Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Travaux dirigés
Alain Kraus

Correction des exercices - Chapitre II

Tests et critères de primalité

Exercice 1

Supposons que p^r soit pseudo-premier en base a. On a $a^{p^r-1} \equiv 1$ mod. p^r autrement dit $a^{p^r} \equiv a$ mod. p^r. On a donc $a^{p-1} \equiv a^{p^r(p-1)}$ mod. p^r. Soit φ la fonction indicatrice d'Euler. On a $\varphi(p^r) = p^{r-1}(p-1)$ et $a^{\varphi(p^r)} \equiv 1$ mod. p^r, d'où $a^{p-1} \equiv 1$ mod. p^r. Inversement, supposons $a^{p-1} \equiv 1$ mod. p^r. Parce que $p-1$ divise $p^r - 1$, en élevant les deux membres de cette congruence à une puissance convenable, on en déduit que l'on a $a^{p^r-1} \equiv 1$ mod. p^r. L'entier p^r est composé car $r \geq 2$, d'où le résultat.

Exercice 2

1) On a démontré dans le cours que 341 est pseudo-premier et n'est pas pseudo-premier d'Euler (voir les remarques 2.2). En particulier, n n'est pas pseudo-premier fort (prop. 2.4) ; on peut aussi remarquer que l'on a $340 = 2^2.85$ et avec les notations du cours, on a donc $s = 2$ et $t = 85$. On vérifie que l'on a les congruences

$$2^t \equiv 32 \text{ mod. } 341 \quad \text{et} \quad 2^{2t} \equiv 1 \text{ mod. } 341.$$

Par suite, n n'est pas pseudo-premier fort (déf. 2.6).

2) Posons $n = 561$. On a $n = 3 \times 11 \times 17$ et $\frac{n-1}{2} = 280$. On a $2^{280} \equiv 1$ mod. 3 et d'après le petit théorème de Fermat, on obtient

$$2^{280} \equiv 1 \text{ mod. } 11.$$

Par ailleurs, on a $280 \equiv 8$ mod. 16, d'où $2^{280} \equiv 2^8 \equiv 1$ mod. 17. On en déduit que l'on a

$$2^{\frac{n-1}{2}} \equiv 1 \text{ mod. } n.$$

On a $561 \equiv 1$ mod. 8, d'où $\left(\frac{2}{n}\right) = 1$ et le résultat.

3) Supposons $3p$ pseudo-premier. On a alors $2^{3p-1} \equiv 1$ mod. $3p$. En particulier, on a

$$2^{3p-1} = 2^{3(p-1)+2} \equiv 1 \text{ mod. } p.$$

Supposons $p \geq 3$. On a $2^{p-1} \equiv 1$ mod. p, d'où $4 \equiv 1$ mod. p, puis $p = 3$. On a $2^5 \not\equiv 1$ mod. 6 et $2^8 \not\equiv 1$ mod. 9, d'où l'assertion.

Exercice 3 (Puissances dans un groupe cyclique)

1) Considérons l'homomorphisme de groupes $\psi : G \to G$ défini par $\psi(x) = x^k$. Vérifions que son noyau est d'ordre d. Soit x un élément de $\mathrm{Ker}(\psi)$. On a $x^k = e$ et $x^n = e$, d'où en utilisant le théorème de Bézout, $x^d = e$. On en déduit que les éléments de $\mathrm{Ker}(\psi)$ sont les éléments $x \in G$ pour lesquels on a $x^d = e$. Puisque G est cyclique, on a donc $|\mathrm{Ker}(\psi)| = d$ et l'ordre de l'image de ψ est n/d. Il en résulte que a est dans l'image de ψ si et seulement si $a^{\frac{n}{d}} = e$, d'où l'assertion.

2) Si $x \in G$ vérifie l'égalité $x^k = a$, on a $(xx_0^{-1})^k = e$, d'où $x = x_0 z$ avec $z^k = e$, et comme on l'a constaté ci-dessus, on a alors $z^d = e$. Inversement, pour tout $z \in G$ tel que $z^d = e$, on a $(x_0 z)^k = a$ car d divise k, d'où l'ensemble des solutions annoncé. Par ailleurs, G étant cyclique, il y a exactement d éléments $z \in G$ tels que $z^d = e$. Cela établit le résultat.

Exercice 4

1) Supposons n pseudo-premier fort en base a. Vérifions que $a^t \equiv \pm 1$ mod. n. Supposons $a^t \not\equiv 1$ mod. n. Il existe alors un entier i tel que l'on ait

$$a^{2^i t} \equiv -1 \text{ mod. } n \quad \text{avec} \quad 0 \leq i \leq s-1.$$

Si l'on a $i \geq 1$, on obtient

$$a^{2^i t} = \left(a^{2^{i-1} t}\right)^2 \equiv -1 \text{ mod. } n.$$

Pour tout diviseur premier p de n, -1 est donc un carré modulo p, ce qui contredit l'existence d'un diviseur premier de n congru à 3 modulo 4. Par suite, on a $i = 0$, d'où $a^t \equiv -1$ mod. n et l'assertion.
Inversement, si $a^t \equiv \pm 1$ mod. n, par définition n est pseudo-premier fort en base a.

