Nombres entiers et division

Définition : a divise b, noté $a \mid b$ si $b = a \cdot k$ pour un certain $k \in \mathbb{Z}$.

Remarque : $\forall n \in \mathbb{Z}$, $1 \mid n$ et $n \mid n$ (si $n \neq 0$).

Remarque : Il faut voir le symbole « | » comme une relation et non comme une opération. Cette relation retourne vrai ou faux.

Exemple : Multiples de $a \in \mathbb{Z}^+$

a) $5 \mid 15$ car $15 = 5 \cdot 3$

b) $5 \nmid 8$ car $\frac{8}{5} \notin \mathbb{Z}$

Proposition 1 : Si $a \mid b$ et $a \mid c$, alors $a \mid (b + c)$. Exemple : $3 \mid 9$ et $3 \mid 27$, donc $3 \mid (9 + 27)$.
Proposition 2 : Si $a \mid b$, alors $a \mid n \cdot b$, pour $\forall n \in \mathbb{Z}$.
Proposition 3 : Si $a \mid b$ et $b \mid c$, alors $a \mid c$. Exemple : $3 \mid 9$ et $9 \mid 27$, donc $3 \mid 27$.

Algorithme de division

Théorème 3 : Si $a \in \mathbb{Z}$ et $d \in \mathbb{Z}^+$, alors il existe $q, r \in \mathbb{Z}$ avec $0 \leqslant r < d$, tel que $a = d \cdot q + r$.

Notation : $r = a \bmod d \Rightarrow$ Reste de la division de a par d.

Exemples

a) Calculer 101 mod 10 : $101 = 10 \cdot 10 + 1$, d'où 101 mod 10 = 1.

b) Calculer -19 mod 5 : on a $-19 = 5 \cdot (-4) + 1$, d'où -19 mod 5 = 1.

Remarque : Un reste est toujours positif ($r \in \mathbb{Z}^+$).

Arithmétique modulaire

Définition : $a \equiv b \pmod m$ si et seulement si $m \mid (a - b)$.

Théorème 4 : $a \equiv b \pmod m$ si et seulement si $a \bmod m = b \bmod m$.

Exemple :

a) $17 \equiv 5 \pmod 6$ car $17 - 5 = 12$ et $6 \mid 12$.

b) $20 \not\equiv 3 \pmod 6$ car $20 - 3 = 17$ et $6 \nmid 17$.

c) on a $20 \equiv 2 \pmod 6$

$20 \equiv 8 \pmod 6$

$20 \equiv 14 \pmod 6$

$20 \equiv -4 \pmod 6$

Théorème 5 : $a \equiv b \pmod m$ si et seulement si $a = b + k \cdot m$ pour un certain $k \in \mathbb{Z}$.

Preuve : on a $a \equiv b \pmod m \iff m(a - b)$

$\iff a - b = m \cdot k$ pour $k \in \mathbb{Z}$

$\iff a = b + k \cdot m$

Proposition 6 : Si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$, alors

1) $a + c \equiv b + d \pmod{m}$
2) $a \cdot c \equiv b \cdot d \pmod{m}$

Exemple : On a $102 \equiv 4 \pmod{7}$ et $61 \equiv 5 \pmod{7}$, alors on a

1) $163 = 102 + 61$
$163 \equiv 4 + 5 \pmod{7}$
$\equiv 9 \pmod{7}$
$\equiv 2 \pmod{7}$

2) $6222 = 102 \cdot 61$
$\equiv 4 \cdot 5 \pmod{7}$
$\equiv 20 \pmod{7}$
$\equiv 6 \pmod{7}$

Application à la cryptologie

Codage de César

Décaler les lettres du message de trois lettres vers l'avant dans l'alphabet ($A \to D$).

