4/I/1E **Numbers and Sets**

Find the unique positive integer a with $a \leq 19$, for which

$$17! \cdot 3^{16} \equiv a \pmod{19}.$$

Results used should be stated but need not be proved.

Solve the system of simultaneous congruences

$$\begin{aligned} x &\equiv 1 \pmod{2}, \\ x &\equiv 1 \pmod{3}, \\ x &\equiv 3 \pmod{4}, \\ x &\equiv 4 \pmod{5}. \end{aligned}$$

Explain very briefly your reasoning.

4/I/2E **Numbers and Sets**

Give a combinatorial definition of the binomial coefficient $\binom{n}{m}$ for any non-negative integers n, m.

Prove that $\binom{n}{m} = \binom{n}{n-m}$ for $0 \leq m \leq n$.

Prove the identities

$$\binom{n}{k}\binom{k}{l} = \binom{n}{l}\binom{n-l}{k-l}$$

and

$$\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{n+m}{k}.$$

4/II/5E **Numbers and Sets**

What does it mean for a set to be countable? Show that $\mathbb{Q} \times \mathbb{Q}$ is countable, and $\mathbb{R}$ is not countable.

Let D be any set of non-trivial discs in a plane, any two discs being disjoint. Show that D is countable.

Give an example of a set C of non-trivial circles in a plane, any two circles being disjoint, which is not countable.

4/II/6E **Numbers and Sets**

Let R be a relation on the set S. What does it mean for R to be an equivalence relation on S? Show that if R is an equivalence relation on S, the set of equivalence classes forms a partition of S.

Let G be a group, and let H be a subgroup of G. Define a relation R on G by $a \; R \; b$ if $a^{-1}b \in H$. Show that R is an equivalence relation on G, and that the equivalence classes are precisely the left cosets gH of H in G. Find a bijection from H to any other coset gH. Deduce that if G is finite then the order of H divides the order of G.

Let g be an element of the finite group G. The order $o(g)$ of g is the least positive integer n for which $g^n = 1$, the identity of G. If $o(g) = n$, then G has a subgroup of order n; deduce that $g^{|G|} = 1$ for all $g \in G$.

Let m be a natural number. Show that the set of integers in $\{1, 2, \ldots, m\}$ which are prime to m is a group under multiplication modulo m. [*You may use any properties of multiplication and divisibility of integers without proof, provided you state them clearly.*]

Deduce that if a is any integer prime to m then $a^{\phi(m)} \equiv 1 \pmod{m}$, where ϕ is the Euler totient function.

4/II/7E **Numbers and Sets**

State and prove the Principle of Inclusion and Exclusion.

Use the Principle to show that the Euler totient function ϕ satisfies

$$\phi(p_1^{c_1} \cdots p_r^{c_r}) = p_1^{c_1-1}(p_1 - 1) \cdots p_r^{c_r-1}(p_r - 1).$$

Deduce that if a and b are coprime integers, then $\phi(ab) = \phi(a)\phi(b)$, and more generally, that if d is any divisor of n then $\phi(d)$ divides $\phi(n)$.

Show that if $\phi(n)$ divides n then $n = 2^c 3^d$ for some non-negative integers c, d.

4/II/8E **Numbers and Sets**

The Fibonacci numbers are defined by the equations $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for any positive integer n. Show that the highest common factor (F_{n+1}, F_n) is 1.

Let n be a natural number. Prove by induction on k that for all positive integers k,

$$F_{n+k} = F_k F_{n+1} + F_{k-1} F_n.$$

Deduce that F_n divides F_{nl} for all positive integers l. Deduce also that if $m \geq n$ then

$$(F_m, F_n) = (F_{m-n}, F_n).$$