

## Correction des exercices sur le chapitre II

### Exercice 1

- 1) On a  $1823 \equiv 5 \pmod{18}$ . D'après le théorème d'Euler, puisque 5 est premier avec 18, on a  $5^{\varphi(18)} \equiv 1 \pmod{18}$  i.e.  $5^6 \equiv 1 \pmod{18}$ . On a  $242 \equiv 2 \pmod{6}$ , d'où l'on déduit que l'on a

$$1823^{242} \equiv 5^{242} \equiv 25 \equiv 7 \pmod{18}.$$

Le reste cherché est donc 7.

- 2) On a la congruence  $2222 \equiv 2 \pmod{20}$ . Parce que 2 n'est pas premier avec 20, la méthode précédente ne s'applique pas. On peut procéder comme suit en étudiant la suite des puissances de 2 modulo 20. Soit  $r_n$  le reste de la division euclidienne de  $2^n$  par 20. On vérifie que pour tout  $n \geq 2$ , on a  $r_n = r_{n+4}$  ; en effet, on démontre par récurrence que pour tout  $n \geq 2$ , on a  $r_n \in \{4, 8, 16, 12\}$ , ce qui entraîne notre assertion. On en déduit que l'on a  $r_{321} = r_5$ , d'où

$$2222^{321} \equiv 12 \pmod{20},$$

et 12 est le reste cherché.

- 3.1) On a  $10^4 \equiv 4 \pmod{7}$ . D'après le petit théorème de Fermat, on a  $10^6 \equiv 1 \pmod{7}$ , d'où  $10^{6n} \equiv 1 \pmod{7}$ , puis le résultat.
- 3.2) On a  $2^6 \equiv 1 \pmod{9}$ , d'où  $2^{6n+2} \equiv 4 \pmod{9}$ . On a ainsi  $2^{6n+2} \equiv 4 \pmod{18}$ . La congruence  $2^{18} \equiv 1 \pmod{19}$  entraîne alors  $2^{2^{6n+2}} + 3 \equiv 0 \pmod{19}$ .
- 4.1) Posons  $n = 4k + 3$  où  $k \in \mathbb{N}$ . On a  $2^4 \equiv 1 \pmod{5}$ , d'où  $2^{4k} \equiv 1 \pmod{5}$ . On a  $2^3 \equiv 3 \pmod{5}$ , d'où  $u_n \equiv 0 \pmod{5}$ .
- 4.2) Posons  $n = 12k + 4$  où  $k \in \mathbb{N}$ . On a  $2^{12} \equiv 1 \pmod{13}$ , d'où  $2^{12k} \equiv 1 \pmod{13}$ . La congruence  $2^4 \equiv 3 \pmod{13}$  implique alors le résultat.
- 4.3) On a  $2^6 \equiv -1 \pmod{65}$ , d'où  $2^{12} \equiv 1 \pmod{65}$ ,  $2^{n+12} \equiv 2^n \pmod{65}$ , puis

$$u_{n+12} \equiv u_n \pmod{65}.$$

- 4.4) On déduit de la question précédente, en considérant les congruences de  $n$  modulo 12, que le reste de la division euclidienne de  $u_n$  par 65 est l'un des entiers

$$1, 5, 13, 29, 30, 46, 54, 58, 60, 61, 63, 64.$$

Il n'est pas nul, d'où l'assertion.

### Exercice 2

Posons  $N = 4(p_1 \cdots p_k)^2 + 1$ . On a  $N \geq 2$  et  $N$  est la somme de deux carrés. Compte tenu de l'indication de l'énoncé,  $N$  est donc divisible par un nombre premier  $q$  congru à 1 modulo 4. Puisque  $q$  divise le produit  $p_1 \cdots p_k$ , on en déduit que  $q$  divise 1, d'où une contradiction.

### Exercice 3

Pour  $p = 3$ , les entiers  $R_n$  avec  $n$  multiple de 3 conviennent. Supposons  $p \geq 7$ . On a alors  $10^{p-1} \equiv 1 \pmod{p}$ , d'où pour tout  $k \in \mathbb{N}$ ,

$$10^{k(p-1)} \equiv 1 \pmod{p}.$$

Parce que  $p \neq 3$ , on obtient

$$R_{k(p-1)} = \frac{10^{k(p-1)} - 1}{9} \equiv 0 \pmod{p},$$

d'où le résultat. Notons que  $R_n$  n'est pas multiple de 5 si  $n \geq 1$ , car on a  $9R_n = 10^n - 1$ ,

