MATH10101, for supervision in week 08. Counting. Definition of GCD — SOLUTIONS

Q1.

($\star$) (i) Write down one example of a function $f\colon \{1,2,3,4\} \to \{a,b,c,d\}$ such that f is not injective but the restriction, $f|_{\{1,2,3\}}$, of f onto the subset $\{1,2,3\}$ of the domain is injective.

(ii) Prove that there are $n(n!)$ functions $f\colon \mathbb{N}_n \to \mathbb{N}_n$ such that the restriction $f|_{\mathbb{N}_{n-1}}$ is injective.

Q1 - solution.

($\star$) (i) One possible example is given by $f(1) = a$, $f(2) = b$, $f(3) = c$ and $f(4) = c$.

The function f is not injective because $3 \neq 4$ in the domain of f but $f(3) = f(4)$. Recall that the restriction $f|_{\{1,2,3\}}$ is the function with domain $\{1,2,3\}$, defined by the same rule as f but only for the arguments 1, 2 and 3. This rule says $1 \mapsto a$, $2 \mapsto b$ and $3 \mapsto c$; by inspection, the function thus defined on $\{1,2,3\}$ is injective.

(ii) Recall from the lectures that the number of injective functions from a finite set X to a finite set Y is $\dfrac{n!}{(n-m)!}$ where $n = |Y|$ and $m = |X|$. Setting $X = \mathbb{N}_{n-1}$ and $Y = \mathbb{N}_n$, this gives $\dfrac{n!}{(n-(n-1))!} = \dfrac{n!}{1!} = n!$ injective functions from $\mathbb{N}_{n-1} = \{1,2,\ldots,n-1\}$ to $\mathbb{N}_n = \{1,2,\ldots,n\}$.

(Aside: this is the same as the number of injective = bijective functions from $\mathbb{N}_n$ to $\mathbb{N}_n$. Think why this is so.)

This means that the restriction $f|_{\mathbb{N}_{n-1}}$, which is required to be injective, can be chosen in $n!$ possible ways.

But if $f|_{\mathbb{N}_{n-1}}$ is given — meaning that the values $f(1), f(2), \ldots, f(n-1)$ are selected — then to define the function f on $\mathbb{N}_n$, one only needs to select the value $f(n)$. There is no restriction on $f(n)$ so $f(n)$ can be any element of $\mathbb{N}_n$, i.e., there are n choices for $f(n)$. This means that each injective function $\mathbb{N}_{n-1} \to \mathbb{N}_n$ is the restriction of n possible functions $f\colon \mathbb{N}_n \to \mathbb{N}_n$. Hence the total number of allowed functions f is n times the number of injections from $\mathbb{N}_{n-1}$ to $\mathbb{N}_n$, that is, $n \times n!$.

($\star$) **Q2**. Find the number of subsets of $\{1,2,\ldots,10\}$ which contain 1 and do not contain 10.

Q2 - solution. Subsets which do not contain 10 are subsets of $\{1,2,\ldots,9\}$. Hence we are counting all subsets of $\{1,2,\ldots,9\}$ which contain 1.

The total number of subsets of $\{1,2,\ldots,9\}$ is $|\mathcal{P}(\{1,2,\ldots,9\})| = 2^{|\{1,2,\ldots,9\}|} = 2^9 = 512$.

The number of subsets of $\{1,2,\ldots,9\}$ which do **not** contain 1 (i.e., subsets of $\{2,\ldots,9\}$) is $2^{|\{2,\ldots,9\}|} = 2^8 = 256$.

Therefore, the number of subsets of $\{1, 2, \dots, 9\}$ which **do** contain 1 is $512 - 256 = 256$.

Q3. (i) Prove, using the Binomial Theorem, that for all $n \in \mathbb{Z}^{\geq}$, $\sum\limits_{r=0}^{n} \binom{n}{r} = 2^n$.

(ii) Now prove the same statement *without* using the Binomial Theorem by considering a set A with $|A| = n$ and calculating the cardinality of $\bigcup_{r=0}^{n} \mathcal{P}_r(A)$.

(iii) Check that the statement in (i) is true for $n = 5$ by direct evaluation of both sides.

