July 21, 2007

Solution to the exam 89-256 for 2007, A

2. Let g be a primitive root modulo prime p and $(a,p) = 1$. Let $g^i \equiv a$ $(mod\ p)$. If there is such x that $x^n \equiv a$ $(mod\ p)$ then $(x,p) = 1$ and hence we have $x \equiv g^u$ $(mod\ p)$ for some u. Hence we have $x^n \equiv (g^u)^n \equiv g^i$. This implies that $nu \equiv i$ $(mod\ p-1)$. Denote by $k = (n, p-1)$. The equation (in u) $nu \equiv i$ $(mod\ p-1)$ has k solutions if $k|i$ and no solutions otherwise. If $k|i$ then $i(p-1)/k \equiv 0$ $(mod\ p-1)$ and hence $a^{(p-1)/k} \equiv g^{i(p-1)/k} \equiv (g^{p-1})^{i/k} \equiv 1$ $(mod\ p)$ on the other hand if $k \not| i$ then $a^{(p-1)/k} \equiv g^{i(p-1)/k} \not\equiv 1$ $(mod\ p-1)$. $\square$

3. A. Let g be a primitive root modulo $p \neq 2$. We have $g^{\phi(p)} \equiv 1$ $(mod\ p)$ or $g^{p-1} = 1+py$ for some integer y. Let $g' = g+px$, $(x,p) = 1$ and consider $(g')^{p-1} = (g+px)^{p-1} = 1+pz$ where $z \equiv y+(p-1)g^{p-2}x$ $(mod\ p)$ according to the binomial formula. Since $(p-1,p) = (g,p) = (x,p) = 1$ we can choose x such that $(z,p) = 1$ (i.e., such that $p \not| y+(p-1)g^{p-2}x$).

B. Let $g' = g+px$ with x as above. Let d be the order of g' modulo p^j, i.e., $(g')^d \equiv 1$ $(mod\ p^j)$. Then according to the Euler theorem we have $d|\phi(p^j) = p^{j-1}(p-1)$. But g' is obviously a primitive root modulo p and hence $p-1|d$ which implies that $d = p^k(p-1)$ for some $k < j$. As p is odd we have $(1+pz)^{p^k} = 1+p^{k+1}z_k$ for some $(z_k,p) = 1$. But then we have $1 \equiv (g')^d \equiv ((g')^{p-1})^{p^k} \equiv (1+pz)^{p^k} = 1+p^{k+1}z_k$ $(mod\ p^j)$ and hence $k+1 = j$ namely that $d = \phi(p^j) = p^{j-1}(p-1)$. $\square$

4. The assumption is that there exists a satisfying $a^{n-1} \equiv 1$ $(mod\ n)$ and $(a^{(n-1)/q}-1, n) = 1$, or what is the same $a^{(n-1)/q} \not\equiv 1$ $(mod\ n)$, with q prime such that $n = q^kR+1$, $(q,R) = 1$. Let prime $p|n$. Then we also have $a^{n-1} \equiv 1$ $(mod\ p)$ and $a^{(n-1)/q} \not\equiv 1$ $(mod\ p)$. This means that the order m of a modulo p satisfy $m|n-1$ and $m \not|(n-1)/q$. Since $n-1 = q^kR$ we have that $q^k|m$. According to the small Fermat theorem $m|\phi(p) = p-1$. Hence $p-1 = q^kr$ for some r. $\square$