**2E Numbers and Sets**

What is an *equivalence relation* on a set $X$? If $\sim$ is an equivalence relation on $X$, what is an *equivalence class* of $\sim$? Prove that the equivalence classes of $\sim$ form a partition of $X$.

---

*A relation $R$ on a set $X$ is a subset of $X \times X$. We write $xRy$ for $(x,y) \in R$. Say $R$ is an equivalence relation if it is reflexive ($xRx$ for all $x$), symmetric ($xRy$ iff $yRx$) and transitive (if $xRy$ and $yRz$ then $xRz$).*

*An equivalence class of $\sim$ is a subset of $X$ of the form $[x] = \{y \in X : y \sim x\}$ for some $x \in X$.*

*Claim: The equivalence classes of $\sim$ partition $X$.*

*Proof: By reflexivity they cover $X$ ($x \in [x]$ for all $x \in X$). For $x_1$ and $x_2$ in $X$ we need to show that $[x_1]$ and $[x_2]$ are disjoint or equal, so suppose there exists $x \in [x_1] \cap [x_2]$. Then $x \sim x_1$ and $x \sim x_2$ so for all $y \in [x_1]$ we have (using symmetry)*

$$y \sim x_1 \sim x \sim x_2.$$

*Transitivity gives $y \sim x_2$ so $y \in [x_2]$ and hence $[x_1] \subset [x_2]$. Similarly*
[5] *$[x_2] \subset [x_1]$ so $[x_1] = [x_2]$, and we're done.* $\square$

---

Let $\sim$ be the relation on the positive integers defined by $x \sim y$ if either $x$ divides $y$ or $y$ divides $x$. Is $\sim$ an equivalence relation? Justify your answer.

---

[2] *No. We have $2 \sim 1$ and $1 \sim 3$ but $2 \nsim 3$, so $\sim$ is not transitive.*

---

Write down an equivalence relation on the positive integers that has exactly four equivalence classes, of which two are infinite and two are finite.

---

*Consider the partition*

$$\{1,2,3,\dots\} = \{1\} \cup \{2\} \cup \{3,5,7,\dots\} \cup \{4,6,8,\dots\}.$$

*Define $x \sim y$ iff $x$ and $y$ lie in the same part of the partition. The*
[3] *equivalence classes are exactly the parts of the partition.*

---

**[10]**

## 5E Numbers and Sets

(a) What is the *highest common factor* of two positive integers $a$ and $b$? Show that the highest common factor may always be expressed in the form $\lambda a + \mu b$, where $\lambda$ and $\mu$ are integers.

---

*(a) The hcf of $a$ and $b$ is a positive integer $c$ such that $c \mid a$ and $c \mid b$ and such that if $d \mid a$ and $d \mid b$ then $d \mid c$ (clearly unique if it exists).*

*Let $S$ be the set of positive integers of the form $\lambda a+\mu b$ for $\lambda, \mu \in \mathbb{Z}$ and let $s$ be its smallest element.*

*Claim:* $\mathrm{hcf}(a, b) = s$.

*Proof: Clearly if $d \mid a$ and $d \mid b$ then $d$ divides every element of $S$, so $d \mid s$. Left to show $s$ divides $a$ and $b$. By division algorithm we have $a = qs + r$ for some $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, s-1\}$. Then*

$$r = (1 - q\lambda)a - q\mu b$$

*is of the form $\lambda' a+\mu' b$ so by minimality of $s$ it must be 0. Hence $a = qs$*
[5] *is divisible by $s$. Similarly $s \mid b$.* □

---

Which positive integers $n$ have the property that, for any positive integers $a$ and $b$, if $n$ divides $ab$ then $n$ divides $a$ or $n$ divides $b$? Justify your answer.

---

*Precisely the primes (and 1). Suppose $n$ composite, say $n = ab$ for some $a$ and $b$ greater than 1. Then $n \mid ab$ but $n \nmid a$ and $n \nmid b$. Conversely suppose $n$ is prime, $n \mid ab$ but $n \nmid a$. Then $n$ and $a$ have no common factor other than 1, so $\mathrm{hcf}(n, a) = 1$. By previous part we have $\lambda n + \mu a = 1$ for some $\lambda, \mu \in \mathbb{Z}$. Then*

$$b = \lambda nb + \mu ab$$

[5] *and $n$ divides the RHS, so $n \mid b$.*

---

Let $a, b, c, d$ be distinct prime numbers. Explain carefully why $ab$ cannot equal $cd$.

[*No form of the Fundamental Theorem of Arithmetic may be assumed without proof.*]

---

*Suppose for contradiction that $ab = cd$. Then $a \mid cd$, so by previous part, since $a$ is prime, we get $a \mid c$ or $a \mid d$. Since $c$ and $d$ are prime, we*
[3] *deduce $a = c$ or $a = d$, contradicting the fact that $a$, $b$, $c$, $d$ are distinct.*

---

(b) Now let $S$ be the set of positive integers that are congruent to 1 mod 10. We say that $x \in S$ is *irreducible* if $x > 1$ and whenever $a, b \in S$ satisfy $ab = x$ then $a = 1$ or $b = 1$. Do there exist distinct irreducibles $a, b, c, d$ with $ab = cd$?

