2015.7.15

数値プログラミング: 公開鍵暗号

公開鍵暗号の基礎としての初等整数論

松谷茂樹

ＲＳＡ暗号の理解に向け、初等整数論を紹介する.

素数とは

整数を $\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}=\mathbb{Z}$ と記す.
整数 $\mathbb{Z}$ の特徴は、足し算、引き算と掛け算が可能であることである. 割り算は必ずしも上手く行かない.
足し算、引き算をひっくるめて加法と呼び、掛け算を積演算と呼ぶことにする.
割り算は必ずしも上手くできない場合があるが、例えば $6\div 3=2$ と割り算が上手くゆく場合がある. これを 6 は 3 で**割り切れる**と言い，6 や 3，2, 1 は 6 の**約数**と呼ぶ. -2 や -3 も約数であるので，区別するために 6 や 3 などを**正の約数**と呼ぶ.
素数とは自分自身と 1 以外に正の約数を持たない 1 以外の正の整数である.
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997

剰余類

剰余類とは割り算した後の余りに着目したものである.
具体的な例として 6 の剰余類 $\mathbb{Z}/6\mathbb{Z}$ を考える.
整数 n を 6 で割った余りは $\{0,1,2,3,4,5\}$ となるので $\mathbb{Z}/6\mathbb{Z}=\{0,1,2,3,4,5\}$ となる.
同じ余りを持つものは等しいとして、「$1\equiv 7\equiv 13$ modulo 6」または「$1\equiv 7\equiv 13 \bmod 6$」または「$1\equiv 7\equiv 13$ 法 6」と書く.
よって，例えば、$4\equiv 10\equiv 16$ 6 となる.
n が非負整数Ｃ言語で表現すれば n%6 としたものである.
重要な性質であるが正の整数 n, m に対して
$((n\%6)\times(m\%6))\%6=(n\times m)\%6$
と
$((n\%6)+(m\%6))\%6=(n+m)\%6$
とできる. これらより $2\times 5\equiv 10\equiv 4 \bmod 6$, $2+5\equiv 7\equiv 1 \bmod 6$ とする.
$2+4\equiv 0 \bmod 6$ より $-2\equiv 4 \bmod 6$ と書くことができる.

素数 p の場合

素数 p に対しては
$\mathbb{Z}/p\mathbb{Z}=\{0,1,2,\ldots,p-1\}$ に対して,
$\mathbb{Z}/p\mathbb{Z}$ の要素 $n\neq 0$ に対して $\mathbb{Z}/p\mathbb{Z}$ の要素 m で $n\times m\equiv 1 \bmod p$ となるものが存在することが判っている. m は n の逆数と見なせる. $m=1/n$ とは書かない.
$\mathbb{Z}/p\mathbb{Z}$ の要素 n に対して $\mathbb{Z}/p\mathbb{Z}$ の要素 ℓ で $n+\ell\equiv 0 \bmod p$ となるものが存在することが判っている. $\ell=-n$ と見なせる.

素数 3, 5 の場合

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	0	4
6	6	0	1	2	3	4	5

演習問題 1

$p=5$ のとき，上記 $p=3,7$ と同様の積と和の表を作成せよ.

素数 17 の場合

$p=17$ のとき，下記の表は $\mathbb{Z}/17\mathbb{Z}=\{0,1,2,\ldots,16\}$ の内、零の除いたものの積を示したものある. $5\times 7\equiv 1 \bmod 17$ となる. それぞれに 1 になるものが存在する.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	**1**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	4	6	8	10	12	14	16	**1**	3	5	7	9	11	13	15
3	3	6	9	12	15	**1**	4	7	10	13	16	2	5	8	11	14
4	4	8	12	16	3	7	11	15	2	6	10	14	**1**	5	9	13
5	5	10	15	3	8	13	**1**	6	11	16	4	9	14	2	7	12
6	6	12	**1**	7	13	2	8	14	3	9	15	4	10	16	5	11
7	7	14	4	11	**1**	8	15	5	12	2	9	16	6	13	3	10
8	8	16	7	15	6	14	5	13	4	12	3	11	2	10	**1**	9
9	9	**1**	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	10	3	13	6	16	9	2	12	5	15	8	**1**	11	4	14	7
11	11	5	16	10	4	15	9	3	14	8	2	13	7	**1**	12	6
12	12	7	2	14	9	4	16	11	6	**1**	13	8	3	15	10	5
13	13	9	5	**1**	14	10	6	2	15	11	7	3	16	12	8	4
14	14	11	8	5	2	16	13	10	7	4	**1**	15	12	9	6	3
15	15	13	11	9	7	5	3	**1**	16	14	12	10	8	6	4	2
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	**1**

公開鍵暗号のトイモデル I

ボブからアリスへ暗号化されたデータを送ることを考える.

1. アリスは素数 p を選択する.（例えば，$p=17$ とする）
2. アリスは $\mathbb{Z}/17\mathbb{Z}$ の数 q を選択し，$q'q\equiv 1 \bmod p$ となる q' を計算し、q' を鍵として記憶する.（例えば，$q=5$ として，$q'=7$ となる）
   ここで q に対して q' を求めることが非常に計算量が大きいと仮定する.
3. アリスは p と q を公開する.（例えば，$p=17$, $q=5$）
4. ボブは公開された鍵 p と q により，送りたいデータ n(ただし $0<n<p$）に対して，$n'=nq \bmod p$ を計算する.
5. ボブはアリスに n' を送る.
6. アリスは，受け取った n' に対して $n'q' \bmod p$ を計算する. $n'q'=nq'q=n \bmod p$ より，複号できた.

