Ciphers and Number Theory

In class we did not have time to finish exercise sheet 5. Here are some comments on the final question, and an expanded version of the answers to the last two questions on the preceding sheet..

Sheet 4

5. Let $b = t(a,n) + c$ with $0 \leq c < (a,n)$. (So b is divisible by (a,n) if and only if $c = 0$.) If $ax \equiv b \bmod n$ then there exists $y \in \mathbb{Z}$ such that

$$ax + yn = b.$$

Bezout's identity tells us that

$$ua + vn = (a,n)$$

for some $u, v \in \mathbb{Z}$, and hence

$$ax + yn - t(ua + vn) = c.$$

But (a,n) divides a and n and hence divides the lefthand side. Therefore (a,n) divides c, and so $c = 0$.

If $c = 0$ then

$$tua + tvn = t(a,n) = b$$

and hence $tua \equiv b \bmod n$, so $x = tu$ is a solution.

6. We have to show that $x \equiv y \bmod n$ is reflexive, symmetric, and transitive. That is, we must show that for all $x, y, z \in \mathbb{Z}$ we have

$$(i)\ x \equiv x \bmod n$$

$$\text{(ii) if} \quad x \equiv y \bmod n \quad \text{then} \quad y \equiv x \bmod n$$

$$\text{(iii) if} \quad x \equiv y \bmod n \quad \text{and} \quad y \equiv z \bmod n \quad \text{then} \quad x \equiv z \bmod n.$$

(i) The first equivalence is obvious, as $x - x = 0$ is clearly divisible by n.
(ii) If $x \equiv y \bmod n$ then there exists $u \in \mathbb{Z}$ such that

$$x - y = un.$$

But then $y - x = -un$ and so $y - x$ is divisible by n.
(ii) If $x \equiv y \bmod n$ and $y \equiv z \bmod n$ then there exists $u, v \in \mathbb{Z}$ such that

$$x - y = un \quad \text{and} \quad y - z = vn.$$

Now

$$x - z = x - y + y - z = un + vn = (u + v)n$$

which is divisible by n.

Sheet 5

7. (a) (i) This function always has an inverse, namely $f^{-1}(\mathbf{x}) = \mathbf{x} - \mathbf{a}$.
(ii) Write `elephant` as a series of vectors, completing the final vector where necessary with zs:

$$(\mathtt{e},\mathtt{l},\mathtt{e}) \quad (\mathtt{p},\mathtt{h},\mathtt{a}) \quad (\mathtt{n},\mathtt{t},\mathtt{z}).$$

Rewrite letters as elements of $\mathbb{Z}_{26}$ in the usual way to get

$$(5,12,5) \quad (16,8,1) \quad (14,20,0).$$

Applying f we obtain

$$\begin{array}{rcccl} f(5,12,5) & = & (5,12,5)+(11,7,3) & = & (16,19,8) \\ f(16,8,1) & = & (16,8,1)+(11,7,3) & = & (1,15,4) \\ f(14,20,0) & = & (14,20,0)+(11,7,3) & = & (25,1,3). \end{array}$$

(iii) This is just the Vignère cipher.
(b) (i)

$$g(f(\mathbf{x})) = g(\mathbf{x}A+\mathbf{a}) = (\mathbf{x}A+\mathbf{a}-\mathbf{a})A^{-1} = \mathbf{x}AA^{-1} = \mathbf{x}.$$

(ii) We have

$$\begin{array}{rcll} f(11,6) & = & (11,6)\begin{pmatrix} -1 & 2 \\ 3 & 5 \end{pmatrix} + (4,7) & \mod 26 \\ & \equiv & (29,52)+(4,7) & \mod 26 \\ & \equiv & (33,59) & \mod 26 \\ & \equiv & (7,7). & \end{array}$$

Now

$$A^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$$

and hence

$$\begin{array}{rcll} g(7,7) & \equiv & ((7,7)-(4,7))\begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} & \mod 26 \\ & \equiv & (-15,6) & \mod 26 \\ & \equiv & (11,6) & \end{array}$$

as required.
(iii) Recall the formula for A^{-1} in terms of the matrix of cofactors C:

$$A^{-1} = \frac{1}{\det A} C^T.$$

The matrix of cofactors is defined only using addition, subtraction, and multiplication, so still makes sense modulo n. However, we can only divide by $\det A$ if $\det A$ is an invertible element of $\mathbb{Z}_n$. Thus if $\det A$ is invertible we can define A^{-1} by the usual formula, and it is easy to check that it will be the inverse of A.

If A is invertible then $AA^{-1} = I$ and so $\det(A)\det(A^{-1}) = 1 \bmod n$. But this implies that $\det(A)$ has an inverse.