2.1) Vérifions qu'il y a une unique solution, à savoir $x = 1$. Le groupe $\left(\mathbb{Z}/p_i\mathbb{Z}\right)^*$ étant cyclique, le nombre de solutions de l'équation $x^t = 1$ dans $\left(\mathbb{Z}/p_i\mathbb{Z}\right)^*$ est le plus grand commun diviseur de t et $p_i - 1$ (exercice 3). Vérifions que l'on a

$$\mathrm{pgcd}(t, p_i - 1) = 1.$$

Soit ℓ un diviseur premier de t. Alors, ℓ divise $n-1$, donc ℓ ne divise pas n. Puisque ℓ est impair, il en résulte que l'on a $\ell > p_k$. Par suite, ℓ ne divise pas $p_i - 1$, d'où l'assertion.

2.2) Les groupes $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ et $\prod\left(\mathbb{Z}/p_i\mathbb{Z}\right)^*$ étant isomorphes (théorème chinois), on déduit de la question précédente que l'ensemble cherché est $\{1\}$.

2.3) C'est le singleton $\{n-1\}$. En effet, supposons n pseudo-premier fort en base a. Puisque n est divisible par 3, n possède en particulier un diviseur premier congru à 3 modulo

4. D'après la première question, on a donc $a^t \equiv \pm 1$ mod. n. Si $a^t \equiv 1$ mod. n, on obtient $a \equiv 1$ mod. n (question 2.2), ce qui contredit les inégalités $1 < a < n$. On a donc $a^t \equiv -1$ mod. n. Puisque t est impair, cela implique $a \equiv -1$ mod. n (*loc. cit.*), d'où l'égalité $a = n - 1$.
Inversement, on a $(n-1)^t \equiv -1$ mod. n, donc n est pseudo-premier fort en base $n-1$, d'où le résultat.

Exercice 5

1) Le résultat est vrai si $p = 2$. On supposera donc $p \geq 3$.
Supposons $2^{n-1} \equiv 1$ mod. n. L'entier n est impair. Soit d l'ordre de 2 modulo n. On a $2^{2p} \equiv 1$ mod. n, donc d divise $2p$. On en déduit que p divise d, sinon d divise 2 ce qui n'est pas. Par ailleurs, on a $2^{\varphi(n)} \equiv 1$ mod. n. Par suite, p divise $\varphi(n)$ (car d divise $\varphi(n)$). On a $\varphi(n) \leq n - 1$, d'où $\varphi(n) = p$ ou $2p$. Or $\varphi(n)$ est pair, donc $\varphi(n) = 2p = n - 1$, ce qui prouve que n est premier. L'implication réciproque résulte du petit théorème de Fermat.
2) Supposons $2^{n-1} \equiv 1$ mod. n. Soit d l'ordre multiplicatif de 2 modulo n. L'entier d divise $n - 1 = hp$. La condition $2^h \not\equiv 1$ mod. n entraîne que d ne divise pas h. D'après le théorème de Gauss, on en déduit que p divise d : si p ne divise pas d, d et p sont premiers entre eux. Puisque d divise $\varphi(n)$ (théorème d'Euler), p divise $\varphi(n)$. Soit $n = p_1^{n_1} \cdots p_r^{n_r}$ la décomposition de n en facteurs premiers. On a

$$\varphi(n) = p_1^{n_1-1} \cdots p_r^{n_r-1}(p_1 - 1) \cdots (p_r - 1).$$

Par hypothèse, p divise $n - 1$, donc il ne divise pas n, ainsi il existe i tel que $p_i \equiv 1$ mod. p. Posons $n = p_i m$. Vérifions que l'on a $m = 1$, ce qui prouvera que n est premier. On a $m \equiv 1$ mod. p car tel est le cas de p_i et n. Posons $p_i = up + 1$ et $m = vp + 1$ où $u, v \in \mathbb{N}$. On a l'égalité $hp + 1 = (up + 1)(vp + 1)$, d'où $h = uvp + u + v$. L'inégalité $h < p$ entraîne alors $v = 0$ et l'assertion.
Inversement, si $n \geq 3$ est premier, on a $2^{n-1} \equiv 1$ mod. n, d'où le résultat.

Exercice 6

1) Supposons n pseudo-premier. Cela signifie que n est un entier composé et que l'on a $2^{n-1} \equiv 1$ mod. n. L'entier M_n est donc composé. On a $2^{n-1} - 1 = \frac{M_n - 1}{2}$. On en déduit que $M_n = 2^n - 1$ divise $2^{\frac{M_n-1}{2}} - 1$. En particulier, M_n divise $2^{M_n-1} - 1$, d'où l'assertion.
2) Posons $n = 2p + 1$.
Supposons que n divise M_p. Dans ce cas, on a les congruences $2^{n-1} = 2^{2p} \equiv 1$ mod. n, et l'on déduit de l'exercice 5 que n est premier.
Inversement, supposons n premier. Parce que $p \equiv 3$ mod. 4 on a $n \equiv 7$ mod. 8, et 2 est donc un carré modulo n. D'après le critère d'Euler, on a $2^{\frac{n-1}{2}} \equiv \left(\frac{2}{n}\right)$ mod. n, d'où le fait que n divise M_p.

Exercice 7 (Nombres de Carmichael)

1) L'implication $(i) \Longrightarrow (ii)$ est immédiate.