Fonction de codage : $f(p) = (p + 3) \bmod 26$

S	I	X		J	U	I	N
18	08	23		09	20	08	13
$\downarrow + 3 \bmod 26$							
21	11	00		12	23	11	16
V	L	A		M	X	L	Q

Fonction de décryptage : $f^{-1}(p) = (p - 3) \bmod 26$

Généralisation du codage de César :

- $f(p) = (p + k) \bmod 26$
- $f(p) = (a \cdot p + k) \bmod 26 \Rightarrow$ doit être bijective.

Exemple : $f(p) = (2p + 1) \bmod 26$

$f(B) = 2 \cdot 1 + 1 = 3 = D$
$f(O) = 2 \cdot 14 + 1 = 29$
$29 \equiv 3 \pmod{26}$
$= D$

Nombres premiers

Définition 1 : p est premier si ses seuls facteurs sont 1 et p (où $p > 1$).
Définition 2 : n est composé s'il existe $a \in \mathbb{Z}^+$ tel que $a \mid n$ et $1 < a < n$.

Ensemble des nombres premiers : $\{2, 3, 5, 7, 11, 13, ...\}$

Théorème 7 (Théorème fondamental de l'arithmétique) : Tout $n > 1$ s'exprime de façon unique, comme un produit de nombres premiers :

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$$

Exemple :

1) $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
2) $641 = 641$ (641 est un nombre premier)
3) $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
4) $1024 = 2^{10}$

Théorème 8 : Si n est composé, alors il possède un facteur premier plus petit ou égal à $\sqrt{n}$.

Preuve : Si n est composé, alors il existe $a \in \mathbb{Z}$ tel que $a \mid n$ et $1 < a < n$. Donc, $n = a \cdot b$ pour $a, b \in \mathbb{Z}^+$. On doit avoir $a \leqslant \sqrt{n}$ ou $b \leqslant \sqrt{n}$ car sinon $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$. Supposons que $a < \sqrt{n}$, soit a est premier ou sinon il possède un facteur premier par le théorème fondamental de l'arithmétique. Ainsi, n possède un facteur premier $\leqslant \sqrt{n}$. □

Exemple : Montrer que 101 est premier.

Nombres premiers $\leqslant \sqrt{101} = \{2, 3, 5, 7\}$
On a $2 \nmid 101$, $3 \nmid 101$, $5 \nmid 101$ et $7 \nmid 101 \Rightarrow 101$ est premier.

Exemple : Trouver la factorisation en nombres premiers de 4641.

$n = 4641 \Rightarrow 2 \nmid 4641 \Rightarrow \boxed{3 \mid 4641}$

$n = \frac{4641}{3} = 1547 \Rightarrow 3 \nmid 1547 \Rightarrow 5 \nmid 1547 \Rightarrow \boxed{7 \mid 1547}$

$n = \frac{1547}{7} = 221 \Rightarrow 7 \nmid 221 \Rightarrow 11 \nmid 221 \Rightarrow \boxed{13 \mid 221}$

$n = \frac{221}{13} = 17$

d'où $4641 = 3 \cdot 7 \cdot 13 \cdot 17$.

Théorème 9 : Il y a une infinité de nombres premiers entiers.

Preuve par contradiction : Supposons un nombre fini de nombres premiers :
$P = \{p_1, p_2, p_3, ..., p_k\}$
Posons $n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k + 1$: aucun premier p_i divise n, car sinon p_i divise aussi 1 qui égale $n - p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k$. Donc, n est premier car il est divisible par aucun nombre premier p_i, mais $n \notin \{p_1, p_2, p_3, ..., p_k\}$, d'où la contradiction.

Nombres premiers de Mersenne

Définition : Un nombre premier de Mersenne est un nombre premier s'écrivant sous la forme $2^p - 1$ où p est premier.

Exemple : $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ sont premiers, mais $2^{11} - 1 = 2047 = 23 \cdot 89$ n'est pas premier.

Plus grand commun diviseur et plus petit commun multiple

Définition : a et b sont relativement premiers si $pgcd(a,b)$.

Exemple : $pgcd(18,24) = 6$ et $pgcd(13,20) = 1$.

Si $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, alors $pgcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)}$ et $ppcm(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k,\beta_k)}$.