### Exercice 4

Soit  $q$  un diviseur premier, distinct de 3, de  $2^p + 1$ . On a

$$2^{2p} \equiv 1 \pmod{q}.$$

Soit  $d$  l'ordre multiplicatif de 2 modulo  $q$  ( $q$  est impair). Il divise  $2p$ , d'où  $d = 1, 2, p, 2p$ . On a  $d \neq 1$ . Par ailleurs, on a  $d \neq 2$  car  $q \neq 3$ . Si  $d = p$ , on obtient  $2^p \equiv 1 \pmod{q}$ , ce qui entraîne  $q = 2$  et une contradiction. On a donc  $d = 2p$ . On a  $2^{q-1} \equiv 1 \pmod{q}$ , donc  $d$  divise  $q - 1$ , d'où  $q \equiv 1 \pmod{2p}$ .

### Exercice 5

Soit  $d$  l'ordre multiplicatif de 2 modulo  $p$ . L'entier  $d$  divise  $m$  et  $p - 1$ . Il existe  $a$  et  $h$  dans  $\mathbb{N}$  tels que l'on ait  $2^d = 1 + ap$  et  $p - 1 = dh$ . On a ainsi

$$2^{p-1} = 2^{dh} = (1 + ap)^h \equiv 1 + ahp \pmod{p^2}.$$

D'après l'hypothèse faite,  $p$  divise donc  $a$ . Par suite, on a  $2^d \equiv 1 \pmod{p^2}$ , ce qui implique le résultat

### Exercice 6

- 1) Il existe un entier  $k$  tel que l'on ait  $t = 1 + k\varphi(n)$ . Soit  $a$  un entier relatif. Compte tenu de l'égalité  $\varphi(n) = (p-1)(q-1)$ , on obtient

$$a^t = a \left( a^{(p-1)(q-1)} \right)^k = a \left( a^{p-1} \right)^{(q-1)k}.$$

Si  $p$  ne divise pas  $a$ , on a  $a^{p-1} \equiv 1 \pmod{p}$ , d'où l'on déduit que  $a^t \equiv a \pmod{p}$ . Si  $p$  divise  $a$ , cette congruence est aussi vérifiée. De même, on a  $a^t \equiv a \pmod{q}$ . Puisque  $p$  et  $q$  sont distincts,  $n$  divise donc  $a^t - a$ .

- 2) Supposons  $n$  et  $\varphi(n)$  connus. Il s'agit d'expliciter  $p$  et  $q$ . On a

$$n = pq \quad \text{et} \quad p + q = n - \varphi(n) + 1.$$

Il en résulte que  $p$  et  $q$  sont les racines du polynôme

$$X^2 - (n - \varphi(n) + 1)X + n \in \mathbb{Z}[X].$$

On obtient ainsi  $p$  et  $q$ . Inversement, si  $p$  et  $q$  sont connus,  $\varphi(n)$  l'est aussi car on a  $\varphi(n) = (p-1)(q-1)$ .

### Exercice 7

- 1) Notons

$$n = \prod_{i=1}^t p_i^{n_i},$$

la décomposition de  $n$  en produit de facteurs premiers. Le nombre de diviseurs de  $p_i^{n_i}$  est  $n_i + 1$ . Il en résulte que l'on a

$$d(n) = \prod_{i=1}^t (n_i + 1).$$

- 2) L'entier  $n$  est un carré si et seulement si tous les exposants  $n_i$  sont pairs, ce qui signifie que  $d(n)$  est impair (question 1).  
 3) On vérifie que l'ensemble des entiers  $n \leq 30$  vérifiant l'égalité  $d(n) = \varphi(n)$  est

$$\{1, 3, 8, 10, 18, 24, 30\}.$$

### Exercice 8

- 1) Posons  $N = a^n - 1$  et notons  $d$  l'ordre de  $a$  modulo  $N$ . On a  $a^n \equiv 1 \pmod{N}$ , donc  $d$  divise  $n$ . Par ailleurs, on a  $a^d \equiv 1 \pmod{N}$  i.e.  $a^n - 1$  divise  $a^d - 1$ . En particulier, on a  $n \leq d$ , d'où  $n = d$ .  
 2) L'entier  $a$  est premier avec  $N$ . On a donc  $a^{\varphi(N)} \equiv 1 \pmod{N}$  (théorème d'Euler). D'après la question précédente, cela entraîne que  $n$  divise  $\varphi(N)$ .

