MAT 246S **Practice Term Test 3** **Winter 2014**

(1) Find a mistake in the following "proof".

Claim: $1 + 2 + \ldots + n = \frac{1}{2}(n + \frac{1}{2})^2$ *for any natural* n.

We proceed by induction on n.

a) The claim is true for $n = 1$.

b) Suppose we have already proved the claim for some $n \geq 1$. *We need to prove it for* $n + 1$.

We know that $1 + 2 + \ldots + n = \frac{1}{2}(n + \frac{1}{2})^2$. *Then* $1 + 2 + \ldots + n + (n + 1) = = \frac{1}{2}(n + \frac{1}{2})^2 + (n + 1) = \frac{1}{2}(n^2 + n + \frac{1}{4} + 2(n + 1)) = \frac{1}{2}(n^2 + 3n + \frac{9}{4}) = \frac{1}{2}(n + \frac{3}{2})^2 = \frac{1}{2}((n + 1) + \frac{1}{2})^2$.

This verifies the claim for $n + 1$ *and therefore the claim is true for all natural* n.

(2) Find $6^{3^{100}} (\mod 22)$.

(3) Let a, b, c be natural numbers such that $gcd(a, b) = 1$. Suppose a divides c and b divides c.

Prove that ab also divides c.

(4) Let $p = 3, q = 5$ and $E = 11$. Let $N = 3 \cdot 5 = 15$. The receiver broadcasts the numbers $N = 15, E = 11$. The sender sends a secret message M to the receiver using RSA encryption. What is sent is the number $R = 3$.

Decode the original message M.

(5) Mark True or False. If true explain why, if false give a counterexample.

(a) The product of any two irrational numbers is irrational.

(b) For any prime p we have $((p - 1)!)^2 \equiv 1(\mod p)$.