

# Test de Primalité

Jean-Didier Pailleux - Robin Feron - Romain Robert - Damien Thenot -  
Maxence Joulin

UVSQ

13/05/2018

- **Tests déterministes** : AKS, Pocklington, Euclide/Computation Bound, Eratosthène/Memory Bound.
- **Test probabiliste** : Miller-Rabin.
- **Rappel** : Miller-Rabin très efficace, méthodes naïves utiles pour les petits nombres et AKS peu performante à cause de NTL.
- **Objectif** : Optimisation des algorithmes et travail sur la parallélisation.

- 1 Optimisation
- 2 Parallélisation
- 3 Résultats
- 4 Bilan Technique
- 5 Problèmes Rencontrés
- 6 Conclusion

- 1 Optimisation
- 2 Parallélisation
- 3 Résultats
- 4 Bilan Technique
- 5 Problèmes Rencontrés
- 6 Conclusion

## Memory Bound

- Suppression des nombres pairs du tableau → Réduction de la taille du tableau.
- Réduction du nombre d'itérations →  $N$  à  $\sqrt{N-3}$ .

## AKS

Implémentation d'une variante d'AKS → Complexité passant de  $O(\log(n))^{12}$  à  $O(\log(n))^3$ .

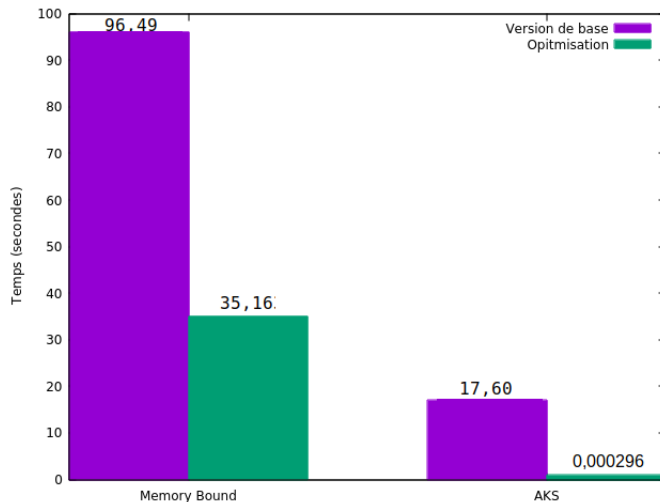


FIGURE – Comparaison de la version de base avec la version optimisé.

- 1 Optimisation
- 2 Parallélisation**
- 3 Résultats
- 4 Bilan Technique
- 5 Problèmes Rencontrés
- 6 Conclusion

## Outils utilisés

- OpenMP
- MPI (Message Passing Interface)



## Outils utilisés

- OpenMP
- MPI (Message Passing Interface)

## Parallélisation des algorithmes

- Implémentations non concluantes : AKS, Conjecture, Miller-Rabin, Pocklington
- Implémentation concluante : Memory Bound

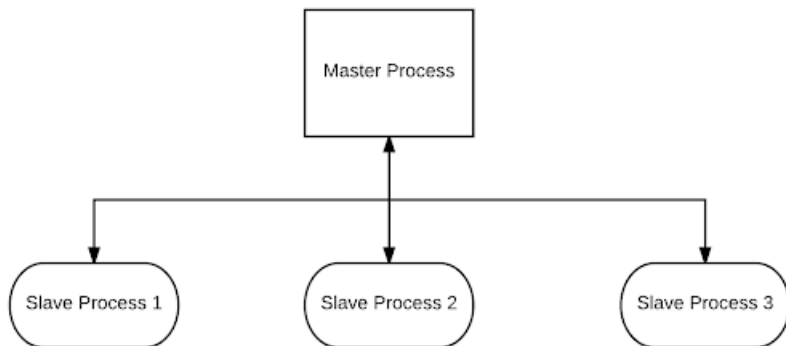


FIGURE – Schéma du Modèle du Master-Slave

- 1 Optimisation
- 2 Parallélisation
- 3 Résultats**
- 4 Bilan Technique
- 5 Problèmes Rencontrés
- 6 Conclusion

- Lancement des tests sur le cluster Poincare de la MDLS.
- Tests réalisés sur 10 itérations.
- Lors de la soumission du job Pocklington et AKS n'ont pas pu finir leur exécution avant d'être tué par le supercalculateur.

