Problem 6.1

$a \equiv b \, [m] \iff m \mid a-b$

$a^{p-1} \equiv 1 \, [p]$ if p is a prime number

$\Rightarrow 6^6 \equiv 1 \, [7]$

$\Rightarrow (6^6)^{76} \equiv 1 \, [7]$

(b) On cherche à introduire un cycle

$\Rightarrow$ objectif : trouver un i t.q $2^{ik} \equiv 1 [5]$

$$2^4 \equiv 1 [5]$$

$$\Rightarrow 2^{4k} \equiv 1 [5]$$

$$\Rightarrow 2^{4k+1} \equiv 2 [5]$$

$$\Rightarrow 2^{4k+2} \equiv 4 [5]$$

$$\Rightarrow 2^{4k+3} \equiv 3 [5]$$

$$981 = 4 \cdot 20 + 25 \cdot 4 \cdot 9 + 1$$

$$= 4k + 1$$

$$2^{981} \equiv 1 [5]$$

c 3

Problem 6.1

(1) (a) 7 est premier

$$\Rightarrow a^6 \equiv 1 \, [7]$$

$$\Rightarrow 6^6 \equiv 1 \, [7]$$

$$\Rightarrow 6^{6 \cdot 76} \equiv 1 \, [7]$$

(b) $$2^4 \equiv 1 \, [5]$$

$$\Rightarrow 2^{4k} \equiv 1 \, [5]$$

$$\Rightarrow 2^{4k+1} \equiv 2 \, [5]$$

$$\Rightarrow 2^{981} \equiv 2 \, [5]$$

c) $3^{?} \equiv 1 \ [16]$

$\Rightarrow$ fonction indicatrice d'Euler

Si $n = \prod_{i=1}^{r} p_i^{k_i}$

alors $\varphi(n) = \prod_{i=1}^{r} (p_i - 1)\, p_i^{k_i - 1}$

$$\varphi(16) = \varphi(2^4) = (2-1)\, 2^{4-1}$$
$$= 8$$

Selon le théorème d'Euler, $a^{\varphi(n)} \equiv 1 \ [n]$,
SI a et n sont premiers entre eux !

$$3^8 \equiv 1 \ [16]$$
$$\Rightarrow 3^{16} \equiv 1 \ [16]$$
$$\Rightarrow 3^{16} \cdot 3^3 \equiv 11 \ [16]$$

$5^8 \equiv 1 \ [16]$

$\Rightarrow 5^{16} \cdot 5^2 \equiv 9 \ [16]$

donc $3^{19} \cdot 5^{18} \equiv 3 \ [16]$

$\downarrow$

$99 - 96 = 3$

$\downarrow$

$16 \cdot 6$

ⓓ $26019 \equiv 6 \ [13]$

$\downarrow$

$26019 - 6 = 26013$

$392 \equiv 2 \ [13]$

$\downarrow$

$130 \cdot 3 = 390$

$392 \cdot 26019 \equiv 12 \ [13]$

② $\varphi(3) = 2$

$a^{\varphi(3)} \equiv 1\ [3]$ şi 3 ne divize pas a

$\Rightarrow a^2 \equiv 1\ [3]$

$\Rightarrow a^{2k} \equiv 1\ [3]$

③ $2^{\overbrace{761^{435}}^{=2k'}} \cdot 2^{\overbrace{97!}^{=2k''}} \equiv 1\ [3]$

$$2^{97!} = \left(2^2\right)^{\frac{97!}{2}} \equiv 1\ [3]$$

because $2^{2k} \equiv 1\ [3]$! (see ②)

remainder is 2.

