# Solutions to Test 1

1 a) $3 \cdot 7 \equiv 1 \bmod 10$ so 7 is the mult. inv. of 3 mod 10.

b) $1413^{162} \equiv 13^{162} \bmod 100$.

$\equiv 13^2 \bmod 100$ by Euler's thm. ($\phi(100) = 40$; $\gcd(13, 100) = 1$).

$\equiv 69 \bmod 100$.

The last two digits are 69.

c) $\det \begin{pmatrix} 1 & 6 \\ 2 & 10 \end{pmatrix} = -2$ which is not invertible mod 26 so this matrix is not invertible.

2

| d | o | n | t |
|---|---|---|---|
| 3 | 14 | 13 | 19 |

| E | L | N | I |
|---|---|---|---|
| 4 | 11 | 13 | 8 |

We are looking for a matrix $M$ such that

$UM = V$ where $U = \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}$, $V = \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix}$.

Checking $U$ is invertible: $\det U \equiv 3 \cdot 19 \bmod 26$

$\equiv 5 \bmod 26$

and 5 is invertible ($-5 \cdot 5 \equiv 1 \bmod 26$).

So $M = U^{-1}V$ and $U^{-1} = -5 \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix}$

so $M = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix}$

h i (7, 8) M = (18, 13)

7 8

so hi is coded as ₹ S n.

3. If the generals are communicating in English we could try to capture as much ciphertext as possible. Given that we know they are using a substitution cipher, we can use letter frequency to make a good guess at what letters have been substituted for what. Once we have several letters determined, an analysis of the partially decipher text should give us the complete cipher.

4. Suppose that $d = \gcd(a,b)$. We know that $d \mid a$ ($d$ divides $a$) and since $d \mid b$, $d$ also divides $b - qa$ so $d$ divides $r$. This shows that $d$ divides $\gcd(a,r)$

In the other direction, if $g = \gcd(a,r)$ then $g \mid a$ and $g \mid r$ so $g \mid qa + r$ so $g \mid b$. This shows that $g \mid d$.

So we have $g \mid d$ and $d \mid g$ so $g = d$.

5

$$418 = 2 \cdot 165 + 88$$
$$165 = 1 \cdot 88 + 77$$
$$88 = 1 \cdot 77 + 11$$
$$77 = 7 \cdot 11$$

$$\gcd(418, 165) = 11$$

| | -1 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| x | 0 | 1 | -2 | 3 | -5 |
| y | 1 | 0 | 1 | -1 | 2 |

$$11 = 2 \cdot 418 - 5 \cdot 165$$