Courbes elliptiques et cryptographie

R. Stancu

Une courbe elliptique E définie sur un corps k est l'ensemble des solutions dans k^2 de l'équation de Weierstrass $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, où les coefficients a_1, a_2, a_3, a_4 et a_6 sont dans k. Sur l'ensemble de ces solutions on peut mettre une loi de groupe (qui a le 'point a l'infini' comme élément neutre). Pour g et h deux points sur la courbe elliptique, trouver n tel que $nh = h + h + ... + h = g$ nécessite, en général, un algorithme de complexité exponentielle (vue comme fonction du nombre d'éléments de k). On étudie comment trouver des 'bonnes' puissances $q = p^r$ de nombres premiers et 'bonnes' courbes elliptiques sur F_q qui fournisses des exemples dans lesquels le problème du logarithme discret plus haut est exponentiel, donc fournit de bonnes clés pour la cryptographie.