1. 设m，n为正整数，m是奇数，求证：2^m-1和2^n+1互素.

要证明两个数互素，即证明$(2^m-1,2^n+1)=1$，设$(2^m-1,2^n+1)=d$

于是$2^m=k_1d+1;\quad 2^n=k_2d-1$

为了利用条件m是奇数，求$(2^n)^m$

$$(2^n)^m=(k_2d-1)^m\equiv(-1)^m\equiv-1(mod\,d)$$

$$(2^n)^m=k_3d-1$$

同理$(2^m)^n=(k_1d+1)^n\equiv1(mod\,d)$

$$(2^n)^m=k_4d+1$$

因此$k_3d-1-(k_4d+1)=0,(k_3-k_4)d=2$

而$d>=1$;因此$k_3-k_4>=1$(为负数和0不可能满足上式)

所以$d=1$或者2

若$d=2,\quad 2^m-1=k_1d=2k_1=$偶数，而$2^m-1$是奇数，所以矛盾

因此$d=1$，两个数互素

2. 设a，b，c为整数，求证：$[(a,b),(a,c)]=(a,[b,c])$.

设

$$a=p_1{}^{s_11}p_2{}^{s_12}\dots p_n{}^{s_1n}$$

$$b=p_1{}^{s_21}p_2{}^{s_22}\dots p_n{}^{s_2n}$$

$$c=p_1{}^{s_31}p_2{}^{s_32}\dots p_n{}^{s_3n}$$

$$[(a,b),(a,c)\ ]=p_1{}^{m_1}p_2{}^{m_2}\dots p_n{}^{m_n}$$

$$m_i=max\{min(s_{1i},s_{2i}),min(s_{1i},s_{3i})\}$$

$$(a,[b,c])=p_1{}^{k_1}p_2{}^{k_2}\dots p_n{}^{k_n}$$

$$k_i=min\{s_{1i},max(s_{2i},s_{3i})\}$$

$$m_i=k_i$$

3. 设p_k为素数，$1\le k\le n$，$k\in\mathbb{N}^+$且$\forall 1\le i<j\le n, p_i\ne p_j$，求证：$\sqrt{\prod_{i=1}^{k}p_i}$为无理数.

反证法：

假设$\sqrt{\Pi^k{}_{i=1}p_i}=\dfrac{a}{b}$

所以$a^2\Pi^k{}_{i=1}p_i=b^2$，而$a^2\Pi^k{}_{i=1}p_i$的标准分解式中，由于a^2的分解式每一项次数是偶数，而$\Pi^k{}_{i=1}p_i$每一项的次数是奇数

所以，整个$a^2\Pi^k{}_{i=1}p_i$的标准分解式每一个非零次素数项的次数是奇数.

但是，b^2的标准分解式非零次素数项的次数必是偶数，两者不会相等，所以矛盾.原假设不成立.

4. 设p为素数，a，$b\in\mathbb{Z}$，求证：

(1) $a^2\equiv b^2(\mathrm{mod}\ \ p)\Leftrightarrow a\equiv b(\mathrm{mod}\ \ p)$或$a\equiv -b(\mathrm{mod}\ \ p)$;

(2) 若$(p,a)=1,p>2$，则$a\equiv b(\mathrm{mod}\ \ p)$，$a\equiv -b(\mathrm{mod}\ \ p)$不可能同时成立.

(1)

由$a^2 \equiv b^2 (mod \quad p)$可得

$p|a^2-b^2, p|(a+b)(a-b)$,因此,$p|(a+b)$或者$p|(a-b)$

若$p|a+b$，则$a+b=kp, a=kp-b$,所以$a\equiv -b(mod \quad p)$

同理，若$p|a-b$,那么$a=kp+b$，所以$a\equiv b(mod \quad p)$

证明成立

(2)

假设同时成立，则有

$2a\equiv b-b\equiv 0(mod \quad p)$

由于p是素数，$p>2$，所以p是奇素数,所以$(2,p)=1, 2x\equiv 1(mod \quad p)$有解$x'$

$x'2a\equiv x'0\equiv 0(mod \quad p)$

所以$a\equiv 0(mod \quad p)$

而$(p,a)=1$，与条件矛盾，因此假设不成立.

同样，也可以通过p是奇素数,那么$2a=2kp, a=kp$,这样$(p,a)=(p,kp)=p!=1$,矛盾

5. 求解同余方程$x^3-2x+4\equiv 0(\mathrm{mod} \quad 5^3)$.

常规解法：

$f(x)=x^3-2x+4, \quad f'(x)=3x^2-2$

首先计算同余式$f(x)\equiv 0(mod \quad 5)$的解,有解$x_1\equiv 3(mod5), x_2\equiv 4(mod5)$

1)

考虑解x_1,以$x=3+5t_1$代入$f(x)\equiv 0(mod \quad 5^2)$,有$f(3+5t_1)\equiv f(3)+f'(3)5t_1\equiv 5^2$

解得$t_1\equiv 0,1,2,3,4\equiv (mod5)$

以$x=(3+5t_1)+25t_2$代入$f(x)\equiv 0(mod \quad 5^3)$,等价于$f(3+5t_1)+f'(3+5t_1)25t_2\equiv 0(mod125)$

$25(9t_1^2+1)\equiv 125$,解得$t_1\equiv 1,4(mod5)$,

于是解为$x=8+25k, 23+25k\equiv 0mod(125), k=0,1,2,3,4$

2)

考虑解x_2,以$x=4+5t_1$代入$f(x)\equiv 0(mod5^2)$,有$60+230t_1\equiv 0(mod \quad 25)$

解得$t_1\equiv 3(mod5)$

以$x=19+25t_2=25t_2-6$代入$f(x)\equiv 0(mod5^3)$,有$f(-6)+f'(-6)25t_2\equiv 0(mod125)$

$50+25t_2\equiv 0(mod \quad 125)$

解得$t_2\equiv 3(mod5)=5k+3$

所以解为$x=25(5k+3)-6=125k+69$

综上,解为$x\equiv 8,33,58,83,108,23,48,73,98,123,69\equiv 0(mod \quad 125)$