素数と暗号*

初等整数論と RSA 暗号系入門

佐藤 篤†

§0　プロローグ

ある日, 学校の掲示板に次のようなメモが貼ってあった:

馬場さんへ

例のカードの暗証番号は

① まず 127 乗して

② その結果を 11021 で割って

③ そのときの余りをここに書いておいて下さい

有島

3733

図 1: 掲示板のメモ I

掲示を出したのは有島先生で, どうやら 3733 という数字は馬場さんが書き込んだものらしい.

これを目にした井深君は, “こんなところで暗証番号のやり取りをするとは不用心な” と思い, 家に帰ると暗証番号の解読に取りかかった. 井深君は数学が得意だが, コンピュータに触れたことはない. 使えるのは電卓だけである. “カードの暗証番号” というからには 4 桁の数だろうと考えた井深君は, 1 から 9999 までの整数に対して順に ①, ②, ③ の操作を施して行くことにした. まずは $n = 1, 2, \ldots, 10$ に対して n^{127} を 11021 で割ったときの余りを計算すると次のようになった:

---

*第 8 回仙台数学セミナー (2001 年 8 月 20 日 – 23 日) 配布資料に加筆修正 [2016 年 4 月 1 日版]

†東北学院大学教養学部 (E-mail: atsushi@mail.tohoku-gakuin.ac.jp)

表 1: n^{127} を 11021 で割ったときの余り

n	1	2	3	4	5	6	7	8	9	10
余り	1	10010	5490	8189	4338	4194	3741	8713	8686	640

ここまで計算するのに要した時間は電卓を使って 2 時間である. この調子では 9999 まで計算するのに 2000 時間 (約 83 日) もかかってしまう.

次の日, 計算に疲れた井深君は, コンピュータのプログラミングが趣味だという小幡君に相談することにした. 小幡君は数学はそれほど得意ではないが, 井深君が計算のやり方を丁寧に説明すると数行のプログラムを書いてくれた. そのプログラムを実行すると —— “暗証番号は 1192 だね” と小幡君. なんと 10 秒で計算が終わってしまった.

数日後, 今度は掲示板に次のようなメモが貼ってあった:

馬場さんへ

例のクレジットカードの番号は

① まず 5167 乗して

② その結果を 10487803534477109 で割って

③ そのときの余りをここに書いておいて下さい

有島

1337757853726307

図 2: 掲示板のメモ II

これを見た井深君と小幡君は再び解読に取りかかることにした. “クレジットカードの番号” というからには 16 桁の数に違いない. 今度は 1 から 9999999999999999 までの整数を順にチェックするだけである. 4 桁の整数を全部チェックするのは 10 秒で済んだから, 16 桁の整数を全部チェックするのはだいたい 10^{13} 秒くらいで終わるだろう. ここで電卓を手にした井深君はあることに気がついた. “10^{13} 秒って 30 万年以上だぞ!” 2 人は途方に暮れてしまった. “いったい有島先生はどんな計算をして解読するんだろう...”

§1　整数の合同

正の整数 m と整数 a, b に対し, $a - b$ が m の倍数であるとき a と b は m を法(ほう)として**合同**であるといい, このことを "$a \equiv b \pmod{m}$" と表す.

注意 1.1 "合同" という言葉が使われているが, 三角形の合同とは特に関係はない.

例 1.2 (i) $m = 2$ の場合. 整数 a, b が 2 を法として合同であるとは a, b の偶奇が一致するということに他ならない.

(ii) $m = 10$ の場合. 0 以上の整数 a, b が 10 を法として合同であるとは a, b の一(いち)の位が一致するということに他ならない (a または b が負の場合には若干の修正を要する).

一般に, m を正の整数とするとき, 任意の整数 a に対して

$$a = qm + r, \qquad 0 \leqq r < m$$

となるような整数 q と r が一意的に存在し (整数 q, r はそれぞれ a の m による**商**, **余り**と呼ばれる), そのとき $a \equiv r \pmod{m}$ が成り立つ. 従って, 任意の整数 a は $0 \leqq r < m$ であるようなただひとつの整数 r ($= a$ の m による余り) と m を法として合同になる.

練習問題 1.3 上に述べた q と r の一意性を証明せよ. すなわち, 整数 q' と r' も

$$a = q'm + r', \qquad 0 \leqq r' < m$$

をみたしたとすると, 実は $q = q'$ かつ $r = r'$ であることを示せ.

容易に確かめられるように, 与えられた法に関する合同関係は次の性質をもつ:

補助定理 1.4 m を正の整数, $a, b, c, \ldots$ を整数とするとき:

(i) $a \equiv a \pmod{m}$.

(ii) $a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$.

(iii) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m}$ ならば $a \equiv c \pmod{m}$.