Exemple : Soit $140 = 2^2 \cdot 5 \cdot 7$ et $1100 = 2^2 \cdot 5^2 \cdot 11$, donc

- $pgcd(140,1100) = 2^2 \cdot 5^1 \cdot 7^0 \cdot 11^0$
- $ppcm(140,1100) = 2^2 \cdot 5^2 \cdot 7^1 \cdot 11^1$

Théorème : $a \cdot b = pgcd(a,b) \cdot ppcm(a,b)$.

Preuve :

$$\begin{aligned} a \cdot b &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \\ &= p_1^{\alpha_1+\beta_1} \cdot p_2^{\alpha_2+\beta_2} \cdot \ldots \cdot p_k^{\alpha_k+\beta_k} \\ &= p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)+\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)+\max(\alpha_k,\beta_k)} \\ &= p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)} \cdot p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k,\beta_k)} \\ &= pgcd(a,b) \cdot ppcm(a,b) \end{aligned}$$

Algorithme d'Euclide

Exemple : Calculer $pgcd(91,287)$.

1) Diviser 287 par 91 $\Rightarrow 287 = 91 \cdot 3 + 14$
   - $\Rightarrow$ Tout diviseur de 91 et 287, divise aussi $287 - 91 \cdot 3 = 14$
   - $\Rightarrow$ Tout diviseur de 14 et 91, divise aussi $91 \cdot 3 + 14 = 287$
   - d'où le $pgcd(91,287) = pgcd(14,91)$.
2) Diviser 91 par 14 $\Rightarrow 91 = 14 \cdot 16 + 7$, on doit avoir $pgcd(14,91) = pgcd(7,14)$.
3) Diviser 14 par 7 $\Rightarrow 14 = 7 \cdot 2 + 0$, donc $pgcd(7,14) = 7$
   - $\Rightarrow pgcd(91,287) = pgcd(14,91) = pgcd(7,14) = 7$

Théorème : Si $a = b \cdot q + r$, alors $pgcd(b,a) = pgcd(r,b)$.

Exemple : Calculer le $pgcd(220,632)$.

$632 = 220 \cdot 2 + 192$

$220 = 192 \cdot 1 + 28$

$192 = 28 \cdot 6 + 24$

$28 = 24 \cdot 1 + 4$

$24 = 4 \cdot 6 + 0$

On regarde au reste non-nul, donc on a $pgcd(220,632) = 4$.

Algorithme d'exponentiation modulaire

Calculer $b^n \bmod m$, où b et n sont des entiers très grands. Ce qui nous intéresse est le résultat suite à une opération modulo.

$n = n_1 + n_2 + n_3 + ...n_k$, alors

$b^n = b^{n_1+n_2+...+n_k}$

$= b^{n_1} \cdot b^{n_2} \cdot ... \cdot b^{n_k} (\bmod m)$

$= (b^{n_1} \bmod m) \cdot (b^{n_2} \bmod m) \cdot ... \cdot (b^{n_k} \bmod m)$

Exemple : Calculer $1230^{1561} \bmod 645$

On a $1561 = 1500 + 61 = 15 \cdot 100 + 61$ donc

$1230^{1561} = 1230^{15 \cdot 100 + 61}$

$= (1230^{15})^{100} \cdot 1230^{61}$

On a

- $1230^{15} \bmod 645 = 245$
- $(1230^{15})^{100} \equiv 285^{100} \bmod 645 = 600 \pmod{645}$
- $1230^{61} \equiv 405 \pmod{645}$

Donc

- $1230^{1561} \equiv 600 \cdot 405 \pmod{645}$
  $\equiv 480 \pmod{645}$

Application de la théorie des nombres

Théorème 11 : $pgcd(a,b) = s \cdot a + t \cdot b$, pour $s,t \in \mathbb{Z}$.

Exemple : Trouver le $pgcd(91,287)$. Utiliser l'algorithme d'Euclide.

