Partie A :

1. Montrer que 6×3 est congru à 6×7 modulo 8. Est-ce que 3 et 7 sont congrus modulo 8 ?
2. Soient a, b, k et n des entiers avec $k\,a \equiv k\,b$ modulo n et n premier avec k. Montrer que a est congru à b modulo n

Partie B :

On cherche à démontrer que « si p est un nombre premier et si n est un entier non multiple de p, alors n^{p-1} est congru à 1 modulo p »
On prend donc p un nombre premier et n un entier non multiple de p. On réalise la division euclidienne de n, $2\,n$, $3\,n$, ... ,$(p-1)\,n$ par p. On note respectivement les reste r_1, r_2,...,r_{p-1}.

1. Déterminer r_1, ..., r_{10} pour $n = 24$ et $p = 11$
2. On prend deux entiers a et b distincts compris entre 1 et $p - 1$.

Montrer que $b\,n - a\,n$ n'est pas multiple de p et en déduire que r_a est différent de r_b.

3. Montrer que $\{r_1, ..., r_{p-1}\} = \{1 ; 2 ; ... ; p-1\}$
4. Montrer que $n \times 2\,n \times ... \times (p-1)\,n$ est congru à $r_1 \times r_2 \times ... \times r_{p-1}$ modulo p.
5. Conclure que n^{p-1} est congru à 1 modulo p

Partie C :

En utilisant le théorème démontré précédemment, et en séparant les cas où p divise n et ceux où p ne divise pas n, montrer que « si p est un nombre premier et si n est un entier alors n^p est congru à n modulo p » (Petit théorème de Fermat)

Partie D :

En utilisant le petit théorème de Fermat, trouver le reste de la division euclidienne de $14^{20} + 9^{33}$ par 17.

Partie E :

1. *a.* L'entier 341 est-il premier ? Justifier
   b. Démontrer que 2^{340} est congru à 1 modulo 341.
   c. Conclure

2. *a.* L'entier 561 est-il premier ? Justifier
   b. Soit n un entier premier avec 561. Avec le théorème de Fermat montrer que n^{560} est congru à 1 modulo 3; n^{560} est congru à 1 modulo 11; n^{560} est congru à 1 modulo 17. En déduire que n^{560} est congru à 1 modulo 561.
   c. Conclure.

CORRECTION

Partie A :

1. $6 \times 7 - 6 \times 3 = 6 \times (7 - 3) = 6 \times 4 = 8 \times 3$ donc $6 \times 7 - 6 \times 3 \equiv 0$ modulo 8 soit $6 \times 7 \equiv 6 \times 3$ modulo 8.
   $7 - 3 = 4$ et 8 ne divise pas 4 donc 3 et 7 ne sont pas congrus modulo 8 ?
2. n divise $k\,a - k\,b$ soit n divise $k\,(a - b)$ or n est premier avec k donc d'après le théorème de Gauss, n divise $a - b$ donc a est congru à b modulo n.

Partie B :

On cherche à démontrer que « si p est un nombre premier et si n est un entier non multiple de p, alors n^{p-1} est congru à 1 modulo p »
On prend donc p un nombre premier et n un entier non multiple de p. On réalise la division euclidienne de n, $2\,n$, $3\,n$, ... ,$(p-1)\,n$ par p. On note respectivement les reste r_1, r_2,...,r_{p-1}.

1. Si $n = 24$ et $p = 11$, $n = 2\,p + 2$ et $0 \leq 2 < p$ donc $r_1 = 2$

$2\,n = 4\,p + 4$ et $0 \leq 4 < p$ donc $r_2 = 4$ — $3\,n = 6\,p + 6$ et $0 \leq 6 < p$ donc $r_3 = 6$ — $4\,n = 8\,p + 8$ et $0 \leq 8 < p$ donc $r_4 = 8$
$5\,n = 10\,p + 10$ et $0 \leq 10 < p$ donc $r_5 = 10$ — $6\,n = 13\,p + 1$ et $0 \leq 1 < p$ donc $r_6 = 1$
$7\,n = 15\,p + 3$ et $0 \leq 3 < p$ donc $r_7 = 3$ — $8\,n = 17\,p + 5$ et $0 \leq 5 < p$ donc $r_8 = 5$
$9\,n = 19\,p + 7$ et $0 \leq 7 < p$ donc $r_9 = 7$ — $10\,n = 21\,p + 9$ et $0 \leq 9 < p$ donc $r_{10} = 9$

2. p est un nombre premier et n est un entier non multiple de p donc n est premier avec p
   Si p divise $b\,n - a\,n = (b - a)\,n$, comme n est premier avec p alors (d'après la partie A) p divise $b - a$
   or $0 \leq a < p$ donc $-p < -a \leq 0$ et $0 < b < p$ donc $-p < b - a < p$
   Le seul multiple de p strictement compris entre $-p$ et p est 0 donc $b - a = 0$ donc $a = b$.
   or si $a = b$ alors $r_a = r_b$
   a et b sont compris entre 1 et $p - 1$ alors $a = r_a$ et $b = r_b$
   a et b sont distincts donc p ne divise pas $b\,n - a\,n$

Si $r_a = r_b$ alors p divise $b - a$ donc p divise $b\,n - a\,n$ ce qui est faux (voir ci-dessus) donc l'hypothèse $r_a = r_b$ est fausse donc $r_a \neq r_b$.