Q3 - solution. (i) Note that $\sum_{r=0}^{n} \binom{n}{r} = \sum_{r=0}^{n} \binom{n}{r} 1^{n-r} 1^r$ equals $(1+1)^n$ by the Binomial Theorem. This is the same as 2^n.

(ii) $\bigcup_{r=0}^{n} \mathcal{P}_r(A)$ is the collection of **all** subsets of A, i.e. $\mathcal{P}(A)$. It is a **disjoint union**. Recall from the lectures that the cardinality of a disjoint union is the sum of the cardinalities. Another result from the lectures is

$$|\mathcal{P}(A)| = 2^n,$$

hence

$$2^n = \left| \bigcup_{r=0}^{n} \mathcal{P}_r(A) \right| = \sum_{r=0}^{n} |\mathcal{P}_r(A)| = \sum_{r=0}^{n} \binom{n}{r},$$

by definition of the binomial coefficients.

(iii) $n = 5$, $\sum\limits_{r=0}^{5} \binom{5}{r} = 1 + 5 + 10 + 10 + 5 + 1 = 32 = 2^5$.

($\star$) **Q4**. (i) Using the Binomial Theorem, prove that $\sum\limits_{r=0}^{n} (-1)^r \binom{n}{r} = 0$.

($\star$) (ii) Use the result of (i) along with **Q3**(i) to evaluate the sums $\sum\limits_{\substack{r=0 \\ r \text{ even}}}^{n} \binom{n}{r}$ and $\sum\limits_{\substack{r=1 \\ r \text{ odd}}}^{n} \binom{n}{r}$.

($\star$) (iii) Check that both of your answers in (ii) are correct for $n = 4$ by direct calculation.

Q4 - solution.

($\star$) (i) The Binomial Theorem states that for all x, y we have

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r.$$

Choose $x = 1$ and $y = -1$ to get

$$0 = (1 + (-1))^n = \sum_{r=0}^{n} \binom{n}{r} (-1)^r$$

as required.

($\star$) (ii) Add $\sum_{r=0}^{n}\binom{n}{r} = 2^n$, from **Q3**(i), to $\sum_{r=0}^{n}(-1)^r\binom{n}{r} = 0$ proved in (i) to get

$$2^n = \sum_{r=0}^{n}(1+(-1)^r)\binom{n}{r} = \sum_{\substack{r=0\\ r\text{ even}}}^{n} 2\binom{n}{r}.$$

Subtract to get

$$2^n = \sum_{r=0}^{n}(1-(-1)^r)\binom{n}{r} = \sum_{\substack{r=0\\ r\text{ odd}}}^{n} 2\binom{n}{r}.$$

Hence the binomial coefficients $\binom{n}{r}$ for r even add up to 2^{n-1}, and the binomial coefficients $\binom{n}{r}$ for r odd also add up to 2^{n-1}.

($\star$) (iii) Example: $n = 4$, $\binom{4}{0}+\binom{4}{2}+\binom{4}{4} = 1+6+1 = 8$, $\binom{4}{1}+\binom{4}{3} = 4+4 = 8$.

Q5. Use the Binomial Theorem to calculate $\sum_{r=0}^{100} 4^{2r}5^{100-2r}\binom{100}{r}$. [*Answer*: 8.2^{100}]

Q5 - solution. $\sum_{r=0}^{n} 4^{2r}5^{n-2r}\binom{n}{r} = \frac{1}{5^n}\sum_{r=0}^{n} 4^{2r}5^{2n-2r}\binom{n}{r} = \frac{1}{5^n}\sum_{r=0}^{n} 16^r 25^{n-r}\binom{n}{r}$, which by the Binomial Theorem equals $\frac{1}{5^n}(16+25)^n = \left(\frac{41}{5}\right)^n$. It remains to set $n = 100$.

Q6. Let A be a finite set and let $\mathcal{Q}(A) = \{(C,D) \in \mathcal{P}(A)\times\mathcal{P}(A) : C \subseteq D\}$. Prove that $|\mathcal{Q}(A)| = 3^{|A|}$.

