Exercise 1

(a) $\gcd(13, 380) = 1$

$\Leftrightarrow [13]_{380}$ inversible

$$\phi(380) = \phi(\underbrace{5 \cdot 2}_{10} \cdot 2 \cdot 19)$$

$$= 4 \cdot 18$$

130
760
390 377

$$13^{18-4} \equiv 1 \ [380]$$

GCD(a, b)	$a = bq + r$	q	u	v	$\tilde{v}$	$\tilde{u} - q\tilde{v}$
(380, 13)	$380 = 13 \cdot 29 + 3$	29	−4	117		
(13, 3)	$13 = 3 \cdot 4 + 1$	4	1	−4		
(3, 1)	$3 = 3 \cdot 1 + 0$	1	0	1		
(1, 0)	$1 = 0 \cdot 0 + 1$	0	1	0		

$1 \cdot u + 0 \cdot v = 1$

$-4 \cdot 380 + 117 \cdot 13 = 1$

$\Rightarrow 117 \cdot 13 - 1 = -4 \cdot 380$

$[117]_3$ inverse

(b) $27 = 3 \cdot 3 \cdot 3$

$9999 = 3 \cdot 3 \cdot k$

$[27]_{9999} \cdot [10 + \dots + 10000]_{9999}$

$9999 = 9 \cdot 10$
$+ 9 \cdot 100$
$+ 9 \cdot 1000$
$+ 9 \cdot 10000$

$\frac{9999}{3 \cdot 3} = 10 + \dots + 10000 = 9(10 + \dots + 10000)$

© $[3^{431}]_{29}$

$\phi(29) = 28$

$3^{280 \cdot 2}$

$3^{420+11} \equiv 3^{11} \; [29]$

$3^3 \equiv -2 \; [29]$

$3^6 \equiv 4 \; [29]$

$\Rightarrow 3^6 \cdot 3^3 = -8 \; [29]$

$\Rightarrow 3^6 \cdot 3^3 \cdot 3^2 = -72 \; [29]$

$= -43 \; [29]$

$= -14 \; [29]$

$= 15 \; [29]$

$$\begin{array}{r} {\scriptstyle 1} \\ 280 \\ +140 \\ \hline 420 \end{array}$$

$$\begin{array}{r} 29 \\ \cdot\ 2 \\ \hline 58 \end{array}$$

$$15 \cdot 2 - 29 \cdot 1 = 1$$

$$\Rightarrow 15 \cdot 2 - 1 = 29$$

l'inverse est $[2]_{29}$

(d)

			$\tilde{v}$	$\tilde{u} - q\tilde{v}$
$GCD(28925, 28899)$	$a = bq + r$	q	u	v
	$28925 = 28899 \cdot 1 + 26$	1		
$(28899, 26)$	$28899 = 26 \cdot 1111 + 13$	1111	13	$-1111 \cdot 13$
$(26, 13)$	$26 = 13 \cdot 2 + 0$	2	0	13
$(13, 0)$	$13 = 0 \cdot 0 + 13$	0	13	0

$$13 = 13 \cdot u + 0 \cdot v$$

$$28899 = 26 \cdot 1000 + 26 \cdot 100$$

1111

$$\begin{array}{r} 28\,899 \\ -\,26\,000 \\ \hline 2\,899 \\ -\,2\,600 \\ \hline 299 \\ -\,260 \\ \hline 39 \\ -\,26 \\ \hline 13 \end{array}$$

$$[28899] \cdot \left[\frac{28925}{13}\right] = [0]$$

22·6 = 132

②

(a) $22x = [19 - 63]_{132}$

$= [-40 - 3 - 1]_{132}$

$= [-44]_{132}$

$= [56 + 32]$

$= [88]_{132}$

$[11]_{132}\,[2]_{132}\,x = [92]_{132}$

$\Rightarrow [11]_{132}\,[2]_{132}\,x = [92]_{132}$

$\Rightarrow$

$$\begin{array}{r} {\scriptstyle 1} \\ 22 \\ \cdot\quad 5 \\ \hline 110 \end{array}$$

