Solution Sheet 4

1. (i) **If** there is an integral solution to $30x^2 - 23y^2 = 1$ then, when we look at the equation modulo 5, we find that $-23y^2 \equiv 1 \bmod 5$, i.e. $-3y^2 \equiv 1 \bmod 5$.

   We can write this as $-3y^2 \equiv 1 + 5 \equiv 6 \bmod 5$, and divide by -3 to get $y^2 \equiv -2 \equiv 3 \bmod 5$. But from the following table we see that this is impossible:

n	$n^2 \bmod 5$
0	0
1	1
2	4
3	4
4	1

   Note that in this table we have
   $$(5-n)^2 = 5^2 - 10n + n^2 \equiv n^2 \bmod 5$$
   so we need only have taken $n = 0, 1$ or 2 to have found all possible residues.

   (ii) If $5x^2 - 14y^2 = 1$ has a solution then, looking modulo 7, we must have $5x^2 \equiv 1 \bmod 7$. Noting that 3 is the inverse of $5 \bmod 7$, i.e. $3 \times 5 \equiv 1 \bmod 7$, we get $x^2 \equiv 3 \bmod 7$. But from the following table we see that this is impossible:

n	$n^2 \bmod 7$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

   (iii) ★ As in part (i) look at the equation modulo 5.

2. (i) Using the hint given, the Diophantine equation $2x^3 + 27y^4 = 23$ becomes $2x^3 \equiv 23 \equiv 5 \bmod 9$. Noting that 5 is the inverse of $2 \bmod 9$, we multiply both sides by 5 to get $x^3 \equiv 25 \equiv 7 \bmod 9$. But from the following table we see that this is impossible:

x	$x^3 \bmod 9$
0	0
1	1
2	8
3	0
4	1
5	8
6	0
7	1
8	8

(ii) Look at $7x^5 + 3y^4 = 4$ modulo 7 to see if there are solutions to $3y^4 \equiv 4 \bmod 7$. Use the table above:

n	$n^2 \bmod 7$	$n^4 \bmod 7$	$3n^4 \bmod 7$
0	0	0	0
1	1	1	3
2	4	2	6
3	2	4	5
4	2	4	5
5	4	2	6
6	1	1	3

Thus we see there is no solution to $3y^4 \equiv 4 \bmod 7$, hence there can have been no integral solution of $7x^5 + 3y^4 = 4$.

(iii) ★ To show that 7 never divides $a^4 + a^2 + 2$ for $a \in \mathbb{Z}$ we need show that there are no solutions of $a^4 + a^2 + 2 \equiv 0 \bmod 7$. For this we can use the table above:

n	$n^2 \bmod 7$	$n^4 \bmod 7$	$n^4 + n^2 + 2 \bmod 7$
0	0	0	2
1	1	1	4
2	4	2	1
3	2	4	1
4	2	4	1
5	4	2	1
6	1	1	4

3. $(\mathbb{Z}_6, +)$

$+$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

and $(\mathbb{Z}_6, \times)$

$\times$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

4. ★ $(\mathbb{Z}_9^*, \times)$

$\times$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[1]_9$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[2]_9$	$[2]_9$	$[4]_9$	$[8]_9$	$[1]_9$	$[5]_9$	$[7]_9$
$[4]_9$	$[4]_9$	$[8]_9$	$[7]_9$	$[2]_9$	$[1]_9$	$[5]_9$
$[5]_9$	$[5]_9$	$[1]_9$	$[2]_9$	$[7]_9$	$[8]_9$	$[4]_9$
$[7]_9$	$[7]_9$	$[5]_9$	$[1]_9$	$[8]_9$	$[4]_9$	$[2]_9$
$[8]_9$	$[8]_9$	$[7]_9$	$[5]_9$	$[4]_9$	$[2]_9$	$[1]_9$

So the inverse of each element is

$$[1]_9^{-1} = [1]_9\,, \qquad [2]_9^{-1} = [5]_9\,, \qquad [4]_9^{-1} = [7]_9\,,$$
$$[5]_9^{-1} = [2]_9\,, \qquad [7]_9^{-1} = [4]_9\,, \qquad [8]_9^{-1} = [8]_9\,.$$

5. (i) $[2]_{93}$: Simply observe that $2 \times 47 = 94 \equiv 1 \bmod 93$ hence $[2]_{93}^{-1} = [47]_{93}$.

(ii) $[5]_{93}$: To find $[x]_{93}$ for which $[5]_{93} \times [x]_{93} = [1]_{93}$ we need solve $5x \equiv 1 \bmod 93$. This can be done by Euclid's Algorithm, but has already been done in the notes, $x = 56$ being a solution. Hence $[5]_{93}^{-1} = [56]_{93}$.

