# Rapport Maths Discrètes

Gaetan Schwaederle, Maxime Poiret

## Question 4 :

Pour analyser la tendance, il suffit de prendre 18 valeurs. Nous pouvons remarquer que la proportion de nombre premier baisse considérablement et rapidement. Cela veut dire que plus i est grand, plus la proportion approche 0.

## Question 5 :

Sans compter la valeur i=1, voici le graphe jusque i=19. On peut voir qu’il n’y a pas d’erreur pour les valeurs de i entre 2 et 7 cependant ensuite, nous pouvons voir qu’il y a toujours des erreurs. La proportion de celles-ci réduit plus i augmente mais dans l’intervalle [8,13], la proportion d’erreur est immense. Seul bémol, pour i=1, il y a un taux d’erreur de 0,5 car TestFermat ne compte pas 2 comme nombre premier.

## Question 6 :

Protocole expérimentale montrant que TestFermat est asymptotiquement (dans le pire des cas) plus rapide que PrimaliteNaif :

Dans l’algorithme TestFermat, on choisit un nombre aléatoire positif a plus petit que n. Ce nombre étant ensuite mis à la puissance n - 1, le pire cas possible est donc a = n-1 mais le calcul reste en O(1).

Ensuite, on calcule le modulo n du résultat précédant, une opération encore une fois en O(1) mais sur un très grand nombre.

Cependant, PrimaliteNaif calcule i mod n pour tout i < n, on peut améliorer l’algorithme en ne regardant que les nombres alant juqu’à , mais l’algorithme reste toujours en O() tandis que Fermat est en O(1).

On peut réaliser un protocole expérimental visant à tester PrimaliteNaif et TestFermat pour n appartenant à [[ et dans ce cas choisir pour TestFermat a = n-1 pour forcer le pire des cas.

## Question 8 :

## Question 9 :

On a n = pq avec p et q deux nombres premiers. On a donc p et q premier entre eux.

Or et donc

Ensuite, on sait que

Donc , on a k existant dans N.

Donc

Prenons maintenant x appartenant à N et x premier avec n :

On sait que x n’est ni un multiple de p ni un multiple de q.

Ainsi, d’après le théorème de Fermat, et

De plus, puisque x n’est pas multiple de q :

De même puisque x n’est pas multiple de p :

Ceci nous permet de conclure que si x est premier avec n alors :

## Question 10 :

On cherche A|A(n1,e1,M1) ->m

On sait que

avec q toujours inconnu

Pour trouver m on doit chercher

On doit donc réaliser une boucle sur les valeurs de q(N) et à chaque itération, vérifier si le résultat est premier avec n1.

De plus, si on trouve un résultat possible m’, il faut ensuite vérifier que m’ est premier avec n2 et n3. Pour finir, nous devons vérifier que :

-

-

Or ce n’est pas réalisable de façon polynomiale.