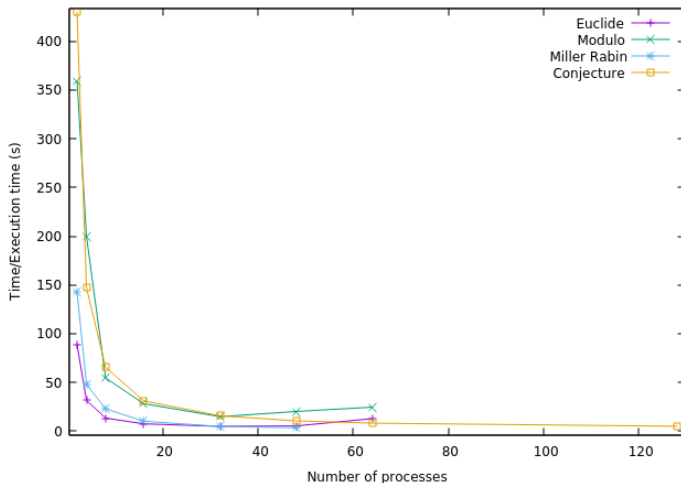


FIGURE – Évolution du temps de calcul pour Conjecture, Miller-Rabin, Euclide et Modulo ; Plage [1, 1 000 000]

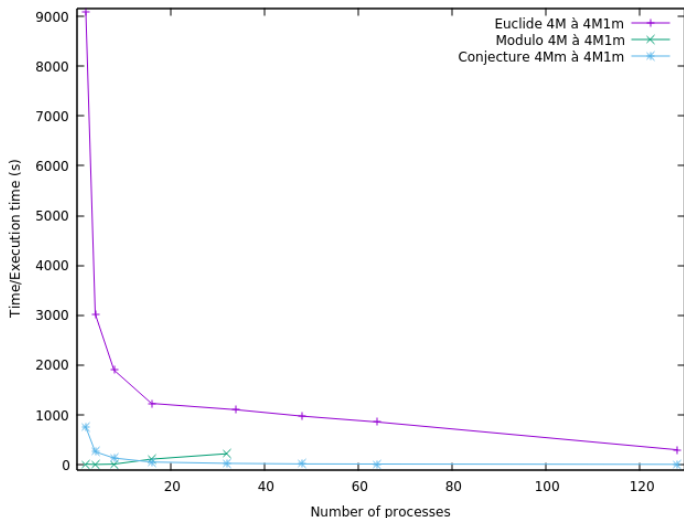


FIGURE – Évolution du temps de calcul pour Conjecture, Euclide et Modulo ; Plage [4M, 4M1m]

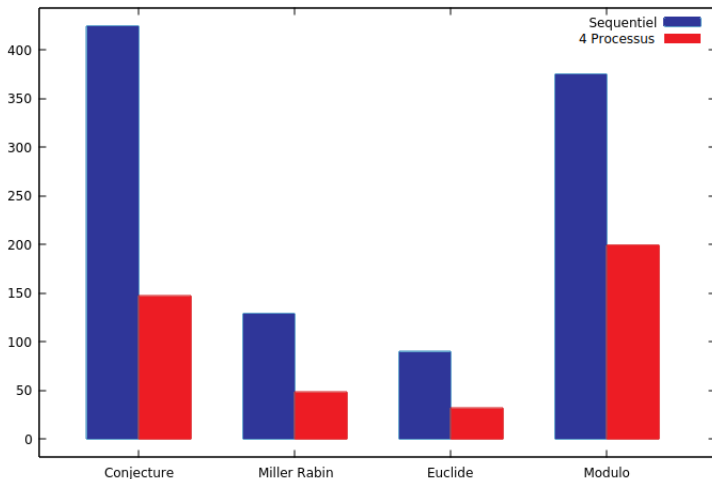


FIGURE – Comparaison Conjecture, Miller-Rabin, Euclide et Modulo avec le séquentiel

