Sheet 7

Due 17.30 Tuesday 6th March

Hand in solutions to questions 1a, 2b, 4b, 4c, 5a.

Please write your student ID number on your work and staple it together.

1. Find $\phi(245)$ and calculate:

**(a) $4^{169} \mod 245$, (2 marks)

Solution. $\phi(245) = \phi(72 \times 5) = 6 \times 7 \times 4 = 168$. Observe that $(4, 245) = 1$, so $4^{168} \equiv 1 \mod 245$. Therefore

$$4^{169} \equiv 4^1 \equiv 4 \mod 245.$$

(b) $13^{1696968} \mod 245$.

Solution. $\phi(245) = \phi(72 \times 5) = 6 \times 7 \times 4 = 168$. Observe that $(13, 245) = 1$, so $13^{168} \equiv 1 \mod 245$. Therefore

$$13^{1696968} = 13^{10101 \times 16}8 \equiv 13^0 \equiv 1 \mod 245.$$

2. Solve the congruences

(a) $x^{101} \equiv 2 \mod 245$,

Solution. $\phi(245) = \phi(72 \times 5) = 6 \times 7 \times 4 = 168$. Note: $(2, 245) = (101, 168) = 1$, so if we let $n = 245$ then the solution of the congruence is $x \equiv 2^c$ where $[c] = [101]^{-1}$. Let $n = 168$ and find $[101]^{-1}$. The Euclidean Algorithm spits out $1 = 5 \times 101 - 3 \times 168$. So $[101]^{-1} = [5]$, and hence $x \equiv 25 \equiv 32 \mod 245$.

**(b) $y^{29} \equiv 1 \mod 245$. (2 marks)

Solution. $\phi(245) = \phi(72 \times 5) = 6 \times 7 \times 4 = 168$. Note: $(29, 168) = 1$ so if we let $n = 245$ the (unique) solution is $y \equiv 1^c \mod 245$ where $[c] = [29]^{-1}$. But $1^c = 1$ regardless of the value of c, so $y \equiv 1 \mod 245$.

3. Solve the congruence $x^{11} \equiv 5 \mod 41$.

Solution. Note that $(41) = 40$ and that $(5, 41) = 1, (11, 40) = 1$. Thus the congruence has a unique solution given by

$$x = 5^c \mod 41$$

where $11c \equiv 1 \mod \phi(41)$. Let us find the inverse of 11 modulo 40. The Euclidean Algorithm gives us $1 = 11 \times 1 - 3 \times 40$. So $c \equiv 11 \mod 40$, and hence $x = 5^{11} \mod 41$. To simplify note that $5^3 \equiv 2 \mod 41$, so

$$5^{11} \equiv 5^9 \times 5^2 \equiv 2^3 \times 5^2 \equiv 200 \equiv 36 \mod 41.$$

4. Consider the matrices:

$$A = \begin{pmatrix} 3 & 2 & 9 & 1 \\ 3 & 1 & 0 & 0 \\ -1 & 0 & 3 & 0 \\ 2 & 2 & 9 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 \\ 1 & -2 \\ 0 & 1 \\ 2 & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

(a) Calculate AB and BC.
Solution.

$$AB = \begin{pmatrix} 3 & 2 & 9 & 1 \\ 3 & 1 & 0 & 0 \\ -1 & 0 & 3 & 0 \\ 2 & 2 & 9 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -2 \\ 0 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 4 & 1 \\ -1 & 2 \\ 8 & 7 \end{pmatrix},$$

$$BC = \begin{pmatrix} 1 & 1 \\ 1 & -2 \\ 0 & 1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ -1 & -2 \\ 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

**(b) Calculate $(AB)C$ and $A(BC)$. Check they are equal (associativity). (2 marks)

Solution.

$$(AB)C = \begin{pmatrix} 7 & 8 \\ 4 & 1 \\ -1 & 2 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 15 & 23 \\ 5 & 6 \\ 1 & 3 \\ 15 & 22 \end{pmatrix},$$

$$A(BC) = \begin{pmatrix} 3 & 2 & 9 & 1 \\ 3 & 1 & 0 & 0 \\ -1 & 0 & 3 & 0 \\ 2 & 2 & 9 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ -1 & -2 \\ 1 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 15 & 23 \\ 5 & 6 \\ 1 & 3 \\ 15 & 22 \end{pmatrix}.$$

**(c) Calculate C^{-1}. (2 marks)
Solution.

$$C^{-1} = \frac{1}{2-1} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}.$$

5. Let $A \in \mathcal{M}(n,m)$ and $B \in \mathcal{M}(m,p)$. Let $\lambda \in \mathbb{R}$.

**(a) Prove that $A(\lambda B) = (\lambda A)B$. (2 marks)
Solution. There are many ways to prove this but it is simplest to give names to the products and to compute their entries. Let $C = A(\lambda B)$ and $D = (\lambda A)B$. Then

$$c_{j\ell} = \sum_{k=1}^{m} a_{jk}(\lambda b_{k\ell}) = \sum_{k=1}^{m} (\lambda a_{jk}) b_{k\ell} = d_{j\ell}$$

so $C = D$ as required.

(b) Prove that $(\lambda A)B = \lambda(AB)$.

Solution. There are many ways to prove this but it is simplest to give names to the products and to compute their entries. Let $E = (\lambda A)B$ and $F = \lambda(AB)$. Then

$$e_{j\ell} = \sum_{k=1}^{m} (\lambda a_{jk}) b_{k\ell} = \lambda \sum_{k=1}^{m} a_{jk} b_{k\ell} = f_{j\ell}$$

so $E = F$ as required.