**MAT 246S** **Solutions to the Term Test** **March 2, 2012**

(1) (10 pts) 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* $n$.

**Solution**

The mistake is that the claim is actually false for the base of induction $n=1$ so the induction can not be started. Indeed for $n=1$ the LHS is equal to 1 but the RHS is equal to $\frac{1}{2}(1+\frac{1}{2})^2=\frac{9}{8}\neq 1$.

(2) (10 pts) Find $6^{3^{100}}(\mod 22)$.

**Solution**

We first find $6^{3^{100}}(\mod 11)$. Snce 11 is prime and $(6,11)=1$ we have that $6^{10}\equiv 1(\mod 11)$. So we need to find $3^{100}(\mod 10)$. Since $(3,10)=1$ we have that $3^{\phi(10)}\equiv 1(\mod 10)$. We compute $\phi(10)=\phi(2\cdot 5)=(2-1)\cdot(5-1)=4$. Therefore $3^4\equiv 1(\mod 10)$. This can also be seen directly without appealing to Euler's theorem because $3^4=81\equiv 1(\mod 10)$. Hence $3^{4k}\equiv 1(\mod 10)$ for any natural $k$ and in particular, $3^{100}=3^{4\cdot 25}\equiv 1(\mod 10)$. In other words $3^{100}=10m+1$ for some $m$ and therefore $6^{3^{100}}=6^{10m+1}\equiv 1\cdot 6^1\equiv 6(\mod 11)$. This means that 11 divides $6^{3^{100}}-6$. But we also obviously have that 2 divides $6^{3^{100}}-6$. Since $(2,11)=1$ this implies that 22 divides $6^{3^{100}}-6$, i.e.

**Answer:** $6^{3^{100}}\equiv 6(\mod 22)$.

(3) (10 pts) Let $a,b,c$ be natural numbers such that $(a,b)=1$. Suppose $a$ divides $c$ and $b$ divides $c$.

Prove that $ab$ also divides $c$.

**Solution**

Since $(a, b) = 1$ we can find integer $x, y$ such that $ax + by = 1$. Multiplying this by $c$ we get $axc + byc = c$. Since $a|c$ we can write $c = ak$ and since $b|c$ we can write $c = lb$ for some integer $k, l$. Therefore

$$c = axc + byc = axlb + byka = ab(xl + ky) \text{ and hence } ab|c.$$

(4) (10 pts) 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 $M$.

**Solution**

First we find $\phi(N) = (3-1)\cdot(5-1) = 8$. We need to find $D$ such that $ED \equiv (1 \mod 8)$. This can be done using the Euclidean algorithm or we can simply notice that $11 \cdot 3 = 33 \equiv 1(\mod 8)$ so $D = 8$ works.

Then $M \equiv R^D(\mod N) = 3^3(\mod 15) = 27(\mod 15) \equiv 12(\mod 15)$.

**Answer:** $M = 12$.

(5) (10 its) 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 $((p-1)!)^2 \equiv 1(\mod p)$.

**Solution**

(a) **False.** For example, take $x = \sqrt{2}$ and $y = \frac{1}{\sqrt{2}}$ then both $x$ and $y$ are irrational but $x \cdot y = 1$ is rational.

(b) **True.** By Wilson's theorem $(p-1)! \equiv -1(\mod p)$ and therefore $((p-1)!)^2 \equiv (-1)^2 = 1(\mod p)$.