のある人は，専門書で学習してほしい．

練習問題 3

(1) 連立合同式 $x \equiv 2 \pmod{5},\ x \equiv 5 \pmod{12},$ を解け．

(2) 連立合同式 $x \equiv 13 \pmod{20},\ x \equiv -12 \pmod{21},\ x \equiv -7 \pmod{23}$ を解け．

(3) $n = 21$ に対して，フェルマー･テストを行うことを考える．$\{a \mid \gcd(a,n) = 1, 1 < a < n\}$ の中で n を「素数の可能性がある」と出力する a をすべて求めよ．

5 RSA 暗号の数学的基礎

5.1 RSA 暗号

公開鍵暗号のひとつである RSA 暗号について紹介する．RSA 暗号は，Rivest-Shamir-Adelman によって 1977 年に提案された暗号アルゴリズムである．

アリスは，

(i) 非常に大きな素数 p, q をえらび，$n = pq$，$M = (p-1)(q-1)$ とおく．

(ii) 次に，M と互いに素な整数 e を $1 < e < M$ の範囲からひとつ選ぶ．すると $ed \equiv 1 \pmod{M}$ となる $1 < d < M$ がただ一つ定まる．

(iii) (n, e) を公開鍵とし，(n, d) は秘密鍵として保持しておく．

ボブがアリスに秘密の文を送りたい場合，次のような操作を行う．

- 送りたい文を $0 < m < n$ となる整数 m に変換する[12]．
- $m^e \pmod{n}$ を計算する．この値を c とし，アリスには c を送信する．

定理 5.1. $c^d \pmod{n} = m$ が成り立つので，アリスはボブから秘密文を復元できる．

証明. まず，$ed \equiv 1 \pmod{M = (p-1)(q-1)}$ であることに注意すると

$$(m^e)^d = n^{ed} = m^{kM+1} = m^{(k(p-1)(q-1)} \times m$$

である．もし素数 p と m が互いに素なら，フェルマーの小定理によって $m^{p-1} \equiv 1 \pmod{p}$ であるから，$(m^e)^d \equiv m \pmod{p}$．もし p が m を割り切ると，$m \equiv 0 \pmod{p}$ だから，$(m^e)^d \equiv 0 \equiv m \pmod{p}$．従って，いずれの場合でも，$(m^e)^d \equiv m \pmod{p}$ が成り立つ．もう 1 つの素数 q についても全く同様に，$(m^e)^d \equiv m \pmod{q}$ が成り立つ．従って，$c^d \equiv (m^e)^d \equiv m$ が mod p でも，mod q でも成り立つ．中国剰余定理によれば，$x \equiv m \pmod{p}$ かつ $x \equiv m \pmod{q}$ となる整数 x は，pq を法としてすべて合同であり，$0 \leqq x < pq$ の範囲にただ一つ存在し，pq を法としてすべて合同であった．$0 < m < n$ だから $c^d \equiv m \pmod{n}$ であることが示された． □

例 5.2. $p = 11, q = 23$ とすると，$n = 11 \cdot 23 = 253$ であり，$M = 10 \cdot 22 = 220$ となる．

次に，M は 3 で割り切れないので，$e = 3$ としてみる．すると，$220 = 3 \times 73 + 1$ より，$d \equiv -73 \equiv 147 \pmod{220}$ となる．公開するのは $(n, e) = (253, 3)$ である．

ボブが $m = 49$ を暗号化する場合を考えよう．暗号文 $c = m^e = 49^3 \equiv 2401 \cdot 49 \equiv 124 \cdot 49 \equiv 6076 \equiv 4 \pmod{253}$ である．これが送られてきたとき，アリスは，$c^d = 4^{147} \pmod{253}$ を計算する．

$$4^2 = 16, \quad 4^{2^2} \equiv 16^2 \equiv 3, \quad 4^{2^3} \equiv 3^2 = 9, \quad 4^{2^4} \equiv 9^2 = 81,$$
$$4^{2^5} \equiv 81^2 = 6561 \equiv 236 \equiv -17, \quad 4^{2^6} \equiv (-17)^2 = 289 \equiv 36, \quad 4^{2^7} \equiv 36^2 = 1296 \equiv 31$$

となる．こうして，$c^d = 4^{147} = 4^{2^7} \cdot 4^{2^4} \cdot 4^2 \cdot 4 \equiv 31 \cdot 81 \cdot 16 \equiv 4 = 2511 \cdot 64 \equiv (-19) \cdot 64 \equiv -204 \equiv 49 \pmod{253}$ と，確かにボブのメッセージ m を復元できている．

[12] ここをどういう変換で行うかは，ここでは扱わない．ボブが整数 m をアリスに送信したい場合を考える．

計算する場合も直接やらず連立合同方程式の形に直して考える方が少し早い．つまり，アリスは p, q も知っているので，4^{147} を mod 11 と mod 23 でそれぞれ計算する．
まず 11 を法として，直接計算してみると

$$4^2 = 16 \equiv 5, \quad 4^{2^2} \equiv 5^2 \equiv 3, \quad 4^{2^3} \equiv 3^2 = 9, \quad 4^{2^4} \equiv 9^2 \equiv 4, \quad 4^{2^5} \equiv 4^2 \equiv 5,$$
$$4^{2^6} \equiv 5^2 \equiv 3, \quad 4^{2^7} \equiv 3^2 = 9$$

より，$4^{147} \equiv 9 \cdot 4 \cdot 5 \cdot 4 \equiv 5 \pmod{11}$.

