Please send any corrections or comments to me at glt1000@cam.ac.uk

Some starter questions

i. Prove by induction that $1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{1}{4}n^2(n+1)^2$ and deduce that $1^3 + 3^3 + 5^3 + ... + (2n-1)^3 = n^2(2n^2-1)$.

ii. In the plane I draw N circles. Show that these divide the plane into no more than $2 + (N-1)N$ regions.

iii. Let $x \in \mathbb{R}$. Show that if $x + \dfrac{1}{x} \in \mathbb{N}$, then $x^n + \dfrac{1}{x^n} \in \mathbb{N}$ for all $n \in \mathbb{N}$.

iv. Using the Inclusion-Exclusion Principle, find $\varphi(1001)$. More generally, for distinct prime numbers p, q, r, find $\varphi(pqr)$.

v. What is $21^{20} \times 20! \pmod{23}$? What is $28^{27} \times 28! \pmod{31}$?

vi. How many functions are there from $\{1,2,3,4,5\}$ to $\{1,2,3\}$? How many are injective? Find how many are surjective by two methods: Inclusion-Exclusion, and counting combinations. (If we did this during the term, do it for $\{1,2,3,4,5,6,7\} \to \{1,2,3,4\}$.)

vii. Give an example of a relation for each of the various subsets of {reflexive, symmetric, transitive}. For example: obeying none of R, S, T; only R and not S, T; etc.

1998/IV/7A

(i) Describe Euclid's algorithm and show that it finds the highest common factor (m,n) of two positive integers m and n. Show further that (m,n) can be written as $am + bn$ for integers a and b. Find an integer solution of

$$15x + 21y + 35z = 1.$$

Is your solution unique?

(ii) Suppose that $(m,n) = 1$. Show that the simultaneous congruences

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

have the same solutions as $x \equiv c \pmod{mn}$, for some $c \in \mathbb{Z}$. Solve the simultaneous equations

$$3x \equiv 1 \pmod{5}$$
$$5x \equiv 1 \pmod{7}$$
$$7x \equiv 1 \pmod{3}.$$

1999/IV/1D, more or less

(i) Prove that any natural number n greater than 1 can be written as a product of prime numbers. Explain, and prove, to what extent the product for n is unique.

(ii) Prove that there are infinitely many prime numbers.

(iii) By considering numbers of the form $6p_1p_2...p_k - 1$, prove that there are infinitely many prime numbers of the form $6n - 1$. What would go wrong if we tried a similar proof to show that there are infinitely many primes of the form $6n + 1$?

A bit of 1998/IV/5A and a bit more

(a) Prove the Euler-Fermat theorem. Show that, if n is any natural number, then n divides $(10^k - 1)10^r$ for some natural numbers k and r.

(b) Prove Wilson's theorem. Let p be a prime number. Show, by induction on r, that for $0 \leq r \leq p - 1$

$$\binom{p-1}{r} \equiv (-1)^r (\text{mod } p).$$

Hence show that mod p, the inverse of $r!$ is $(-1)^{r+1}(p - r - 1)!$, for all $0 \leq r \leq p - 1$.

1998/IV/1A

Let $f : X \to Y$ be a function. For $A \subseteq X$ let $f(A) = \{f(x) \mid x \in A\}$. For $B \subseteq Y$ let $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$. Give proofs or counter-examples to the following claims:

i. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;
ii. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$;
iii. $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$;
iv. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

1999/IV/5D, more or less

(a) Let A, B be finite non-empty sets, with $|A| = a, |B| = b$. How many mappings are there from A to B? How many of these mappings are injective? How many are bijective?

(b) State and prove the Inclusion-Exclusion Principle.

(c) Prove that the number of surjections from a set of size n to a set of size k $(1 \leq k \leq n)$ is

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

Deduce that

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