上智大学 2011 年度オープンキャンパス
情報理工学科体験授業 (2011 年 7 月 24 日)

「有限の算術と秘密分散の数理技術」

角皆 宏 (つのがい ひろし)
http://www.ics.sophia.ac.jp/tsunogai/

本日のお品書き

- 情報技術・数理技術 — 数理現象の探求と応用
- 有限の算術 (剰余系)・有限体
  - ⋆ 実習 : 剰余系の掛け算の表を作ろう
- 有限の算術を利用した数理技術の例 : 秘密分散
  - ⋆ 実習 : 分散された秘密情報を復元しよう
- 割り算って何さ ? — 定義に立ち戻ること
- 代数と幾何 — 数と図形 — の共働
- 数理技術とその応用
- 情報理工学科で触れられること

御案内

- 数学図書室公開 (4 号館 5 階 4-595A)
- 情報理工学科 教員・在校生相談コーナー (1 号館 1 階 1-103)

2011 年度オープンキャンパス

情報理工学科体験授業「有限の算術と秘密分散の数理技術」 (角皆)

1 (剰余系の掛け算)

$m = 3, 4, 5, 6, 7$ について、m を法とする掛け算表を埋めてみよう。
(m の値による様子の違いは ?)

$m = 3$

$\times$	1	2
1		
2		

$m = 4$

$\times$	1	2	3
1			
2			
3			

$m = 5$

$\times$	1	2	3	4
1				
2				
3				
4				

$m = 6$

$\times$	1	2	3	4	5
1					
2					
3					
4					
5					

$m = 7$

$\times$	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

2 (秘密分散)

$p = 7$ を法とする計算で、自分の鍵ともう一人の鍵とから秘密情報 b を復元しよう。

- 自分の鍵 $(x_0, y_0) = (\quad , \quad)$
- もう一人の鍵 $(x_1, y_1) = (\quad , \quad)$
- 直線の傾き (ランダムに選んだ秘密のパラメタ)

$$a = \frac{y_1 - y_0}{x_1 - x_0} = \frac{\square - \square}{\square - \square} = \frac{\square}{\square} = \square$$

- 秘密情報

$$b = y_0 - ax_0 = \square - \square \cdot \square = \boxed{\square}$$