信息安全数学基础 2005 年考题

1、已知 a=66,b=75，求正整数 x,y，使 ax-by=(a,b)成立 .

2、证明：对于任意整数 a、b、c，如果(a,c)=1，c|ab，则必有 c|b .

3、集合{0，1，・・・・・・9998}中有多少个元素与 9999 互素？

4、已知 a=5,b=42,n=265, 求 $a^b \bmod n$.

5、求如下同余式组的解

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 2 \pmod 9 \end{cases}$$

6、求同余式 $x^5-x^4+x^2+6 \equiv \pmod{7^3}$ 的所有解。

7、求 J(29,97)的值。

8、求 $x^2 \equiv 13 \pmod{113}$ 的解。

9、已知 $59582=2\times31^3$，求模 59582 的一个原根。

信息安全数学基础 2007 学年第二学期 陈恭亮老师作业题

2008-06-06 交，共 5 题

1.2008-05-16 课堂补充
$g_2(x)=x+1$ 是 F_2^8 生成元，求 $g_2(x)=x+1$ 的定义多项式 h(y)，判断 h(y)是否为本原多项式

2.2008-05-16 课堂补充
求出 F_2^8 的子域及其生成元，以及相应的定义多项式

3.2008-05-23 课堂补充
求 $F_2^8=F_2[x]/(x^8+x^4+x^3+x^2+1)$的一个正规基

4.2008-05-28 课堂补充
F_{17} 上椭圆曲线 E $y^2=x^3+2x+5$，求该椭圆曲线的全部点以及阶

5.2008-05-28 课堂补充
F_{17} 上椭圆曲线 E $y^2=x^3+2x-1$，求该椭圆曲线的全部点以及阶

2008-05-16 交，共 8 题

1.2008-05-04 课堂补充
求 $F_2[x]$中 $f(x)=x^8+x^4+x^3+x+1$ 的周期，并求 $y\in F_2[x]/(f(x))$，使得 $y、y^2、y^4、y^8$ 为 $F_2[x]/(f(x))$ 的基底

2.2008-05-04 课堂补充
求 $F_2[x]$中 $f(x)=x^8+x^4+x^3+x^2+1$ 的周期，并求 $y\in F_2[x]/(f(x))$，使得 $y、y^2、y^4、y^8$ 为 $F_2[x]/(f(x))$ 的基底

3.2008-05-04 课堂补充
设 $a(x)=x^3+x+1$，$b(x)=x^2+x+1$，计算 a(x)+b(x)、a(x)．b(x)、a(x)/b(x)

4.第 11 章课件 2
证明：如果 $\alpha\neq 0$ 和 β 都是有理数域 Q 上的代数数，则 $\alpha+\beta$ 和 α^{-1} 也是有理数域 Q 上的代数数

5.第 11 章课件 3
α 叫做代数整数，如果存在一个首一正系数多项式 f(x)，使得 $f(\alpha)=0$。证明：如果 $\alpha\neq 0$ 和 β 是代数整数，则 $\alpha+\beta$ 和 α^{-1} 也是代数整数

6.第 12 章课件 3
证明 $x^8+x^4+x^3+x+1$ 是 $F_2[x]$中的不可约多项式，从而 $F_2[x]/(x^8+x^4+x^3+x+1)$是一个 F_2^8 域

7.第 12 章课件 4
求 $F_2^8=F_2[x]/(x^8+x^4+x^3+x+1)$中的生成元 g(x)，并计算 $g(x)^t$，t=1,2,…,255 和所有生成元

8.第 12 章课件 3
证明 $x^8+x^4+x^3+x^2+1$ 是 $F_2[x]$中的不可约多项式，从而 $F_2[x]/(x^8+x^4+x^3+x^2+1)$是一个 F_2^8 域

2008-05-04 交，共 3 题

1.2008-04-18 课堂补充
求 F_2 上的所有 8 次不可约多项式
注：$x^8+x^4+x^3+x+1$ 是不可约非本原多项式，用于 AES；$x^8+x^4+x^3+x^2+1$ 是不可约本原多项式，用于欧洲通信标准
提示：非零多项式有 $2^8-1=255$ 个，次数为偶数时一定可约，奇数次系数为 0 时可约