Démontrons l'implication $(ii) \Longrightarrow (iii)$: vérifions que n est sans facteurs carrés. Supposons le contraire. Il existe alors un nombre premier p, un entier $r \geq 2$ et un entier q, non divisible par p, tels que l'on ait $n = p^r q$. Le groupe $\left(\mathbb{Z}/p^r\mathbb{Z}\right)^*$ est d'ordre $p^{r-1}(p-1)$, qui est divisible par p. D'après le théorème de Cauchy pour les groupes abéliens, il existe donc un élément $a + p^r\mathbb{Z} \in \left(\mathbb{Z}/p^r\mathbb{Z}\right)^*$ d'ordre p. Puisque p et q sont premiers entre eux, il existe d'après le théorème chinois un entier b tel que l'on ait

$$b \equiv a \text{ mod. } p^r \quad \text{et} \quad b \equiv 1 \text{ mod. } q.$$

L'entier b est en particulier premier avec n (p ne divise pas a). Par hypothèse, on a donc

$$b^{n-1} \equiv 1 \text{ mod. } n.$$

On a ainsi $b^{n-1} \equiv 1$ mod. p^r, et l'ordre de $b + p^r\mathbb{Z}$ divise $n-1$. Il en est donc de même de l'ordre de $a + p^r\mathbb{Z}$. Par suite, p divise $n-1$. Le fait que p divise n conduit alors à une contradiction, d'où notre assertion.
Considérons alors un diviseur premier p de n. On a $n = pq$ où q est un produit de nombres premiers sans facteurs carrés et distincts de p. Le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ est cyclique. Soit $a + p\mathbb{Z}$ un de ses générateurs. D'après le théorème chinois, il existe un entier b tel que l'on ait

$$b \equiv a \text{ mod. } p \quad \text{et } b \equiv 1 \text{ mod. } q.$$

L'entier b est premier avec n (a n'est pas divisible par p). Par suite, on a la congruence $b^{n-1} \equiv 1$ mod. n, en particulier $b^{n-1} \equiv 1$ mod. p. L'ordre de b modulo p étant $p-1$, cela entraîne que $p-1$ divise $n-1$, d'où l'implication.

Démontrons l'implication $(iii) \Longrightarrow (i)$: Soit a un entier. Considérons un diviseur premier p de n. D'après le petit théorème de Fermat, a^{p-1} est congru à 0 ou 1 modulo p suivant que a soit ou non divisible par p. Par hypothèse $p-1$ divise $n-1$, on a donc aussi $a^{n-1} \equiv 0$ ou 1 mod. p, d'où $a^n \equiv a$ mod. p. Cette congruence étant vérifiée pour tous les diviseurs premiers de n, et n étant sans facteurs carrés, on en déduit que $a^n - a$ est divisible par n.

Démontrons l'équivalence $(ii) \Longleftrightarrow (iv)$: Supposons que $\lambda(n)$ divise $n-1$. Pour tout entier a premier avec n, on a $a^{\lambda(n)} \equiv 1$ mod. n. Par suite, on a $a^{n-1} \equiv 1$ mod. n et la condition (ii) est donc satisfaite. Inversement, $\lambda(n)$ étant le plus petit commun multiple des ordres des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$, on en déduit que $\lambda(n)$ divise $n-1$.

2) On a $561 = 3 \times 11 \times 17$ et $1105 = 5 \times 13 \times 17$, et l'on constate que la condition (iii) est satisfaite.

3.1) On a $(-1)^n \equiv -1$ mod. n et $n \neq 2$ car n n'est pas premier, donc n est impair. Par ailleurs, n est sans facteurs carrés. Supposons que l'on ait $n = pq$ où p et q sont deux nombres premiers. On a l'égalité $n - 1 = (p-1)q + (q-1)$. Parce que p divise n, d'après la première question $p-1$ divise $n-1$, donc $p-1$ divise $q-1$. De même $q-1$ divise $p-1$, ainsi $p = q$, d'où une contradiction et le résultat.

3.2) Soit p un diviseur premier de n. Alors, $p-1$ divise $n-1$ et on a

$$\frac{n-1}{p-1} = \frac{p(n/p)-1}{p-1} = \frac{(p-1)(n/p)+n/p-1}{p-1} = \frac{n}{p} + \frac{n/p-1}{p-1}.$$

Il en résulte que $p-1$ divise $n/p-1$, puis que $p \leq n/p$ i.e. $p^2 \leq n$. On a $n \neq p^2$, d'où $p < \sqrt{n}$ et le résultat. Notons que cela fournit une autre démonstration du fait que n a au moins trois diviseurs premiers.

4) Posons $n = (6m+1)(12m+1)(18m+1)$. On a $n-1 = 1296m^3 + 396m^2 + 36m$, qui est divisible par $6m$, $12m$ et $18m$, d'où l'assertion. (Pour $m = 1$, on a $n = 7.13.19 = 1729$ qui est donc un nombre de Carmichael.)

Exercice 8

Pour tout entier a premier à n, on a $a^{n-1} \equiv 1$ mod. n. D'après l'exercice 7, n est donc sans facteurs carrés. Par suite, il suffit de prouver que n ne peut pas s'écrire sous la forme mm' avec $\text{pgcd}(m, m') = 1$, les entiers m et m' étant impairs > 1. Supposons qu'il existe deux tels entiers m et m'. D'après le théorème chinois, il existe un entier c tel que l'on ait

$$c \equiv b \text{ mod. } m \quad \text{et} \quad c \equiv 1 \text{ mod. } m'.$$

On a donc

$$c^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} \equiv -1 \text{ mod. } m \quad \text{et} \quad c^{\frac{n-1}{2}} \equiv 1 \text{ mod. } m'.$$

Il en résulte $c^{\frac{n-1}{2}}$ n'est pas congru à 1 ni à -1 modulo n, sinon m ou m' divise 2, ce qui n'est pas vu que m et m' sont impairs > 1. On obtient ainsi une contradiction à la première condition de l'énoncé, d'où le résultat. (Inversement, on notera que si n est premier, les deux conditions de l'énoncé sont satisfaites.)