$x = 1$ $\quad [22]_{132}$

$x = 2$ $\quad [44]_{132}$

$x = 3$ $\quad [66]_{132}$

$+6k$ $\quad x = 4$ $\quad [88]_{132}$

$x = 5$ $\quad [110]_{132}$

$x = 6$ $\quad [0]_{132}$

⋮

(b)

$$(9989)_x = [21]_{100}$$

$$\Leftrightarrow [-1]_{100}\, x = [21]_{100}$$

$$\Rightarrow x = [-21]_{100}$$

Problem 9.2

e doit être copriime avec $\phi(m)$ si on veut avoir $ed - k\phi(m) = 1$

① @ $m = pq$

$$ed - k\,\phi(m) = 1$$

$$\phi(m) = \underline{(p-1)(q-1)}$$

$\Rightarrow$ we need to find d st.

$$\underbrace{ed}_{①} - \underbrace{k}_{②}\underbrace{(p-1)(q-1)}_{③} = 1$$

$28 \downarrow 2^2 \cdot 7$ $\quad$ $40 \downarrow 5 \cdot 2^3$

$4 \cdot 7 \cdot 5 \cdot 2 = k$

$(ed)_{280} = 1$

$k(-1)(p-1)(q-1) - 1 = -ed$

$\Rightarrow \quad ed \equiv 1 [k]$

$\Rightarrow$ on cherche l'inverse de e mod k

			$\tilde{v}$	$\tilde{u} - q\tilde{v}$
GCD(a, b)	$a = bq + r$	q	u	v
(280, 9)	$280 = 9 \cdot 31 + 1$	31	1	31
(9, 1)	$9 = 9 \cdot 1 + 0$	1	0	1
(1, 0)	$1 = 0 \cdot 0 + 1$	0	1	0
			1	-31

$9 \cdot 30 = 270$ $\quad 280 - 31 \cdot 9 = 1$

$+ \ 9 \quad = 279 \quad \Leftrightarrow \quad -31 \cdot 9 - 1 = -280$

$a = [-31]_{280}$ 249

(b) 66 97

$33 \cdot 2$

$= 11 \cdot 3 \cdot 2$

97

pas valide

$$\begin{array}{r} {\scriptstyle 1} \\ 127 \\ \cdot \quad 2 \\ \hline 254 \end{array}$$

$$\begin{array}{r} {\scriptstyle 2} \\ 38 \\ \cdot \quad 3 \\ \hline 114 \end{array}$$

(c) 4 72

2^2

$2^2 \cdot 3^2$

72

$$\begin{array}{r} {\scriptstyle 1} \\ 73 \\ \cdot \quad 4 \\ \hline 292 \end{array}$$

GCD(a,b)	$a = bq + r$	q	u	v
			$\tilde{v}$	$\hat{v} - q\tilde{v}$

(292, 127)	$292 = 127 \cdot 2 + 38$	2	10	$3 - 2 \cdot 10$
(127, 38)	$127 = 38 \cdot 3 + 13$	3	3	-10
(38, 13)	$38 = 13 \cdot 2 + 12$	2	-1	3
(13, 12)	$13 = 12 \cdot 1 + 1$	1	1	-1
(12, 1)	$12 = 1 \cdot 12 + 0$	12	0	1
(1, 0)	$1 = 0 \cdot 0 + 1$	0	1	0
	r	$a - qv$	$27 + 28 = 55$	$13 - 3 = 51$

GCD(127, 72)	$a = bq + r$	q	u	v
(127, 72)	$127 = 72 \cdot 1 + 55$	1	-17	$13 + 17 = 30$
(72, 55)	$72 = 55 \cdot 1 + 17$	1	13	$-4 - 13 = -17$
(55, 17)	$55 = 17 \cdot 3 + 4$	3	-4	$1 - 3 \cdot (-4) = 13$