(4) $n \equiv 3\ [4]$

$n \equiv 5\ [8]$

$n - 3 = 4k \Rightarrow n = 4k + 3$

impossible

$n - 5 = 8k \Rightarrow n = 8k + 5$

$\Rightarrow n = 4k' + 5$

(5) Fast exponentiation algorithm.

$$(x_1)^{b_1} \cdot (x_1)^{2b_2} \cdot (x_1)^{4b_3} \cdot \ldots = x^e$$

$$x^e \bmod m = [x_1 \bmod m]^{b_1}$$

$$\cdot [x_1^2 \bmod m]^{b_2}$$

$$\cdot [x_2^2 \bmod m]^{b_3} \ldots$$

⑥ 5^{59} $48 + 11$

$59 = 111011$

$5^{59} \equiv 5 \cdot 2 \cdot 4^0 \cdot 16 \cdot 3 \cdot 9$

$25 \% 23$ $\quad 2^2 \% 23$ $\quad 4^2 \% 23$ $\quad 16^2 \% 23$ $\quad 253$

$\equiv 19 \ (23)$

Problem 6.2

1 a $\varphi(7) = 6.$

$$37^{6} \equiv 1 \, [7]$$

$$\Rightarrow 37^{6k} \equiv 1 \, [7]$$

$$\Rightarrow 37^{6k+1} \equiv 2 \, [7]$$

$$\Rightarrow 37^{121} \equiv 2 \, [7]$$

b $\varphi(19) = 18$

198
216
234
252

$$18^{18} \equiv 1 \, [19]$$

$$\Rightarrow \underbrace{\left[18^{18}\right]^{\frac{234}{18}}}_{\equiv 1} \cdot 18^{9}$$

ⓒ $\varphi(27) = 2 \cdot 3^2 = 18$

$27 = 3 \cdot 3 \cdot 3$

$$3^{3} \equiv 0 \; [27]$$

$$\Rightarrow \left[3^3\right]^{\frac{17!}{3}} \equiv 0 \; [27]$$

ⓓ $460002 \equiv 2 \; [23]$

$25 \equiv 2 \; [23]$

$$460002 \cdot 25 \equiv 4 \; [23]$$

ⓔ $111 \ldots 79 \equiv 3 \; [8]$

(2) Somme des chiffres : 58.

$58 - 4 = 54$ div par 9.

$653 \ldots 917 \equiv 4 [9]$

(3) $23456 \equiv 2 [9]$

$6453601 \equiv 7 [9]$

$6453601 \cdot 23456 \equiv 5 [9]$

$151379566 5056 \equiv 2 [9]$ $\neq$ FAUX

Σ 56

(4) $d_0 \cdot 10^0 + d_1 \cdot 10^1 + \ldots + d_n \cdot 10^n$

$$10 \equiv -1\ [11] \qquad 11 \cdot 90$$
$$10^n \equiv (-1)^n\ [11] \qquad = 990$$

$$10\,000$$

$$d_n \cdot 10^n \equiv (-1)^n \cdot d_i\ [11]$$

$$a \equiv b\ [m]$$
$$c \equiv d\ [m]$$
$$a+c \equiv b+d\ [m]$$

$$d_0 \cdot 10^0 + d_1 \cdot 10^1 + \dots + d_n \cdot 10^n$$
$$\equiv \sum_{i=0}^{k} (-1)^i d_i$$

(S) $97\ldots16 \equiv 6\ [11]$

(6) 406700072

$$d_0d_1d_2 \cdot 1000^0 + d_3d_4d_5 \cdot 1000^1$$
$$+ d_6d_7d_8 \cdot 1000^2$$

$$1000 \equiv -1 \; [1001]$$
$$1000^k \equiv (-1)^k \; [1001]$$

$$442 - 258 + 7 - 67 + 4 = \underline{128}$$

(7)

$$\overline{67\quad\quad} \equiv 0 \; [11]$$

$$67 \equiv 1 \; [11]$$

$$\Rightarrow 67^{\dots} \equiv 1 \; [11]$$

$$+ \quad 21 \equiv -1 \; [11]$$ car exposant pair

$$\Rightarrow 21 \equiv 1 \; [11]$$

$$+ \quad 9 \equiv 9 \; [11]$$

$$\Rightarrow \quad \text{total} \equiv 0 \; [11]$$

$$109 \equiv -1 \; [11]$$

$$\Rightarrow 109^{\dots} \equiv -1 \; [11]$$

$$56 \equiv 1 \; [11]$$

$$\Rightarrow 56^{\dots} \equiv 1 \; [11]$$

$$\Rightarrow \quad \text{tot} \equiv 1 \; [11]$$

$36 \equiv 3\ [11]$ $\qquad \varphi(11) = 10$

$36^{10} \equiv 1\ [11]$

$90 \equiv 1\ [11]$

$+7$ no ?