Exercice 9

1) Cela résulte du lemme 1.3 du premier chapitre, car $\varphi(n)$ est pair où φ est la fonction indicatrice d'Euler.

2) Supposons que n soit la puissance d'un nombre premier p. Alors, p étant impair, le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique. Pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $a^{\lambda(n)} = 1$, d'où $a^{\frac{\lambda(n)}{2}} = \pm 1$, ce qui montre que $S = (\mathbb{Z}/n\mathbb{Z})^*$.
Inversement, il existe un élément $b \in (\mathbb{Z}/n\mathbb{Z})^*$ d'ordre $\lambda(n)$ (cf. le théorème chinois ou la théorie des groupes abéliens finis). On a donc $b^{\frac{\lambda(n)}{2}} = -1$. Supposons que n soit

divisible par deux nombres premiers distincts p et q. D'après le théorème chinois, il existe $c \in \mathbb{Z}$ tel que l'on ait

$$c \equiv 1 \text{ mod. } p, \quad c \equiv b \text{ mod. } q \quad \text{et} \quad c \equiv 1 \text{ mod. } \ell,$$

pour tout diviseur premier ℓ de n distinct de p et q (en notant encore b un représentant de la classe de b modulo n). L'entier c est premier avec n. On a $c^{\frac{\lambda(n)}{2}} \equiv 1$ mod. p et $c^{\frac{\lambda(n)}{2}} \equiv -1$ mod. q. Parce que p et q sont impairs, on a donc $c^{\frac{\lambda(n)}{2}} \not\equiv \pm 1$ mod. n, d'où une contradiction et le résultat.

Exercice 10

1) Supposons N est pair. On a $n \equiv h + 1$ mod. 3.

   Si $h \equiv 2$ mod. 3, alors 3 divise n d'où $\left(\frac{n}{3}\right) = 0$. Si $h \equiv 1$ mod. 3, on a $n \equiv 2$ mod. 3 d'où $\left(\frac{n}{3}\right) = -1$.

   Supposons N impair. On a $n \equiv 2h + 1$ mod. 3.

   Si $h \equiv 1$ mod. 3, n est divisible par 3 d'où $\left(\frac{n}{3}\right) = 0$. Si $h \equiv 2$ mod. 3, on a $n \equiv 2$ mod. 3 d'où $\left(\frac{n}{3}\right) = -1$.

2) On a $n \equiv 1$ mod. 4. D'après la loi de réciprocité de Jacobi, on a donc $\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right)$.

3) Si N est pair et $h \equiv 2$ mod. 3, ou bien si N est impair et $h \equiv 1$ mod. 3, alors 3 divise n. Par suite, n n'est pas premier et on a $3^{\frac{n-1}{2}} \not\equiv -1$ mod. n, donc l'équivalence annoncée est vraie.

   Sinon, on a $\left(\frac{3}{n}\right) = -1$ et d'après le critère de primalité de Proth (Corollaire 2.4 du cours), on obtient le résultat.

4) Parce que n n'est pas multiple de 3, on a $\left(\frac{3}{n}\right) = -1$ (questions 1 et 2). L'entier n étant par hypothèse composé, on a $3^{\frac{n-1}{2}} \not\equiv -1$ mod. n (question 3). Par suite, 3 est un témoin d'Euler pour n (Définition 2.3).

Remarque. Notons que 2 n'est pas toujours un témoin d'Euler pour n. Par exemple, avec $n = 2^{32} + 1$, on a $h = 2$, $N = 4$, $2^{\frac{n-1}{2}} \equiv 1$ mod. n et $\left(\frac{2}{n}\right) = 1$.

Exercice 11 (Critère de primalité de Proth généralisé)

1) Parce que l'on a $1 \leq a \leq n - 1$, le nombre premier n ne divise pas a. On a donc $a^{n-1} \equiv 1$ mod. n. Par ailleurs, on a les égalités

$$a^{n-1} - 1 = \left(a^{\frac{n-1}{p}}\right)^p - 1 = \left(a^{\frac{n-1}{p}} - 1\right)\Phi_p\left(a^{\frac{n-1}{p}}\right).$$

   Par hypothèse, n ne divise pas $a^{\frac{n-1}{p}} - 1$, d'où le résultat.

2) On a $\frac{n-1}{p} = p^{N-1}h$. On a ainsi

$$\Phi_p\left(b^{p^{N-1}}\right) \equiv 0 \text{ mod. } n.$$

On a l'égalité

$$b^{p^N} - 1 = \big(b^{p^{N-1}} - 1\big)\Phi_p\big(b^{p^{N-1}}\big),$$

d'où la congruence annoncée.

3) D'après la question 2, on a $b^{p^N} \equiv 1$ mod. q. Par suite, l'ordre de b modulo q divise p^N. Supposons qu'il existe $j < N$ tel que l'on ait

$$b^{p^j} \equiv 1 \text{ mod. } q.$$

On a alors

$$b^{p^{N-1}} = \big(b^{p^j}\big)^{p^{N-1-j}} \equiv 1 \text{ mod. } q.$$

D'après l'hypothèse faite, on a la congruence

$$\Phi_p\big(b^{p^{N-1}}\big) \equiv 0 \text{ mod. } q.$$

Il en résulte que l'on a

$$\Phi_p\big(b^{p^{N-1}}\big) \equiv \Phi_p(1) \equiv 0 \text{ mod. } q.$$

On a $\Phi_p(1) = p$, d'où $p = q$, ce qui conduit à une contradiction car p ne divise pas n, d'où l'assertion.

