$\mathbb{F}_7$ の 2次方程式

$\mathbb{F}_7 = \{0,1,2,3,4,5,6\}$ を係数とる2次方程式 ← (7で割って1余る数全体を 1 mod 7 とか1と表すが、ここでは単に1と書く)

(1) $x^2+ax+b=0 \quad (a,b \in \mathbb{F}_7)$

のうちどれが因数分解できるのかを調べたい。

通常のように個別に因数分解していくのではなく、逆に

(2) $(x-c)(x-d)=0 \quad (c,d \in \mathbb{F}_7)$

の左辺を展開し、それを表にして、$x^2+ax+b=0$ がその表にあるか検索するという方法をとる。

$(x-c)(x-d) = x^2-(c+d)x+cd$ なので

$a=-(c+d)$, $b=cd$ だから c,d から a,b を計算しそれを表にする。詳しくは Excel ファイルの「計算式」というシートを参照。

ひとたび表が出来たらそれを a,b に基づいた順序に並べ換える。これには Excel の「データ」のところにある「フィルター」を用いる。

注) (1)の形の2次式は $7\times7=49$ 個あるが、

(2)の形のものは $7+\frac{7\times6}{2}=28$ 個ある。

残りの $49-28=21$ 個は因数分解不可能。