北京航空航天大學
BEIHANG UNIVERSITY

《网络空间安全数学基础》

习题作业参考解答

授 课 老 师：高莹

授 课 学 院：网络空间安全学院

编　　辑：陈晓峰

2020 年 12 月 01 日

目 录

第一次作业　密码学的信息论基础

题 1：考虑一个密码体制 $M=\{a,b,c\}$， $K=\{k_1,k_2,k_3\}$ 和 $C=\{1,2,3,4\}$。假设加密矩阵为

	a	b	c
k_1	2	3	4
k_2	3	4	1
k_3	1	2	3

已知密钥概率分布为：$p(k_1)=\frac{1}{2}$，$p(k_2)=p(k_3)=\frac{1}{4}$，且明文概率分布为 $p(a)=\frac{1}{3}$，$p(b)=\frac{8}{15}$， $p(c)=\frac{2}{15}$，计算 $H(M)$， $H(K)$， $H(C)$， $H(M\mid C)$，$H(K\mid C)$。

解：由加密矩阵得出密文分布如下

$$P(1)=\frac{1}{3}\times\frac{1}{4}+\frac{2}{15}\times\frac{1}{4}=\frac{7}{60} \qquad P(2)=\frac{1}{3}\times\frac{1}{2}+\frac{8}{15}\times\frac{1}{4}=\frac{3}{10}$$

$$P(3)=\frac{1}{3}\times\frac{1}{4}+\frac{8}{15}\times\frac{1}{2}+\frac{2}{15}\times\frac{1}{4}=\frac{23}{60} \qquad P(4)=\frac{8}{15}\times\frac{1}{4}+\frac{2}{15}\times\frac{1}{2}=\frac{1}{5}$$

根据熵的定义

$$H(M)=H(a)+H(b)+H(c)=-P(a)\log_2 P(a)-P(b)\log_2 P(b)-P(c)\log_2 P(c)$$

$$=-\frac{1}{3}\log_2\frac{1}{3}-\frac{8}{15}\log_2\frac{8}{15}-\frac{2}{15}\log_2\frac{2}{15}$$

$$\approx 1.40\ bit/\text{符号}$$

$$H(K)=H(k_1)+H(k_2)+H(k_3)$$

$$=-P(k_1)\log_2 P(k_1)-P(k_2)\log_2 P(k_2)-P(k_3)\log_2 P(k_3)$$

$$=-\frac{1}{2}\log_2\frac{1}{2}-\frac{1}{4}\log_2\frac{1}{4}-\frac{1}{4}\log_2\frac{1}{4}$$

$$=1.50\ bit/\text{符号}$$

$$H(C)=H(1)+H(2)+H(3)+H(4)$$

$$=-P(1)\log_2 P(1)-P(2)\log_2 P(2)-P(3)\log_2 P(3)-P(4)\log_2 P(4)$$

$$=-\frac{7}{60}\log_2\frac{7}{60}-\frac{3}{10}\log_2\frac{3}{10}-\frac{23}{60}\log_2\frac{23}{60}-\frac{1}{5}\log_2\frac{1}{5}$$

$$\approx 1.88\ bit/\text{符号}$$

根据 *Bayes* 定理计算给定密文后，明文空间上的条件概率分布

$$P(a|1)=\frac{P(a)P(k_3)}{P(1)}=\frac{5}{7} \qquad P(c|1)=\frac{P(c)P(k_2)}{P(1)}=\frac{2}{7}$$

$$P(a|2)=\frac{P(a)P(k_2)}{P(2)}=\frac{5}{9} \qquad P(b|2)=\frac{P(b)P(k_3)}{P(2)}=\frac{4}{9}$$

$$P(a|3)=\frac{P(a)P(k_2)}{P(3)}=\frac{5}{23} \qquad P(b|3)=\frac{P(b)P(k_1)}{P(3)}=\frac{16}{23}$$

$$P(c|3)=\frac{P(c)P(k_3)}{P(3)}=\frac{2}{23} \qquad P(b|4)=\frac{P(b)P(k_2)}{P(4)}=\frac{2}{3}$$

$$P(c|4)=\frac{P(c)P(k_1)}{P(4)}=\frac{1}{3}$$

$$\begin{aligned}H(M|C)=&-P(a,1)\log_2 P(a|1)-P(a,2)\log_2 P(a|2)-P(a,3)\log_2 P(a|3)\\&-P(b,2)\log_2 P(b|2)-P(b,3)\log_2 P(b|3)-P(b,4)\log_2 P(b|4)\\&-P(c,1)\log_2 P(c|1)-P(c,3)\log_2 P(c|3)-P(c,4)\log_2 P(c|4)\\\approx&1.02\ bit/\text{符号}\end{aligned}$$

