Problème 1. Autour du théorème de Fermat

Partie I - Inverse modulo n

1) Notons que $3 \times (-2) + 7 \times 1 = 1$,

$$3u + 7v = 1 \iff 3(u+2) = 7(-v+1) \iff \left\{ \begin{array}{c} 3(u+2) = 7(-v+1) \\ 7|3(u+2) \text{ (on ajoute cette condition nécessaire)} \end{array} \right.$$

$7|3(u+2)$ et $3 \wedge 7 = 1$ donc d'après le théorème de Gauss $7|(u+2)$.

$$3u + 7v = 1 \iff \exists k \in \mathbb{Z}, \left\{ \begin{array}{c} u = -2 + 7k \\ 3(u+2) = 7(-v+1) \end{array} \right. \iff \exists k \in \mathbb{Z}, \left\{ \begin{array}{c} u = -2 + 7k \\ v = 1 - 3k \end{array} \right. \quad \text{car } 7 \neq 0$$

L'ensemble $\mathcal{S}$ des solutions est donc

$$\boxed{\mathcal{S} = \{(-2 + 7k, 1 - 3k) \mid k \in \mathbb{Z}\}}$$

Comme $3 \times (-2) + 7 \times 1 = 1$ alors $3 \times (-2) \equiv 1\ [7]$. Donc -2 est un inverse modulo 7 de 3.

Pour déterminer tous les inverses modulo 7 de 3, il s'agit de déterminer les entiers u tels que $3u \equiv 1\ [7]$ c'est-à-dire les entiers u tels qu'il existe $v \in \mathbb{Z}$ tel que $3u = 1 + 7v$, et donc d'après la résolution qui précède **les inverses de 3 modulo 7 sont les entiers $-2 + 7k$ où $k \in \mathbb{Z}$**.

2) Par l'absurde supposons qu'il existe $a \in \mathbb{Z}$ tel que $4a \equiv 1\ [6]$. Alors il existe $k \in \mathbb{Z}$ tel que $4a = 1 + 6k$ donc $1 = 4a - 6k$ est pair ce qui est absurde. Donc **4 n'admet pas d'inverse modulo 6**.

3) Soit $a \in \mathbb{Z}$.

$$\begin{aligned} a \text{ admet un inverse modulo } n &\Leftrightarrow \exists a' \in \mathbb{Z} \,/\, aa' \equiv 1\ [n] \\ &\Leftrightarrow \exists (a', k) \in \mathbb{Z}^2 \,/\, aa' - kn = 1 \end{aligned}$$

a admet un inverse modulo $n \Leftrightarrow a \wedge n = 1$ d'après le théorème de Bezout

4) Soit $a \in \mathbb{Z}$ et on suppose $a \wedge n = 1$. On pose a' un inverse de a modulo n.
Soit $x \in \mathbb{Z}$,

$$ax \equiv b\ [n] \Leftrightarrow a'ax \equiv a'b\ [n] \Leftrightarrow x \equiv a'b\ [n].$$

L'implication $\Rightarrow$ est obtenue en multipliant la congruence par a' puis en utilisant $aa' \equiv 1\ [n]$.
L'implication $\Leftarrow$ est obtenue en multipliant la congruence par a et en utilisant $aa' \equiv 1\ [n]$.
L'ensemble solution de l'équation $ax \equiv b\ [n]$ est donc $\{a'b + kn \,/\, k \in \mathbb{Z}\}$.

5) **Application**. On résout (E_1) $3x \equiv 4\ [20]$.

$$(E_1)\ 3x \equiv 4\ [20] \qquad (E_2)\ 12x \equiv 8\ [34].$$

Notons que 7 est un inverse modulo 20 de 3 ($3 \times 7 = 21 \equiv 1\ [20]$).
D'après I-4), **l'ensemble solution de (E_1) est $\{28 + 20k \,/\, k \in \mathbb{Z}\}$**
On résout (E_2) $12x \equiv 8\ [34]$ équivalente à (E_2) $6x \equiv 4\ [17]$. Notons que 3 est un inverse modulo 17 de 6 ($3 \times 6 = 18 \equiv 1\ [17]$).
D'après I-4), **l'ensemble solution de (E_2) est $\{12 + 17k \,/\, k \in \mathbb{Z}\}$**

6) Soit $(a, b) \in \mathbb{Z}^2$. On pose $d = a \wedge n$.
L'équation (E) $ax \equiv b\ [n]$ est équivalente à : $\exists k \in \mathbb{Z} \,/\, ax = b + kn$.