(iv) $a \equiv a' \pmod{m}$ かつ $b \equiv b' \pmod{m}$ ならば $a + b \equiv a' + b' \pmod{m}$.

(v) $a \equiv a' \pmod{m}$ かつ $b \equiv b' \pmod{m}$ ならば $ab \equiv a'b' \pmod{m}$.

練習問題 1.5 上の補助定理を証明せよ.

以上のことを用いると, "3^{127} を 11021 で割ったときの余り" は次のように計算できる:

例 1.6 (井深君の計算) 127 の二進展開 $127 = 1 + 2 + 4 + 8 + 16 + 32 + 64$ より,

$$
\begin{aligned}
3^1 &= 3, & 3^1 &= 3;\\
3^2 &= 3^2 = 9, & 3^3 &= 3 \cdot 9 = 27;\\
3^4 &= 9^2 = 81, & 3^7 &= 27 \cdot 81 = 2187;\\
3^8 &= 81^2 = 6561, & 3^{15} &= 2187 \cdot 6561 = 14348907 \equiv 10586;\\
3^{16} &= 6561^2 = 43046721 \equiv 9716, & 3^{31} &\equiv 10586 \cdot 9716 = 102853576 \equiv 5604;\\
3^{32} &\equiv 9716^2 = 94400656 \equiv 5791, & 3^{63} &\equiv 5604 \cdot 5791 = 32452764 \equiv 6940;\\
3^{64} &\equiv 5791^2 = 33535681 \equiv 9799, & 3^{127} &\equiv 6940 \cdot 9799 = 68005060 \equiv 5490.
\end{aligned}
$$

ただし, ここでは $\equiv$ は 11021 を法とする合同を表すものとする.

練習問題 1.7 正の整数 a の一(いち)の位を a_0, 十(じゅう)の位を a_1, 百の位を a_2, 千の位を a_3, ... とするとき, 次が成り立つことを示せ:

(i) $a \equiv a_0 + a_1 + a_2 + a_3 + \cdots \pmod 9$.

(ii) $a \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pmod{11}$.

§2 ユークリッドの互除法

2 つの整数 a, b (0 や負の整数でも可) に対し, a と b の両方を割り切る整数を a と b の**公約数**という. また, a と b の正の公約数のうちで最も大きいものを a と b の**最大公約数**といい $\mathrm{GCM}(a, b)$ で表す (GCM ではなく GCD と書いたり, あるいは小文字で書くこともある). ただし, a, b が共に 0 の場合には, それらの最大公約数は 0 と定めておく. $\mathrm{GCM}(a, b) = 1$ であるとき, a と b は**互いに素** (または単に**素**) であるという.

通常, 正の整数 a, b の最大公約数を求めるためには次のような計算を行う:

$(\mathbf{A_0})$ a, b の (1 より大きい) 公約数を探す;

$(\mathbf{B_0})$ 公約数 d_0 (> 1) が見つかったら, $a_1 = a/d_0,\ b_1 = b/d_0$ と置く;

$(\mathbf{A_1})$ a_1, b_1 の (1 より大きい) 公約数を探す;

$(\mathbf{B_1})$ 公約数 d_1 (> 1) が見つかったら, $a_2 = a_1/d_1,\ b_2 = b_1/d_1$ と置く;

.....;

$(\mathbf{A_n})$ a_n, b_n の (1 より大きい) 公約数を探す;

$(\mathbf{B_n})$* 1 より大きい公約数が見つからなければ, $\mathrm{GCM}(a, b) = d_0 d_1 \cdots d_{n-1}$.

例 2.1 $a = 336,\ b = 180$ の場合.

$$\begin{array}{lll} d_0 = 2 &) \quad a = 336 & b = 180 \\ d_1 = 2 &) \quad a_1 = 168 & b_1 = 90 \\ d_2 = 3 &) \quad a_2 = 84 & b_2 = 45 \\ & \quad a_3 = 28 & b_3 = 15 \end{array}$$

より,

$$\mathrm{GCM}(336, 180) = 2 \cdot 2 \cdot 3 = 12.$$

上で述べた最大公約数の計算方法は万能のように見えるが, 実はそうではない. 実際, a や b が非常に大きな数の場合には, それらの公約数を探すことは難しく (一方の数の約数を見つけるだけでも大変!), また "1 以外の公約数は存在しない" と判断するのは容易ではない. しかし, 次の補助定理を用いると, 整数 a, b の約数を直接求めることなしにそれらの最大公約数を計算することができる:

