2. 求解同余式 $x^2+x+7\equiv 0\ (\mathrm{mod}\ 27)$。

$f(x)=x^2+x+7, f'(x)=2x+1;$

由于$27=3^3$;可以先求$f(x)\equiv 0 \pmod 3$

$f(x)=x^2+x+7\equiv 0 \pmod 3$,解得$x\equiv 1 \pmod 3$;

考虑$x=1+3t_1 \pmod 9$代入$f(x)=x^2+x+7\equiv 0 \pmod{3^2=9}$中,得:

$f(1+3t_1)\equiv f(1)+f'(1)3t_1\equiv \pmod 9$,即$9+9t_1\equiv \pmod 9$

因此$t_1\equiv 0,1,2 \pmod 3$, $x=1+3t_1 \pmod 9=1,4,7 \pmod 9$

考虑$x=(1,4,7)+9t_2 \pmod{27}$代入$f(x)\equiv \pmod{3^3=27}$

$x=1+9t_2$时

$f(1)+f'(1)9t_2=9+27t_2 \pmod{27}$, t_2无解

$x=4+9t_2$时

$f(4)+f'(4)9t_2=27+9*9t_2=27+81t_2\equiv 0 \pmod{27}$,解得$t_2=0,1,2 \pmod 3$

$\therefore$原式有解$x\equiv 4,13,22 \pmod{27}$

$x=7+9t_2$时

$f(7)+f'(7)9t_2=63+15*9t_2=63+135t_2\equiv 0 \pmod{27}$,

即$135t_2\equiv 18 \pmod{27}$,而$(135,27)=27!|18$,原式无解

综上所述,原式有解$x\equiv 4,13,22 \pmod{27}$

3 求同余式 $x^2\equiv 13\ (\mathrm{mod}\ 101)$ 的解。

解:101是素数,查原根表得到其一个原根$g=2$,方程指标化:

$2ind_g(x)\equiv ind_g(13)(mod\equiv \quad \varphi(101)=100)$

设$ind_g(13)=r$,即$g^r=2^r\equiv 13(mod \quad 101)$

解得$r=66$,原方程化为:$2ind_g(x)=66(mod \quad 100)$

解得$ind_g(x)=33,83(mod \quad 100)$

因此,原方程解$x\equiv g^{ind_g(x)}\equiv 2^{33},2^{83}(mod \quad 101)$,化简得

$x\equiv 35,66(mod \quad 101)$

4. 求 $F_{2^4}=F_2[x]/(x^4+x^3+1)$ 中的生成元 $g(x)$,并且计算出所有的生成元。

g是F_{2^n}的生成元的条件是$g^{(2^n-1)/q}\neq 1$; q是2^n-1的每个素因数

$2^4-1=15$,因数$1,3,5,15$,素因数为$3,5$;对应的$\dfrac{2^4-1}{q}=5,3$

所以,$g(x)$需要满足$g(x)^3\neq 1 \pmod{x^4+x^3+1}$, $g(x)^5\neq 1 \pmod{x^4+x^3+1}$

取$g(x)=x$,有$g(x)^5=x^5 \pmod{x^4+x^3+1}\equiv -x^3-1\equiv x^3+1$(在$F_2[x]$中)

$g(x)^3=x^3 \pmod{x^4+x^3+1}$

因此$g^3,g^5\neq 1 \pmod{x^4+x^3+1}$, $g(x)=x$是F_{2^4}的生成元

所以F_{2^4}的生成元(本原元)是$F_{2^4}*$的生成元,因此形式是$g^j,(j,15)=1, j=\{1,2,4,7,8,11,13,14\}$

所以生成元是$g\equiv x,x^2,x^3+1,x^2+x+1,x^3+x^2+x,x^3+x^2+1,x^2+x,x^3+x^2$