- **Si d ne divise pas b** alors comme d divise a et n, **(E) n'a pas de solution**.
- **Si d divise b**, comme d est le PGCD de a et n alors il divise a et n. Posons alors $(\alpha, \beta, \nu) \in \mathbb{Z}^2$ tel que

$$a = d\alpha \qquad b = d\beta \qquad n = d\nu.$$

Alors, en simplifiant par d,

$$(E) \Leftrightarrow \exists k \in \mathbb{Z} \,/\, \alpha x = \beta + k\nu \Leftrightarrow \alpha x \equiv \beta\ [\nu].$$

On est donc ramené à la question I-4), car $\alpha \wedge \nu = 1$.
L'ensemble solution de l'équation est $\{\alpha'\beta + k\nu \,/\, k \in \mathbb{Z}\}$ où α' est un inverse modulo ν de α.

Partie II - Une autre démonstration du petit théorème de Fermat

Dans cette partie p est un entier premier et $a \in \mathbb{Z}$.
Dans les questions II) 1),2),3),4), on suppose que p ne divise pas a.

1) Soit $k \in [\![1, p-1]\!]$, r_k est le reste de la division euclidienne de ka par p, donc $r_k \in [\![0, p-1]\!]$.

Puis, par l'absurde supposons que $r_k = 0$ alors $p|ka$. Or p est premier et $1 \leqslant k \leqslant p-1$ donc $p \wedge k = 1$ alors d'après le théorème de Gauss, $p|a$, ce qui est absurde par hypothèse.

Par conséquent, $\boxed{r_k \in [\![1, p-1]\!]}$.

2) On a donc défini une application $\begin{array}{rccc} f: & [\![1,p-1]\!] & \to & [\![1,p-1]\!] \\ & k & \mapsto & r_k \end{array}$.

- **Surjectivité de** f. Soit $b \in\in [\![1, p-1]\!]$.
  NB: on note b et pas r_k, sinon cela sous-entend qu'on a déjà trouvé k alors qu'on le cherche.
  On cherche donc $k \in [\![1, p-1]\!]$ tel que $f(k) = b$ alors $ka \equiv b\,[p]$.
  Comme p est premier et p ne divise pas a alors $a \wedge p = 1$ on est donc ramené à l'équation de I-4)dont les solutions sont $a'b + jp$ où $j \in \mathbb{Z}$ et a' est un inverse modulo p de a.
  Quitte à faire la division euclidienne de $a'b$ par p, il existe donc une valeur de $j \in \mathbb{Z}$ tel que $k = a'b + jp \in [\![1, p-1]\!]$. Et on alors $ka \equiv b\,[p]$ donc $f(k) = b$. D'où la surjectivité de f.
- **Injectivité de** f. Soit $(k, k') \in [\![1, p-1]\!]^2$, tel que $f(k) = f(k')$. Alors $ka \equiv k'a\,[p]$ c'est-à-dire $a(k-k') \equiv 0\,[p]$.
  Comme p est premier et p ne divise pas a alors a admet un inverse modulo n, alors d'après I-4), $k - k' = jp$ où $j \in \mathbb{Z}$.
  Comme $0 \leqslant k \leqslant p-1$ et $0 \leqslant k' \leqslant p-1$ alors $-(p-1) \leqslant k - k' \leqslant p-1$, la seule possibilité est $k - k' = 0$ soit $k = k'$.
  L'injectivité est prouvée.

Conclusion : $\boxed{f \text{ est bijective}}$.

3) Comme f est bijective :

$$\{r_k \;/\; k \in [\![1, p-1]\!]\} = f([\![1, p-1]\!]) = [\![1, p-1]\!].$$

Les r_k sont donc une permutation des éléments de $[\![1, p-1]\!]$, par conséquent :

$$\boxed{\prod_{k=1}^{p-1} r_k = \prod_{k=1}^{p-1} k = (p-1)!}.$$

4) Par ailleurs, par définition de r_k, $ka \equiv r_k\,[p]$.
On fait le produit :

$$\prod_{k=1}^{p-1} r_k \equiv \prod_{k=1}^{p-1} ka\,[p] \text{ c'est-à-dire } \prod_{k=1}^{p-1} r_k \equiv a^{p-1}(p-1)!\,[p].$$

En combinant avec II-3), il vient

$$a^{p-1}(p-1)! \equiv (p-1)!\,[p] \quad \text{c'est-à-dire} \quad (a^{p-1}-1)(p-1)! \equiv 0\,[p].$$

