中校生のための数学教室　　東京大学
「素数と暗号」　　玉原国際セミナーハウス
講義（2）　大島　利雄　　2007 年 10 月 6 日

「素数と暗号」

１．エラトステネスの篩い（ふるい）

エラトステネス（BC 275 – BC 194）は地球の大きさを測ったギリシャの天文学者

例. 100 以下の素数の表を作るには
1 から 100 までを順に書いて，1 を消す.
2 を残して 2 の倍数を消す.　3 を残して 3 の倍数を消す.
5 を残して 5 の倍数を消す.　7 を残して 7 の倍数を消す.
残ったものが 100 以下の素数

● 素数はだんだん減ってくる.
n 桁の素数は，n が十分に大きいと，$2.3\times n$ 個に 1 個程度.
すなわち，50 桁の素数は，115 個の中に 1 個程度しかない.

２．ユークリッドの互除法

２つの自然数の最大公約数を求めることを考えてみよう.
●２つの数の素因数分解が分かれば，最大公約数は簡単にわかる.
●大きな数の素因数分解は難しい！

ユークリッド（BC 330? – BC 275）はギリシャの数学者.
「**自然数 m と n の最大公約数は，m を n で割った余りと n の最大公約数に等しい**」という原理を繰り返し使って，最大公約数をもとめる方法.

$$\begin{aligned}
\mathbf{336} &= \mathbf{180}\cdot 1 + 156 \\
\mathbf{180} &= \mathbf{156}\cdot 1 + \ 24 \\
\mathbf{156} &= \ \mathbf{24}\cdot 6 + \ 12 \\
\mathbf{24} &= \ \mathbf{12}\cdot 2
\end{aligned}
\qquad
\begin{aligned}
\mathbf{13} &= \mathbf{5}\cdot 2 + 3 \\
\mathbf{5} &= \mathbf{3}\cdot 1 + 2 \\
\mathbf{3} &= \mathbf{2}\cdot 1 + 1 \\
\mathbf{2} &= \mathbf{1}\cdot 2
\end{aligned}
\qquad
\begin{aligned}
\mathbf{28829} &= \mathbf{14351}\cdot \ 2 \ + 127 \\
\mathbf{14351} &= \ \ \mathbf{127}\cdot 113
\end{aligned}$$

● n 桁以下の 2 つの自然数の最大公約数を求めるには，$5n$ 回以下の割算で済む（計算量が少なくてすむ）.

● **m と n が互いに素なときに $mx+ny=1$ を解く** (x, y は整数)

例. $m=13$, $n=5$ のとき：　$13x+5y=1$

$$\begin{aligned}
1 &= 3-2\cdot 1 \\
&= 3-(5-3\cdot 1)\cdot 1 = 5\cdot(-1)+3\cdot 2 \\
&= 5\cdot(-1)+(13-5\cdot 2)\cdot 2 = 13\cdot 2+5\cdot(-5)
\end{aligned}$$

３．余りの計算

● 自然数を沢山掛けたとき，答えが奇数か偶数かは，積を実際に計算しなくても分かる（奇数を掛ける個数の偶奇による）.
これを 2 で割った余り以外でも考えてみよう.

a を p で割った余りと b を p で割った余りが等しいとき（すなわち $a-b$ が p の整数倍のとき），$a \equiv b \pmod{p}$ と表そう．

$$4 \equiv 1 \pmod{3} \qquad 4 \cdot 4 \equiv 1 \pmod{3} \qquad 4^{100} \equiv 1 \pmod{3}$$
$$5 \equiv 2 \pmod{3} \qquad 5^2 \equiv 1 \pmod{3} \qquad 5^{99} = 5^2 \cdots 5^2 \cdot 5 \equiv 2 \pmod{3}$$
$$4 \cdot 5 \equiv 1 \cdot 2 \equiv 2 \pmod{3}$$

● 余りのみに注目した計算は計算量が少ない！

５．素数の性質

自然数 p が素数かどうかの判定

p が素数のときに成り立つ公式

Wilson の定理. $2 \times 3 \times \cdots \times (p-2) \equiv 1 \pmod{p}$

Fermat の小定理. $a^{p-1} \equiv 1 \pmod{p} \qquad (a = 1, 2, \ldots, p-1)$

証明. [1] $a, 2a, \ldots, (p-1)a$ の $p-1$ 個の整数を p で割った余りは全て異なるので，並び替えると $1, \ldots, p-1$ となる．

[2] a に対して $a' \cdot a \equiv 1 \pmod{p}$ となる p 未満の正整数 a' がある．これを a の相棒と呼ぼう．

[3] $1 \times 2 \times \cdots \times (p-1) \times a^{p-1} = a \times 2a \times \cdots \times (p-1)a \equiv 1 \times 2 \times \cdots \times (p-1) \pmod{p}$

[4] $1 \times 2 \times \cdots \times (p-1)$ を p で割った余りの相棒を [3] の式に掛けると，Fermat の小定理が得られる．

● Wilson の定理は，2 以上 $p-2$ 以下の整数の相棒は元の整数と異なることから示される（$m^2 \equiv 1 \pmod{p}$ ならば $(m-1)(m+1) \equiv 0 \pmod{p}$）．

フェルマーテスト．与えられた p に対し，いくつかの a で Fermat の小定理が成り立つかどうかテストする．

● $a = 2, 3, 5, 7$ に対してフェルマーテストをパスしてしまう 2.5×10^{10} 以下の素数でない数は $3215031751 = 151 \cdot 751 \cdot 28351$ のみ．

６．RSA 暗号

RSA 暗号は，最初に発見された公開鍵暗号で，最もよく使われている．

●暗号の方法は公開される．それを用いて文章を暗号化したものが漏れても，復元できるのは公開元のみ．

大きな２つの素数の積が与えられても，それを２つの素数に分解するのが困難な（実際上不可能な）ことに基づいている（２つの素数は公開元のみが知っている）．

[1] 異なる素数 p, q を選び，$n = pq$ と $r = (p-1)(q-1)$ を計算する．
[2] r と互いに素な整数 e を選ぶ．
[3] $de \equiv 1 \pmod{r}$ となる d を求める（ユークリッドの互除法）．
[4] p, q, d を秘密にして，e, n を公開する．
[5] **暗号化**：n 未満の数 m を暗号化した数は m^e を n で割った余り（x とする）．
[6] **復元**：x^d を n で割った余りが m．

原理：$m^{(p-1)(q-1)} - 1 = (m^{q-1})^{p-1} - 1$ は p で割り切れる．同様に q でも割り切れるので，$n = pq$ で割り切れる．よって $m^r \equiv 1 \pmod{n}$

$de = rk + 1$ となる正整数 k によって

$$x^d \equiv (m^e)^d = m^{de} = m^{rk+1} = (m^r)^k \cdot m \equiv m \pmod{n}$$