Université Paris 7, Paris Diderot

La factorisation d’entier

LEMOINNE Marianne VOVARD Hugo
Encadré par BRUNAT Olivier
lemoinne.marianne@gmail.com hugo.vovard@wanadoo.fr

June 5, 2018

Content

Des divisions successives au crible quadratique, quels sont les outils que nous donnes l'algèbre pour factoriser des entiers de l'ordre de 10^{50} ?

Test de primalité

Pour factoriser un nombre il faut déjà se demander si il est premier.
Nous utiliserons l'algorithme probabiliste de Miller Rabin.

Test de primalité

Pour factoriser un nombre il faut déjà se demander si il est premier. Nous utiliserons l'algorithme probabiliste de Miller Rabin.

$\pi(B)$

Soit $B \in \mathbb{N}$ on défini $\pi(B) = \frac{B}{logB}$ comme le nombre de nombres premiers inférieur ou égale à B.

Principe des divisions successives

Soit n l'entier que l'on cherche à factoriser, il suffit de diviser n par tous les nombres premiers qui sont inférieur à $\sqrt{n}$ jusqu'à trouver sa factorisation.

Principe des divisions successives

Soit n l'entier que l'on cherche à factoriser, il suffit de diviser n par tous les nombres premiers qui sont inférieur à $\sqrt{n}$ jusqu'à trouver sa factorisation.

exemple

On cherche la factorisation de 15 :

$$\sqrt{15} \approx 3.9$$

$$15 \equiv 1[2]$$

$$15 \equiv 0[3]$$

De plus $15 \div 3 = 5$ et 5 est premier donc

$$15 = 3 * 5$$

Principe de Fermat

La méthode de Fermat consiste à écrire n (le nombre dont on cherche la factorisation) comme une différence de carrés parfaits pour pouvoir le factoriser grâce à l'identité remarquable :
$(a+b)(a-b) = a^2 - b^2$

Principe de Fermat

La méthode de Fermat consiste à écrire n (le nombre dont on cherche la factorisation) comme une différence de carrés parfaits pour pouvoir le factoriser grâce à l'identité remarquable :
$(a+b)(a-b) = a^2 - b^2$

Lemme

L'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que $n = ab$ avec $b \leq a$, et celui des couples $(r, s) \in \mathbb{N}^2$ tels que $n = r^2 - s^2$,sont en bijection.

1. def fermat(n):
2. $\quad r$ prend la valeur $\lfloor \sqrt{n} \rfloor + 1$
3. $\quad$ Tant que $r^2 - n$ n'est pas un carré parfait:
4. $\quad\quad r$ prend la valeur $r + 1$
5. $\quad s$ prend la valeur $r^2 - n$
6. $\quad$ retourner $[r - \sqrt{s}, r + \sqrt{s}]$

Principe de Kraitchik

L'idée de Gauss repris par Kraitchik est de trouver une différence de carré égale à un multiple de n, i.e. deux entiers u et v tel que

$$u^2 \equiv v^2[n] \; et \; u \not\equiv \pm v[n]$$

En effet, dans ce cas on aura que n divise $(u-v)(u+v)$ sans diviser ni $u-v$ ni $u+v$, ainsi les valeurs $pgcd(u-v,n)$ et $pgcd(u+v,n)$ fournissent des diviseurs non triviaux de n.

Principe de Kraitchik

Il faut donc trouver u et v qui vérifient la condition précédente. Pour cela, partons du polynôme de Kraitchik: $Q(X) = X^2 - n \in \mathbb{Z}[X]$ L'idée va être ici de trouver une famille de $(x_i)_{i\in[1,k]}$ tel que le produit des $Q(x_i)$ soit un carré. Ainsi on pose

$$v^2 = Q(x_1) \cdot ... \cdot Q(x_k)$$

et

$$u = x_1 \cdot ... \cdot x_k$$

Comment trouver les $Q(x_i)$ tels que leur produit soit un carré ?

Définition

x est B-friable si tous les diviseurs premiers de x sont inférieurs ou égales à B.

Définition

x est B-friable si tous les diviseurs premiers de x sont inférieurs ou égales à B.

Lemme

Soient k et B des entiers naturels tels que $k \geq \pi(B) + 1$. Soient $m_1, ..., m_k$ des entiers naturels B-friables. Il existe une sous-famille non vide des m_i dont le produit est un carré.

En pratique:

- On pose pour tout entier i compris entre 1 et k, $k > \pi(B)$, $Q(x_i) = \prod_{j=1}^{\pi(B)} p_j^{\alpha_{i,j}}$ la décomposition en facteurs premiers de $Q(x_i)$ avec $\alpha_{i,j} \geq 0$

En pratique:

- On pose pour tout entier i compris entre 1 et k, $k > \pi(B)$, $Q(x_i) = \prod_{j=1}^{\pi(B)} p_j^{\alpha_{i,j}}$ la décomposition en facteurs premiers de $Q(x_i)$ avec $\alpha_{i,j} \geq 0$
- Soit M la matrice de taille $(k, \pi(B))$, où l'élément à la place (i, j) correspond à $\alpha_{i,j} mod(2)$ et l_i le i-éme vecteur de M.