Q6 - solution. Solution 1: Let $n = |A|$ and let us count pairs (C,D) of subsets of A where $C \subseteq D$ and additionally $|D| = r$. A set D with $|D| = r$ can be chosen in $\binom{n}{r}$ ways, and to each such choice of D there corresponds 2^r choices of C, since C is an arbitrary subset of D. Hence there are $\binom{n}{r}2^r$ pairs $(C,D) \in \mathcal{P}(A)\times\mathcal{P}(A)$ such that $C \subseteq D$ and $|D| = r$. The total number of elements of $\mathcal{Q}(A)$ is obtained by summing over all possible r: that is,

$$|\mathcal{Q}(A)| = \sum_{r=0}^{n}\binom{n}{r}2^r = (1+2)^n = 3^n.$$

Solution 2: Given a pair (C,D) of subsets of A such that $C \subseteq D$, define the function $f\colon A \to \{0,1,2\}$ by

$$f(a) = \begin{cases} 0, & a \notin D,\\ 1, & a \in D\setminus C,\\ 2, & a \in C.\end{cases}$$

Informally, for $a \in A$, $f(a)$ is the number of entries out of two entries of the pair (C, D) which contain a. It turns out that each function $f \in Fun(A, \{0, 1, 2\})$ corresponds to exactly one pair $(C, D) \in \mathcal{Q}(A)$, namely $C = \{a \in A : f(a) = 2\}$ and $D = \{a \in A : f(a) \geq 1\}$. We have thus constructed a bijection between $\mathcal{Q}(A)$ and the set $Fun(A, \{0, 1, 2\})$. The latter set has cardinality $3^{|A|}$ (a result from the course), hence so does $\mathcal{Q}(A)$.

($\star$) **Q7**. Find the quotient q and remainder r on dividing the following numbers by 17:

(i) 1; (ii) -1; (iii) 100; (iv) -100.

Q7 - solution.

($\star$) (i) $1 = 17 \times 0 + 1$ and $0 \leq 1 < 17$, so $q = 0$, $r = 1$;

($\star$) (ii) $-1 = 17 \times (-1) + 16$ and $0 \leq 16 < 17$, so $q = -1$, $r = 16$;

($\star$) (iii) $100 = 17 \times 5 + 15$ and $0 \leq 15 < 17$, so $q = 5$, $r = 15$;

($\star$) (iv) $-100 = 17 \times (-6) + 2$ and $0 \leq 2 < 17$, so $q = -6$, $r = 2$.

Recall that by the Division Theorem, the answer in each case is **unique**. Importantly, the remainders are always **non-negative**.

Q8. Let a, b be integers such that $b \,|\, a$.

($\star$) (i) Carefully prove the following proposition: $\forall c \in \mathbb{Z}, \big((c \,|\, b) \implies (c \,|\, a)\big)$.

($\star$) (ii) Assume $b \geq 0$. Use the definition of $\gcd$ to prove that $\gcd(a, b) = b$.

Q8 - solution.

($\star$) (i) Let $c \in \mathbb{Z}$. To prove the implication $(c \,|\, b) \implies (c \,|\, a)$, assume that $c \,|\, b$. Then by definition of a divisor, $b = ck$ for some $k \in \mathbb{Z}$. We are also given that $b \,|\, a$, so again by definition $a = b\ell$ for some $\ell \in \mathbb{Z}$. Substituting, we obtain $a = c(k\ell)$. Since $k\ell$ is an integer (as product of two integers), by definition $c \,|\, a$.

($\star$) (ii) It is best to deal with the case $b = 0$ straight away. If $b = 0$ and $b \,|\, a$ then $a = 0$ (because $a = b\ell = 0\ell$ for some $\ell \in \mathbb{Z}$), so $\gcd(a, b) = \gcd(0, 0) = 0$ (by definition) which is b.

Now assume $b > 0$. To show that b is the greatest common divisor of a and b, we will show two things: that b is a common divisor, and that b is greater than or equal to any other common divisor of a and b.

1. *b is a common divisor*: indeed, $b \,|\, a$ (given) and $b \,|\, b$ (because $b = b \times 1$).

2. *If c is a common divisor of a and b then $c \leq b$:* this step requires $b > 0$. If c is a common divisor of a and b then in particular $c \,|\, b$, so $b = ck$ for some $k \in \mathbb{Z}$. Then $k \neq 0$ as $b \neq 0$ so

$$c \leq |c| = \frac{|b|}{|k|} = \frac{b}{|k|} \leq b$$

as $|k| \geq 1$. From 1. and 2. it follows that b is indeed the greatest common divisor of a and b.