$(17, 4)$
$(4, 1)$
$(1, 0)$

$17 = 4 \cdot 4 + 1$	4	1	-4
$4 = 1 \cdot 4 + 0$	4	0	1
$1 = 0 \cdot 0 + 1$	0	1	0

$$127 \cdot (-17) + 72 \cdot 30 = 1$$

$$\Rightarrow 127 \cdot -17 = 72 \cdot 30 - 1$$

$$127 \cdot (-17) \equiv 1 \; [72]$$

$d = -17$

$-17 + 72 = 55$

(2)

$$[t^e]_m$$

$$[48^9]_{p\cdot q = m}$$

$$[48^{9\cdot 249}]$$

$$\phi(m) = (p-1)(q-1) = (28)(40)$$

$$= 2^2 \cdot 7 \cdot 5 \cdot 2 \cdot 2^2$$

$$= 2^5 \cdot 5 \cdot 7$$

$$9 \cdot 249 = 2\phi(m) + 1$$

$\Rightarrow$ ok

③

$$[84^{55}]_{127}$$

$$= 42$$

Problem 9.3

① mod 7

mod 5	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

$\Phi(5) = 4$

②

$$3 \equiv 2 \ [5]$$

$$\Rightarrow 3^{\Phi(5)\cdot k \cdot 2} \equiv 4 \ [5]$$

$$\Rightarrow 3^{\Phi(6)\cdot k+2} \equiv 2 \ [7] \qquad \Phi(7) = 6$$

Problem 9.4

① $ak + bmn = 1$

Supposons que $[k]_m$ n'est pas copremier avec m.

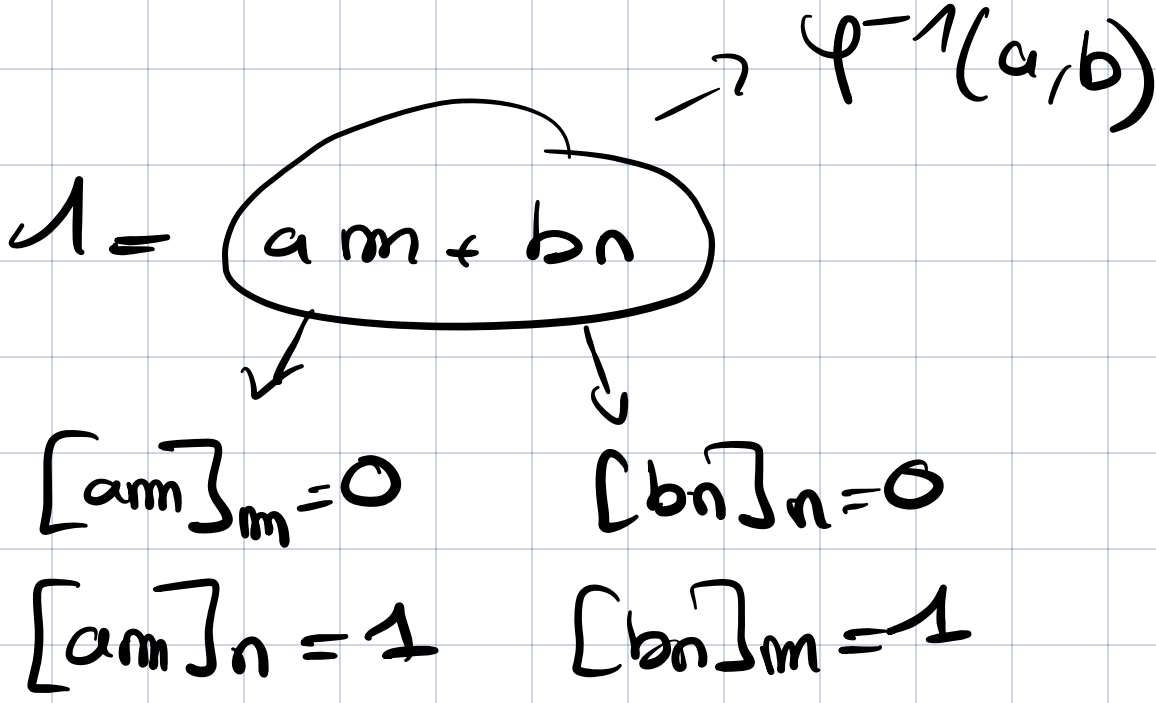
$\exists c \neq 1 \quad [k]_m = cq$

$m = cq'$

$\Rightarrow [ak + bmn]_m = 1$

$\Rightarrow [ak]_m = 1$

(2)