En pratique:

- On pose pour tout entier i compris entre 1 et k, $k > \pi(B)$, $Q(x_i) = \prod_{j=1}^{\pi(B)} p_j^{\alpha_{i,j}}$ la décomposition en facteurs premiers de $Q(x_i)$ avec $\alpha_{i,j} \geq 0$
- Soit M la matrice de taille $(k, \pi(B))$, où l'élément à la place (i, j) correspond à $\alpha_{i,j} mod(2)$ et l_i le i-éme vecteur de M.
- Comme $k \geq (\pi(B) + 1)$, $\exists(\varepsilon_1, ..., \varepsilon_k) \in F_2^k$ tel que $\sum_{i=1}^{k} \varepsilon_i l_i = 0$. Donc $(\varepsilon_1, ..., \varepsilon_k) \in ker(M^t)$.

En pratique:

- On pose pour tout entier i compris entre 1 et k, $k > \pi(B)$, $Q(x_i) = \prod_{j=1}^{\pi(B)} p_j^{\alpha_{i,j}}$ la décomposition en facteurs premiers de $Q(x_i)$ avec $\alpha_{i,j} \geq 0$
- Soit M la matrice de taille $(k, \pi(B))$, où l'élément à la place (i, j) correspond à $\alpha_{i,j} mod(2)$ et l_i le i-éme vecteur de M.
- Comme $k \geq (\pi(B) + 1)$, $\exists(\varepsilon_1, ..., \varepsilon_k) \in F_2^k$ tel que $\sum_{i=1}^{k} \varepsilon_i l_i = 0$. Donc $(\varepsilon_1, ..., \varepsilon_k) \in ker(M^t)$.
- Soit $I \subseteq \{1, ..., k\}$ l'ensemble des i tels que $\varepsilon_i = 1$. On a donc $\sum_{i \in I} l_i = 0$, i.e. $\prod_{i \in I} Q(x_i)$ est un carré.

Comment choisir B ?

Comment trouver des $Q(x_i)$ B-friable ?

Nous admettrons que la constante B doit être de l'ordre de

$$exp(\frac{1}{2}\sqrt{log(n)log(log(n))})$$

Lemme

Soit p un nombre premier impaire.

1. Alors $Q(X)$ a exactement 2 racines modulo p.
2. Soit p un nombre premier et a un entier tel que $Q(a) \equiv 0[p^k]$. Alors il existe $b \in [|1; p-1|]$ tel que $2ab \equiv 1[p]$. De plus on a :

$$Q(a + (n + a^2) * b) \equiv 0[p]$$

Trouver des $Q(x_i)$ B-friable, $i \in [|\lfloor\sqrt{n}\rfloor + 1; \lfloor\sqrt{n}\rfloor + A|]$:

def B-friable(B, n, A):
    $T = [(\lfloor\sqrt{n}\rfloor + 1)^2 - n; (\lfloor\sqrt{n}\rfloor + 2)^2 - n; ...; (\lfloor\sqrt{n}\rfloor + A)^2 - n]$, $P = \{p \leq B \mid p \textit{ premier}\}$, puissance=1
    Pour $p \in P$:
        (a_1, a_2)=racine Q mod(p)
        for $a \in (a_1, a_2)$:
            Cribler T avec a
        Tant que $(a_1, a_2) \in T$:
            (a_1, a_2)=racine sup((a_1, a_2), p, puissance)
            for $a \in (a_1, a_2)$:
                Cribler T avec a
    Retourner $\{(\lfloor\sqrt{n}\rfloor + i)^2 - n | i \in [|1; A|], \; T[i] = 1\}$

Principe du crible

- Soit n l'entier à factoriser
- On calcule B
- On trouve au moins $\pi(B) + 1$ $Q(x_i)$ B-friable
- On recherche les congruences carrées u et v comme vu précédemment
- On calcule $pgcd(u - v, n)$
- Si le pgcd est premier on à trouver un facteurs premier sinon on relance l'algorithme sur $pgcd(u - v, n)$

Conclusion

Bibliographie

- Cours de cryptographie MM067-2012/13. Alain Kraus
- Algorithme Miller Rabin : http://python.jpvweb.com/python/mesrecettespython/doku.php?id=est_premier
- Test des différents algorithmes de factorisation https://www.utc.fr/~wschon/sr06/UtCrible/CFRACMethodPage.php
- Factoriser un nombre entier : http://villemin.gerard.free.fr/Wwwgvmm/Premier/Facto.htm

Merci de votre attention.
Avez vous des questions ?