Towards Euclid's Algorithm

1. If a and b are relatively prime, then there exist integers m and n such that $ma + nb = 1$.

2. If a and b are relatively prime and a divides qb then a divides q.

3. Suppose a and b are two integers, d is the greatest common divisor of a and b, $S = \{ma + nb : m, n \in \mathbb{Z}\}$ and $T = \{kd : k \in \mathbb{Z}\}$. Show that $S = T$.

4. If a, b, k are integers then $\gcd(a, b) = \gcd(a - kb, b)$

5. Let a, b be two integers. State and prove Euclid's algorithm that will provide the $\gcd(a, b)$.

Puzzle:

1. Snack's in the ISI canteen are being eaten by an over eating enthusiast. The supreme food council decided to secure daily snack in a safe with a combination number lock. They decide that two students can be trusted but not one. So the secret of this number should be shared among all students but only in a way which it needs at least two students to get the secret. Device an algorithm by which any two members together can reconstruct the secret.

2. The student toffee counter has many valuable chocolates. Chief Warden decides to secure it with a combination number lock. She decides that three students can be trusted but not two or one. So the secret of this number should be shared among all students but only in a way which it needs at least three students to get the secret. Device an algorithm by which any three members together can reconstruct the secret.

3. Can you generalise this ? You want to share a secret among N people, so that any k ($k < N$) of the people can recover the secret but no fewer than k people can possibly know enough to recover the secret.