MTH 4104 Example Sheet II Solutions Shu SASAKI

II-1. $x\mathscr{R}y$ if and only no integer r satisfies $x < r\pi < y$ or $y < r\pi < x$. We show the transitivity by its contrapositive– if $x\not\mathscr{R}z$ then either $x\not\mathscr{R}y$ or $y\not\mathscr{R}z$. Suppose $x\not\mathscr{R}z$ holds, i.e. there exists an integer r such that $x < r\pi < z$ or $z < r\pi < z$ holds. Suppose $x < r\pi < z$ holds. Comparing y with $r\pi$, we see that they cannot possibly be equal, hence either $r\pi < y$ or $y < r\pi$ holds. If the former holds, then $x < r\pi < y$, hence $x\not\mathscr{R}y$. If the latter holds, then $y < r\pi < z$, hence $y\not\mathscr{R}z$.

The equivalence class $[24]_{\mathscr{R}}$ is $\{22, 23, 24, 25\}$.

II-2. The set of all squares in the plane $\mathbb{R}^2$ with horizontal and vertical sides and centre $(0, 0)$.

II-3. Parts (elements of a partition) are defined to be non-empty. It is therefore necessary to assume T is non-empty, as well as it is a proper subset of S. To prove that $\{T, S - T\}$ is a partition, we note (1) by the added assumption, neither T nor $S - T$ is empty (2) $T \cap (S - T) = \varnothing$ holds by definition (3) $T \cup (S - T) = S$. By definition, T and $S - T$ are both subsets of S, hence $T \cup (S - T) \subseteq S$ holds. On the other hand, if x is an element of S, then exactly one of the following two cases holds: either x lies in T (in which case x lies in T) or x does not lie in T (in which case x lies in $S - T$). Therefore $S \subseteq T \cup (S - T)$.

II-4. Let $X = [a]$ and $Y = [b]$. Then X (resp. Y) is the set of all integers of the form $a + nr$ (resp. $b + ns$), where r (resp. s) ranges over $\mathbb{Z}$. Therefore $S = \{x + y \mid x \in X, y \in Y\}$ is the set of integers of the form $(a + b) + n(r + s)$. This set is nothing other than the set $[a + b] = [a] + [b]$.

II-5. Let $n = 5, X = [2]_5, Y = [3]_5$. Then X (resp. Y) is the set of all integers congruent to 2 (resp. 3) mod 5. While XY is defined to be the set of all integers congruent to 1 mod 5, the set $\{xy \mid x \in X, y \in Y\}$ does not have 1 as its element.

II-6.

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

×	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

II-7.

r	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
$r^2 - 3r$	[0]	[8]	[8]	[0]	[4]	[0]	[8]	[8]	[0]	[4]

$[6] = [-4], [7] = [-3], [8] = [-2], [9] = [-1]$ might have simplified the calculations.

II-8. $[0]+[1]+\cdots+[n-1] = [0+1+\cdots+n-1] = [n(n-1)/2]$. Therefore, $[n(n-1)/2] = [0]$ if and only if n divides $n(n-1)/2$ if and only if 2 divides $n-1$.

II-9.

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

In general, the number of $[0]_n$'s in the $[a]_n$ row is $r = \gcd(a, n)$. For example, when $n = 1$, there should be $\gcd(2, 6) = 2$ in the $[2]_6$ row and $\gcd(3, 6) = 3$ in the $[3]_6$ row etc.

To see this we need to count the number of distinct $[b]_n$'s in $\mathbb{Z}_n$ such that $[a]_n[b]_n = [0]_n$. For such b, it follows that n divides ab. Let s be a the positive integer defined by $rs = n$. By definition, s is coprime to a, i.e. $\gcd(s, a) = 1$. As s divides ab, it divides b.

The elements $[s]_n, [2s]_n, \ldots, [rs]_n$ of $\mathbb{Z}_n$ are distinct and they all yield $[0]_n$ when multiplied by $[a]_n$.

II-10. Firstly, we compute $[9]_{17}^{-1}$. By definition, this is $[y]$ such that $[9][y] = [1]$. It therefore suffices to find an integer y such that $9y + 17z = 1$. By Euclid's algorithm or otherwise, we find that $9 \cdot 2 + 17 \cdot (-1) = 1$. Hence $[9]^{-1} = [2]$. Plugging this into the equation, we are asked to solve $[9][x] + [1] = [11][2] = [22] = [5]$, i.e. $[9][x] = [4]$. Multiplying $[9]^{-1}$ on both sides, the LHS becomes $[9]^{-1}[9][x] = [1][x] = [x]$, while the RHS becomes $[9]^{-1}[4] = [2][4] = [2 \cdot 4] = [8]$. In conclusion, $[x] = [8]$.

II-11. If n is a positive integer, $[a]_n$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$ (see lecture notes!). For brevity, we let $\phi(n)$ denote the number of integers $1 \leqslant a \leqslant n$ which are coprime to n– this is often referred to as Euler's totient/ϕ function. Following this nomenclature, $\phi(19) = 18, \phi(20) = 8$ and $\phi(66) = 20$.

For example, to compute $\phi(20)$ as follows. Firstly, $20 = 2^2 \cdot 5$, so we need to eliminate from $\{1, \ldots, 20\}$ the integers that are divisible by 2 or 5. There are $20/2 = 10$ integers that are divisible by 2, while $20/5 = 4$ integers that are divisible by 5. However, multiples of $10 (= 5 \cdot 2)$ are counted twice, so need to subtract $20/10 = 2$ from the list of 'to-be-eliminated' integers. Perhaps, drawing a Venn's diagram might be helpful. In conclusion, $\phi(20) = 20 - (10 + 4 - 2) = 20 - 12 = 8$.

There is indeed a formula for computing $\phi(n)$. If p is a prime number, it is an easy exercise to check $\phi(p^r) = p^{r-1}(p-1)$. On the other hand, it is a much harder exercise to check if a and b are positive integers that are coprime, then $\phi(ab) = \phi(a)\phi(b)$. Granted, if $n = \prod_p p^{r_p}$, then $\phi(n) = \prod_p p^{r_p - 1}(p-1)$. For example, $\phi(20) = \phi(2^2 \cdot 5) = \phi(2^2)\phi(5) = 2^{2-1}(2-1)(5-1) = 8$. Also $\phi(66) = \phi(2 \cdot 3 \cdot 11) = (2-1)(3-1)(11-1) = 20$.