$$H(K|C)=H(K)+H(M)-H(C)=1.4+1.5-1.88\approx 1.02\ bit/\text{符号}$$

题 2：考虑一个密码系统$\{P,K,C\}$。

a. 说明为什么$H(P,K)=H(C,P,K)=H(P)+H(K)$。

b. 假设这个系统具有完全保密。证明$H(C,P)=H(C)+H(P)$和$H(C)=H(K)-H(K|C,P)$。

c. 假设这个系统有完全保密，并且对每个明文密文对，最多只有一个相应的密钥能够加密。证明$H(C)=H(K)$。

解：a 证：由于$H(C,P,K)=H(P,K)+H(C|P,K)$，且密钥和明文唯一确定密文，所以$H(C|P,K)=0$，即有$H(C,P,K)=H(P,K)$。又由于明文和密钥相互独立，所以有$H(P,K)=H(P)+H(K)$。综上，有$H(P,K)=H(C,P,K)=H(P)+H(K)$。

b 证：由于该系统具有完全保密性，则有$\forall x\in P,\forall y\in C$都有$P(x|y)=P(x)$.

所以有$H(C,P)=H(C)+H(P|C)$

$$\begin{aligned}&=H(C)-\sum_{y\in C}\sum_{x\in P}P(x,y)\log_2 P(x|y)\\&=H(C)-\sum_{y\in C}\sum_{x\in P}P(x)P(y)\log_2 P(x)\\&=H(C)-\sum_{x\in P}P(x)\log_2 P(x)\\&=H(C)+H(P)\end{aligned}$$

根据 a 得证$H(P,K)=H(C,P,K)=H(P)+H(K)$，有$H(C,P,K)=H(C,P)+H(K|C,P)=H(P)+H(K)$，且明文和密文相互独立有$H(C,P)=H(C)+H(P)$，

即 $H(C)+H(P)+H(K|C,P)=H(P)+H(K)$。

∴综上，即 $H(C)=H(K)-H(K|C,P)$，得证。

c 证：由(b)可知，对于完全保密的密码系统有 $H(C)=H(K)-H(K|C,P)$

∵ 对于 $\forall x\in P,\forall y\in C$，最多有一个相应的密钥 $k\in K$ 能够加密

已知 x,y 可以唯一确定密钥 k，即 $H(K|C,P)=0$

$\therefore H(C)=H(K)$

题 3：假设在“一次一密”密码体制中，密文 y 和 y'（两个二进制的 n 元数组）是使用同一个密钥 K，分别加密明文 x 和 x' 得到的。证明 $x+x'=y+y' \bmod 2$。

解：由一次一密体制可知

$y\equiv x+k=\bmod 2$ …… ①

$y'\equiv x'+k=\bmod 2$ …… ②

则①+②得 $y+y'\equiv(x+x'+2k)\bmod 2$，即 $x+x'=y+y' \bmod 2$，得证。

第二次作业　代数学基础(1)

题 1：假设S_1是移位密码(密钥等概率)，S_2是密钥满足概率分布P_k(不必是等概率的)的移位密码。证明$S_1 * S_2 = S_1$。

解：记S_1, S_2的密钥空间分别为K_1, K_2，$S_1 * S_2$的密钥空间为K，其加密规则为

$$e_{(K_1,K_2)}(x) = (x + K_1 + K_2) \bmod 26$$

$\therefore S_1 * S_2$也是移位密码，且有$K = (K_1 + K_2) \bmod 26$

$\because S_1$的密钥等概率分布，则有$P(K_1 = k_{1i}) = \dfrac{1}{26}$和$\sum_{i=0}^{25} P(K_2 = k_{2i}) = 1$

$\because S_1 * S_2$的密钥概率分布为

$$P(K) = \sum_{i=0}^{25}\sum_{j=0}^{25} P(K_1 = k_{1i})P(K_2 = k_{2i}) = \frac{1}{26}\sum_{i=0}^{25} P(K_2 = k_{2i}) = \frac{1}{26}$$

故$S_1 * S_2$的密钥也是等概率分布的，即$S_1 * S_2 = S_1$，得证。

题 2： Suppose that $g^a \equiv 1 (\bmod m)$ and that $g^b \equiv 1 (\bmod m)$. Prove that $g^{\gcd(a,b)} \equiv 1 (\bmod m)$.

解：对于任意两个正整数a, b，存在整数x, y，使得$\gcd(a,b) = xa + yb$

则 $g^{\gcd(a,b)} = g^{ax+yb} = g^{xa} \cdot g^{yb} = (g^a)^x \cdot (g^b)^y$

$\because g^a \equiv 1 (\bmod m), g^b \equiv 1 (\bmod m)$

$\therefore (g^a)^x \cdot (g^b)^y \equiv 1 (\bmod m)$

$\therefore g^{\gcd(a,b)} \equiv 1 (\bmod m)$.

