Quiz Section 5: Number Theory, Induction

Review

5 Steps to an Induction Proof: To prove $\forall n \in \mathbb{N}\ P(n)$ (or equivalently $\forall n \geqslant 0\ P(n)$ for $n \in \mathbb{Z}$).

1. "Let $P(n)$ be ⟨fill in⟩. We will show that $P(n)$ is true for every $n \in \mathbb{N}$ (or equivalently integer $n \geqslant 0$) by induction."
2. "Base Case:" Prove $P(0)$
3. "Inductive Hypothesis: Suppose $P(k)$ is true for some arbitrary integer $k \geqslant 0$"
4. "Inductive Step:" Prove that $P(k+1)$ is true.

   Use the goal to figure out what you need.
   Make sure you are using I.H. and point out where you are using it.
   (Don't assume $P(k+1)$!)
5. "Conclusion: The claim follows by induction"

Task 1 – Multiplicative inverses

For each of the following choices of a and m, determine whether a has a multiplicative inverse modulo m. If yes, *guess* a multiplicative inverse of a modulo m *and check* your answer.

a) $a = 3$ and $m = 8$

b) $a = 6$ and $m = 28$

c) $a = 5$ and $m = 29$

Task 2 – Extended Euclidean Algorithm Practice

a) Find the multiplicative inverse of y of 7 mod 33. That is, find y such that $7y \equiv 1 (\text{mod } 33)$, You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leqslant y < 33$.

b) Now solve $7z \equiv 2$ (mod 33) for all of its integers solutions z.

Task 3 – Induction with Divides

Prove that $9 \mid (n^3 + (n+1)^3 + (n+2)^3)$ for all integers $n > 1$.

Task 4 – Induction with Inequality

Prove that $6n + 6 < 2^n$ for all integers $n \geqslant 6$.

Task 5 – In Harmony with Ordinary Induction

Define

$$H_i = \sum_{j=1}^{i} \frac{1}{j} = 1 + \frac{1}{2} + \cdots + \frac{1}{i}$$

The numbers H_i are called the *harmonic* numbers.
Prove that $H_{2^n} \geqslant 1 + \frac{n}{2}$ for all integers $n \geqslant 0$.

Task 6 – Cantelli's Rabbits

Xavier Cantelli owns some rabbits. The number of rabbits he has in year n is described by the function $f(n)$:

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(n) &= 2f(n-1) - f(n-2) \text{ for } n \geqslant 2 \end{aligned}$$

Determine, with proof, the number, $f(n)$, of rabbits that Cantelli owns in year n. That is, construct a formula for $f(n)$ and prove its correctness.

Task 7 – Strong Induction

Consider the function $a(n)$ defined for $n \geqslant 1$ recursively as follows.

$$a(1) = 1$$

$$a(2) = 3$$

$$a(n) = 2a(n-1) - a(n-2) \text{ for } n \geqslant 3$$

Use strong induction to prove that $a(n) = 2n - 1$ for all integers $n \geqslant 1$.

Task 8 – Induction with Equality

a) Define the triangle numbers as $\triangle_n = 0 + 1 + 2 + \cdots + n$, where $n \in \mathbb{N}$. In class we showed $\triangle_n = \frac{n(n+1)}{2}$.

Prove the following equality for all $n \in \mathbb{N}$:

$$0^3 + 1^3 + \cdots + n^3 = \triangle_n^2$$

b) For every $n \in \mathbb{N}$, define S_n to be the sum of the squares of the natural numbers up to n, or

$$S_n = 0^2 + 1^2 + \cdots n^2.$$

For all $n \in \mathbb{N}$, prove that $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Task 9 – Efficient Modular Exponentiation

a) Compute $2^{71} \bmod 25$ using the efficient modular exponentiation algorithm.

b) How many modular multiplications does the algorithm use for this computation?