補助定理 2.2 a を整数, b を正の整数とするとき, $a \equiv a' \pmod{b}$ であるような整数 a' に対し, a と b の最大公約数は a' と b の最大公約数に一致する:

$$\mathrm{GCM}(a, b) = \mathrm{GCM}(a', b).$$

[証明] 整数 a' が $a \equiv a' \pmod{b}$ をみたすとすると, $a' = a + kb$ となるような整数 k が取れる. いま, $d = \mathrm{GCM}(a, b),\ d' = \mathrm{GCM}(a', b)$ と置く. このとき, d は a と b の公約数であるから, $a' = a + kb$ と b の公約数でもある. また, $d > 0$. ところで, d' は a' と b の正の公約数のうち最大のものであったから, $d \leqq d'$ でなければならない. 一方, d' は a' と b の公約数であるから, $a = a' - kb$ と b の正の公約数でもある. よって, 上と同様の議論により $d' \leqq d$ となることがわかる. 以上より $d = d'$, すなわち $\mathrm{GCM}(a, b) = \mathrm{GCM}(a', b)$. (証明終わり)

いま, a を整数, b を正の整数とし, 次のような操作を行う:

($\mathbf{E_0}$) q_0, r_1 をそれぞれ a の b による商, 余りとする:

$$a = q_0 b + r_1, \qquad 0 \leqq r_1 < b;$$

($\mathbf{E_1}$) $r_1 \neq 0$ のときには, q_1, r_2 をそれぞれ b の r_1 による商, 余りとする:

$$b = q_1 r_1 + r_2, \qquad 0 \leqq r_2 < r_1;$$

($\mathbf{E_2}$) $r_2 \neq 0$ のときには, q_2, r_3 をそれぞれ r_1 の r_2 による商, 余りとする:

$$r_1 = q_2 r_2 + r_3, \qquad 0 \leqq r_3 < r_2;$$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots;$

($\mathbf{E}_{\boldsymbol{n}}$) $r_n \neq 0$ のときには, q_n, r_{n+1} をそれぞれ r_{n-1} の r_n による商, 余りとする:

$$r_{n-1} = q_n r_n + r_{n+1}, \qquad 0 \leqq r_{n+1} < r_n;$$

($\mathbf{E}_{\boldsymbol{n+1}}$)* $r_{n+1} = 0$ となったら操作は終了.

このとき

$$b > r_1 > r_2 > r_3 > \cdots \geqq 0$$

であるから上の操作は必ず終了する. また,

$$a \equiv r_1 \pmod{b}, \quad b \equiv r_2 \pmod{r_1}, \quad r_1 \equiv r_3 \pmod{r_2}, \quad \ldots, \quad r_{n-1} \equiv 0 \pmod{r_n}$$

であるから, 補助定理 2.2 を繰り返し用いることにより

$$\begin{aligned} \mathrm{GCM}(a,b) &= \mathrm{GCM}(b,r_1) = \mathrm{GCM}(r_1,r_2) = \mathrm{GCM}(r_2,r_3) \\ &= \cdots = \mathrm{GCM}(r_{n-1},r_n) = \mathrm{GCM}(r_n,r_{n+1}) = \mathrm{GCM}(r_n,0) = r_n \end{aligned}$$

となることがわかる. このようにして最大公約数を求める方法を**ユークリッドの互除法**という.

注意 2.3 (i) 上の議論では b は正としているが, b が負の場合には $-b$ (これは正) を改めて b と思って同じ計算を行えばよい (一般に $\mathrm{GCM}(a,-b) = \mathrm{GCM}(a,b)$ が成り立つことに注意). なお, $b = 0$ の場合には, 明らかに $\mathrm{GCM}(a,b) = |a|$.

(ii) 上の計算

$$\begin{aligned} a &= q_0 b + r_1, \\ b &= q_1 r_1 + r_2, \\ r_1 &= q_2 r_2 + r_3, \\ &\cdots\cdots\cdots\cdots\cdots\cdots , \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

を (最下行は無視して) 下から順に変形して行くことにより,

$$ka + lb = \mathrm{GCM}(a,b) \ (= r_n)$$

となるような整数 k, l が構成できることがわかる.

例 2.4 $a = 336,\ b = 180$ の場合.

$$\begin{aligned} 336 &= 1 \cdot 180 + 156, \\ 180 &= 1 \cdot 156 + 24, \\ 156 &= 6 \cdot 24 + 12, \\ 24 &= 2 \cdot 12 + 0 \end{aligned}$$

より,

$$\mathrm{GCM}(336, 180) = 12.$$

このときには, $ka + lb = \mathrm{GCM}(a, b)$ となるような整数 k, l は次のように計算される:

$$\begin{aligned} 12 &= 156 - 6 \cdot 24 = 1 \cdot 156 + (-6) \cdot 24 \\ &= 1 \cdot 156 + (-6) \cdot (180 - 1 \cdot 156) = (-6) \cdot 180 + 7 \cdot 156 \\ &= (-6) \cdot 180 + 7 \cdot (336 - 1 \cdot 180) = 7 \cdot 336 + (-13) \cdot 180. \end{aligned}$$

練習問題 2.5 $2^{32} + 1$ と $2^{16} + 1$ は互いに素であることを示せ.