3. r_1 est le reste de la division de n par p or n est un entier non multiple de p donc $1 \leq r_1 \leq p - 1$
   On prend deux entiers a et b distincts compris entre 1 et $p - 1$, r_a est différent de r_b.
   p est un nombre premier, donc est premier avec a, il l'est aussi avec n donc avec $n\,a$ donc $r_a \neq 0$ donc $1 \leq r_a \leq p - 1$
   On a donc $p - 1$ restes deux à deux distincts compris entre 1 et $p - 1$ donc $\{r_1, ..., r_{p-1}\} = \{1 ; 2 ; ... ; p-1\}$

4. $n \equiv r_1$ modulo p $\quad 2\,n \equiv r_2$ modulo p $\quad 3\,n \equiv r_3$ modulo p …. et $\quad (p-1)\,n \equiv r_{p-1}$ modulo p
donc en effectuant le produit terme à terme : $n \times 2\,n \times ... \times (p-1)\,n \equiv r_1 \times r_2 \times ... \times r_{p-1}$ modulo p.

5. $\{r_1, ..., r_{p-1}\} = \{1 ; 2 ; ... ; p-1\}$ donc en réordonnant : $r_1 \times r_2 \times ... \times r_{p-1} = 1 \times 2 \times \ldots \times (p-1) = (p-1)\,!$
$n \times 2\,n \times ... \times (p-1)\,n \equiv r_1 \times r_2 \times ... \times r_{p-1}$ modulo $p \Leftrightarrow n^{p-1} \times (p-1)\,! \equiv (p-1)\,!$ modulo p.
p est un nombre premier donc p est premier avec $1 ; 2 ; \ldots p-1$ donc p est premier avec $(p-1)\,!$ donc d'après la question 2. de la partie A, $n^{p-1} \equiv 1$ modulo p.

Partie C :
Si p est un nombre premier et p divise n alors $n \equiv 0$ modulo p donc $n^p \equiv 0$ modulo p donc $n^p \equiv n$ modulo p

Si p est un nombre premier et p ne divise pas n (donc est premier avec n) alors $n^{p-1} \equiv 1$ modulo p donc en multipliant par n :
$n^p \equiv n$ modulo p
Dans tous les cas, si p est un nombre premier et si n est un entier alors n^p est congru à n modulo p

Partie D :
14 est premier avec 17 donc $14^{16} \equiv 1$ modulo 17 donc $14^{20} \equiv 14^4$ modulo 17 soit $14^{20} \equiv 13$ modulo 17
9 est premier avec 17 donc $9^{16} \equiv 1$ modulo 17 donc $9^{32} \equiv 1$ modulo 17 donc $9^{33} \equiv 9$ modulo 17
donc par addition membre à membre : $14^{20} + 9^{33} \equiv 13 + 9$ modulo 17 soit $14^{20} + 9^{33} \equiv 5$ modulo 17
Le reste de la division euclidienne de $14^{20} + 9^{33}$ par 17 est 5.

Partie E :
1. *a.* $341 = 11 \times 31$ donc 341 n'est pas premier.

b. $2^{10} = 1024 = 341 \times 3 + 1$ donc $2^{10} \equiv 1$ modulo 341 donc en élevant à la puissance 34 : $2^{340} \equiv 1$ modulo 341.

c. $2^{340} \equiv 1$ modulo 341 donc $2^{341} \equiv 2$ modulo 341
La réciproque du petit théorème de Fermat est fausse : si n^p est congru à n modulo p on ne peut pas conclure que p est premier (exemple $n = 2$ et $p = 341$)

2. *a.* $561 = 3 \times 11 \times 17$ donc 561 n'est pas un nombre premier
b. Soit n un entier premier avec 561 donc n est premier avec 3 ; 11 ; 17
3 est un nombre premier, n un entier premier avec 3 donc $n^2 \equiv 1$ modulo 3 donc en élevant à la puissance 280 alors $n^{560} \equiv 1$ modulo 3
11 est un nombre premier, n un entier premier avec 11 donc $n^{10} \equiv 1$ modulo 11 donc en élevant à la puissance 28 alors $n^{560} \equiv 1$ modulo 11
17 est un nombre premier, n un entier premier avec 17 donc $n^{16} \equiv 1$ modulo 17 donc en élevant à la puissance 35 alors $n^{560} \equiv 1$ modulo 17

3 et 11 sont premiers entre eux et 3 et 11 divisent $n^{560} - 1$ donc 3×11 divise $n^{560} - 1$
3×11 et 17 sont premiers entre eux et 3×11 et 17 divisent $n^{560} - 1$ donc $3 \times 11 \times 17$ divise $n^{560} - 1$
$n^{560} - 1 \equiv 0$ modulo 561 soit $n^{560} \equiv 1$ modulo 561.

c. Il existe des nombres p non premiers tels que si n est premier avec p, alors $n^{p-1} \equiv 1$ modulo p