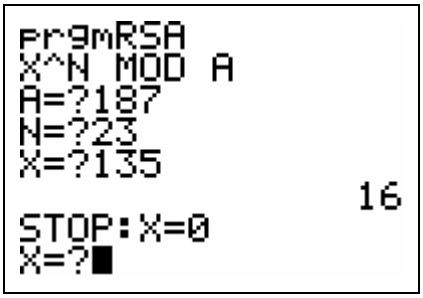
Calcul efficace de x^n et congruences.

L'activité suivante concerne le niveau terminale S, spécialité maths et plus particulièrement dans la partie arithmétique et congruences : le cryptage RSA.

Le cryptage RSA est un exemple d'application de l'arithmétique à la cryptographie qui a le mérite de montrer aux élèves une utilisation actuelle de leur travail.

Dans les applications numériques, il met en jeu des calculs de puissances et de congruences, par exemple on peut être amené à calculer le reste dans la division euclidienne par 187 de 13523 (exemple tiré du manuel Déclic TS 2006).

Un calcul direct avec une calculatrice courante de 135^{23} ne donne pas de résultat exact, la machine ne peut pas afficher autant de chiffres et passe automatiquement en notation scientifique, voire en dépassement de capacité.



Si les nombres proposés ne sont pas ridiculement petits, les calculs sont vite fastidieux. Pour une puissance donnée, on peut appliquer la technique qui consisterait dans l'exemple ci-dessus à étudier les puissances de 135 modulo 187 et simplifier les calculs le plus possible, comme c'est proposé dans le document d'accompagnement des programmes.

Si l'on veut coder ne serait-ce qu'un petit message, des puissances de bases différentes interviennent et le temps de cryptage ou décryptage à la main devient prohibitif.

Pour y remédier, on peut créer un petit programme sur calculatrice qui traite ces calculs. Il repose sur une façon efficace de calculer les puissances ainsi que leur compatibilité avec les congruences.

Utilisation en classe

On peut donner la fiche élève comme une fiche outil à utiliser lors d'un exercice de cryptage/décryptage, sans approfondir le côté algorithmique à priori. Il est toujours temps après coup de répondre aux éventuelles questions pour expliquer le calcul d'une puissance.

Note : 1. Il n'y a pas d'erreur dans le manuel Déclic 2006:
135^{23} est bien congru à 16 modulo 187, cela permet de vérifier le programme!

2. pour un meilleur confort de lecture, il vaut mieux imprimer la fiche élève.

3. les calculatrices plus puissantes donnent un résultat correct.