4) D'après la question précédente, p^N divise $q - 1$. En particulier, on a $p^N < q$. On a donc les égalités $p^N < q \leq \sqrt{n}$, d'où $p^{2N} < n$ i.e. $p^{2N} \leq n - 1 = p^N h$. On obtient ainsi $p^N \leq h$, d'où la contradiction cherchée et le résultat.

5) Le groupe $\mathbb{F}_n^*$ étant cyclique, l'ordre du noyau du morphisme de groupes $\mathbb{F}_n^* \to \mathbb{F}_n^*$ qui à x associe $x^{\frac{n-1}{p}}$ est $\frac{n-1}{p}$. Il y a donc exactement $\frac{n-1}{p}$ entiers a compris entre 1 et $n-1$ tels que $a^{\frac{n-1}{p}} \equiv 1$ mod. n. Le nombre d'entiers a entre 1 et $n-1$ ne vérifiant pas cette condition est donc $(n-1)\big(1 - \frac{1}{p}\big)$. Ainsi, la probabilité cherchée est $1 - \frac{1}{p}$.

6) Considérons l'entier $n = 2.3^{1454} + 1$. Avec les notations précédentes, on a $p = 3$ et $h = 2$. On choisit l'entier $a = 2$. On vérifie alors, par un calcul dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ (et non pas dans $\mathbb{Z}$), que l'on a $2^{\frac{n-1}{3}} \not\equiv 1$ mod. n. Par ailleurs, on a $\Phi_3 = X^2 + X + 1$. On constate alors que $\Phi_3\big(2^{\frac{n-1}{3}}\big) \equiv 0$ mod. n, ce qui établit le fait que n est premier.

On procède de même avec l'entier $n = 4.7^{894} + 1$, à ceci près que l'on a dans $\mathbb{Z}/n\mathbb{Z}$ l'égalité $2^{\frac{n-1}{7}} = 1$. Avec l'entier $a = 3$, on vérifie que l'on a $3^{\frac{n-1}{7}} \neq 1$ et $\Phi_7\big(3^{\frac{n-1}{7}}\big) = 0$, d'où le fait que n soit premier.

Exercice 12 (Généralisation du petit théorème de Fermat)

Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Notons $\overline{A} \in \mathbb{M}_n(\mathbb{F}_p)$ la matrice déduite de A par réduction de ses coefficients modulo p et $\lambda_1, \cdots, \lambda_n$ ses valeurs propres dans $\overline{\mathbb{F}_p}$. On a

$$\mathrm{Tr}(\overline{A}) = \sum_{i=1}^{n} \lambda_i,$$

d'où (petit théorème de Fermat)

$$\mathrm{Tr}(A)+p\mathbb{Z}=\Big(\mathrm{Tr}(A)+p\mathbb{Z}\Big)^p=\Big(\mathrm{Tr}(\overline{A})\Big)^p=\left(\sum_{i=1}^n\lambda_i\right)^p=\sum_{i=1}^n\lambda_i^p.$$

Par ailleurs, $\overline{A}$ est trigonalisable sur $\overline{\mathbb{F}_p}$ i.e. $\overline{A}$ est semblable dans $\mathbb{M}_n(\overline{\mathbb{F}_p})$ à une matrice triangulaire, ses coefficients diagonaux étant les λ_i. La matrice $\overline{A}^p$ est donc semblable à une matrice triangulaire dont les coefficients diagonaux sont les λ_i^p. On a donc

$$\mathrm{Tr}(\overline{A}^p)=\sum_{i=1}^n\lambda_i^p.$$

On a $\overline{A}^p=\overline{A^p}$. Les égalités

$$\mathrm{Tr}(A^p)+p\mathbb{Z}=\mathrm{Tr}(\overline{A^p})=\mathrm{Tr}(\overline{A}^p)$$

impliquent alors l'assertion.

Exercice 13

Si k est pair, 2^p-k est pair, et tout nombre premier p tel que $2^p-k\neq 2$ convient.

Supposons désormais k impair.

Si $k=3$, pour tout nombre premier p congru à 3 modulo 4, on a $2^p-3\equiv 0$ mod. 5.

Supposons $k>3$. On a $k-2\geq 2$ et $k-2$ est impair. Il existe donc un diviseur premier $q\geq 3$ de $k-2$. Pour tout nombre premier p congru à 1 modulo $q-1$, on a ainsi

$$2^p-k\equiv 2-k\equiv 0 \text{ mod. } q.$$

Parce qu'il existe une infinité de tels nombres premiers p, on obtient le résultat.

Exercice 14

Reprenons les indications faites dans l'énoncé. On peut supposer k impair. Soit a un entier naturel. Il suffit de prouver l'existence d'un entier n tel que $2^{2^n}+k$ ne soit pas premier et que $2^{2^n}+k>a$. Puisque k est distinct de 1, il existe $s\in\mathbb{N}$ et un entier impair h tels que

$$k-1=2^sh.$$

Soit t un entier naturel tel que l'on ait

$$p=2^{2^t}+k>a \quad \text{et} \quad t>s.$$

On peut supposer que p est un nombre premier. Il existe un entier impair h_1 tel que

$$p-1=2^sh_1.$$

D'après le théorème d'Euler, on a

$$2^{\varphi(h_1)} \equiv 1 \text{ mod. } h_1,$$

d'où l'on déduit la congruence

$$2^{s+\varphi(h_1)} \equiv 2^s \text{ mod. } p-1.$$

Puisque l'on a $t > s$, on obtient

$$2^{t+\varphi(h_1)} \equiv 2^t \text{ mod. } p-1.$$

L'entier p étant premier impair, on a $2^{p-1} \equiv 1$ mod. p. Il en résulte que

$$2^{2^{t+\varphi(h_1)}} + k \equiv 0 \text{ mod. } p.$$

L'entier $2^{2^{t+\varphi(h_1)}} + k$, qui est strictement plus grand que p, n'est donc pas premier. Il est plus grand que a, d'où le résultat.

