

MA 437 Applicable Algebra, Homework 1, Jan 21 05

- The b-nary expansion of a is $(c_n, \dots, c_1, c_0)_b$ means that $a = \sum_{i=0}^n c_i b^i$.
 - Compute the hexadecimal ($b = 16$) expansions of 101 (one hundred and one) and of 10^4
 - Compute $2199^{2269} \bmod 2633$ (Try Maple!)
 - Compute $541^{-1} \bmod 8692$ and $29^{-1} \bmod 2622$
- Decipher the following messages
 - KEEWS IHTKR OWEMO HEVAH ODEW
Hint: Try a transposition cipher.
 - mst ds cn b xprsd n fwr ltrs
bt th xprnc s mst nplsnt
 - MSTDS CNBXP RSDNF WRLTR SBTTH XPRNC SMSTN PLSNT
 - IICEC SORAA NEMWQ DEIUX
Hint: Try a 4×5 square.
- If $M = \begin{bmatrix} BA - I & B \\ 2A - ABA & I - AB \end{bmatrix}$ show that $M = M^{-1}$.
Use the Levine-Hill cipher $\mathbf{y} = M\mathbf{x}$, with $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, to encipher the message “we do have home work this week”. Use the alphabet map α_0 , where $a \rightarrow 0$ and $b \rightarrow 1 \bmod 26$ etc. and COLUMN-inscription.
 - If $ABA = A$, $BAB = B$ and $M(A, B) = \begin{bmatrix} A & I - AB \\ I - BA & B \end{bmatrix}$, show that $M(A, B)^{-1} = M(B, A)$.
- Show that $(k, mn) = 1$ iff $(k, m) = 1$ and $(k, n) = 1$ (over \mathbb{Z})
- Solve $2x_1 + 3x_2 + 7x_3 + 14x_4 + 27x_5 = 37$ if $x_i = 0, 1$
What property of the coefficients makes this solvable ?
- Cryptanalyze the following **affine**-cipher and **SHOW** your analysis:
TIVWI ZIVER GIMRG VCTXE
REPCW MWMWI WWIRX MEP