In [1]:

```
# Hill-3-cipher matrix
A=matrix([[1,2,3],[0,1,1],[1,1,0]])
show(A)
```

Out[1]:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

In [2]:

```
# check if A is invertible
det(A)
```

Out[2]: -2

In [3]:

```
# the characters "LIN"
#
b=vector(ZZ,[11,8,13]).column()
show(b)
```

Out[3]:

$$\begin{pmatrix} 11 \\ 8 \\ 13 \end{pmatrix}$$

In [4]:

```
# Hill cipher with key A
#
show(A*b)
```

Out[4]:

$$\begin{pmatrix} 66 \\ 21 \\ 19 \end{pmatrix}$$

In [5]:

```
# divide each by 29 and get the remainders
#
show(A*b.mod(29))
```

Out[5]:

$$\begin{pmatrix} 8 \\ 21 \\ 19 \end{pmatrix}$$

In [6]:

```
# the characters "EAR"
#
b=vector(ZZ,[4,0,17]).column()
show(b)
```

Out[6]:

$$\begin{pmatrix} 4 \\ 0 \\ 17 \end{pmatrix}$$

In [7]:

```
# Hill cipher with key A
#
show(A*b)
```

Out[7]:

$$\begin{pmatrix} 55 \\ 17 \\ 4 \end{pmatrix}$$

In [8]:

```
# divide each by 29 and get the remainders
#
show(A*b.mod(29))
```

Out[8]:

$$\begin{pmatrix} 26 \\ 17 \\ 4 \end{pmatrix}$$

In [9]:

```
# the characters "_AL"
#
b=vector(ZZ,[28,0,11]).column()
show(b)
```

Out[9]:

$$\begin{pmatrix} 28 \\ 0 \\ 11 \end{pmatrix}$$

In [10]:

```
# Hill cipher with key A
#
show(A*b)
```

Out[10]:

$$\begin{pmatrix} 61 \\ 11 \\ 28 \end{pmatrix}$$

In [11]:

```
# divide each by 29 and get the remainders
#
show(A*b.mod(29))
```

Out[11]:

$$\begin{pmatrix} 3 \\ 11 \\ 28 \end{pmatrix}$$

In [12]:

```
# the characters "GEB"
#
b=vector(ZZ,[6,4,1]).column()
show(b)
```

Out[12]:

$$\begin{pmatrix} 6 \\ 4 \\ 1 \end{pmatrix}$$

In [13]:

```
# Hill cipher with key A
#
show(A*b)
```

Out[13]:

$$\begin{pmatrix} 17 \\ 5 \\ 10 \end{pmatrix}$$

In [14]:

```
# divide each by 29 and get the remainders
#
show(A*b.mod(29))
```

Out[14]:

$$\begin{pmatrix} 17 \\ 5 \\ 10 \end{pmatrix}$$

In [15]:

```
# the characters "RA?"
#
b=vector(ZZ,[17,0,27]).column()
show(b)
```

Out[15]:

$$\begin{pmatrix} 17 \\ 0 \\ 27 \end{pmatrix}$$

In [16]:

```
# Hill cipher with key A
#
show(A*b)
```

Out[16]:

$$\begin{pmatrix} 98 \\ 27 \\ 17 \end{pmatrix}$$

In [17]:

```
# divide each by 29 and get the remainders
#
show(A*b.mod(29))
```

Out[17]:

$$\begin{pmatrix} 11 \\ 27 \\ 17 \end{pmatrix}$$

In [18]:

```
# get inverse key
#
show(A^(-1))
```

Out[18]:

$$\begin{pmatrix} \frac{1}{2} & -\frac{3}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{3}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

In [19]:

```
# recall the Hill cipher of "LIN" with key A
#
b=vector(ZZ,[8,21,19]).column()
show(b)
```

Out[19]:

$$\begin{pmatrix} 8 \\ 21 \\ 19 \end{pmatrix}$$

In [20]:

```
# decipher with inverse key of A
#
show(A^(-1)*b)
```

Out[20]:

$$\begin{pmatrix} -18 \\ 37 \\ -16 \end{pmatrix}$$

In [21]:

```
# convert the vector into ZZ ring (so that we can take mod)
#
bb=(A^(-1)*b).change_ring(ZZ)
show(bb)
```

Out[21]:

$$\begin{pmatrix} -18 \\ 37 \\ -16 \end{pmatrix}$$

In [22]:

```
# add 29 (or integer multiple of 29) to each to
# get non-negative entries so as to take mod(29)
# and get the decipher
# and the result is "LIN"
#
show((bb+29*ones_matrix(ZZ,3,1)).mod(29))
```

Out[22]:

$$\begin{pmatrix} 11 \\ 8 \\ 13 \end{pmatrix}$$

In [23]:

```
# we can also try the bulit-in Hill Cipher of CoCalc
# again we use Hill-3-cipher
#
H = HillCryptosystem(AlphabeticStrings(), 3)
```

In [24]:

```
# the bulit-in Hill cipher is without special characters,
# so it is mod(26) instead of mod(29)
#
R = IntegerModRing(26)
```

In [25]:

```
# we just try to encode "ABCDEF"
#
M = H.encoding("ABCDEF")
show(M)
```

Out[25]:

$$ABCDEF$$

In [26]:

```
# we generate a random key AA
#
AA = H.random_key()
show(AA)
```

Out[26]:

$$\begin{pmatrix} 5 & 6 & 6 \\ 12 & 15 & 19 \\ 17 & 3 & 22 \end{pmatrix}$$

In [27]:

```
# and we compute the inverse key
#
BB = H.inverse_key(AA)
show(BB)
```

Out[27]:

$$\begin{pmatrix} 13 & 8 & 12 \\ 23 & 4 & 21 \\ 1 & 11 & 21 \end{pmatrix}$$

In [28]:

```
# check that the two keys are inverse to each other
#
show(AA*BB)
```

Out[28]:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

In [29]:

```
# Hill cipher of "ABCDEF" using key AA
#
H.enciphering(AA, M)
```

Out[29]: UVLSPW

In [30]:

```
# store the ciphered message in CM
#
CM=H.enciphering(AA, M)
show(CM)
```

Out[30]:

$$UVLSPW$$

In [31]:

```
# decipher CM using the inverse key
# and we get back the original
#
show(H.enciphering(BB,CM))
```

Out[31]:

$$ABCDEF$$