(1) 证明题：设 m是大于1的整数，a是与 m互素的整数。则当m的标准分解式为$m=2^n p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 时，有$ord_m(a)=[ord_{2^n}(a),ord_{p_1^{\alpha_1}}(a),\cdots ord_{p_k^{\alpha_k}}(a)]$;

由于a与m互素，因此a和m的最大公因数是1，而$m=2^np_1^{\alpha_1}\ldots p_k^{\alpha_k}$，因此$2^n,p_k^{\alpha_k}$都是$m$的因数，于是$a$与$m$的因数的最大公因数也应该是$1$，$a$与$2^n$互素，而$m$的标准分解式中$2$，$\ldots$，$p_k$都是素数，所以有：$2^n..p_k^{\alpha_k}$互素，进而根据 $<$定理$5.1.7>$有：$ord_{2^np_1^{\alpha_1}}(a)=[ord_{2^n}(a),ord_{p_1^{\alpha_1}}(a)]$

进而有$2^np_1^{\alpha_1}$与$p_2^{\alpha_2}$也互素，于是$ord_{2^np_1^{\alpha_1}p_2^{\alpha_2}}(a)=[[ord_{2^n}(a),ord_{p_1^{\alpha_1}}(a)],ord_{p_2^{\alpha_2}}(a)]$

根据 $<$定理$1.4.6>$，有$[a_1,a_2]=D_1,[D1,a_3]=D_2$,那么$[a_1,a_2,a_3]=D_2$,于是$[[ord_{2^n}(a),ord_{p_1^{\alpha_1}}(a)],ord_{p_2^{\alpha_2}}(a)]=[ord_{2^n}(a),ord_{p_1^{\alpha_1}}(a),ord_{p_2^{\alpha_2}}(a)]$

由以上证明归纳可得：$ord_m(a)=ord_{2^np_1^{\alpha_1}\ldots p_k^{\alpha_k}}(a)=[ord_{2^n}(a),ord_{p_1^{\alpha_1}}(a)\ldots ord_{p_k^{\alpha_k}}(a)]$

证明成立

(2) 证明题：设 $\alpha\geq 1$，g是模p^α的一个原根，g为偶数时 $g+p^\alpha$是模$2p^\alpha$的一个原根.

即 $<$定理$5.2.5>$的证明：

g是模p^α的一个原根，原根的前提条件是与模数互素，因此$(g,p^\alpha)=1$，注意到g是偶数，于是：

$--p^\alpha$必是奇数，$g+p^\alpha$必是奇数，令$d=\varphi(p^\alpha),\varphi(2p^\alpha)=\varphi(2)\varphi(p^\alpha)=\varphi(p^\alpha)=d$

于是有：$(g+p^\alpha)^{\varphi(p^\alpha)}\equiv g^{\varphi(p^\alpha)}\equiv 1(mod\quad p^\alpha)$

$---(g+p^\alpha)^r\equiv g^r!\equiv 1(mod\quad p^\alpha),1\leq r\leq\varphi(p^\alpha)$　　因为g是模p^α的原根

而$g+p^\alpha$又是奇数，所以$(g+p^\alpha)\equiv 1(mod\quad 2)$

根据 $<$定理$2.1.12>$,$(g+p^\alpha)^r\equiv 1(mod\quad [2,p^\alpha]=2p^\alpha)$，当且仅当$r\equiv\varphi(p^\alpha)=\varphi(2p^\alpha)$时成立

所以$(g+p^\alpha)$是模$2p^\alpha$的一个原根

(5)求解同余方程$x^8\equiv 41\ (mod\ 23)$.

23是素数，$(42,23)=1$,查找23的原根$g=5$,将方程指标化

$8ind_gx\equiv ind_g41(mod\quad\varphi(23)=22)$

而$indg41=12,(8,22)=2|12$,因此方程有解，解数为$(8,22)=2$

$8ind_gx=12(mod\quad 22)$

$ind_g(x)\equiv 7(mod\quad 11)\equiv 7,18(mod\quad 22)$

$x\equiv 17,6(mod\quad 23)$