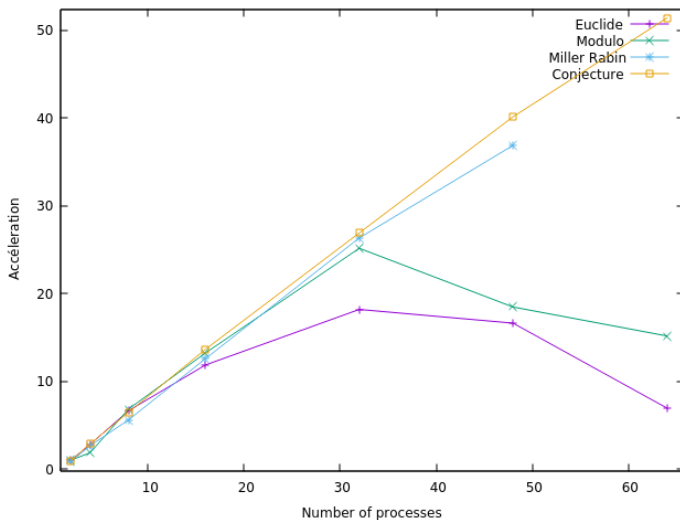


FIGURE – Évolution de l'accélération en fonction du nombre de processus; Plage [1, 1 000 000].



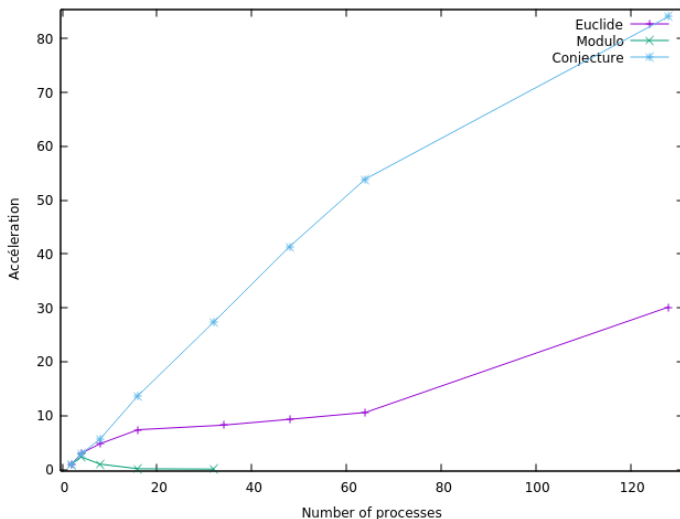
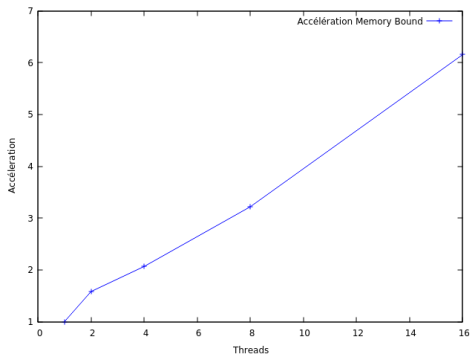
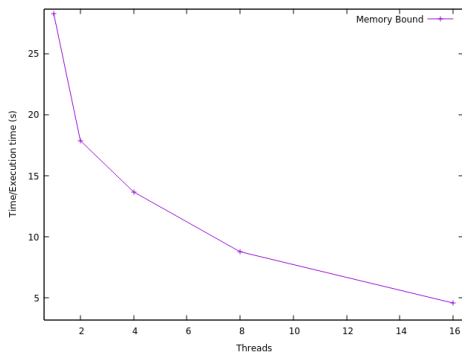


FIGURE – Évolution de l'accélération en fonction du nombre de processus; Plage [4M, 4M1m].



**Figures** - Évolution du temps de calcul et de l'accélération pour Memory Bound en fonction du nombre de threads.

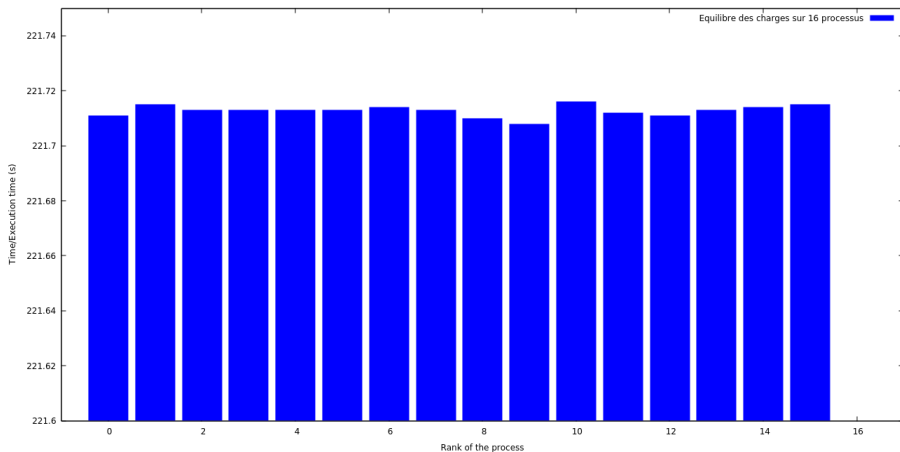


FIGURE – Exemple d'équilibre des charges obtenu avec 16 processus MPI.