§3 互除法の応用

a, b を互いに素な整数とするとき, 注意 2.3 で述べたように, ユークリッドの互除法を用いて

$$ka + lb = 1$$

となるような整数 k, l を具体的に構成することができる. 本節では, この事実の応用をいくつか述べる.

3.1 m を法とする逆数

正の整数 m と整数 a, b に対し, $ab \equiv 1 \pmod{m}$ が成り立つとき a と b は m を法として**逆数**であるという.

定理 3.1 m を正の整数とするとき, 整数 a に対し, a の m を法とする逆数が存在するためには a と m が互いに素であることが必要かつ十分.

[証明] まず, a の m を法とする逆数 b が存在したとすると, $ab - 1 = km$ となるような整数 k が取れる. このとき, a と m の公約数は $ab - km = 1$ を割り切るから ± 1 に限られる. 従って $\mathrm{GCM}(a, m) = 1$ でなければならない.

逆に, $\mathrm{GCM}(a, m) = 1$ だとすると, $ka + lm = 1$ となるような整数 k, l が取れる. このとき $ka \equiv 1 \pmod{m}$ となるから k は a の m を法とする逆数である. (証明終わり)

注意 3.2 上の証明からわかるように, m と素であるような a に対し, a の m を法とする逆数 (のひとつ) はユークリッドの互除法を用いて具体的に求めることができる.

3.2　素数の特徴付け

2 以上の整数で, 1 と自分自身以外に正の約数をもたないものを**素数**といい, そうでないものを**合成数**という. 例えば, 10 以下の整数の中では, 素数は $2, 3, 5, 7$ の 4 個で, 合成数は $4 = 2^2$, $6 = 2 \cdot 3$, $8 = 2^3$, $9 = 3^2$, $10 = 2 \cdot 5$ の 5 個である (1 は素数とも合成数とも呼ばない).

いま, p を素数とするとき, 任意の整数 a に対して $\mathrm{GCM}(a, p)$ は (p の約数であるから) 1 または p になる. より正確には, a が p で割り切れるとき $\mathrm{GCM}(a, p) = p$ であって, そうでないときには $\mathrm{GCM}(a, p) = 1$ になる. このことと本節の冒頭に述べた事実を用いると, 次が示せる:

定理 3.3 p を素数とするとき, 2 つの整数 a, b の積が p で割り切れるならば, a または b の少なくとも一方は p で割り切れる.

[証明] p が a を割り切らないとすると, 上で述べたように $\mathrm{GCM}(a, p) = 1$ であるから, $ka + lp = 1$ となるような整数 k, l が取れる. このとき

$$b = 1 \cdot b = (ka + lp)b = k(ab) + (lb)p$$

となるから, ab が p で割り切れるならば b も割り切れなければならない. (証明終わり)

3.3　互いに素な数の倍数

次の事実も定理 3.3 の証明と同様にして示すことができる:

定理 3.4 a, b を互いに素な整数とするとき, 整数 c が a でも b でも割り切れるならば, c は ab で割り切れる.

練習問題 3.5 上の定理を証明せよ.

§4　フェルマーの小定理

本節では, 整数の累乗に関するいくつかの合同式を素数の性質を用いて証明する. その出発点となるのは次の事実である (二項係数の定義や基本的な性質については付録 A を参照のこと):

補助定理 4.1 p を素数とするとき:

(i) $1 \leqq k \leqq p - 1$ であるような整数 k に対し, ${}_p\mathrm{C}_k \equiv 0 \pmod{p}$.

(ii) 任意の整数 a, b に対し, $(a + b)^p \equiv a^p + b^p \pmod{p}$.

練習問題 4.2 上の補助定理を証明せよ.

上の補助定理を用いると次が示せる:

定理 4.3 p を素数とするとき, 任意の整数 a に対し,

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

[証明] まず, $a = 0, 1$ に対しては明らか. 次に, 補助定理の (ii) より,

$$2^p = (1+1)^p \equiv 1^p + 1^p \equiv 1 + 1 \equiv 2 \pmod{p}.$$

再び補助定理の (ii) と既に証明した $2^p \equiv 2 \pmod{p}$ より,

$$3^p = (2+1)^p \equiv 2^p + 1^p \equiv 2 + 1 \equiv 3 \pmod{p}.$$

以下同様の計算を繰り返すことにより, 0 以上の任意の整数 a に対して $a^p \equiv a \pmod{p}$ が成り立つことがわかる.

