Éléments de correction de l'examen de première session

Exercice 1.

1. Facile.
2. Par hypothèse f est paire donc $b_n(f) = 0$ pour tout $n \geq 1$. On a
$$a_0(f) = \frac{2}{2\pi}\int_0^\pi (x+\pi/2)\,\mathrm{d}x = \frac{1}{2\pi}[(x+\pi/2)^2]_0^\pi = \pi\,.$$
Pour $n \geq 1$:
$$a_n(f) = \frac{2}{\pi}\int_0^\pi (x+\pi/2)\cos(nx)\,\mathrm{d}x = \frac{2}{\pi}\left([(x/n)\sin(nx)]_0^\pi - \frac{1}{n}\int_0^\pi \sin(nx)\,\mathrm{d}x\right) = \frac{2}{\pi n^2}((-1)^n - 1)\,.$$
3. La N-ème somme partielle de la série de Fourier de f est :
$$S_N(f)(x) = \pi + \frac{2}{\pi}\sum_{n=1}^{N}\frac{(-1)^n-1}{n^2}\cos(nx) = \pi - \frac{4}{\pi}\sum_{k=0}^{\lfloor (N-1)/2\rfloor}\frac{\cos((2k+1)x)}{(2k+1)^2}\,.$$
Comme f est $C^{1,\mathrm{m}}$ sur $\mathbb{R}$, le théorème de Dirichlet affirme que $S_N(f)(x) \to f(x)$, lorsque $N \to \infty$ en tout $x \in \mathbb{R}$ tel que f est continue en x. Par définition f est continue sur $]0,\pi[$ et par parité f est continue sur $]-\pi,\pi[$. La limite à droite de f en π est égale, par 2π-périodicité, à la limite à droite de f en $-\pi$. Par parité cette limite coïncide avec la limite à gauche de f en π. Donc f est continue en π, puis continue sur $\mathbb{R}$ par 2π-périodicité. Ainsi pour tout $x \in \mathbb{R}$
$$f(x) = \pi - \frac{4}{\pi}\sum_{k=0}^{\infty}\frac{\cos((2k+1)x)}{(2k+1)^2}\,.$$
4. On applique le résultat de la question précédente en $x = 0$:
$$f(0) = \frac{\pi}{2} = \pi - \frac{4}{\pi}\sum_{k=0}^{\infty}\frac{1}{(2k+1)^2}\,.$$
La somme à calculer vaut donc $\pi^2/8$.
5. On applique la formule de Parseval à f 2π-périodique $C^{0,\mathrm{m}}$ sur $\mathbb{R}$.
$$\frac{2}{2\pi}\int_0^\pi (x+\pi/2)^2\,\mathrm{d}x = \frac{1}{3\pi}[(x+\pi/2)^3]_0^\pi = \frac{13\pi^2}{12} = \pi^2 + \frac{8}{\pi^2}\sum_{k=0}^{\infty}\frac{1}{(2k+1)^4}\,.$$
La somme à calculer vaut donc $\pi^4/96$.

Exercice 2.

1. (a) On a $(2^{ab}-1)/(2^a-1) = 1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a} \in \mathbb{Z}$. Donc $2^a - 1$ divise $2^{ab}-1$. Si $a, b > 1$, on obtient un diviseur $d = 2^a - 1$ de $2^{ab}-1$ distinct de 1 et de $2^{ab}-1$, donc $2^{ab}-1$ n'est pas premier.
   (b) Si l'on montre la propriété souhaitée pour tout facteur premier q de M_p alors elle sera vraie pour tout diviseur d de M_p car tout diviseur premier de d est alors un diviseur premier de M_p donc est $\equiv 1 (\mathrm{mod}\, 2p)$; le produit d de tels diviseurs est donc encore $\equiv 1 (\mathrm{mod}\, 2p)$.

(c) $M_p = 2^p - 1$ est impair car $p \geq 3$, donc tout diviseur de M_p (en particulier q) est impair. Ainsi, 2, premier à q, est inversible modulo q. Comme $q \mid M_p$, on a $2^p \equiv 1 (\mathrm{mod}\, q)$. L'ordre de 2 modulo q est donc un diviseur de p i.e. 1 ou p. Cet ordre ne peut pas être 1 ; donc l'ordre de 2 modulo q est p.

(d) D'après Lagrange, on déduit que $p \mid (q-1)$ qui est l'ordre de $(\mathbb{Z}/q\mathbb{Z})^\times$.