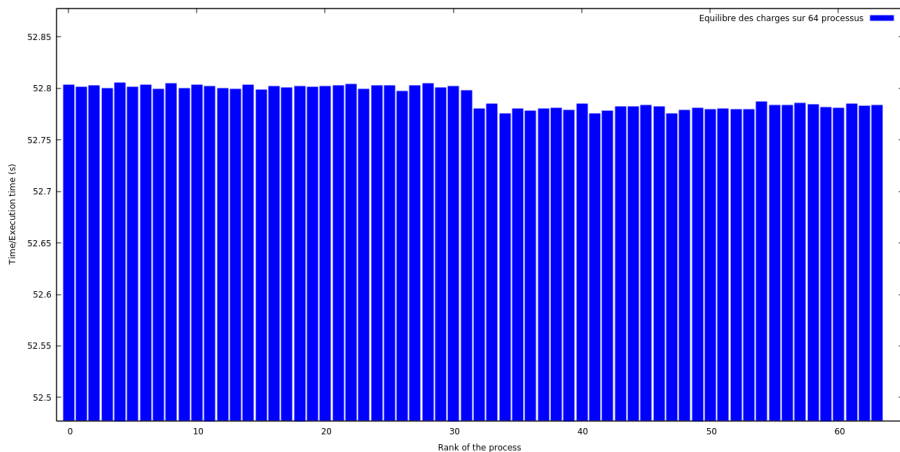


FIGURE – Exemple d'équilibre des charges obtenu avec 64 processus MPI.

- 1 Optimisation
- 2 Parallélisation
- 3 Résultats
- 4 Bilan Technique**
- 5 Problèmes Rencontrés
- 6 Conclusion

- Une bonne scalabilité forte.
- Un palier max d'accélération.
- Le processus Maître trop chargé en travail.

## De meilleurs schémas de communications

- Augmentation du nombre données à traiter par un esclave à chaque communication du Maître.
- Augmentation du nombre de Maîtres.

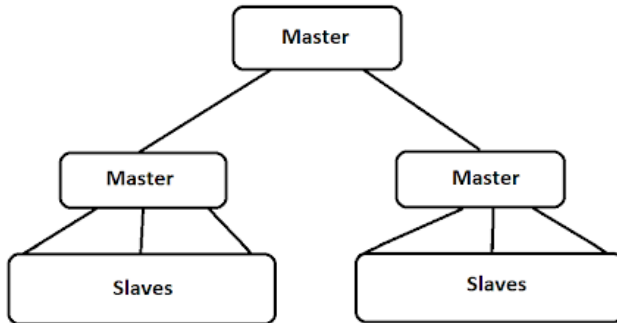


FIGURE – Schéma avec augmentation du nombre de Maître



- Un équilibrage des charges efficace.
- Des temps de calcul très courts.
- Des temps de calcul répartis de manière uniforme.
- Des différences finales négligeable entres les processus.

- Les tests de primalité sont peu parallélisable.
- Seule l'augmentation du volume de donnée permet de tirer avantage du parallélisme.

- 1 Optimisation
- 2 Parallélisation
- 3 Résultats
- 4 Bilan Technique
- 5 Problèmes Rencontrés**
- 6 Conclusion

- Utilisation de bibliothèques sur le supercalculateur (NTL, GMP).
- Manque de temps.
- Dysfonctionnement du supercalculateur.

- 1 Optimisation
- 2 Parallélisation
- 3 Résultats
- 4 Bilan Technique
- 5 Problèmes Rencontrés
- 6 Conclusion**

- Résultat final satisfaisant et équilibrage des charges efficace.
- Possibilité d'étudier d'autres techniques de parallélisation.
- Utilisation d'algorithmes nativement parallèle.