(iii) $[25]_{93}$: We can use the method as in part (ii) and solve $25x \equiv 1 \bmod 93$ using Euclid's Algorithm. Alternatively, note that $[25]_{93} = [5^2]_{93} = [5]_{93}^2$. Hence,

$$\begin{aligned} [25]_{93}^{-1} &= \left([5]_{93}^{-1}\right)^2 = [56]_{93}^2 \quad \text{by part (ii)}, \\ &= \left[56^2\right]_{93} = [67]_{93}\,. \end{aligned}$$

(iv) $[32]_{93}$: Perhaps start from $[32]_{93} = [2^5]_{93} = [2]_{93}^5$. Thus

$$\begin{aligned} [32]_{93}^{-1} &= \left([2]_{93}^{-1}\right)^5 = [47]_{93}^5 \quad \text{by part (i)}, \\ &= \left[47^5\right]_{93} = [32]_{93}\,. \end{aligned}$$

6. (i) $\mathcal{R} = \{(1,7)\,,(2,5)\,,(3,3)\,,(4,1)\}\,,$

(ii) $\mathcal{S} = \{(1,1)\,,(1,2)\,,(1,3)\,,(1,4)\,,(1,5)\,,(2,1)\,,(2,2)\,,$
$(2,3)\,,(2,4)\,,(3,1)\,,(3,2)\,,(3,3)\,,(4,1)\,,(4,2)\,,(5,1)\},$

(iii) $\mathcal{T} = \{(1,1)\,,(2,4)\,,(3,9)\,,(4,16)\,,(5,25)\,,....\}\,.$

7. ★

	Reflexive	Symmetric	Transitive
(i)	No	No	Yes
(ii)	Yes	Yes	Yes
(iii)	No	Yes	No
(iv)	Yes	Yes	No
(v)	Yes	Yes	Yes
(vi)	No	No	No

Reasons:

i) **Not reflexive:** $(1,1) \notin \mathcal{R}_1$,
Not symmetric: $(2,4) \in \mathcal{R}_1$ but $(4,2) \notin \mathcal{R}_1$.

ii) **All** properties satisfied.

iii) **Not reflexive:** $(1,1) \notin \mathcal{R}_3$,
Not transitive: $(2,4), (4,2) \in \mathcal{R}_3$ but $(2,2) \notin \mathcal{R}_3$.

iv) **Not transitive**: $(4,3), (3,1) \in \mathcal{R}_4$ but $(4,1) \notin \mathcal{R}_4$.

v) **All** properties satisfied.

vi) **Not reflexive**: $(1,1) \notin \mathcal{R}_6$,
Not symmetric: $(1,4) \in \mathcal{R}_6$ but $(4,1) \notin \mathcal{R}_6$,
Not transitive: $(1,3), (3,1) \in \mathcal{R}_6$ but $(1,1) \notin \mathcal{R}_6$.

8.

	Reflexive	Symmetric	Transitive
(i)	No	Yes	No
(ii)	Yes	Yes	Yes
(iii)	No	Yes	Yes
(iv)★	Yes	No	Yes

Reasons:

i) **Not Reflexive**. Counterexample: $1 \nsim 1$ since $1+1$ is not odd;

Is Symmetric. Proof: $x \sim y \Rightarrow x+y$ is odd $\Rightarrow y+x$ is odd $\Rightarrow y \sim x$;

Not Transitive. Counterexample: $1 \sim 2$ and $2 \sim 1$ but $1 \nsim 1$.

ii) **Is Reflexive**. Proof: for all integers $2x$ is even so $x \sim x$;

Is Symmetric. Proof $x \sim y \Rightarrow x + y$ is even $\Rightarrow y + x$ is even $\Rightarrow y \sim x$;

Is Transitive. Proof If $x \sim y$, i.e. $x + y$ is even, then x and y have the same *parity*, i.e. they are both odd or both even. So if $x \sim y$ and $y \sim z$ then all three of x, y and z have the same parity. In particular x and z have the same parity and so $x \sim z$.

iii) **Not Reflexive**. Counterexample: $2 \nsim 2$ since 2×2 is not odd;

Is Symmetric. Proof: $x \sim y \Rightarrow xy$ is odd $\Rightarrow yx$ is odd $\Rightarrow y \sim x$;

Is Transitive. Proof: If xy is odd then both x and y are odd. So if $x \sim y$ and $y \sim z$ then all three of x, y and z are odd. In particular x and z are odd and so $x \sim z$.

iv) ★ **Is Reflexive**. Proof: For any integer x we note that $x + xx = x(x + 1)$ and one of x or $x + 1$ has to be even, thus $x \sim x$.

Not Symmetric. Counterexample $2 \sim 1$, since $2 + 2 \times 1$ is even but $1 \nsim 2$ since $1 + 1 \times 2$ is not even.

Is Transitive. Proof: Assume $x \sim y$ and $y \sim z$.

Thus $x(1 + y) = 2m$ and $y(1 + z) = 2n$ for some $m, n \in \mathbb{Z}$. Multiply the first equality by $(1 + z)$ to get

$$x((1 + z) + y(1 + z)) = 2m(1 + z).$$

Substitute in to get

$$x((1 + z) + 2n) = 2m(1 + z).$$

Rearrange to get

$$x(1 + z) = 2(m(1 + z) - nx),$$

which implies $x \sim z$.

9. (i) No. The sets are not disjoint.

(ii) Yes.

(iii) Yes,

(iv) No. Not every element of the set is in some element of the partition.

10. (i) No. 0 is in neither of the sets,

    (ii) No. The sets are not disjoint. An integer $m \in \mathbb{Z}$ is in both T_m and T_{m-1}, for example, $1 \in T_1$ and $1 \in T_0$.

    (iii) No. 0 is in both sets,

    (iv) Yes.

11.

$$\mathcal{R} = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,1), (3,4), (4,3)\}.$$

12. (i) $[1] = \{1,2\}$, $[2] = \{1,2\}$, $[3] = \{3\}$, $[4] = \{4,5\} = [5]$ and $[6] = \{6\}$.

    (ii) $\{1,2\} \cup \{3\} \cup \{4,5\} \cup \{6\}$.