January 26, 2007

Solution to the exam Number Theory (88/89-576), Spring 2005, "Moed" A

1. Answers: 99, 243.

2. Any integer has the representation $a = \pm p_1^{e_1} \dots p_k^{e_k}$ for all j. As for any $p|a$ also $p^2|a$ we have $e_j \geq 2$. Then we can choose $b = \prod_{e_j-even} p_j^{e_j/2} \cdot \prod_{e_j-odd} p_j^{(e_j-3)/2}$ and $c = \prod_{e_j-odd} p_j$.

Remark: In fact, the proof is immediate once we notice that any non-negative number e is representable in the form $e = 2x + 3y$ with $x, y \in \mathbb{Z}$ and non-negative.

3. We have $b \equiv a^{-1}$ and hence $b^h \equiv (a^{-1})^h \equiv (a^h)^{-1} \equiv 1$ $(mod\ p)$. Hence $ord(b)|ord(a)$. Changing the role of a and b we get $ord(a)|ord(b)$ and hence $ord(a) = ord(b)$.

4. We have to prove that $x^x \equiv (x + p(p-1))^{x+p(p-1)}$ $(mod\ p)$. We have:

$(x + p(p-1))^{x+p(p-1)} \equiv x^{x+p(p-1)} \equiv x^x \cdot x^{p(p-1)}$ $(mod\ p)$.

If $x \equiv 0$ $(mod\ p)$ then $x^x \equiv (x + p(p-1))^{x+p(p-1)} \equiv 0$ $(mod\ p)$. If $x \not\equiv 0$ $(mod\ p)$ then $x^{p(p-1)} \equiv (x^p)^{p-1} \equiv x^{p-1} \equiv 1$ $(mod\ p)$ by Fermat theorem and hence in this case $x^x \equiv (x + p(p-1))^{x+p(p-1)}$ $(mod\ p)$ too.

We have to show that $p(p-1)$ is the minimal period. The period have to be divisible by p since $x^x \equiv 0$ $(mod\ p)$ for any x divisible by p. Let g be a primitive root $mod\ p$. If kp is the period then $g^{kp} \equiv (g^p)^k \equiv g^k \equiv 1$ $(mod\ p)$ and hence $p-1|k$.

5. Let $p > 2$ be a prime. The equation $x^2 \equiv 1$ $(mod\ p)$ has only two roots ± 1. Let g be a primitive root $mod\ p$. We have $(g^{(p-1)/2})^2 \equiv g^{p-1} \equiv 1$ and hence $g^{(p-1)/2} \equiv -1$ (otherwise $ord(g) \neq p-1$).

Let $p \equiv 3$ $(mod\ 4)$ i.e., $p = 4m+3$ and $(p-1)/2 = 2m+1$ is odd.

Then $(-g)^{(p-1)/2} \equiv (-1)^{2m+1} g^{(p-1)/2} \equiv (-1) \cdot (-1) \equiv 1$ $(mod\ p)$.
Hence $ord(-g) \leq (p-1)/2$ – it is not a primitive root.

Let $p \equiv 1$ $(mod\ 4)$ i.e., $p = 4m+1$ and $(p-1)/2 = 2m$ is even.

We want to compute $ord(-g)$ i.e., find minimal $k > 0$ such that $g^k \equiv 1$ $(mod\ p)$. If $ord(-b) < p-1$ then $ord(-g)$ can not be even since $(-g)^{2l} \equiv g^{2l} \not\equiv 1$.

We have $(-g)^{(p-1)/2} \equiv (-1)^{2m} g^{(p-1)/2} \equiv (1) \cdot (-1) \equiv -1$ $(mod\ p)$.
Hence $ord(-g) \not| (p-1)/2$.
But $p-1 = 4m$ and $(p-1)/2 = 2m$ have the same odd divisors and if $ord(-b) < p-1$ then it is odd. We have $ord(-b)|p-1$ by Fermat theorem and hence $ord(-g) = (p-1)$ – it is a primitive root.

Remark: There are many similar solutions.