Université Pierre et Marie Curie Licence A

Devoir 3

Problème 1. *Soit $n \geqslant 2$ un entier. Montrez que les conditions suivantes sont équivalentes*

- *n est sans facteurs carrés et $p|n \Rightarrow p-1|(n-1)/2$;*
- *$\forall a \in \mathbb{Z}$ premier avec n, on a $a^{(n-1)/2} \equiv 1 \bmod n$.*

Un entier $n \in \mathbb{N}^*$ est dit pseudo-premier de base b si $b^{n-1} \equiv 1 \bmod n$.

(a) Montrez que $n = 105 = 3.5.7$ est pseudo-premier de base 13 mais qu'il ne l'est pas de base 2.

(b) Le petit théorème de Fermat dit qu'un nombre premier p est pseudo-premier de base b pour tout b premier à p. Réciproquement un nombre n est dit de Carmichael s'il est pseudo-premier de base b pour tout b premier avec n, sans être premier. Montrez que $n = 561 = 3.11.17$ est un nombre de Carmichael.

(c) Un entier $n = 1 + 2^k q$ impair, q impair, est dit fortement pseudo-premier de base b si l'une des conditions suivantes est vérifiée:

$$b^q \equiv 1 \bmod n \qquad \exists 0 \leqslant j < k,\ b^{2^j q} \equiv -1 \bmod n$$

(i) Montrez que si n est premier alors il est fortement pseudo-premier de base b pour tout $1 \leqslant b < n$ et qui si n est fortement pseudo-premier de base b alors il est pseudo-premier de base b.

(ii) Montrez que $n = 561$ n'est pas fortement pseudo-premier de base 2.

(iii) Pour n impair soit

$$B_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ n \text{ est fortement pseudo-premier de base } x\}.$$

On veut montrez le théorème de Rabin: si n est non premier alors $\frac{|B_n|}{\phi(n)} \leqslant 1/4$ sauf pour $n = 9$. Sous une autre forme, si $|B_n| \geqslant \phi(n)/4$ alors n est premier.

(α) Considérons $p_1 \equiv 3 \bmod 4$ premier tel que $p_2 = 2p_1 - 1$ soit premier (exemple $p_1 = 40039, 41011, 42727$). Montrez alors que pour $n = p_1 p_2$, on a $4|B_n| = \phi(n)$.

(β) Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition en facteurs premiers de $n = 1 + 2^k q$, q impair; on écrit $p_i = 1 + 2^{k_i} q_i$ avec q_i impair et $k_1 \leqslant \cdots \leqslant k_r$. Montrez alors que

$$|B_n| = (q, q_1) \cdots (q, q_r)(1 + \sum_{j=0}^{k_1 - 1} 2^{jr})$$

En déduire que $\frac{|B_n|}{\phi(n)} \leqslant \frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{k_1 r}} K$, avec $K = \prod_{i=1}^r \frac{(q, q_i)}{q_i p_i^{\alpha_i - 1}}$. En outre si tous les k_i ne sont pas tous égaux, on peut améliorer l'inégalité précédente d'un facteur 2.

(γ) Montrez le résultat dans le cas où n est une puissance d'un nombre premier, puis traitez le cas général.

Remarque: Ainsi si n est fortement pseudo-premier dans m bases tirées au hasard, on peut présumer, avec une probabilité d'erreur inférieure à $1/4^m$, qu'il est premier.

(d) *La méthode de cryptographie RSA: soit p et q deux nombres premiers distincts impairs et $n = pq$. Soit $0 \leqslant c < n$ un entier premier avec $\varphi(n)$. Etant donné un message en clair $0 \leqslant x < n$, $x \in \mathbb{N}$, on calcule $y = x^c$ qui représente le message codé.*

(i) *Expliquez comment décrypter le message.*

(ii) *On suppose maintenant que p et q sont fortement pseudo-premier pour r bases choisies au hasard. Que peut-on dire du système cryptographique précédent.*

Ce critère de primalité statistique est très utilisé dans le système cryptographique RSA; expliquons brièvement de quoi il s'agit. C'est un système dit à clef publique, c'est à dire que tout le monde connait le procédé de cryptage mais seul une presonne (le receveur) connait la clef qui permet de déchiffrer. Concrètement si A veut envoyer un message à R, il le coupe d'abord en bouts et le transforme en un nombre m plus petit que n connu de tous; ensuite il envoie m^d modulo n où d est un entier à nouveau connu de tous. Le problème pour R ou pour B indiscret et de retrouver m connaissant n et d et sachant que $n = pq$ avec p, q premiers connus seulement de R. Pour R la méthode est assez simple, il lui suffit de connaitre l'inverse e de d dans $(\mathbb{Z}/n\mathbb{Z})^\times$ qui a été choisi par R tel que $(d, n) = 1$. En effet on a alors $(m^d)^e \equiv m \bmod n$ en vertu du théorème d'Euler (cf. la proposition (??)). Pour calculer e, R utilise le théorème chinois (cf. le théorème ??) et calcule donc les inverses e_p et e_q de d dans respectivement $(\mathbb{Z}/p\mathbb{Z})^\times$ et $(\mathbb{Z}/q\mathbb{Z})^\times$ qui est d'après le petit théorème de Fermat (cf. la proposition ??) égal à d^{p-2} et d^{q-2}. On construit alors facilement e en utilisant la version constructive du théorème chinois (cf. la remarque ??). Pour B, la situation est plus critique; pour l'instant sa stratégie est de casser n, i.e. de trouver p ce qui est très long pourvu que R ait choisi p et q très grand convenablement. Le problème, on le voit alors, est donc de construire des nombres premiers très grand. Or tester la primalité d'un nombre est couteux en temps, même si récemment on a trouvé un algorithme en temps polynomial. C'est à ce moment qu'entre en jeu le test de Rabin qui comme on le voit est particulièrement bien adapté à RSA puisqu'il assure que $100.(1-(1/4)^m)$ pour cent des messages seront bien décryptés.

