**LÝ THUYẾT MẬT MÃ**

**1. Cơ sở toán học**

**1.1. Số học các số nguyên**

Tập số nguyên Z, tập số nguyên dương Z+ đóng kín đối với phép cộng, trừ, nhân nhưng không đóng kín với phép chia.

VD: a = 2, b = 3 thuộc Z

* a + b = 5 thuộc Z
* a - b = -1 thuộc Z
* a \* b = 6 thuộc Z
* a / b = 2/3 không thuộc Z

Hai số nguyên bất kỳ a và n, n>1:  
a=q.n+r,0<r<n

* q = a div n: số chia
* r = a mod n: số dư