Nombres de Sophie Germain :

premier tel que est aussi premier.

Conjecture :

On obtient un meilleur temps de réponse en faisant varier le coefficient plutôt que le nombre premier.

####Insérer courbe pour k=2####

Intérêt théorique :

Pour aléatoire, divise d’après le théorème de Lagrange.

Donc l’ordre de est inférieur à ou est multiple de .

Donc on effectue pour variant de à et si pour tout alors l’ordre de est strictement supérieur à et donc multiple de .

Ainsi est un générateur d’un sous-groupe de d’un cardinal satisfaisant.