on veut montrer $\longrightarrow$ $\operatorname{pgcd}(am+bn, m) = 1$

$\operatorname{pgcd}(am+bn, n) = 1$

Supposons qu'il existe c t.q

$$[am+bn]_m = [am]_m + [bn]_m$$

$$= [1]_m$$

donc $am + bn = 1 + mk$

supposons que $pgcd(am+bn, m) \neq 1$

$\exists\, c$ t.q $c \mid am+bn$ et $c \mid m$

$\Rightarrow \quad cz = am + bn$
$\quad\quad ck = mk$

$\Rightarrow \quad cz = 1 + ck$

$\Rightarrow \quad c(z-k) = 1$

≥ 1, entier (par supp) ; entier aussi ≥ 1

donc $\Rightarrow \boxed{c = 1}$ ■

③ $\phi(mn) = \prod_p (p-1)^{k-1}$

si pas de facteurs en commun

$$\phi(m) \cdot \phi(n) = \phi(mn)$$

④

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$$

$$\phi(n) = \phi(p_1^{k_1}) \cdot \phi(p_2^{k_2}) \cdot \ldots \cdot \phi(p_3^{k_3})$$

$$= p_1^{k_1} - p_1^{k_1-1} + p_2^{k_2} - p_2^{k_2-1} + p_3^{k_3} - p_3^{k_3-1} + \ldots + p_m^{k_m} - p_m^{k_m-1}$$

$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right) + \dots + p_m^{k_m}\left(1-\frac{1}{p_m}\right)$$

Problem 9.5

① $[t^e]^d \bmod m$

$[\log_2(pq)]^3$

② (a) $[c]_p^{dp}$

$[c]_p^{dp} = [t]_p$

$$t^{e^{dp}} = t$$

$$e \cdot dp = \phi(p) + 1$$

$$= p - 1 + 1$$

$$= p$$

$$\Leftrightarrow e[(p-1)k + d] = p$$

$$\Leftrightarrow d = \frac{p}{e} - (p-1)k$$

$$d_p = d \bmod (p-1)$$

$$\Rightarrow d_p - d = (p-1)k$$

$$\Rightarrow d = (p-1)k + d_p$$

$$[c]_p^{d_p} = [c^{d_p}]_p$$

$$= [c^{d-(p-1)k}]_p$$

$$= [c^d]_p [c^{q(p-1)}]_p$$

$$= [c^d]_p$$

By assumption:

$$[c^d]_{pq} = [E]_{pq}$$

$\Rightarrow$ CRT $[c^d]_p = [t]_p$

(b) Reverse CRT

We know that

$t_p = t \bmod p$

$t_q = t \bmod q$

$pu + qv = 1 \Rightarrow \begin{cases} qv \equiv 1 \,[p] \\ pu = 1 \,[q] \end{cases}$

what is $t \bmod pq$?

$$\begin{cases} qv \equiv 1 \,[p] \\ qvt_p \equiv t_p \,[p] \end{cases}$$

$$\begin{cases} pu \equiv 1 \,[q] \\ put_q \equiv t_q \,[q] \end{cases}$$

$$qvtp + pvtp = t \quad \checkmark$$

(c) $(\log_2 p)^3 + (\log_2 q)^3$

(3) $(\log_2 m)^3$ for the 1st method

$$\log_2 p \simeq \log_2 q$$

$$\Rightarrow \log(m) \simeq \log(p \cdot p)$$
$$\simeq 2\log(p)$$

$$(\log_2 p)^3 + (\log_2 q)^3$$
$$\simeq \frac{(\log_2 m)^3}{2^3} \cdot 2 = \frac{1}{4}(\log_2 m)^3$$