Exercice 15

1.1) Supposons que q divise $m-1$. On a alors $\Phi_p(m) \equiv p$ mod. q. Parce que q divise $\Phi_p(m)$, on en déduit que q divise p et donc que $q = p$. Par hypothèse, p divise m, donc il en est de même de q, d'où une contradiction.

1.2) On a $m^p - 1 = (m-1)\Phi_p(m)$, d'où $m^p \equiv 1$ mod. q. D'après la question précédente, p est donc l'ordre de m modulo q, d'où $q \equiv 1$ mod. p.

2) Posons $N = \Phi_p(p_1 \cdots p_r p)$. Soit q un diviseur premier de N. L'entier q ne divise pas $p_1 \cdots p_r$, sinon q diviserait 1. Ainsi, q est distinct des nombres premiers p_i. Or d'après la question 1.2, on a $q \equiv 1$ mod. p, d'où la contradiction cherchée et le résultat.

Exercice 16

1) On a l'égalité

$$F = X^{p-1} - A_1 X^{p-2} + A_2 X^{p-3} + \cdots - A_{p-2}X + A_{p-1} \ ^{(1)}.$$

En substituant X par p, on obtient

$$(p-1)! = p^{p-1} - A_1 p^{p-2} + A_2 p^{p-3} + \cdots - A_{p-2}p + A_{p-1}.$$

Le fait que l'on ait $(p-1)! = A_{p-1}$ entraîne alors le résultat.

2) Parce que $p-1$ est pair, on a

$$F(-p)=\prod_{k=1}^{p-1}(p+k) \quad \text{et} \quad F(-p)=p^{p-1}+A_1p^{p-2}+\cdots+A_{p-2}p+A_{p-1}.$$

D'après la première question, on a l'égalité

$$p^{p-1}+A_2p^{p-3}+\cdots+A_{p-3}p^2=A_1p^{p-2}+A_3p^{p-4}+\cdots+A_{p-2}p,$$

d'où l'égalité annoncée.

3) On a

$$(p-1)!\ \binom{2p-1}{p-1}=\prod_{k=1}^{p-1}(p+k).$$

Par ailleurs, d'après le petit théorème de Fermat, en posant $\overline{A_i}=A_i+p\mathbb{Z}$, on a dans $\mathbb{F}_p[X]$ l'égalité

$$X^{p-1}-1=X^{p-1}-\overline{A_1}X^{p-2}+\overline{A_2}X^{p-3}+\cdots-\overline{A_{p-2}}X+\overline{A_{p-1}}.$$

En particulier, on a $A_{p-3}\equiv 0$ mod. p. Il résulte alors de la question 2 que l'on a la congruence

$$(p-1)!\ \binom{2p-1}{p-1}\equiv A_{p-1} \text{ mod. } p^3,$$

d'où le résultat vu que $A_{p-1}=(p-1)!$.

Exercice 17 (Test de Lucas des nombres de Mersenne)

1) L'égalité est vérifiée si $n=1$ car on a $u+u'=4=u_1$. Supposons qu'elle le soit pour un entier $n\geq 1$. Compte tenu de l'égalité $uu'=1$, on a alors

$$u_{n+1}=\left(u^{2^{n-1}}+u'^{2^{n-1}}\right)^2-2=u^{2^n}+u'^{2^n},$$

d'où l'assertion.

---

(1) Rappelons pourquoi. Soit $f=X^n+u_{n-1}X^{n-1}+\cdots+u_1X+u_0$ un polynôme unitaire de degré n à coefficients dans un corps K. Notons $a_1,\cdots,a_n$ ses racines dans une clôture algébrique de K. En écrivant que l'on a $f=(X-a_1)\cdots(X-a_n)$, on déduit que pour tout $k=1,\cdots,n$, on a

$$u_{n-k}=(-1)^k\sum a_{i_1}\cdots a_{i_k},$$

où la somme est étendue à toutes les parties $\{i_1,\cdots,i_k\}$ de l'ensemble $\{1,\cdots,n\}$. La somme $\sum a_{i_1}\cdots a_{i_k}$ s'appelle la k-ième fonction symétrique élémentaire des racines de f.

2) Soit $\psi : \mathbb{Z}[X] \to A/qA$ l'application définie pour tout $F \in \mathbb{Z}[X]$ par l'égalité

$$\psi(F) = F\big(\sqrt{3}\big) + qA.$$

C'est un homomorphisme d'anneaux surjectif. Vérifions que l'on a

$$\mathrm{Ker}(\psi) = (q, X^2 - 3). \tag{1}$$

L'idéal $(q, X^2 - 3)$ est par définition contenu dans $\mathrm{Ker}(\psi)$. Inversement, soit F un élément de $\mathrm{Ker}(\psi)$. Le polynôme $X^2 - 3 \in \mathbb{Z}[X]$ étant unitaire, il existe Q et R dans $\mathbb{Z}[X]$ tels que l'on ait

$$F = (X^2 - 3)Q + R \quad \text{avec } \deg(R) \leq 1.$$

Il existe a et b dans $\mathbb{Z}$ tels que $R = aX + b$. On a $F\big(\sqrt{3}\big) = R\big(\sqrt{3}\big)$, donc $R\big(\sqrt{3}\big)$ appartient à qA. Par suite, il existe u et v dans $\mathbb{Z}$ tels que l'on ait