---

*Yes. Let $a = 3 \times 7$, $b = 13 \times 17$, $c = 3 \times 17$ and $d = 13 \times 7$. Each of these is 1 mod 10, and has only one non-trivial factorisation in positive integers, but the factors are not 1 mod 10, so they are each irreducible in*
[7] *$S$. They are clearly distinct (say by previous part) and satisfy $ab = cd$.*

---

**[20]**

**7E Numbers and Sets**

Define the binomial coefficient $\binom{n}{i}$, where $n$ is a positive integer and $i$ is an integer with $0 \leqslant i \leqslant n$. Arguing from your definition, show that $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

---

*$\binom{n}{i}$ is defined to be the number of subsets of $\{1, 2, \ldots, n\}$ of size $i$. Thus*

$$\sum_{i=0}^{n} \binom{n}{i} = \textit{Total number of subsets of } \{1, 2, \ldots, n\},$$

*and this is $2^n$ (each of the $n$ elements is either* in *or* not in *any given*
[3] *subset).*

---

Prove the binomial theorem, that $(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$ for any real number $x$.

---

*Imagine multiplying out the $n$ copies of $(1+x)$. All terms are of the form $x^i$ for $0 \leqslant i \leqslant n$, and each $x^i$ comes from multiplying the $x$'s from $i$ of the brackets with the 1's from the remaining $n-i$ brackets. The number of copies of $x^i$ is therefore the number of ways of choosing the*
[2] *$i$ brackets from which to take the $x$, which is exactly $\binom{n}{i}$.*

---

By differentiating this expression, or otherwise, evaluate $\sum_{i=0}^{n} i \binom{n}{i}$ and $\sum_{i=0}^{n} i^2 \binom{n}{i}$.

---

*Differentiating the binomial theorem with respect to $x$ gives*

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

*for all real $x$. Differentiating again gives*

$$n(n-1)(1+x)^{n-2} = \sum_{i=0}^{n} i(i-1) \binom{n}{i} x^{i-2}$$

*for all $x$. Setting $x = 1$ we obtain*

$$\sum_{i=0}^{n} i \binom{n}{i} = n2^{n-1}$$

*and*

$$\sum_{i=0}^{n} i(i-1) \binom{n}{i} = n(n-1)2^{n-2}.$$

*Adding these gives*

$$\sum_{i=0}^{n} i^2 \binom{n}{i} = n2^{n-2}\big((n-1)+2\big) = n(n+1)2^{n-2}.$$

[6]

By considering the identity $(1+x)^n(1+x)^n = (1+x)^{2n}$, or otherwise, show that

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}.$$

*We have*

$$\begin{aligned}\binom{2n}{n} &= \textit{Coeff of } x^n \textit{ in } (1+x)^{2n} \\ &= \textit{Coeff of } x^n \textit{ in } (1+x)^n(1+x)^n \\ &= \sum_{i=0}^{n} \Big(\textit{Coeff of } x^i \textit{ in } (1+x)^n\Big)\Big(\textit{Coeff of } x^{n-i} \textit{ in } (1+x)^n\Big) \\ &= \sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}.\end{aligned}$$

*Sending a subset of* $\{1, 2, \ldots, n\}$ *to its complement gives a bijection between subsets of size* $i$ *and subsets of size* $n-i$ *so* $\binom{n}{n-i} = \binom{n}{i}$ *and*

[3] *we get the result.*

Show that $\displaystyle\sum_{i=0}^{n} i\binom{n}{i}^2 = \frac{n}{2}\binom{2n}{n}$.

*Differentiating* $(1+x)^n(1+x)^n = (1+x)^{2n}$ *we get*

$$\begin{aligned}2n(1+x)^{2n-1} &= 2(1+x)^n \frac{\mathrm{d}}{\mathrm{d}x}(1+x)^n \\ &= 2\left(\sum_{j=0}^{n}\binom{n}{j}x^j\right)\left(\sum_{i=0}^{n} i\binom{n}{i}x^{i-1}\right).\end{aligned}$$

*Equating coeffs of* $x^{n-1}$ *we get*

$$2n\binom{2n-1}{n-1} = 2\sum_{i=0}^{n} i\binom{n}{i}\binom{n}{n-i} = 2\sum_{i=0}^{n} i\binom{n}{i}^2.$$

*So left to show*

$$2\binom{2n-1}{n-1} = \binom{2n}{n},$$

*or equivalently that*

$$\binom{2n-1}{n-1} + \binom{2n-1}{n} = \binom{2n}{n}.$$

*To prove this equality note that the RHS counts subsets of* $\{1, 2, \ldots, 2n\}$ *of size* $n$ *whilst the LHS counts the same thing, split into 'subsets*

[6] *containing* $2n$*' and 'subsets not containing* $2n$*'.*

**[20]**