题 3：编程实现多项式的扩展欧几里得算法，语言不限。要求完整的实验报告。

解：掌握多项式的扩展欧几里得基本运算即可，代码略。

第三次作业　代数学基础(2)

题 1：设 $F[x]$ 中的多项式 $f(x),g(x)$ 互素，求证存在唯一一组 $u(x),v(x)$ 使得 $u(x)f(x)+v(x)g(x)=1$ 且 $\deg u(x)<\deg g(x),\deg v(x)<\deg f(x)$。

解：（**存在性**）由题可知多项式 $f(x),g(x)$ 互素，则有 $(f(x),g(x))=1$

$\therefore \exists h(x),k(x)$ 使得 $f(x)h(x)+g(x)k(x)=1\cdots$ ①

设 $\deg h(x)<\deg g(x)$，则 $\exists q(x),u(x)$ 使得 $h(x)=g(x)q(x)+u(x)\cdots$ ②

且 $\deg u(x)<\deg g(x)$，并将②代入①中有

$$f(x)(g(x)q(x)+u(x))+g(x)k(x)=1.$$

$\therefore$ 即有 $f(x)u(x)+g(x)(f(x)q(x)+k(x))=1$

令 $v(x)=f(x)q(x)+k(x)$，若 $\deg v(x)>\deg f(x)$

则有 $\deg(f(x)u(x)+g(x)v(x))\geq\deg(f(x)u(x)+g(x)f(x))\geq 2\neq\deg(1)$

$\therefore$与前面矛盾，即存在 $\deg u(x)<\deg g(x),\deg v(x)<\deg f(x)$，得证。

(唯一性)假设另有 $u_1(x),v_1(x)$ 满足条件，即

$$f(x)u_1(x)+g(x)v_1(x)=f(x)u(x)+g(x)v(x)=1$$

$\therefore$ 有 $f(x)(u(x)-u_1(x))=g(x)(v_1(x)-v(x))$

又$\because f(x),g(x)$ 互素，故有 $\begin{cases}u(x)-u_1(x)=g(x)\text{或}0\\ v_1(x)-v(x)=f(x)\text{或}0\end{cases}$，且 $g(x)\mid(u(x)-u_1(x))$

即有 $\deg(u(x)-u_1(x))<\deg g(x)$，只能 $u(x)-u_1(x)=0$

$\therefore$ 综上所述，$u(x)=u_1(x)$，同理可证 $v(x)=v_1(x)$，得证。

题 2：构造一个 2^8 元有限域，并说明理由。

解：设 F_{2^8} 上有多项式 $f(x)=x^8+x^4+x^3+x+1$，需对次数 ≤ 4 的不可约多项式 $p(x)$ 作整除 $p(x)\mid f(x)$，判断其是否成立。