フェルマーの小定理から $4^{10} \equiv 1$ であることを使って計算する方が少し早い．$4^{147} = (4^{10})^{14} \times 4^7 \equiv 4^{4+2+1} \equiv 3 \cdot 5 \cdot 4 \equiv 5 \pmod{11}$.

次に 23 を法として，直接計算すると

$$4^2 = 16, \quad 4^{2^2} \equiv 16^2 \equiv 3, \quad 4^{2^3} \equiv 3^2 = 9, \quad 4^{2^4} \equiv 9^2 \equiv 12, \quad 4^{2^5} \equiv 12^2 \equiv 6,$$
$$4^{2^6} \equiv 6^2 \equiv 13, \quad 4^{2^7} \equiv 13^2 \equiv 8$$

より，$4^{147} \equiv 8 \cdot 12 \cdot 16 \cdot 4 \equiv 4 \cdot 16 \cdot 4 = 4^4 \equiv 3 \pmod{23}$.

こちらもフェルマーの小定理から $4^{22} \equiv 1$ であることを使って計算する方が少し早い．$4^{147} = (4^{22})^6 \cdot 4^{15} \equiv 4^{8+4+2+1} \equiv 9 \cdot 3 \cdot 16 \cdot 4 \equiv 3$.

よって元のメッセージ m は，$m \equiv 5 \pmod{11}$ かつ $m \equiv 3 \pmod{23}$ を満たす $0 < m < 253$ である．

連立合同方程式を解くために，$11x+23y = 1$ となる x, y を見つける．$23 = 11\times2+1$ より，$(x, y) = (-2, 1)$ が見つかる．すると m の候補は，$5\times(23\times1)+3\times(11\times(-2)) = 115-66 = 49$ と n を法として合同．よって $m = 49$ と復元できる．

5.2 実用上はいろいろ問題がある

RSA 暗号が「安全」であることの根拠は，公開されている n の値から素数 p, q を求める素因数分解が困難であること（予想）に基づいている．素因数分解の困難性についてはまだ証明は知られていないが，正しいと信じられている．しかしその一方で，RSA 暗号を解読するのに n の素因数分解を求めることが本当に必要かどうかは未解決であり，素因数分解を経由しない易しい解読法が今後現れる可能性はある．また，実用上は上で述べた RSA 暗号をそのまま自由に使ってしまってよいわけではなく，いくつか注意しなければならない点や安全上の問題もある．ここではそのうちの非常に簡単な 2 つの観点だけを紹介する．

2 つの素数 p, q が接近していてはいけない．

n は 2 つの素数の積として $n = pq$ と表されている．ところがこれは，

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

とも表せる．p, q は（素数だが 2 は小さすぎて使わないので）奇数であるため，$\frac{p \pm q}{2}$ はいずれも整数である．つまり n は 2 つの平方数の差として表されていることになる．すると，もし p, q が接近している場合，つまり $p > q$ かつ $p - q$ が小さいと $\frac{p-q}{2}$ は非常に小さい整

数であることから，$\left(\dfrac{p+q}{2}\right)^2$ は n に近く，$\dfrac{p+q}{2}$ は $\sqrt{n}$ よりも少しだけ大きい整数となっている．すると，$\sqrt{n}$ よりも大きい整数 t を小さいほうから順番にとり，t^2-n が平方数になるかどうかを調べていくと，$t=\dfrac{p+q}{2}$ と $\dfrac{p-q}{2}$ が求められてしまう．すると p,q が確定し，暗号は破られる．

例 5.3. $n=23360947609$ の場合を考えてみよう．$\sqrt{n}=152842.8\ldots$ である．そこで，$t=152843$ とすると，$t^2-n=35040$．これは平方数ではない．($\sqrt{35040}=187.1\ldots$.)
$t=152844$ とすると，$t^2-n=340727$．これは平方数ではない．($\sqrt{340727}=583.7\ldots$.)
$t=152845$ とすると，$t^2-n=646416=804^2$ となって，平方数となる．従って，$\dfrac{p+q}{2}=152845$ かつ $\dfrac{p-q}{2}=804$ を解くと，$p=153649$，$q=152041$ と求められる．