Donc $p|(a^{p-1}-1)(p-1)!$ or p premier donc $p \wedge (p-1)! = 1$ donc d'après le théorème de Gauss, $p|(a^{p-1}-1)$.
On a donc comme voulu, retrouvé le petit théorème de Fermat :

$$\boxed{a^{p-1} \equiv 1\,[p] \quad \text{(si } p \text{ ne divise pas } a)}.$$

NB: on peut aussi simplifier $(*)$ $a^{p-1}(p-1)! \equiv (p-1)!\,[p]$ par $(p-1)!$ en multipliant par un inverse de $(p-1)!$ modulo p.
Un tel inverse existe car comme ci-dessus $p \wedge (p-1)! = 1$, notons α cet inverse. En multipliant $(*)$ par α, on obtient

$$a^{p-1}(p-1)!\alpha \equiv (p-1)!\alpha\,[p] \quad \text{c'est-à-dire} \quad a^{p-1} \equiv 1\,[p].$$

5) Soit $a \in \mathbb{Z}$, $a^p - a = a(a^{p-1}-1)$ $(*)$. Par conséquent deux cas de figure :

- si p divise a, alors d'après $(*)$, p divise $a^p - a$
- si p ne divise pas a, d'après II-4) et $(*)$, p divise $a^p - a$.

Dans les deux cas, on a donc comme voulu : $\boxed{a^p \equiv a\,[p].}$.

6) **Applications du petit théorème de Fermat**

-a- Comme 13 est premier et 2 et 3 ne divise pas 13 on a d'après II-4) :

$$2^{12} \equiv 1\,[13] \qquad 3^{12} \equiv 1\,[13].$$

Donc

$$2^{70} = 2^{12\times 5}2^{10} \equiv 2^{10}\,[13] \qquad 3^{70} = 3^{12\times 5}3^{10} \equiv 3^{10}\,[13].$$

En utilisant $2^6 = 64 \equiv -1\,[13]$ et $3^3 = 27 \equiv 1\,[13]$, il vient

$$2^{10} + 3^{10} \equiv -3 + 3 = 0\,[13].$$

Et donc comme voulu, $\boxed{13|2^{70} + 3^{70}}$.

-b- -i- Soit $(m, n) \in \mathbb{Z}^2$. Comme 3 est premier, on peut appliquer le petit théorème de Fermat de II-5)

$$m^3 \equiv m\,[3] \text{ et } n^3 \equiv n\,[3] \quad \text{donc} \quad m^4 \equiv m^2\,[3] \text{ et } n^4 \equiv n^2\,[3]$$

Et donc par opérations sur les congruences, $mn(m^4 - n^4) \equiv mn(m^2 - n^2)\,[3]$.
Or $mn(m^2 - n^2) = m^3n - mn^3 \equiv mn - nm = 0\,[3]$.
On a donc bien $\boxed{3|mn(m^4 - n^4)}$.

On applique le théorème de Fermat de II-5) avec 5 entier premier :

$$m^5 \equiv m\ [5] \text{ et } n^5 \equiv n\ [5].$$

Donc par opérations $mn(m^4-n^4) = m^5n - mn^5 \equiv mn - nm = 0\ [5]$. On a donc bien $\boxed{5|mn(m^4-n^4)}$.

-ii- Enfin, comme $3 \wedge 5 = 1$, de II-6)-a- et 6)-b- il découle $\boxed{15|mn(m^4-n^4)}$.

Partie III - Indicatrice d'Euler

1) Les entiers compris entre 1 et 6 premiers avec 7 sont : 1,2,3,4,5,6. Il y en a 6 donc $\boxed{\varphi(7)=6}$.

Les entiers compris entre 1 et 14 premiers avec 15 sont : 1,2,4,7,8,11,13,14. Il y en a 8 donc $\boxed{\varphi(15)=8}$.

2) Soit p un entier premier et $\alpha \in \mathbb{N}^*$.

Comme p est premier, tous les entiers de $[\![1, p-1]\!]$ sont premiers avec p. Donc $\boxed{\varphi(p) = p-1}$.

Pour le calcul de $\varphi(p^\alpha)$. On va compter les entiers $1 \leqslant a < p^\alpha$ tels que $a \wedge p^\alpha \neq 1$.
Comme p est premier, a est alors nécessairement un multiple de p de la forme bp où $b \in \mathbb{N}^*$. Donc $a = bp < p^\alpha$ donc $b < p^{\alpha-1}$ donc $1 \leqslant b \leqslant p^{\alpha-1}-1$. Il y a donc $p^{\alpha-1}-1$ entiers de $[\![1, p^\alpha - 1]\!]$ non premiers avec p^α. On déduit

$$\varphi(p^\alpha) = (p^\alpha - 1) - p^{\alpha-1} - 1 \quad \text{donc} \quad \boxed{\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}}.$$

