Number Theory
B. Math. (Hons.) First year
Assignment I - Due by 8th October 2021
Instructor - B. Sury

Q 1. Using induction or otherwise, prove:
For any $r \geq 1$, given $2^r n - n + 1$ distinct elements of $\{1, 2, \cdots, 2^r n\}$, there exist $r+1$ of them, say $a_0, a_1, \cdots, a_r$ so that $a_0 | a_1 | \cdots | a_r$.

Q 2. Prove the arithmetic mean - Geometric Mean inequality by "backward induction" as follows.
(i) Prove by induction on n, that any given positive real numbers $a_1, a_2, \cdots, a_{2^n}$ (not necessarily distinct) satisfy the AM-GM inequality

$$(\sum_{i=1}^{2^n} a_i)^{2^n} \geq (2^n)^{2^n} \prod_{i=1}^{n} a_i$$

with equality if, and only if, all a_i's are equal.
(ii) Prove that if $k \geq 2$ and the AM-GM inequality holds for any k positive real numbers (with equality if and only if they are all equal), then it folds for any $k-1$ positive real numbers with equality if and only if the numbers are all equal.

Q 3. For each $d \geq 0$, consider the polynomial $P_d(x)$ of degree d defined by $P_d(x) = \frac{x(x-1)\cdots(x-d+1)}{d!}$ with coefficients in $\mathbb{Q}$ (here $P_0(x) = 1$). Prove that every polynomial $P(x)$ of degree r satisfying the property that $P(\mathbb{Z}) \subset \mathbb{Z}$ is expressible as

$$P(x) = c_0 P_0(x) + c_1 P_1(x) + \cdots + c_r P_r(x)$$

where c_i's are uniquely determined integers.

Q 4. (You are supposed to use only completely elementary results and not to use advanced results like Fermat's little theorem in the problems below).
(i) Given positive integers $a, n > 1$ with a coprime to n, prove that there is some integer $d > 0$ so that $a^d - 1$ is a multiple of n.
(ii) Prove that for any positive integers a, m, n we have $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.
(iii) If $a_1, a_2, \cdots, a_n$ are integers (not necessarily distinct), prove that there

exist $i < j$ such that $a_i + a_{i+1} + \cdots + a_j$ is a multiple of n.
(iv) If $1 \leq a, r$, show that $\frac{1}{a} \pm \frac{1}{a+1} \pm \cdots \pm \frac{1}{a+r}$ is not an integer, whatever may be the choices of signs.
(v) If $P(x)$ is a polynomial of degree > 1 with integer coefficients, prove that not all values of P at positive integers can be prime numbers.

Q 5.* If a, b are positive integers such that $\frac{a^2+b^2}{1+ab}$ is an integer, then show that it must be a perfect square.