公開鍵に使用する e が小さすぎると危険である．

公開鍵に e を使用している e 人の人を考えよう．例えば，e 人に同じメッセージ m を暗号化して送る場合である．e 人の公開鍵が $(n_1,e),(n_2,e),\ldots,(n_e,e)$ であるとし，$0<m<n_i$ $(i=1,2,\ldots,e)$ であるとする．簡単のため $n_1,n_2,\ldots,n_e$ はどの 2 つをとっても互いに素であるとしよう．すると各人への暗号文が c_i $(i=1,2,\ldots,e)$ であったとする．

中国剰余定理によれば，連立合同式 $x\equiv c_i \pmod{n_i}$ $(i=1,2,\ldots,e)$ を満たす x は，$0\leqq x<n_1n_2\cdots n_e$ の範囲にただ一つ存在する．

$x=m^e$ は $x\equiv c_i \pmod{n_i}$ を満たしており，しかも $0<m<n_i$ から $0<m^e<n_1n_2\cdots n_e$ を満たしている．従ってこの連立合同式の $0\leqq x<n_1n_2\cdots n_e$ にある解は m^e そのものである．m^e 自身が求まってしまうと，e 乗根を求める計算は容易にできる．

例 5.4. 公開鍵 $(391,3),(55,3),(87,3)$ を利用している 3 人の顧客に同じメッセージ m が RSA 暗号を用いて送信されており，その暗号文は $208,38,32$ であるという．このとき，m を求めてみよう．

そのために，連立合同式

$$x\equiv 208 \pmod{391},\quad x\equiv 38 \pmod{55},\quad x\equiv 32 \pmod{87}$$

の解を求めよう．まず

$$55\times 87u_1\equiv 1 \pmod{391},\quad 391\times 87u_2\equiv 1 \pmod{55},\quad 391\times 55u_3\equiv 1 \pmod{87},$$

となる u_1,u_2,u_3 を求める．

$55\times 87u_1\equiv 93u_1\equiv 1 \pmod{391}$.
$391=93\times 4+19$，$93=19\times 4+17$，$19=17\times 1+2$，$17=2\times 8+1$．よって，$(a_0,a_1)=(391,93),(x_0,y_0)=(1,0),(x_1,y_1)=(0,1)$ から始めて，$q_1=4,(x_2,y_2)=(1,-4)$．$q_2=4,(x_3,y_3)=(-4,17)$．$q_3=1,(x_4,y_4)=(5,-21)$．$q_4=8,(x_5,y_5)=(-44,185)$．よって，$391\times(-44)+93\times 185=1$．より $u_1=185$.

同様に，$391\times 87u_2\equiv 27u_2\equiv 1 \pmod{55}$.
$55=27\times 2+1$ より，$55\times 1+27\times(-2)=1$．より $u_2=-2$.

$391\times 55u_3\equiv 16u_3\equiv 1 \pmod{87}$,
$87=16\times 5+7$，$16=7\times 2+2$，$7=2\times 3+1$．よって，$(a_0,a_1)=(87,16),(x_0,y_0)=$

$(1,0),(x_1,y_1)=(0,1)$ から始めて，$q_1=5,(x_2,y_2)=(1,-5)$．$q_2=2,(x_3,y_3)=(-2,11)$．$q_3=3,(x_4,y_4)=(7,-38)$．よって，$87\times 7+16\times(-38)=1$．より $u_3=-38$．

よって，$x\equiv 208\times 55\times 87\times 185+38\times 391\times 87\times(-2)+32\times 391\times 55\times(-38)\equiv 103823 \pmod{391\times 55\times 87=1870935}$．

m^3 は，上で解いた連立合同式の解であり，しかも $0\leqq m^3<391\cdot 55\cdot 87$ を満たしているから，$m^3=103823$ である．($40^3<103823<50^3$ と見当をつけて調べることにより)3 乗根を求めると，$m=47$．

練習問題 4 アリスは，$p=29,q=31$ を選び，$(n,e)=(899,11)$ を公開鍵として，RSA 暗号を用いる．

(1) アリスの秘密鍵 d を求めよ．

(2) ボブがアリスへ $m=15$ を送るとき，この公開鍵を用いて得られる暗号文 c を求めよ．

(3) ボブからアリスへ暗号文 $c=467$ が送られてきた．ボブの元のメッセージ m を求めよ．

練習問題 5 公開鍵 $(143,3),(391,3),(899,3)$ を用いている 3 人の顧客に，RSA 暗号を用いて暗号文 $60,203,711$ がそれぞれ送信された．この 3 つの暗号文が同じメッセージ m の暗号化であるとするとき，上で述べた方法を用いて（つまり，$143,391,899$ を素因数分解することなしに）元のメッセージ m を求めよ．
（手計算では大変なので電卓などを利用するとよい.）