1) $287 = 91 \cdot 3 + 14$

2) $91 = 14 \cdot 6 + 7 \Rightarrow$ On a que le $pgcd(91,287) = 7$

3) $14 = 7 \cdot 2 + 0$

Par 2) on a $7 = 91 - 6 \cdot 14$

Par 1) on a

$$\begin{aligned} 7 &= 6(287 - 3 \cdot 91) \\ &= 91 - 6 \cdot 287 + 18 \cdot 91 \\ &= 19 \cdot 91 + (-6) \cdot 287 \\ &= s \cdot 91 + t \cdot 287 \end{aligned}$$

où $s = 19$ et $t = -6$.

Théorème 12 : Cas général : $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$. L'inverse est faux, sauf si $pgcd(c,m) = 1$.

Exemple :

$$3 \cdot 2 \equiv 5 \cdot 2 \pmod{4}$$

$$6 \equiv 10 \pmod{4}$$

mais $3 \not\equiv 5 \pmod{4}$

Exemple :

$$2 \cdot 7 \equiv 0 \pmod{14}$$

mais $2 \not\equiv 0 \pmod{14}$

et $7 \not\equiv 0 \pmod{14}$

Congruences linéaires

Résoudre $ax \equiv 1 \pmod{m}$.

Définition : b est l'inverse de $a \bmod m$ si $ab \equiv 1 \pmod{m}$.

Notation : $b = a^{-1} \bmod m$, avec $1 \leqslant a^{-1} < m$.

Exemple : On a $2 \cdot 2 = 4 \equiv 1 \pmod{3}$ d'où l'inverse de $2 \bmod 3$ est 2

$\Rightarrow 2^{-1} \equiv 2 \pmod{3}$

Exemple : 3 est l'inverse de $5 \bmod 7$ car $3 \cdot 5 = 15 \equiv 1 \pmod{7}$

$\Rightarrow 5^{-1} \equiv 3 \pmod{7}$ et $3^{-1} \equiv 5 \pmod{7}$

Théorème 13 : Si $pgcd(b,m) = 1$, alors a admet un inverse $a^{-1} \bmod m$

$\Rightarrow a \cdot a^{-1} \equiv 1 \pmod{m}$ et $1 \leqslant a^{-1} < m$.

Exemple : Le nombre 6 n'est pas inversible modulo 9, car $pgcd(6,9) = 3 \neq 1$.

$\Rightarrow$On ne peut pas résoudre $6x \equiv 1 \pmod{9}$.

Exemple : On a $pgcd(4,5) = 1$

$\Rightarrow 4$ est inversible modulo 5, on a $4^{-1} \equiv 4 \pmod{5} \Rightarrow 4 \cdot 4 = 16 \equiv 1 \pmod{5}$.

Exemple : Le nombre 4 est-il inversible modulo 9 ?

On utilise l'algorithme d'Euclide.

1) $9 = 4 \cdot 2 + 1$

2) $4 = 1 \cdot 4$

d'où $pgcd(4,9) = 1$. 4 est inversible modulo 9 par théorème 13.

Exemple : Trouver l'inverse de 4 modulo 9.

$\Rightarrow$ Résoudre $4x \equiv 1 \pmod 9$

Par 1) on a

$$1 = 9 - 2 \cdot 4$$

$$1 = 9 + (-2) \cdot 4$$

$$1 = 9s + 8t$$

où $s = 1$ et $t = -2$.

Ainsi on trouve $t = -2 \equiv 7 \pmod 9$ car $-2 + 9 = 7$ et $4^{-2} \equiv 7 \pmod 7$.

Exemple : Résoudre $55x \equiv 2 \pmod{81}$. Avec l'algorithme d'Euclide, calculer $pgcd(55, 81)$.

1) $81 = 55 \cdot 1 + 26$
2) $55 = 26 \cdot 2 + 3$
3) $26 = 3 \cdot 8 + 2$
4) $3 = 2 \cdot 1 + 1$
5) $2 = 1 \cdot 2 + 0$

Donc, $pgcd(55, 81) \Rightarrow 55$ inversible $\bmod 81$

Trouver $55^{-1} \bmod 81$.