他方, 負の整数 a に対しては, 0 以上の整数 b で $a \equiv b \pmod{p}$ をみたすものを取れば, 既に証明した $b^p \equiv b \pmod{p}$ より

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

がわかる. (証明終わり)

さて, 定理 4.3 の主張は "$a\,(a^{p-1} - 1)$ は p で割り切れる" と書き直すことができる. ここで a が p と素であると仮定すると, 定理 3.3 より, $a^{p-1} - 1$ が p で割り切れなければならないことになる. すなわち:

定理 4.4 (フェルマーの小定理) p を素数とするとき, p と素であるような任意の整数 a に対し,

$$a^{p-1} \equiv 1 \pmod{p}.$$

注意 4.5 上の合同式は $a \cdot a^{p-2} \equiv 1 \pmod{p}$ とも書ける. これより, p と素であるような整数 a に対して a^{p-2} は a の p を法とする逆数を与えることがわかる.

最後に, フェルマーの小定理を用いると次が示せる:

定理 4.6 p, q を相異なる素数とし, $N = pq$, $M = (p-1)(q-1)$ と置く. また, f を $f \equiv 1 \pmod{M}$ であるような正の整数とする. このとき, 任意の整数 a に対し,

$$a^f \equiv a \pmod{N}.$$

[証明] $f \equiv 1 \pmod{M}$ より, $f = 1 + k(p-1)(q-1)$ となるような整数 k が取れる. ここで, $f > 0$ より $k \geqq 0$ である. いま, a が p と素であるとすると, フェルマーの小定理より,

$$a^f = a^{1+k(p-1)(q-1)} = a\,(a^{p-1})^{k(q-1)} \equiv a \cdot 1 \equiv a \pmod{p}.$$

a が p と素でない場合には明らかに

$$a^f \equiv a \equiv 0 \pmod{p}$$

となるから, いずれにしても $a^f \equiv a \pmod{p}$ が成り立つ. 同様にして $a^f \equiv a \pmod{q}$ が成り立つこともわかるから, 定理 3.4 より, $a^f \equiv a \pmod{pq}$ となる. (証明終わり)

§5 RSA 暗号系

ここで言う**暗号**とは, メッセージの外見を変えることにより正当な受信者にしか読めないようにする方法のことである. かつては軍事目的にしか使われなかった暗号も, 今日のネットワーク社会においては多くの人にとって欠かせないものとなった. 本節では, 公開鍵暗号の代表である RSA 暗号系を紹介する.

まず, 公開鍵暗号とは何かを理解するために, 次のような状況を考えてみる:

* * *

インターネットにハマっている小幡君は, “有栖川書房” という本屋のホームページで探し求めていたコミックが売られているのを発見し, それを購入することにした. 料金の支払いにはクレジットカードが使える. 住所・氏名の他にカードの番号と有効期限を入力すれば, あとは送られて来るのを待つだけである. いったんクレジットカードの番号を入力しようとした小幡君だが, ふと手を止め, 次のように考えた:

“この番号が関係ない人に読まれて悪用されたら困るなあ.”
“他人には読めないように細工したいなあ.”
“でも, 細工するには, まず有栖川書房にメールしなくちゃなあ.”
“そのメールも人に読まれちゃったら意味ないなあ.”

小幡君の考えは堂々巡りになってしまった. さらに小幡君は考える:

“そうだ. 有栖川書房が細工の仕方を指定しておけばいいんだ!”
“細工の仕方はホームページに載せておいてもらえばいいしね.”
“でも, それだと誰でも読めるから意味ないか.”

小幡君が思い描くような “暗号化する手順は公開しているにも関わらず, 手順を指定した本人 (上の例では有栖川書房) にしか解読できないような暗号” というものは可能なのだろうか?

* * *

1977 年, リヴェスト (R. L. Rivest), シャミア (A. Shamir), エイドルマン (L. Adleman) の 3 人は, 上で述べたような暗号 (**公開鍵暗号**という) を現実のものにすることに成功した (論文が出版されたのは 1978 年). 3 人のイニシャルを取って, この暗号は **RSA 暗号系**と呼ばれる. 以下, その仕組みを解説する. なお, 話を簡単にするため, 暗号化したいメッセージは j 桁の正の整数であるものとする (実際には, メッセージを適当な方法で整数に変換してから通信を行う).

5.1 RSA 暗号系の仕組み

(a) 受け手の下準備 I メッセージの受け手は, まず相異なる素数 p, q を用意し, $N = pq$ と $M = (p-1)(q-1)$ を計算しておく. p と q は $N \geqq 10^j$ となるように十分大きく取っておく.

(b) 受け手の下準備 II 続いて, 受け手は M と素であるような正の整数 e をひとつ取り, $de \equiv 1 \pmod{M}$ となるような正の整数 d をひとつ求めておく. このような d の存在は定理 3.1 が保証し, 整数 e が M と素であることの確認や d の具体的な計算にはユークリッドの互除法が用いられる.

(c) 暗号化鍵の公開 以上の準備が整ったら, 受け手は N と e を誰もが読める場所に公開する. 公開された (N, e) を**公開鍵**という. なお, 受け手は p, q, M や d を決して他人に知られてはならない.