Exercice 1. *Montrez que si $a^n - 1$ est premier alors $a = 2$ et n est premier; $M_p = 2^p - 1$ est appelé un nombre de Mersenne pour p premier. On veut montrer le test de primalité de Lucas-Lehmer: M_q est premier ($q \geqslant 3$ premier) si et seulement si $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \bmod M_q$.*

(i) *Montrez que l'anneau $A = \mathbb{Z}[\sqrt{3}]$ est euclidien et caractérisez les unités.*

(ii) *Remarquez que pour q impair, $M_q \equiv 7 \bmod 12$ et en déduire qu'il existe un premier $p \not\equiv \pm 1 \bmod 12$ divisant M_q et remarquer que p reste irréductible dans $\mathbb{Z}[\sqrt{3}]$. Montrez que si M_q vérifie la congruence ci-dessus, alors $p = M_q$.*

(iii) *En utilisant la loi de réciprocité quadratique, montrez que 3 est un résidu quadratique modulo $p \neq 2, 3$ si et seulement si $p \equiv \pm 1 \bmod 12$. En supposant M_q est premier, montrez le*

petit théorème de Fermat suivant dans $\mathbb{Z}[\sqrt{3}]$*:* $(x+y\sqrt{3})^p \equiv x - y\sqrt{3} \bmod p$*. En remarquant que* 2 *est un carré modulo* p*, on définit dans* $\mathbb{Z}[\sqrt{3}]/(p)$*:* $\tau = \frac{1+\sqrt{3}}{\sqrt{2}}$ *et* $\overline{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}$*. A partir des relations* $\tau^2 = 2+\sqrt{3}$ *et* $\tau\overline{\tau} = -1$*, en déduire la congruence de l'énoncé.*

(iv) Montrez le test de primalité suivant sur M_q *pour* $q \geqslant 3$ *premier: soit* $(L_i)_{i\geqslant 0}$ *la suite de Lucas-Lehmer définie par* $L_0 = 4$ *et* $L_{i+1} = L_i^2 - 2 \bmod M_q$*, alors* M_q *est premier si et seulement si* $L_{q-2} \equiv 0 \bmod M_q$*.*

Fonctions arithmétiques

Exercice 2. *Soit* μ *la fonction de Möbius sur* $\mathbb{N}$ *définie comme suit*

$$\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ s'il existe } p \text{ premier tel que } p^2 | n \\ (-1)^r \text{ si } n \text{ est sans facteur carré et si } n = \prod_{i=1}^r p_i \end{cases}$$

Une fonction $f : \mathbb{N}^* \longrightarrow \mathbb{R}$ *est dite multiplicative si* $f(mn) = f(m)f(n)$ *pour* n *et* m *premiers entre eux.*

(i) Montrez que si f *est multiplicative, il en est de même de* $g(n) = \sum_{d|n} f(d)$*.*

(ii) Montrez que μ *est multiplicative et que* $\sum_{d|n} \mu(d)$ *vaut* 1 *pour* $n = 1$ *et est nulle si* $n > 1$*.*

(iii) Montrez que pour $g(n) = \sum_{d|n} f(d)$ *avec* $n \geqslant 1$*, on a*

$$f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d)$$

c'est la première formule d'inversion de Möbius.

(iv) Réciproquement si $g : \mathbb{N}^* \longrightarrow \mathbb{R}$ *est telle que* $f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d)$ *pour tout* n *alors* $g(n) = \sum_{d|n} f(d)$*.*

(v) Soit $F : [1, +\infty[\longrightarrow \mathbb{R}$ *et* $G(x) = \sum_{n=1}^{[x]} F(\frac{x}{n})$*. Montrez la deuxième formule de Möebius*

$$F(x) = \sum_{1 \leqslant n \leqslant x} \mu(n) G(\frac{x}{n})$$

pour $x \geqslant 1$ *et prouvez la réciproque.*

Exercice 3. *Pour* d *entier et* x *réel, soit* $H_d^x = \{(u,v) \in \mathbb{N}^2 \ / \ 1 \leqslant u, v \leqslant x, \ (u,v) = d\}$*. On va montrer le théorème de Dirichlet, à savoir que*

$$\lim_{n \to +\infty} \frac{|H_1^n|}{n^2} = \frac{6}{\pi^2}$$

(i) Montrez que $|H_1^x| = \sum_{k \geqslant 1} \mu(k) [x/k]^2$*, où* μ *est la fonction de Möbius (cf. l'exercice précédent).*

(ii) Montrez que $\lim_{n \to +\infty} \frac{|H_1^n|}{n^2} = \sum_{k=1}^{\infty} \mu(k)/k^2$ *et conclure en remarquant que* $(\sum_{k=1}^{\infty} \mu(k)/k^2)(\sum_{k=1}^{\infty} 1/k$ 1*.*