On a : $1 = 3 - 1 \cdot 2$ par 4)
$= 3 - 1 \cdot (26 - 8 \cdot 3)$ par 3)
$= 3 - 2 \cdot 26 + 8 \cdot 3$
$= 9 \cdot 3 - 1 \cdot 26$
$= 9 \cdot (55 - 2 \cdot 26) - 1 \cdot 26$ par 2)
$= 9 \cdot 55 - 18 \cdot 26) - 1 \cdot 26$
$= 9 \cdot 55 - 19 \cdot 26$
$= 9 \cdot 55 - 19 \cdot (81 - 1 \cdot 55)$ par 1)
$= 9 \cdot 55 - 19 \cdot 81 - 19 \cdot 55$
$= \boxed{28} \cdot 55 - 19 \cdot 81$
$= t \cdot 55 + s \cdot 81$ où $t = 28$ et $s = -19$.

Donc, $55^{-1} \equiv 28 \pmod{81}$. En effet, on a $28 \cdot 55 = 1540 \equiv 1 \pmod{81}$.

On obtient $55x \equiv 2 \pmod{81}$

$$55^{-1} \cdot 55x \equiv 55^{-1} \cdot 2 \pmod{81}$$
$$1 \cdot x \equiv 28 \cdot 2 \pmod{81}$$
$$x \equiv 56 \pmod{81}$$

Solution « unique » modulo 81 $\Rightarrow x \equiv 56 \pmod{81}$

Toutes les solutions $x \in \mathbb{Z}$

$x = 56$, $x = 56 + 81 = 137$, $x = 56 + 2 \cdot 81 = 218$, etc.

$x = 56 - 81 = -25$, $x = 56 - 2 \cdot 81 = -106$, etc.

Exemple : Résoudre $2x \equiv 5 \pmod 6$

$pgcd(2, 6) = 2 \neq 1$

$\Rightarrow 2$ n'est pas inversible $\bmod 6$.

$2 \cdot 0 \equiv 0 \pmod 6$, $2 \cdot 1 \equiv 2 \pmod 6$, $2 \cdot 2 = 4 \equiv 4 \pmod 6$, $2 \cdot 3 \equiv 0 \pmod 6$, $2 \cdot 4 \equiv 2 \pmod 6$, $2 \cdot 5 \equiv 4 \pmod 6$.

Donc, $2x \equiv 5 \pmod 6$ n'admet aucune solution.

Exemple : Résoudre $2x \equiv 4 \pmod 6$.

Deux solutions : $x = 2$ et $x = 5$.

Solutions $x \in \mathbb{Z}$:

$x = 2, x = 5, x = 8, x = 11, x = 14, x = 17, ..., x = -4, x = -1, x = -18, x = -7, ...$

Nombres pseudo-premiers

Théorème 14 : Théorème du reste chinois : p est premier si et seulement si $2^{p-1} \equiv 1 \pmod p$ ⟵ faux !

Exemple : $2^{5-1} = 2^4 = 16 \equiv 1 \pmod 5$

Contre-exemple : $n = 341 = 11 \cdot 31$ et $2^{341-1} = 2^{340} \equiv \pmod{341}$.

Crytographie à clé publique

Exemple de cryptographie à clé secrète (ou clé symétrique) :

Crypter : $c = (p + k) \pmod{26}$, ou c est le message codé et k est la clé pour crypter et décripter.
Décrypter : $p = (c - k) \pmod{26}$

Le problème est l'échange de clé, il faut que les deux parties se rencontrent pour se les échanger. Peut être aussi problématique si la clé est compromise, il devient difficile de communiquer une nouvelle clé à distance.

Clé publique

Clé publique notée P_k et clé privée notée S_k.

$$m \xrightarrow[\text{Crypté avec } P_k]{} \{m\}_{P_k} \xrightarrow[\text{Transmission}]{} \{m\}_{P_k} \xrightarrow[\text{Décrypté avec } S_k]{} m$$

Cryptosystème RSA

Cryptosystème à clé publique.