演習問題 2：公開鍵暗号のトイモデル I

隣の席の人と、$p=17$ の場合のアリス側、ボブ側となって n' を聞き、元のデータ n を複合せよ. それぞれ 2 回,（アリスは q を自由に選択する.、ボブは n を自由に選択する.）

演習問題 3：公開鍵暗号のトイモデル I

隣の席の人と、$32 > p > 17$ の素数で、上記のトイモデル I による公開鍵暗号による暗号化されたデータ通信を実施せよ．各 2 回．（アリスは q を自由に選択する．、ボブは n を自由に選択する．）

演習問題 4：公開鍵暗号のトイモデル I

隣の席の人と、$p > 22$ の素数で、上記のトイモデル I による公開鍵暗号による暗号化されたデータ通信を実施せよ． 各 2 回

フェルマーの小定理：素数 p の場合

素数 p に対しては
$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ に対して，
$\mathbb{Z}/p\mathbb{Z}$ の任意の要素 $x \neq 0$ に対して，
$x^{p-1} \equiv 1 \mod p$
となる．

素数 17 の場合

例えば，$p = 17$ のとき，$7^5 \equiv 11 \mod 17$ となる．

×＼n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

演習問題 5

$p = 5, 7, 13$ のときに上記の表を作成せよ．

フェルマーの小定理：素数 p, q に対する合成数 pq の場合

素数 p，q に対しては
$\mathbb{Z}/pq\mathbb{Z} = \{0, 1, 2, \ldots, pq-1\}$ に対して，
$\mathbb{Z}/pq\mathbb{Z}$ の任意の要素 $x \neq 0$ で x が p または q の倍数でないものに対して，
$x^{(p-1)(q-1)} \equiv 1 \mod pq$
となる．

素数 5,3 の場合

例えば，$p = 5, q = 3$ のとき，

×＼n	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1
3	3	9	12	6	3	9	12	6
4	4	1	4	1	4	1	4	1
5	5	10	5	10	5	10	5	10
6	6	6	6	6	6	6	6	6
7	7	4	13	1	7	4	13	1
8	8	4	2	1	8	4	2	1
9	9	6	9	6	9	6	9	6
10	10	10	10	10	10	10	10	10
11	11	1	11	1	11	1	11	1
12	12	9	3	6	12	9	3	6
13	13	4	7	1	13	4	7	1
14	14	1	14	1	14	1	14	1

素数 5,7 の場合

例えば，$p = 5, q = 7$ のとき，

x＼r	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	29	23	11	22	9	18	1
3	3	9	27	11	33	29	17	16	13	4	12	1
4	4	16	29	11	9	1	4	16	29	11	9	1
6	6	1	6	1	6	1	6	1	6	1	6	1
8	8	29	22	1	8	29	22	1	8	29	22	1
9	9	11	29	16	4	1	9	11	29	16	4	1
11	11	16	1	11	16	1	11	16	1	11	16	1
12	12	4	13	16	17	29	33	11	27	9	3	1
13	13	29	27	1	13	29	27	1	13	29	27	1
16	16	11	1	16	11	1	16	11	1	16	11	1
17	17	9	13	11	12	29	3	16	27	4	33	1
18	18	9	22	11	23	29	32	16	8	4	2	1
19	19	11	34	16	24	1	19	11	34	16	24	1
22	22	29	8	1	22	29	8	1	22	29	8	1
23	23	4	22	16	18	29	2	11	8	9	32	1
24	24	16	34	11	19	1	24	16	34	11	19	1
26	26	11	6	16	31	1	26	11	6	16	31	1
27	27	29	13	1	27	29	13	1	27	29	13	1
29	29	1	29	1	29	1	29	1	29	1	29	1
31	31	16	6	11	26	1	31	16	6	11	26	1
32	32	9	8	11	2	29	18	16	22	4	23	1
33	33	4	27	16	3	29	12	11	13	9	17	1
34	34	1	34	1	34	1	34	1	34	1	34	1

判るように $x^{(p-1)(q-1)/2} \equiv 1 \mod pq$ となっている．

演習問題 6

$p = 3, q = 7$ のときに上記の表を作成せよ．

公開鍵暗号ＲＳＡの基本原理

$\mathbb{Z}/pq\mathbb{Z}$ のある数 x（データ）に対して，$(p-1)(q-1)$ と公約数が 1 以外にない数 e を用意し，$d = e^{-1} \mod (p-1)(q-1)$ を計算し、鍵として d を記憶する．
(pq, e) を公開し，公開した pq によりデータ $y = x^e \mod$ pq を計算し、y を送る．
これを送られてきた側で $y^d \mod$ pq を計算する．
$y^d = (x^e)^d = x^{de} = x$ となり，複号ができた．

公開鍵暗号のトイモデル I I　ＲＳＡ

アリスは例えば，$p = 5, q = 7$ を選び，$((p-1)(q-1) = 24)$ $e = 31$ を例えば選ぶ．
公開鍵としては $(35, 31)$ を公開する．他方，$31 \times 7 \equiv 1 \mod 24$ より d として 7 を記憶する．
ボブはデータとして $x = 17$ のとき，$y = 17^{31} (= 17^7) = 3 \mod 35$ を暗号化されたデータとして送る．
復号は，$3^7 = 17 \mod 24$ とすればよい．

演習問題 7：公開鍵暗号のトイモデル I I(add)

$p = 7, q = 13$ の場合に上記の RSA 暗号を模擬せよ

課題

上記、演習問題 1 ～6 までの指示されたものをレポートにまとめワードファイル 5SXX_kadai10 として提出せよ．(必須)
余裕がある人は演習問題 7 を示し，ワードファイルにまとめ提出よせ．5SXX_kadai10add として提出せよ．