(d) 送り手による暗号化 送り手は, メッセージ a を N を法として e 乗することにより暗号化されたメッセージを作る. つまり, 送り手は a^e の N による余り b を計算するのだが, 例 1.6 のように e の二進展開を利用すれば, この計算は難しくない. そして, 暗号化されたメッセージ b を受け手に発送する.

(e) 受け手による復号化 暗号化されたメッセージ b を受け取った受け手は b^d の N による余り c を計算する. 既に述べたように, この計算は難しくない. すると

$$c \equiv b^d \equiv (a^e)^d \equiv a^{de} \pmod{N}$$

となるが, 整数 d は $de \equiv 1 \pmod{M}$ となるように取ってあったから, 定理 4.6 より $a^{de} \equiv a \pmod{N}$ となり, 結局 $c \equiv a \pmod{N}$ となる. ここで, $0 < a < 10^j \leqq N$ と $0 \leqq c < N$ に注意すると, $c = a$ であることがわかる. これで元々のメッセージ a が復元できたことになる.

例 5.1 (有島先生と馬場さんの計算 I) (a) 有島先生は, 2 つの素数として $p = 103$ と $q = 107$ を選んだ. このとき, $N = pq = 11021,\ M = (p-1)(q-1) = 10812$.

(b) 有島先生は $M = 10812$ と素な正の整数として $e = 127$ を選んだ. このとき

$$10812 = 85 \cdot 127 + 17,$$
$$127 = 7 \cdot 17 + 8,$$
$$17 = 2 \cdot 8 + 1,$$
$$8 = 8 \cdot 1 + 0$$

より, 確かに $\mathrm{GCM}(10812, 127) = 1$ となっている. また, 上の計算より

$$15 \cdot 10812 - 1277 \cdot 127 = 1$$

となることがわかるから, $d = 10812 - 1277 = 9535$ と置けば,

$$de = 9535 \cdot 127 \equiv (-1277) \cdot 127 \equiv 1 \pmod{10812}.$$

(c) 有島先生は掲示板にメモを貼る.

(d) メモを見た馬場さんは, 暗証番号 $a = 1192$ を $N = 11021$ を法として $e = 127$ 乗する. 例 1.6 と同様の計算をして得られた数 $b = 3733$ を掲示板のメモに書き込む (図 1).

(e) 馬場さんが書き込んだ数 $b = 3733$ を見た有島先生は, それを $N = 11021$ を法として $d = 9535$ 乗する. 今度は d の二進展開

$$9535 = 1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^8 + 2^{10} + 2^{13}$$

を使って例 1.6 と同様の計算をすると, $3733^{9535} \equiv 1192 \pmod{11021}$ が得られる. これで暗証番号 $a = 1192$ が復元できた.

例 5.2 (有島先生と馬場さんの計算 II) (a) 有島先生は, 2 つの素数として $p = 101364911$ と $q = 103465819$ を選んだ. このとき,

$$N = pq = 10487803534477109, \qquad M = (p-1)(q-1) = 10487803329646380.$$

(以下略.)

練習問題 5.3 電卓を使って, 例 5.1 の計算を確認せよ. また, コンピュータを使って巨大な整数の計算ができる人は, 暗号を解読して例 5.2 を完成させよ.

5.2 RSA 暗号系の安全性

いま, メッセージの正当な受信者ではない者が暗号化されたメッセージ b を手に入れたとする. このとき, 公開鍵 (N, e) と b から元々のメッセージ a を解読されてしまう恐れはないだろうか?

もちろん, $n = 1, 2, \ldots, 10^j - 1$ に対して n^e の N による余りを順に計算していけば, いつかは余りとして b が現れるはずであるから, そのときの n として a を知ることができる. しかし, メッセージの桁数 j が非常に大きい場合には, この方法は時間がかかり過ぎて事実上使い物にならない. 秘密にされている数 d を知らなければ b から a を求めることは実質上不可能なのである. N による余りを取っていない a^e から a の大体の値を求めることは対数関数を使えばすぐにできるのだが, 余りを取ったことによって a がどのくらいの大きさの数なのかは隠蔽されてしまう.

では, 公開鍵 (N, e) から d を求めることはできないだろうか? メッセージの受け手が d を簡単に計算できたのは M という数を知っていたからである. ところが, 受け手以外の人にとっては $N = pq$ から $M = (p-1)(q-1)$ を求めるのは容易ではない. 秘密にされている M や d を短時間で求めることができるのは, N という数の "素性" を知っている受け手だけなのである.

実は, N と e から d を求めることは N から p と q を求めること, すなわち N を素因数分解することと同程度に難しいということが知られている. 一般に, 2 つの素数 p, q から積 $N = pq$ を計算することと, 逆に N から p と q を求めることとでは, 後者の方が桁違いに手間がかかる. RSA 暗号系の安全性は, この "巨大な整数の素因数分解の難しさ" により支えられているのである.

