高校生のための現代数学講座　　東京大学
「素数の世界」　　玉原国際セミナーハウス
講義 (3)　坪井　俊　　2009 年 7 月 31 日

「暗号による通信の実際」

1　暗号化と復号の手順

ＲＳＡ暗号は、素因数分解には現在のところ時間がかかることを安全性の根拠に使い、一方、素数に関係した数学の定理を用いて、暗号化し復号する方法であり、現在のコンピュータ・ネットワークに非常に多く用いられている。

次の手順を踏む。

- 素数を 2 つ用意し、沼女に保管する。例えば、$p = 13$, $q = 17$ としよう。
- 沼女では $n = pq$ を計算する。$n = pq = 221$ である。

  この n の桁数が十分大きいと、約数を見つけるのに今の計算機の方法では長い時間がかかる。例えば、10000 年以上かかるという桁数の n を作っておく。例えば 100 桁の p, q の積として 10000 桁の n を作っておく。
- 沼女では $(p-1)(q-1)$ と互いに素となる f を適当にとり、合同式

  $$fd = 1 \bmod (p-1)(q-1)$$

  をユークリッドの互除法で解いておき、解 d を保管する。

  桁数が 10000 桁でも、この合同式の計算は短い時間でできる。

  例えば、$f = 7$ として、$7d = 1$ mod192 の解（の一つ）は $d = 55$ である。
- 沼女の掲示板に、「手紙をくれる人は、$n = 221$, $f = 7$ を使ってください」と掲示する。

  実際には、コンピュータ同士が、桁数が 10000 桁の n と、f をやり取りする。
- 沼高では、文章を $n = 221$ よりも小さい数字の列 $a_1, a_2, \ldots, a_k$ に直す。たとえば、「Let's go to Tambara!」は、アスキー・コードにすると

  $$76, 101, 116, 39, 115, 32, 103, 111, 32, 116, 111, 32, 84, 97, 109, 98, 97, 114, 97, 33$$

  となる。

  実際には、あとで述べるように　絶対に!　こうしてはいけない。実際には、数字を並べたものを、10 進法なら 10 桁、20 桁くらいずつに分ける。
- それから

  $$b_1 \equiv (a_1)^f \mod n,\ b_2 \equiv (a_2)^f \mod n,\ \ldots,\ b_k \equiv (a_k)^f \mod n$$

  を計算し、この列 $b_1, b_2, \ldots, b_k$ を沼女に送る。例について、7 乗　mod 221 を計算すると、

  $$15, 101, 142, 78, 106, 59, 103, 19, 59, 142, 19, 59, 33, 7, 216, 123, 7, 75, 7, 84$$

  となる。

- 沼女では、この列 $b_1, b_2, \ldots, b_k$ に対し、保管してあった (n, d) を取り出し、

$$c_1 \equiv (b_1)^d \mod n,\ c_2 \equiv (b_2)^d \mod n,\ \ldots,\ c_k \equiv (b_k)^d \mod n$$

を計算する。例について、55 乗 mod 221 を計算すると

$$76, 101, 116, 39, 115, 32, 103, 111, 32, 116, 111, 32, 84, 97, 109, 98, 97, 114, 97, 33$$

となる。

d 乗 mod n の計算は、後で説明するように d を 2 進展開して、 mod n の d 倍の計算、 mod n の 2 乗の計算を繰り返して効率的におこなう。

- アスキー・コードを文字に直して、「Let's go to Tambara!」と読める。

2 累乗の計算と合同式と２進法

- 7 乗を計算するのは、3 桁の１００前後の数字の７乗は、１５桁でかろうじで電卓上に表せるくらいである。
- 55 乗を計算するのはそのままでは１００桁を超えて無理である。
- しかし、 mod 221 の計算は、常に 3 桁であるので、合同式として計算することに大きなメリットがある。
- ３桁同士の掛け算といっても５５回掛けるのは大変である。
- 55 は 2 進数で 110111 と表わされる。すなわち、

$$55 = 2^5 + 2^4 + 2^2 + 2 + 1 = (((2+1) \times 2^2 + 1) \times 2 + 1) \times 2 + 1$$

である。

- これを使うと、

$$b^{55} = b^{(((2+1)\times 2^2+1)\times 2+1)\times 2+1} = ((((b^2 \cdot b)^2)^2 \cdot b)^2 \cdot b)^2 \cdot b$$

と 9 回の b の掛け算と 2 乗の計算で済むことになる。もちろん、合同式の計算をしている。この 9 は、2 進法の桁数と 1 の個数の和から 2 を引いた数である。つまり、d 乗 mod n の計算は、後で説明するように d を 2 進展開してした桁数の 2 倍の回数の計算である。

3 上の暗号の問題点

ここで説明したのは、暗号の基本原理で、それを良く理解していないと暗号が役に立たないことがすぐに起きる。

- 上の暗号の使い方は、一文字だけを送るときには、原理的に、暗号として使えるものである。だから、工夫して暗号として実用化されている。
- 一方、上の例のように、一文字に対応する数字を暗号化しても、それは、アスキー・コードの数字を別の数字の組に置き換えただけのものになる。そういう暗号は、文章の中の文字の並び方の規則、出現頻度などから、自然に解読されることが多い。
- 実際には、少なくとも一文字ごとに暗号化するようなことは決して行われていない。

4　演習

アスキー・コードは大文字の A が 65 で以後大文字の 26 個のアルファベット、小文字の a が 97 で以後小文字の 26 個のアルファベットが z の 122 まで並んでいる。スペースは 32, ! は 33, コンマは 44, ピリオドは 46 である。

　あるアルファベットで書かれた文を、上の方法で、暗号化して得られた次の文を解読してください。つまり、55 乗　mod 221 を計算して、アスキー・コードを得て、さらにアルファベットに直してください。電卓、携帯電話等はもちろん使ってよいです。

$$155, 7, 142, 26, 101, 216, 7, 142, 79, 57, 106, 59, 79, 106, 59, 119, 195, 202, 84$$