Clé publique (clé pour crypter) : Deux nombres entiers positifs n et e où $n = p \cdot q$, où p et q sont deux grands nombres premiers et e est relativement premier avec $(p - 1)(q - 1)$.

Soit M le message et C le message codé.

Crypter

La fonction pour crypter se résume à :

$C = M^e \bmod n$

Convention : A→00, B→01, ..., Z→25, ␣→26

Exemple : RSA avec $p = 43$, $q = 59$ et $e = 13$, donc $n = 43 \cdot 59 = 2537$.

On a $(p-1)(q-1) = 42 \cdot 58 = 2436$ et $pgcd(13, 2436) = 1 \Rightarrow e = 13$ est relativement premier avec $(p-1)(q-1) = 2436$.

$pgcd(e, (p-1)(q-1))$

Message à coder : STOP

1) Traduire en chiffres : S→18, T→19, O→14, P→15. Donc, le message est 1819 1415 (séparé en blocs de 4 chiffres).
2) Crypter chaque bloc séparément : $M_1 = 1819$ et $M_2 = 1415$.
   $C = M^{13} \bmod 2537$
   $C_1 = M_1^{13} \bmod 2537 \Rightarrow 1819^{13} \bmod 2537 = 2081$
   $C_2 = M_2^{13} \bmod 2537 \Rightarrow 1415^{13} \bmod 2537 = 2182$
3) Message crypté $C = 2081\,2182$

Décrypter

La clé privée ou clé de décryptage :

D =inverse de e modulo $(p-1)(q-1)$

$D = e^{-1} \bmod (p-1)(q-1)$, alors l'algorithme pour décrypter est $M = C^D \bmod n$.

Preuve

Exemple : RSA avec $p = 43$, $q = 59$, $n = 2537$ et $e = 13$.

Trouver l'inverse de $e = 13 \bmod (p-1)(q-1) = 2436$.

Utiliser l'algorithme d'Euclide :

1) $2436 = 13 \cdot 187 + 5$
2) $13 = 5 \cdot 2 + 3$
3) $5 = 3 \cdot 1 + 2$
4) $3 = 2 \cdot 1 + \boxed{1}$
5) $2 = 1 \cdot 2 + 0$

On a $pgcd(13, 2436) = 1$

On trouve $1 = 3 - 1 \cdot 2$ par 4)
$= 3 - 1 \cdot (5 - 13)$ par 3)
$= 2 \cdot 3 - 1 \cdot 5$
$= 2(13 - 2 \cdot 5) - 1 \cdot 5$ par 2)
$= 2 \cdot 13 - 5 \cdot (2436 - 187 \cdot 13)$ par 1)
$= 937 \cdot 13 - 5 \cdot 2436$

s Inverse t

D'où $d = 937 \equiv 13^{-1} (\mathrm{mod}\, 2436)$.

Décrypter le message :

$$\underbrace{2081}_{C_1} \quad \underbrace{2182}_{C_2}$$

$M_1 = C_1^{937} \bmod 2537 \Rightarrow 2081^{937} \bmod 2537 =$ et
$M_2 = C_2^{937} \bmod 2537 \Rightarrow 2182^{937} \bmod 2537 =$

On a $937 = 9 \cdot 100 + 37$

Ainsi $M_1 = 2081^{937} \bmod 2537$

$\equiv (2081^9)^{100} \cdot (2081)^{37} \bmod 2537$

$\equiv (1288)^{100} \cdot 2293 \bmod 2537$

$\equiv (606) \cdot 2293 \bmod 2537$

$\equiv 1819 \bmod 2537$

$M_2 = (2182^9)^{100} \cdot (2182)^{37} \bmod 2537$

$\equiv 825^{100} \cdot 825 \bmod 2537$

$\equiv 1415 \bmod 2537$

D'où $M = 1819 \quad 1415 \Rightarrow$ ST OP