付録 A　二項係数について

正の整数 n に対し, 1 から n までの整数を全て掛け合わせてできる数を n の**階乗**といい, $n!$ で表す:

$$n! = n(n-1)\cdots 2 \cdot 1.$$

また, 便宜上 0 の階乗 0! は 1 と定めておく.

条件 $0 \leqq k \leqq n$ をみたす整数 k, n に対し, "n 個のものから k 個のものを取り出す取り出し方 (組み合わせ) の数" を ${}_n\mathrm{C}_k$ で表す. これは階乗を使って

$${}_n\mathrm{C}_k = \frac{n!}{k!(n-k)!}$$

と表せる. この式の右辺は分数の形をしているが, きちんと約分されて整数になることに注意せよ.

さて, $x + y$ のように 2 つの項からなる式を二項式というが, その n 乗を展開したときの係数として ${}_n\mathrm{C}_k$ が現れる:

$$(x+y)^n = x^n + nx^{n-1}y + \cdots + {}_n\mathrm{C}_k\, x^{n-k}y^k + \cdots + nxy^{n-1} + y^n.$$

この公式を**二項定理**という. また, 組み合わせの数 ${}_n\mathrm{C}_k$ のことを**二項係数**とも呼ぶ.

例 A.1 (i) $n = 1$ の場合.

$${}_1\mathrm{C}_0 = 1, \quad {}_1\mathrm{C}_1 = 1; \qquad (x+y)^1 = x + y.$$

(ii) $n = 2$ の場合.

$$ {}_2\mathrm{C}_0 = 1, \quad {}_2\mathrm{C}_1 = 2, \quad {}_2\mathrm{C}_2 = 1; \qquad (x+y)^2 = x^2 + 2xy + y^2. $$

(iii) $n = 3$ の場合.

$$ {}_3\mathrm{C}_0 = 1, \quad {}_3\mathrm{C}_1 = 3, \quad {}_3\mathrm{C}_2 = 3, \quad {}_3\mathrm{C}_3 = 1; \qquad (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3. $$

(iv) $n = 4$ の場合.

$$ {}_4\mathrm{C}_0 = 1, \quad {}_4\mathrm{C}_1 = 4, \quad {}_4\mathrm{C}_2 = 6, \quad {}_4\mathrm{C}_3 = 4, \quad {}_4\mathrm{C}_4 = 1; $$
$$ (x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4. $$

(v) $n = 5$ の場合.

$$ {}_5\mathrm{C}_0 = 1, \quad {}_5\mathrm{C}_1 = 5, \quad {}_5\mathrm{C}_2 = 10, \quad {}_5\mathrm{C}_3 = 10, \quad {}_5\mathrm{C}_4 = 5, \quad {}_5\mathrm{C}_5 = 1; $$
$$ (x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5. $$

付録 B　積み残しの問題

本稿では触れられなかった話題について簡単に述べておく. これらの話題については, 付録 C で挙げている文献の中に詳しい説明がある.

B.1　計算量

本当ならば, どのような計算には長い時間がかかってどのような計算は素早くできるのかといった “計算に要する時間の見積もり” をきちんと考えなければならない. また, 巨大な数の加法や乗法を高速に計算するための方法も考える必要がある.

B.2　電子署名

冒頭に述べた掲示板のメモの話において, 有島先生は 3733 という数を馬場さん本人が書き込んだということをどうやったら確認できるだろうか？ この場合には, かろうじて数字の筆跡を鑑定すれば本人と確認できるかもしれない. では, 筆跡が残らない電子メールにおいて差出人の確認をするためにはどうすればいいだろうか？ 実は, RSA 暗号系と同様の方法によって, 上で述べたような本人の確認 (**電子署名**という) が実現できることがわかっている. ちなみに, RSA 暗号系が発表された論文のタイトルは “A method for obtaining digital signatures and public-key cryptosystems” (直訳すると “ディジタル署名と公開鍵暗号系を得るための一方法”) である.

B.3　素数判定法

RSA 暗号系を使うためには, まず大きな素数を用意しなければならない. 従って, (巨大な) 整数 n が素数か否かを判定する方法が必要になる. もちろん, n を $m = 2, 3, \ldots$ で順に割って行けば, 途中で割り切れたら合成数, 割り切れないまま m が $\sqrt{n}$ を越えたら素数と判定できる. しかし, 巨大な n に対しては, この素朴な方法は時間がかかり過ぎて全く役に立たない.