2.2008-04-30 课堂补充
求 $Q(\sqrt{2},3\sqrt{3})$的基底

3.2008-04-30 课堂补充
求 u 使 $Q(\sqrt{2},\sqrt{3})=Q(u)$

2008-04-18 交，共 9 题

1.对 3DES 对称密码算法的 S 盒进行轮换分解
补充：DES 算法标准 FIPS 46-2 - (DES), Data Encryption Standard
页面中搜索“PRIMITIVE FUNCTIONS FOR THE DATA ENCRYPTION ALGORITHM”就可找到标准建议的 S 盒函数
还有一个 C 语言的 3DES 实现 FPGA 芯片上的 3DES 实现思路

2.第十章课件 14
证明：置换群 S_4 的一组生成元为(1,2),(1,3),(1,4)
进一步，用该组生成元来给出 S_4 的所有子群

3.第十章课件 15

$$证明：GL_2(Z)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| a,b,c,d\in Z, ad-bc=1\right\}对于矩阵乘法构成群。$$

$$且T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}，S=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}是GL_2(Z)的一组生成元$$

4.2008-04-11 课堂补充
假设 K 是有限域，p 是 K 的特征。证明：p 是奇数，且 K 的元素个数为 p^n

5.2008-04-11 课堂补充
设 R 是特征为 p 的交换环，证明：$\psi:x\rightarrow x^p$ 是 R 的一个自同态

6.2008-04-16 课堂补充
证明：若 a/b=a'/b'，c/d=c'/d'，则必有(ad+bc)/bd=(a'd'+b'c')/b'd'以及 ac/bd=a'c'/b'd'（不依赖代表元选择）

7.2008-04-16 课堂补充
证明课本 10.3 定理 1

8.2008-04-16 课堂补充
证明：整数环是主理想环

9.2008-04-16 课堂补充
设(a)是 Z 的理想，(b)是 Z 的理想，证明(a,b)生成的理想是(gcd(a,b))

2008-03-21 交，共 2 题

1.第九章课件 10+上课补充
分别求出(**Z**/31**Z**)*中的一个 2 阶元 a、3 阶元 b、5 阶元 c，并计算 ord(abc)，证明 abc 是生成元

2.第九章课件 11
求(**Z**/(31・43)**Z**)*中的所有元素的阶，并计算各阶的元素个数

2008-03-07 交，共 9 题

1.第八章课件 11
证明 F_{23} 的非零元对于乘法构成一个循环群，并求出其生成元

2.第八章课件 12
证明：**Z**/n**Z** 中的可逆元对乘法构成一个群，记作 $\mathbf{Z}/n\mathbf{Z}^*$

3.第八章课件 13
证明：**Z**/26**Z** 对乘法不构成一个群

4.第八章课件 14
构造 26 元的一个乘法群

5.2008-02-22 课堂补充 1
证明：假设 H 是 Z 的真子群，则存在 n，使得 H=nZ

6.2008-02-22 课堂补充 2
设群 G，$\{H_i\}_{i\in I}$ 是 G 的一族子群，则$\cup_{i\in I}H_i=H_1\cup H_2\cup\cdots\cup H_n\cup\cdots$是否是 G 的子群？
注：可以设 G=Z(整数乘群或整数加群)，用 Z 的子群来表达
答案：不是

7.第八章课件 2
证明：群 G 是交换群的充要条件是对任意 a,b∈G，有$(ab)^2=a^2b^2$

8.第八章课件 7
设 a 是群 G 的一个元素，证明：映射 $\delta:x\rightarrow axa^{-1}$ 是 G 到自身的自同构

9.第八章课件 8
设 H 是群 G 的子群。在 G 中定义关系 R:aRb 如果 $b^{-1}a\in H$。证明：
⑴R 是等价关系
⑵aRb 的充要条件是 aH=bH