Problem 6.3

(1) $100 \cdot 4$

$+ 100 \cdot 10 \cdot 9$

$+ 100^2 \cdot 8$

$+ 100^2 \cdot 10 \cdot 7$

$+ 100^3 \cdot 5$

$+ 100^3 \cdot 10 \cdot 9$

$+ 100^4 \cdot 3$

$+ 100^4 \cdot 10 \cdot 1$

$+ 100^5 \cdot 2$

$$\equiv \cancel{3\cdot 4} + \cancel{3\cdot 10}\cdot 9 + 9\cdot \cancel{8} + 9\cdot \cancel{10}\cdot 7$$

$$+ \cancel{27}\cdot 5 + 27\cdot \cancel{10}\cdot 9 + \cancel{81}\cdot 3 + \cancel{81}\cdot 10$$

$$+ 81\cdot \cancel{3}\cdot 2$$

$$\equiv 114 + 3(\overbrace{94+81}^{175}) + 81(\overbrace{30+10+6}^{46})$$

$$27(138)$$

$$+ 9(8+70)$$

$$\equiv 38 + 3\cdot 78 + 27(41) + 9(78)$$

$$\equiv 38 + 40 + 9(123) + 3\cdot(40)$$

$$\equiv 78 + 9\cdot 26 + 120$$

$$\equiv 78 + 3\cdot 78 + 120 \qquad 3\cdot 78 = \begin{array}{r} 24 \\ +\,210 \\ \hline =234 \end{array}$$

$$\equiv 2\cdot 59 \qquad 23 \qquad 97\cdot 2 = \begin{array}{r} 14 \\ +\,180 \\ \hline \end{array}$$

$= \underline{44}$

194

$41 \cdot 3 = \begin{array}{r} 120 \\ +\ 3 \\ \hline 123 \end{array}$

$3 \cdot 26 = \begin{array}{r} 60 \\ +\ 18 \\ \hline 78 \end{array}$

$78 \cdot 2 = \begin{array}{r} 16 \\ +\ 140 \\ \hline 156 \end{array}$

② $r = 44$

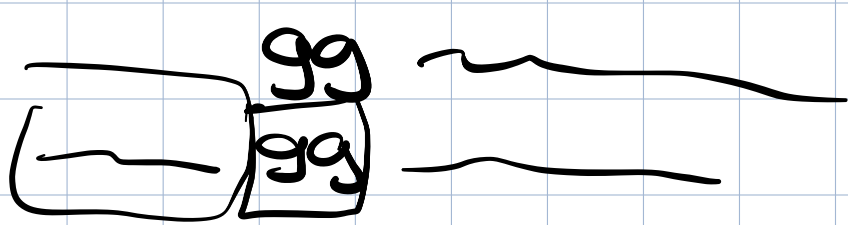
$98 - r = 98 - 44 = 54$

$021\ 395\ 7884\ 54\ \%\ 97 = 1$

③ $97 \mid z - z'$

$z - z' \equiv 0\ [97]$

- $z \equiv 1\ [97]$
- $z' \equiv 1\ [97]$



$$c \cdot 10^{a+d}$$

$$99 \cdot 10^{a} + b \equiv 99 \cdot 10^{a} + b \; [97]$$
$$02 \cdot 10^{a} + b \equiv 2 \cdot 10^{a} + b \; [97]$$

$$99 \cdot 10^{a} + b - [2 \cdot 10^{a} + b]$$

$$\equiv (99-2) \cdot 10^{a} \equiv 0 \; [97]$$