13.4.0 公開鍵暗号

暗号系の本質：　１つの通信文を，鍵と暗号文との２つの通信路に分けて送る.

鍵は，次の３通りのどの方法で送信してもよい.

(1) 送信者から受信者に送る.
(2) 受信者から送信者に送る.
(3) 第三者が送信者と受信者に送る.

公開鍵暗号系の概念　W. Diffie, M. Hellman (1976)

- 受信者が鍵の対(ついい) e, d を作って、暗号化用の鍵 e だけを送信者に送る.
- 復号用の鍵 d は受信者だけの秘密にしておく.
- 暗号化用の鍵 e から秘密の復号用の鍵 d が算出できなければ安全である.

13.4.1 剰余演算（割った余りについての演算）

知っていると便利な剰余

例： 4 日ごとの休日の日付を知る方法

2017 年 11 月

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

4 で割ると余りは 1

2017 年 12 月

日	月	火	水	木	金	土
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

4 で割ると余りは 3

2018 年 1 月

日	月	火	水	木	金	土
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

4 で割ると余りは 0

2018 年 2 月

日	月	火	水	木	金	土
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28			

4 で割ると余りは 1

2018 年 3 月

日	月	火	水	木	金	土
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

4 で割ると余りは 1
（28 が 4 で割り切れるから）

例：　時計の算数（**法**（ほう） 60 で割る）

227 分 ＝ □ 時間 □ 分

分の **元**（げん）（要素）は，0〜59 の 60 個である．

記法

47 ≡ 227　(modulo 60)
47 ≡ 167　(modulo 60)
47 ≡ 107　(modulo 60)
47 ≡ 47　(modulo 60)
47 ≡ −13　(modulo 60)
47 ≡ −73　(modulo 60)

まとめて書くと，

167 ≡ 107 ≡ 47 ≡ −13　(modulo 60)

法が 60 のとき，47＋60k（k は整数）はすべて合同な数である．

四則演算

加算　47＋20 ≡ 7　(modulo 60)

減算　7−20 ≡ 47　(modulo 60)

7＋40 ≡ 47　(modulo 60)

20 を引く代わりに 40 を加えても結果は同じだ!

a に対して，**法**$-a$ を“a の補数”という．
法が 60 のとき，60−20＝40 が 20 の補数である．

乗算　56×7 ≡ 32　(modulo 60)

56×7 ≡ (60−4)×7 ≡ 60×7 − 4×7
≡ −4×7 ≡−28 ≡ 32　(modulo 60)

除算　32÷7 ≡ 56？　(modulo 60)

法が 60 のときの 7 の**逆元**（7^{-1}）は 43 だ！

検算：　7×43 ＝ 301 ≡ 1　(modulo 60)

32÷7 ≡ 32×7^{-1} ≡ 32×43 ≡ 56 (modulo 60)

法と元とが互いに素（1 以外に共通の約数をもたない）のとき，乗法の逆元が存在する．（したがって，法が素数なら，0 以外のすべての元に逆元が存在する．）

13.4.2 **逆関数の表記**

関数　　f　　←→　逆関数 f^{-1}
暗号化　$\mathbf{E}$　　←→　復号　　$\mathbf{E}^{-1}$　(=**D**)

逆元の表記と記法は同じだが，意味は異なる.