3) Soient m et n deux entiers premiers distincts. Pour le calcul de $\varphi(mn)$ on détermine les entiers a tels que $1 \leqslant a < mn$ et $a \wedge (mn) \neq 1$.
Comme m et n sont premiers alors un diviseur supérieur à 2 commun à a et mn est nécessairement m, n ou mn. Donc a est un multiple de m ou un multiple de n.
Il y a $m-1$ multiples de n compris entre 1 et mn exclu : $n, 2n, ..., (m-1)n$.
Il y a $n-1$ multiples de m compris entre 1 et mn exclu : $m, 2m, ..., (n-1)m$.
Comme m et n sont premiers il n'y a pas d'entiers en communs dans les multiples ci-dessus.
Donc $\varphi(mn) = (mn-1) - (m-1) - (n-1) = mn - m - n + 1 = (m-1)(n-1)$.
On m et n sont premiers donc d'après III-2), $\varphi(m) = m-1$ et $\varphi(n) = n-1$.
Finalement, $\boxed{\varphi(mn) = \varphi(m)\varphi(n)}$.
On admet que ce résultat reste vrai si m et n sont deux entiers premiers entre eux.

4) Soit $n \in \mathbb{N}$, on pose sa décomposition en facteurs premiers $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ où les p_i sont des entiers premiers deux à deux distincts et les α_i sont des entiers naturels non nuls. Comme les $p_i^{\alpha_i}$ donc premiers entre eux deux à deux alors d'après le résultat admis de III-3) puis III-2), il vient

$$\varphi(n) = \prod_{i=1}^{N} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{N} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right).$$

On déduit,

$$\begin{aligned}\varphi(n) &= \prod_{i=1}^{N} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^{N} p_i^{\alpha_i} \prod_{i=1}^{N}\left(1 - \frac{1}{p_i}\right)\end{aligned}$$

$$\boxed{\varphi(n) = n\prod_{i=1}^{N}\left(1 - \frac{1}{p_i}\right)}.$$

beginalign*

5) Soit $n \in \mathbb{N}^*$. On pose $A_n = \{k_1, \ldots, k_{\varphi(n)}\}$ l'ensemble des entiers de $[\![1, n-1]\!]$ premiers avec n.
Soit $a \in [\![1, n-1]\!]$ tel que $a \wedge n = 1$. On définit l'application $k_i \in A_n \mapsto r_{k_i}$ où r_{k_i} est le reste de la division euclidienne de ak_i par n.

-a- Soit $k_i \in A_n$.
Comme r_{k_i} est le reste de la division euclidienne de ak_i par n alors $r_{k_i} \in [\![0, n-1]\!]$.
Puis $r_{k_i} \neq 0$, car par l'absurde si $r_{k_i} = 0$ alors $ak_i \equiv 0\ [n]$. Donc $n|ak_i$, or $a \wedge n = 1$ donc d'après le théorème de Gauss $n|k_i$ ce qui est absurde car par définition $k_i \leqslant n$.
Enfin, $r_{k_i} \wedge n = 1$. En effet, comme $a \wedge n = 1$ et $k_i \wedge n = 1$ alors $ak_i \wedge n = 1$ donc d'après la propriété d'Euclide $r_{k_i} \wedge n = 1$.
Bilan : $\boxed{\text{pour tout } k_i \in A_n,\ r_{k_i} \in A_n.}$

On montre comme dans II)2) que l'application $\begin{array}{ccc} A_n & \to & A_n \\ k_i & \mapsto & r_{k_i} \end{array}$ est bijective.

-b- D'une part, comme l'application $\begin{array}{ccc} A_n & \to & A_n \\ k_i & \mapsto & r_{k_i} \end{array}$ est bijective,

$$\prod_{i=1}^{\varphi(n)} r_{k_i} = \prod_{j \in A_n} j = \prod_{i=1}^{\varphi(n)} k_i.$$

D'autre part, on fait le produit des congruences $ak_i \equiv r_{k_i}\ [n]$,

$$\prod_{i=1}^{\varphi(n)} r_{k_i} \equiv \prod_{i=1}^{\varphi(n)} ak_i\ [n] \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} k_i\ [n].$$

En combinant ces deux résultats, il vient :

$$\prod_{i=1}^{\varphi(n)} k_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} k_i\ [n] \quad \text{c'est-à-dire} \quad \prod_{i=1}^{\varphi(n)} k_i \left(a^{\varphi(n)} - 1\right) \equiv 0\ [n].$$

Donc n divise $\prod_{i=1}^{\varphi(n)} k_i \left(a^{\varphi(n)} - 1\right)$. Or n est premier avec chacun des k_i donc n est premier avec leur produit et donc d'après le théorème de Gauss :

$$n | a^{\varphi(n)} - 1 \quad \text{c'est-à-dire} \quad \boxed{a^{\varphi(n)} \equiv 1\ [n]}.$$