**Exercice 9**

On a les égalités

$$(1) \quad n - 1 = (q - 1)p + (p - 1) \quad \text{et} \quad n - 1 = (p - 1)q + (q - 1).$$

Par suite, on a

$$2^{n-1} \equiv 2^{p-1} \pmod{q} \quad \text{et} \quad 2^{n-1} \equiv 2^{q-1} \pmod{p}.$$

Supposons  $2^{n-1} \equiv 1 \pmod{n}$ . D'après les congruences précédentes, on a alors

$$2^{p-1} \equiv 1 \pmod{q} \quad \text{et} \quad 2^{q-1} \equiv 1 \pmod{p}.$$

Puisque l'on a  $2^{p-1} \equiv 1 \pmod{p}$  et  $2^{q-1} \equiv 1 \pmod{q}$ , on obtient

$$2^{p-1} \equiv 1 \pmod{n} \quad \text{et} \quad 2^{q-1} \equiv 1 \pmod{n}.$$

Ainsi,  $n$  divise le pgcd de  $2^{p-1} - 1$  et  $2^{q-1} - 1$ , qui n'est autre que  $2^d - 1$  (cf. la démonstration du lemme 2.9).

Inversement, si  $2^d \equiv 1 \pmod{n}$ , on a  $2^{p-1} \equiv 1 \pmod{n}$  et  $2^{q-1} \equiv 1 \pmod{n}$ . On déduit alors de la première égalité de (1) la congruence  $2^{n-1} \equiv 1 \pmod{n}$ , d'où le résultat.

**Exercice 10**

On a l'égalité

$$a^{2^s t} - 1 = (a^t - 1) \prod_{i=0}^{s-1} (a^{2^i t} + 1).$$

En effet, cette formule est vraie si  $s = 0$  (un produit vide vaut 1). Si on la suppose vérifiée pour  $s \in \mathbb{N}$ , alors elle l'est aussi pour  $s + 1$ , vu que l'on a

$$a^{2^{s+1}t} - 1 = (a^{2^s t})^2 - 1.$$

D'après le petit théorème de Fermat,  $p$  divise  $a^{p-1} - 1$ , d'où l'assertion.

**Exercice 11**

Supposons que  $n$  ne soit pas premier. Il existe alors un nombre premier  $p \leq \sqrt{n}$  qui divise  $n$ . On a  $q > p - 1$ , en particulier  $q$  est premier avec  $p - 1$ . Il existe donc un entier  $u \geq 1$  tel que l'on ait

$$uq \equiv 1 \pmod{p-1}$$

(cf. l'alinéa 5 des exemples 2.1). D'après la congruence  $a^{n-1} \equiv 1 \pmod{n}$ ,  $p$  ne divise pas  $a$ , d'où  $a \equiv a^{uq} \pmod{p}$ . On obtient ainsi

$$a^{\frac{n-1}{q}} \equiv a^{uq \frac{(n-1)}{q}} = a^{u(n-1)} \equiv 1 \pmod{p}.$$

Cela contredit le fait que les entiers  $a^{\frac{n-1}{q}} - 1$  et  $n$  sont premiers entre eux, d'où le résultat.

### Exercice 12

1) On a

$$(1) \quad N_p = 1 + p + \cdots + p^{p-1}.$$

Par suite,  $N_p$  est un entier naturel.

2) Pour tout  $k \geq 1$ , on a  $p^k - p = p(p^{k-1} - 1)$ . L'entier  $p^{k-1} - 1$  est divisible par  $p - 1$ . Ainsi  $p$  et  $p - 1$  divisent  $p^k - p$ . Les entiers  $p$  et  $p - 1$  sont premiers entre eux, d'où la congruence annoncée.

3) On déduit de (1) et de la question précédente, que l'on a

$$N_p \equiv 1 + p(p - 1) \equiv 1 \pmod{(p^2 - p)}.$$

4.1) Il existe  $k \in \mathbb{N}$  tel que  $N_p = 1 + k(p^2 - p)$ . Ainsi  $\ell$  ne divise pas  $p^2 - p$ , sinon  $\ell$  diviserait  $N_p - k(p^2 - p)$  qui vaut 1.

4.2) De l'égalité

$$(p - 1)N_p = p^p - 1,$$

on déduit que l'on a  $p^p \equiv 1 \pmod{\ell}$ . L'ordre  $d$  de  $p$  modulo  $\ell$  divise donc  $p$ . On a  $d \neq 1$  car  $\ell$  ne divise pas  $p - 1$ , d'où  $d = p$ . Par ailleurs, on a  $\ell \neq p$ . D'après le petit théorème de Fermat, on a donc  $p^{\ell-1} \equiv 1 \pmod{\ell}$ . Il en résulte que  $p$  divise  $\ell - 1$ .

---