$$a\sqrt{3} + b = q(u + \sqrt{3}v),$$

d'où $a = qv$ et $b = qu$. On a ainsi $R = q(vX + u)$, et F est dans l'idéal $(q, X^2 - 3)$, d'où l'égalité (1). Les anneaux $\mathbb{Z}[X]/(q, X^2 - 3)$ et A/qA sont donc isomorphes. Il reste à vérifier que les anneaux $\mathbb{Z}[X]/(q, X^2 - 3)$ et $\mathbb{F}_q[X]/(X^2 - 3)$ le sont aussi. On considère pour cela l'application composée

$$\gamma : \mathbb{Z}[X] \to \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(X^2 - 3),$$

définie pour tout $F \in \mathbb{Z}[X]$ par l'égalité

$$\gamma(F) = \overline{F} + (X^2 - 3),$$

où $\overline{F} \in \mathbb{F}_q[X]$ désigne le polynôme déduit de F par réduction de ses coefficients modulo q. C'est un homomorphisme d'anneaux surjectif et l'on a

$$\mathrm{Ker}(\gamma) = (q, X^2 - 3). \tag{2}$$

En effet, $(q, X^2 - 3)$ est par définition contenu dans $\mathrm{Ker}(\gamma)$. Inversement, si F appartient à $\mathrm{Ker}(\gamma)$, il existe $H \in \mathbb{F}_q[X]$ tel que l'on ait $\overline{F} = H(X^2 - 3)$. Si $\widetilde{H} \in \mathbb{Z}[X]$ est un relèvement de H, cette égalité signifie que $F - \widetilde{H}(X^2 - 3)$ appartient à $q\mathbb{Z}[X]$, donc F est dans l'idéal $q\mathbb{Z}[X] + (X^2 - 3)$, d'où l'égalité (2), puis le résultat.

3) On a $q \equiv 3$ mod. 4 et $q \equiv 1$ mod. 3. D'après la loi de réciprocité quadratique, on a

$$\Big(\frac{3}{q}\Big) = -\Big(\frac{q}{3}\Big) = -1,$$

donc 3 n'est pas un carré modulo q. Ainsi, $X^2-3 \in \mathbb{F}_q[X]$ est irréductible sur $\mathbb{F}_q$, donc $\mathbb{F}_q[X]/(X^2-3)$ est un corps. D'après la question 2, il en est de même de K. Par ailleurs, $\mathbb{F}_q[X]/(X^2-3)$ est un $\mathbb{F}_q$-espace vectoriel de dimension 2, donc son cardinal, qui est celui de K, est q^2.

4) Parce que K est un corps, le polynôme $X^q - X \in K[X]$ a exactement q racines, qui sont les éléments de $\mathbb{F}_q$. L'ensemble des points fixes de f est donc $\mathbb{F}_q$. Dans K, on a l'égalité $x^2 = 3$, d'où $f(x)^2 = f(3) = 3$. Les racines du polynôme $X^2 - 3 \in K[X]$ étant $\pm x$, on en déduit que $f(x) = \pm x$. D'après la question 3, x n'est pas dans $\mathbb{F}_q$, d'où $f(x) = -x$. Par ailleurs, on a

$$\eta = 2 + x, \quad \eta' = 2 - x, \quad y = 1 + x, \quad y' = 1 - x,$$

d'où $f(\eta) = \eta'$ et $f(y) = y'$.

5) En utilisant les égalités $f(y) = y^q = y'$ et $y^2 = 2\eta$, on obtient

$$-2 = yy' = y^{q+1} = \left(y^2\right)^{\frac{q+1}{2}} = 2^{\frac{q+1}{2}} \eta^{\frac{q+1}{2}}.$$

Par ailleurs, on a $q \equiv 7 \bmod. 8$, donc 2 est un carré modulo q. D'après le critère d'Euler, on a donc $2^{\frac{q-1}{2}} \equiv 1 \bmod. q$. On en déduit que $\eta^{\frac{q+1}{2}} = -1$. L'égalité $f(\eta) = \eta'$ entraîne alors l'assertion.

6) On a $\eta\eta' = 1$. D'après la question 5, on a donc

$$\left(\eta^{\frac{q+1}{4}} + {\eta'}^{\frac{q+1}{4}}\right)^2 = \eta^{\frac{q+1}{2}} + {\eta'}^{\frac{q+1}{2}} + 2 = -2 + 2 = 0.$$

Par ailleurs, on a $\frac{q+1}{4} = 2^{p-2}$. La question 1, utilisée avec $n = p-1$, entraîne alors

$$u_{p-1} + qA = \eta^{2^{p-2}} + {\eta'}^{2^{p-2}} = 0.$$

Ainsi, u_{p-1} appartient à qA, d'où l'on déduit que q divise u_{p-1} (dans $\mathbb{Z}$).

7) Par hypothèse, u_{p-1} est multiple de M_p, donc q divise u_{p-1}. D'après la question 1, utilisée avec $n = p-1$, on obtient l'égalité annoncée.

8) En tenant compte du fait que $\eta\eta' = 1$, on en déduit que $\eta^{2^{p-1}} = -1$, d'où $\eta^{2^p} = 1$. L'ordre de η dans le groupe K^* des éléments inversibles de K est donc une puissance de 2 et les égalités précédentes entraînent l'assertion.

9) D'après le théorème de Lagrange et la question 8, 2^p divise l'ordre de K^*. En particulier, on a $2^p \leq q^2$. Par ailleurs, on a les inégalités $q^2 \leq M_p < 2^p$, d'où une contradiction et le résultat.