(e) q est impair donc $q \equiv 1 (\mathrm{mod}\, 2)$. Aussi $q \equiv 1 (\mathrm{mod}\, p)$ donc $q \equiv 1 (\mathrm{mod}\, 2p)$, par le théorème des restes chinois, puisque p est impair donc premier à 2.

2. (a) Voir le cours ; le calcul de F_n par exponentiation rapide est en $O(\log(2^n)) = O(n)$ opérations dans $\mathbb{Z}$.

(b) Comme $q \mid F_n$, on a $F_n = 2^{2^n} \equiv -1 (\mathrm{mod}\, q)$. En élevant au carré, on obtient la congruence souhaitée.

(c) Par hypothèse, q est impair, donc 2 est inversible modulo q. Par la question précédente, son ordre modulo q divise 2^{n+1} ; cet ordre est donc une puissance de 2.

(d) D'après les deux questions précédentes, l'ordre de 2 modulo q est une puissance de 2 inférieure ou égale à 2^{n+1}. Ça ne peut pas être 2^n puisque $2^{2^n} \equiv -1 (\mathrm{mod}\, q)$. Si cet ordre est 2^k avec $k < n$; alors en élevant à un puissance de 2 convenable la congruence $2^{2^k} \equiv 1 (\mathrm{mod}\, q)$, on contredit $2^{2^n} \equiv -1 (\mathrm{mod}\, q)$. On conclut que l'ordre de 2 modulo q est 2^{n+1}.

Exercice 3.

1. Si $P = Q^2 R$ dans $\mathbb{C}[X]$ alors, en dérivant, $P' = 2QQ'R + Q^2R' = Q(2Q'R + QR')$. Si Q est non constant alors il admet une racine dans $\mathbb{C}$. C'est une racine commune à P et P' d'après ce qui précède. Réciproquement si $\alpha \in C$ est une racine commune à P et P', écrivons $P(X) = (X-\alpha)P_1(X)$ pour un $P_1 \in \mathbb{C}[X]$. Alors $P'(X) = P_1(X) + (X-\alpha)P_1'(X)$. En /valuant en α, on obtient $P_1(\alpha) = 0$. Ainsi $P_1(X) = (X-\alpha)P_2(X)$ pour un $P_2 \in \mathbb{C}[X]$, puis $P(X) = (X-\alpha)^2 P_2(X)$ admet un facteur carré.
2. Le dernier reste non nul (qui, au signe près, vaut R_n) dans l'algorithme d'Euclide pour P et P' est le pgcd de P et P'. Or d'après la question 1, $\mathrm{pgcd}(P, P') = 1$. Donc $|R_n| = 1$.
3. Par l'absurde, si $R_i(a) = R_{i+1}(a) = 0$ pour un $a \in \mathbb{R}$ et un $i \geq 0$, alors, par préservation du pgcd dans l'algorithme d'Euclide, $\mathrm{pgcd}(R_i, R_{i+1}) = \mathrm{pgcd}(P, P')$ est non constant. C'est la contradiction cherchée.
4. Par définition $R_{i-1} = Q_i R_i - R_{i+1}$, où $-R_{i+1}$ est le reste dans la division euclidienne de R_{i-1} par R_i. En évaluant en a, on obtient l'égalité souhaitée. D'après la question précédente $R_{i+1}(a) \neq 0$ car $R_i(a) = 0$.
5. Supposons $|z| \geq 1$. On a $|z|^d \leq \sum_{i=0}^{d-1} |a_i| \cdot |z|^i$. En divisant par $|z|^{d-1}$, on obtient, puisque $|z| \geq 1$,

$$|z| \leq \sum_{i=0}^{d-1} \frac{|a_i|}{|z|^{d-1-i}} \leq \sum_{i=0}^{d-1} |a_i| .$$

6. **Entrée** : $P = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1} + X^d \in \mathbb{Q}[X]$ de degré $d \geq 1$, sans facteur carré.
   1. Calculer $M = \max\left(1, \sum_{i=0}^{d-1} |a_i|\right)$.
   2. Utiliser l'algorithme d'Euclide pour calculer la suite de Sturm $(R_0, \ldots, R_n)$ associée à P.
   3. Calculer le nombre de changements de signe k^- de la suite $(R_0(-M), \ldots, R_n(-M))$ et le nombre de changements de signes k^+ de la suite $(R_0(M), \ldots, R_n(M))$.

   Sortie : $k^+ - k^-$.