ところで, n が合成数だと判定するためには (1 と n 以外の) 約数をひとつ見つければ十分なのであるが, 約数を求めることなしに合成数だと判定する方法もある:

定理 B.1 n を 2 以上の整数とするとき, $0 < a < n$ であるようなある整数 a に対して

$$a^{n-1} \equiv 1 \pmod{n}$$

が成立しないならば n は素数ではない.

[証明] 仮に n が素数であるとすると, $0 < a < n$ であるような任意の整数 a は n と素であるから, フェルマーの小定理 (定理 4.4) より

$$a^{n-1} \equiv 1 \pmod{n}$$

とならなければならない. これは仮定に反する. (証明終わり)

与えられた n に対し, $0 < a < n$ であるような整数 a をひとつ取り, $a^{n-1} \equiv 1 \pmod{n}$ が成立するか否かを見て n が合成数かどうかを調べることを a を底(てい)とするフェルマーテストという. なお, ひとつの底に対するフェルマーテストをパスしたからといって素数であるとは限らない. 実際, $341 = 11 \cdot 31$ は合成数であるが, 2 を底とするフェルマーテストはパスしてしまう. すなわち, $2^{340} \equiv 1 \pmod{341}$ が成り立つ.

さて, フェルマーテストは素数でないことの判定にしか使えないとはいうものの, ランダムに選ばれた巨大な整数の中から素数らしい数を絞り込むためには極めて有効である. いくつかの底に対するフェルマーテストをパスした整数に対して本格的な素数判定法 (その詳細はここでは述べられない) を適用することにより, 巨大な素数は容易に手に入れることができる.

B.4　素因数分解の方法

整数を素因数分解するためには, 約数を探すことと素数判定の 2 つができればよい. 後者については上で述べた. 前者の “与えられた整数の約数を見つける” 方法は現在でも盛んに研究されている. 特別な形をした整数の約数を見つける方法は多数発見されているが, いまだに決定的と呼べる方法は確立されていない. 現在は “与えられた整数 n と公約数をもちそうな数を効率よく

作る方法” が主に研究されている. そのような数 k を次々に作ってユークリッドの互除法により $\mathrm{GCM}(n,k)$ を計算すると, 運がよければ $\mathrm{GCM}(n,k) \neq 1, n$ となって n の約数が得られるという寸法である.

B.5　素数は沢山あるのか

RSA 暗号系が多くの人に対して有効に機能するためには, (例えば 100 桁の) 素数が沢山なければならない. つまり, “素数の個数” についても検討する必要がある. これは**素数分布の問題**と呼ばれる整数論の主要な問題のひとつである. ここでは述べないが, **素数定理**というものがあって, 素数は十分に沢山あることが既に証明されている.

付録 C　文献案内

本稿で扱った話題に関連する文献をいくつか紹介しておく (筆者が参考にした文献を全て挙げている訳ではない).

C.1　初等整数論について

[1-1] S. C. Coutinho (林彬 訳), 暗号の数学的基礎 数論と RSA 暗号入門, 丸善出版, 2012 年.

本稿とほぼ同じ主題で書かれた RSA 暗号系への入門書. 整数論への入門書としても読める.

[1-2] 中島匠一, 代数と数論の基礎, 共立講座 21 世紀の数学 9, 共立出版, 2000 年.

初等整数論と抽象代数学への入門書. 非常に丁寧で読み易い.

[1-3] P. Ribenboim (吾郷孝視 訳編), 素数の世界 その探索と発見 (第 2 版), 共立出版, 2001 年.

素数に関する色々な話題に詳しい.

[1-4] J. H. Silverman (鈴木治郎 訳), はじめての数論 原著第 3 版, 丸善出版, 2014 年.

整数論への入門書. 少ない予備知識で楽しく読める.

C.2　暗号について

[2-1] M. Gardner (一松信 訳), ガードナー数学ギャラリー 落し戸暗号の謎解き, 丸善出版, 1992 年.

著者が Scientific American 誌上に連載したコラム “数学ゲーム” の選集のひとつ. 第 6 章 “落し戸暗号” (1977 年 8 月号に掲載) は RSA 暗号系を初めて紹介した文章として名高い. また, 第 7 章 “落し戸暗号その後” は後日談に詳しい.

[2-2] S. Levy (斉藤隆央 訳), 暗号化 プライバシーを救った反乱者たち, 紀伊國屋書店, 2002 年.

公開鍵暗号の誕生や普及に至るまでの歴史に詳しい.

[2-3] 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 年.
暗号理論とそれを支える数学の事情に詳しい.

[2-4] S. Singh (青木薫 訳), 暗号解読 上・下, 新潮文庫, 新潮社, 2007 年.
非専門家向けに書かれた暗号史の本. 公開鍵暗号に関する親切な解説もある.

[2-5] 結城浩, 暗号技術入門 秘密の国のアリス (第 3 版), SB クリエイティブ, 2015 年.
情報の安全性を守るための技術についてバランス良く解説されている.