Exercice 18

1. Questions préliminaires

1) On a $\left(\frac{5}{2}\right) = 1$. Supposons $p \neq 2$. D'après la loi de réciprocité quadratique, on a

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

On obtient ainsi

$$\left(\frac{5}{p}\right) = 1 \quad \text{si} \quad p \equiv \pm 1 \text{ mod. } 5 \quad \text{et} \quad \left(\frac{5}{p}\right) = -1 \quad \text{si} \quad p \equiv \pm 2 \text{ mod. } 5 \quad \text{et} \quad p \neq 2.$$

2) On a $\alpha^2 - \alpha - 1 = 0$ i.e. $\alpha(\alpha - 1) = 1$, donc α et $1 - \alpha$ sont inversibles dans A.

3) Le système $(1, \alpha)$ est une base du $\mathbb{F}_p$-espace vectoriel A. Cherchons u et v dans $\mathbb{F}_p$ tels que l'on ait

$$(u + v\alpha)(2\alpha - 1) = 1.$$

On obtient $2u + v = 0$ et $2v - u = 1$. On a $p \neq 5$ et A est de caractéristique p, donc 5 est inversible dans A. Par suite, on a $u = -\frac{1}{5}$ et $v = \frac{2}{5}$. Ainsi $2\alpha - 1$ est inversible dans A et l'on a

$$(2\alpha - 1)^{-1} = \frac{2\alpha - 1}{5}.$$

4) On a $u_0 = 0$ et $u_1 = 1$, donc l'égalité à démontrer est vraie pour $n = 0$ et $n = 1$. Soit $n \geq 2$ un entier tel que l'on ait

$$u_k + p\mathbb{Z} = \frac{\alpha^k - (1 - \alpha)^k}{2\alpha - 1} \quad \text{pour} \quad k = n - 2 \quad \text{et} \quad k = n - 1.$$

On a alors l'égalité

$$u_n + p\mathbb{Z} = \frac{\alpha^{n-1} - (1 - \alpha)^{n-1} + \alpha^{n-2} - (1 - \alpha)^{n-2}}{2\alpha - 1},$$

ce qui conduit à

$$u_n + p\mathbb{Z} = \frac{\alpha^{n-2}(\alpha + 1) - (1 - \alpha)^{n-2}(2 - \alpha)}{2\alpha - 1}.$$

D'après l'égalité $\alpha^2 = \alpha + 1$, on a $2 - \alpha = (1 - \alpha)^2$, d'où

$$u_n + p\mathbb{Z} = \frac{\alpha^n - (1 - \alpha)^n}{2\alpha - 1},$$

et le résultat.

2. Cas où $p \equiv \pm 1$ mod. 5

5) Dans ce cas, on a $\left(\frac{5}{p}\right) = 1$ (question 1). Le discriminant du polynôme F, qui est 5, est donc un carré non nul dans $\mathbb{F}_p$. Par suite, F a deux racines distinctes a et b dans $\mathbb{F}_p$. Considérons l'application $\psi : \mathbb{F}_p[X] \to \mathbb{F}_p \times \mathbb{F}_p$ définie pour tout $P \in \mathbb{F}_p[X]$ par l'égalité

$$\psi(P) = \big(P(a), P(b)\big).$$

C'est un morphisme d'anneaux. Par ailleurs, a étant distinct de b, son noyau est l'idéal engendré par $(X-a)(X-b)$ qui n'est autre que F. Il en résulte que l'application déduite de ψ par passage au quotient

$$\overline{\psi} : A \to \mathbb{F}_p \times \mathbb{F}_p$$

définie par

$$\overline{\psi}\big(P + (F)\big) = \big(P(a), P(b)\big),$$

est un morphisme d'anneaux injectif. C'est un isomorphisme vu que A et $\mathbb{F}_p \times \mathbb{F}_p$ ont le même cardinal p^2, d'où l'assertion.

6) Pour tout $y \in \mathbb{F}_p$, on a $y^p = y$. D'après la question précédente, on a donc $x^p = x$ pour tout x dans A.

7) On a en particulier $\alpha^p = \alpha$ et $(1-\alpha)^p = 1 - \alpha$. Puisque α et $1 - \alpha$ sont inversibles dans A (question 2), on en déduit que $\alpha^{p-1} = 1$ et $(1-\alpha)^{p-1} = 1$. La question 4 implique alors $u_{p-1} \equiv 0$ mod. p.

3. Cas où $p \equiv \pm 2$ mod. 5

8) Si $p = 2$, le polynôme $X^2 + X + 1 \in \mathbb{F}_2[X]$ étant irréductible sur $\mathbb{F}_2$, A est un corps. Supposons $p \neq 2$. On a $\left(\frac{5}{p}\right) = -1$ (question 1), donc 5 n'est pas un carré dans $\mathbb{F}_p$. Ainsi, F n'a pas de racines dans $\mathbb{F}_p$ et F est irréductible sur $\mathbb{F}_p$. Par suite, A est un corps.

9) La somme des racines de F dans A est 1. Ses racines sont donc α et $1 - \alpha$.

10) L'élément α^p est aussi une racine de F. Puisque α n'est pas dans $\mathbb{F}_p$, on a $\alpha^p \neq \alpha$, d'où $\alpha^p = 1 - \alpha$. Par le même argument, on obtient l'égalité $(1-\alpha)^p = \alpha$.

11) D'après ce qui précède, on a $\alpha^{p+1} = (1-\alpha)^{p+1} = -1$. La question 4 entraîne alors $u_{p+1} \equiv 0$ mod. p.