TP 3 : Primalité, factorisation, RSA

Exercice 1 (factorisation naïve) 1. Écrire une fonction `factor_1(N)` qui factorise N en faisant la division euclidienne de N par tous les entiers $d \leq \sqrt{N}$. Pourquoi peut–on s'arrêter à $\sqrt{N}$?

2. Écrire une fonction `factor_2(N)` semblable, mais qui ne divise que par 2 et les entiers impairs.

3. Idem en ne divisant que par 2, 3, puis les entiers congrus à ± 1 modulo 6.

4. Idem en ne divisant que par les nombres premiers (utiliser la commande `next_prime`).

5. Comparer les temps des différentes procédures (ainsi que celle de Sage) pour $N = 3^{23} + 1$?

Exercice 2 (test de pseudo-primalité) 1. Trouver un entier (aléatoire) N ayant environ 200 chiffres décimaux qui passe le test de pseudo-primalité de Fermat pour la base $a = 3$. En moyenne, combien faut–il choisir de N avant d'en trouver un convenable ?

2. Même question pour le test de Miller–Rabin.

3. Trouver un pseudo-premier de Fermat en base 3, mais non pseudo-premier fort de Miller-Rabin en base 3 (on pourra chercher un nombre N d'environ 5 chiffres).

Exercice 3 (nombres de Carmichael) On dit que N est un nombre de Carmichael si N est composé et si $a^N = a \mod N$ pour tout entier a, ou de manière équivalente si $a^{N-1} = 1 \mod N$ pour toute base a première à N. Ils sont rares, mais on sait depuis peu qu'il en existe une infinité (1994, Alford, Granville et Pomerance).

1. Ecrire une procédure qui teste si un nombre N est de Carmichael (utiliser la commande `power_mod` pour l'exponentiation rapide modulo N, procédure qu'il faut savoir coder !).

2. Vérifier que 561 est un nombre de Carmichael, puis lister les nombres de Carmichael < 100000.

3. Quelle est la probabilité qu'un nombre de Carmichael N soit pseudo-premier de Fermat dans une base aléatoire $1 \leq a \leq N - 1$? Tester expérimentalement ce résultat avec $N = 75361$, en considérant 1000 tirages de bases aléatoires. Comparer avec le taux d'échec du test de Miller-Rabin.

4. Montrer que si $N = p_1 \cdots p_r$ où $r \geq 2$ et les $p_i \geq 3$ sont des nombres premiers distincts tels que $p_i - 1$ divise $N - 1$ pour tout i, alors N est un nombre de Carmichael (la réciproque est vraie, théorème de Korselt, 1899). En déduire une autre procédure pour lister les nombres de Carmichael < 100000. Quelle approche est la plus rapide ?

Exercice 4 (preuves de primalité) 1. A l'aide du théorème de Lucas, montrer que les nombres suivants sont premiers:

$$p_0 = 2017 \qquad p_1 = 2^{16} + 1 \qquad p_2 = 2^{34}3^{29}5^27^{29} + 1.$$

2. Un nombre de *Sophie Germain* est un nombre premier p tel que $2p + 1$ est aussi premier. Montrer à l'aide du Théorème de Lucas que

$$p = 2^{22}7^{15} + 1$$

est un nombre de Sophie Germain.

Exercice 5 (RSA, protocole et attaques) Le destinataire choisit deux nombres premiers p et q, puis calcule $N = pq$ et $\varphi = (p-1)(q-1)$. Il choisit aléatoirement $e \in (\mathbb{Z}/\varphi\mathbb{Z})^*$ et calcule $d < \varphi$ tel que $ed = 1 \mod \varphi$.

- La *clé publique* est (N, e), rendue publique par le destinataire.
- La *clé privée* est (p, q, d), gardée secrète par le destinataire.

Tout message est transmis sous la forme d'un entier $M \in \mathbb{Z}/N\mathbb{Z}$ (e.g. avec le code ASCII), quitte à le découper en plusieurs messages plus petits.

Chiffrement. L'expéditeur calcule $m := M^e \mod N$ et expédie son message chiffré m.

Déchiffrement. Le destinataire récupère le message clair en calculant $m^d = M \mod N$ avec sa clé privée.

1. Écrivez une procédure `GenClef` qui génère aléatoirement une clef publique (N, e) et une clef privée (p, q, d) où p, q sont choisis au hasard parmi les nombres premiers dans $[10^6, 10^7]$ et e est choisi uniformément entre 2 et $(p-1)(q-1)$.
2. Construire avec `GenClef` une clé publique et une clé privée. Chiffrer le message 1234567890 en utilisant la clé publique et vérifier que la clé privée permet effectivement de déchiffrer le message reçu.
3. Un utilisateur de RSA publie sur sa page personnelle sa clé publique (N, e). Par inadvertance, il publie aussi φ. Comment une personne mal intentionnée peut–elle en tirer parti pour retrouver la clé privée $[p, q, d]$? Tester votre méthode pour casser le cryptosystème construit à la question 2.
4. Même question si l'utilisateur publie d.

   Indication : On pose $M = ed - 1$. On sait que c'est un multiple de $\varphi(N)$. Choisir a au hasard. Si a n'est pas premier avec N, youpi ! On a trouvé un facteur $gcd(a, N)$ de N. Sinon, d'après le théorème de Fermat-Euler, on a $a^M = 1 \mod N$. Calculer s et t tels que $M = 2^s \times t$ avec t impair. On pose $b = a^t \mod N$. Donc $b^{2^s} = 1 \mod N$. On calcule $b \mod N, b^2 \mod N$, $(b^2)^2 \mod N$... jusqu'à trouver 1. Soit X la dernière valeur trouvée avant le 1 final. On a donc $X^2 = 1 \mod N$ et $X \neq 1 \mod N$. Si $X \neq -1 \mod N$ (cela arrive avec probabilité $\approx 2/3$ car il y a 4 solutions de $X^2 = 1 \mod N$ – cf exo 6 – et on sait que $X \neq 1 \mod N$), alors $N = \mathrm{pgcd}(X-1, N)\,\mathrm{pgcd}(X+1, N)$ est une factorisation non triviale de N, c'est gagné. Sinon, on recommence avec un autre a.

Exercice 6 (racine carrée) Dans cet exercice, on considère des entiers N impairs. À l'aide de la méthode de votre choix, déterminer le nombre de solutions de l'équation $x^2 = 1$ dans $\mathbb{Z}/N\mathbb{Z}$ pour chaque valeur

$$N = 1049,\ 1079,\ 1139,\ 1209,\ 1289,\ 4913.$$

Proposer une conjecture reliant le nombre de solutions modulo N et la factorisation de N, puis tester cette conjecture sur d'autres valeurs de N.