① 一次不可约多项式：$x,x+1$

$f(x)=(x^7+x^3+x^2+1)\cdot x+1$

$f(x)=(x^7+x^6+x^5+x^4+x^2+x)\cdot(x+1)+1$

② 二次不可约多项式：x^2+x+1

先证明二次不可约多项式不可约，$x^2+x+1=(x+1)\cdot x+1$

$f(x)=(x^6+x^5+x^3)\cdot(x^2+x+1)+(x+1)$

③ 三次不可约多项式：x^3+x+1,x^3+x^2+1

先证明三次不可约多项式不可约

$x^3+x+1=(x^2+1)\cdot x+1$　　$x^3+x^2+1=(x^2+x)\cdot x+1$

$x^3+x+1=(x^2+x)\cdot(x+1)+1$　　$x^3+x^2+1=x^2\cdot(x+1)+1$

$x^3+x+1=(x+1)\cdot(x^2+x+1)+x$　　$x^3+x^2+1=x\cdot(x^2+x+1)+x+1$

$f(x)=(x^5+x^3+x^2+1)\cdot(x^3+x+1)+x^2$

$f(x)=(x^5+x^4+x^3)\cdot(x^3+x^2+1)+x+1$

④ 同理对四次不可约多项式：x^4+x+1, x^4+x^3+1，$x^4+x^3+x^2+x+1$

$x^4+x+1=(x^3+1)\cdot x+1$　　$x^4+x^3+1=(x^3+x^2)\cdot x+1$

$x^4+x+1=(x^3+x^2+x)\cdot(x+1)+1$　　$x^4+x^3+1=x^3\cdot(x+1)+1$

$x^4+x+1=(x^2+x)\cdot(x^2+x+1)+1$　　$x^4+x^3+1=(x^2+1)\cdot(x^2+x+1)+x$

$x^4+x^3+x^2+x+1=(x^3+x^2+x+1)\cdot x+1$

$x^4+x^3+x^2+x+1=(x^3+x)\cdot(x+1)+1$

$x^4+x^3+x^2+x+1=x^2\cdot(x^2+x+1)+x+1$

$f(x)=(x^4+x)\cdot(x^4+x+1)+(x^3+x^2+1)$

$f(x)=(x^4+x^3+x^2+x+1)\cdot(x^4+x^3+1)+(x^3+x^2)$

$f(x)=(x^4+x^3+1)\cdot(x^4+x^3+x^2+x+1)+(x^3+x^2)$

$\therefore f(x)=x^8+x^4+x^3+x+1$是不可约多项式，$GF(2^8)=\mathbb{Z}_2[x]/f(x)$ 为构造的有限域。

第四次作业　椭圆曲线

题 1：椭圆曲线 $E: y^2 = x^2 + 2x + 7$ 定义在 $\mathbb{Z}_{31}$ 上。

(1) 计算椭圆曲线的点数.

(2) $P = (2,9)$ 是 E 中阶为 39 的点.

(3) 计算 $Q = 8P$.

(4) 确定 17 的 NAF 表示并利用快速算法计算 $17P$.

解：(1) 当 $x = 0,1,2,...,30$ 时，分别计算 y，遍历所有可能的情况并计算点数。得出下表：

x	$y^2 = x^2 + 2x + 7 (\mathrm{mod}\, 31)$	y		x	$y^2 = x^2 + 2x + 7 (\mathrm{mod}\, 31)$	y
0	7	10,21		16	12	无解
1	10	14,17		17	25	5,26
2	19	9,22		18	16	4,27
3	9	3,28		19	22	无解
4	17	无解		20	18	7,24
5	18	7,24		21	10	14,17
6	18	7,24		22	4	2,29
7	23	无解		23	6	无解
8	8	15,16		24	22	无解
9	10	14,17		25	27	无解
10	4	2,29		26	27	无解
11	27	无解		27	28	11,20
12	23	无解		28	5	6,25
13	29	无解		29	26	无解
14	20	12,19		30	4	2,29
15	2	8,23				

综上，椭圆曲线 $E: y^2 = x^2 + 2x + 7$ 在 $\mathbb{Z}_{31}$ 上，包括无穷远点，共有 39 个点。

附 1：计算椭圆曲线的点数 python 参考代码（个人巩固练习，仅供参考）

(2) 要证 $P = (2,9)$ 的阶是39，即证 $39P = 0$，其中0为无穷远点，用倍点快速计算如下表所示。由于 $39 = 2^5 + 2^2 + 2^1 + 2^0$，则 $39P = 2^5P + 2^2P + 2^1P + 2^0P$，如下表蓝色标注。

Step i	*n*	$Q=2^iR$	*R*
0	39	**(2,9)**	0
1	19	**(10,2)**	(2,9)
2	9	**(15,8)**	(28,6)
3	4	**(8,15)**	(6,24)
4	2	(17,26)	(6,24)
5	1	**(6,7)**	(6,24)
6	0	(20,7)	0

即 $39P=(2,9)+(10,2)+(15,8)+(6,7)=0$，故 P 的阶为 39。

(3) 方法 1：由加法规则，直接计算。

$2P=P+P=(2,9)+(2,9)$，计算 $\lambda=\frac{(3x^2+A)}{2y}=\frac{7}{9}(\mathrm{mod}\,31)=18$，则 $x'=x^2-2x$ $=320(\mathrm{mod}\,31)=10, y'=\lambda(x-x')-y=-153(\mathrm{mod}\,31)=2$，则 $2P=(10,2)$。同理 $4P=2P+2P, 8P=4P+4P$，最终得 $8P=(8,15)$。

方法 2：也可由(2)可知 $2^3P=(8,15)$，如上表红色标注。

(4) 确定 17 的 NAF 表示，并利用快速算法计算 $17P$。

$17=2^4+2^0$，则 NAF 表示为 $(1,0,0,0,1)_2$

所以由(3)中表可知 $17P=2^4P+2^0P=(17,26)+(2,9)=(21,17)$

附 2：椭圆曲线中的点加运算 python 参考代码（个人巩固练习，仅供参考）

题 2：令 L_i 代表 NAF 表示中恰好有 i 个系数，并且首系数为 1 的所有正整数的集合。记 $k_i=|L_i|$

(1) 通过对 L_i 进行适当的分解，证明 k_i 满足下列递推关系

$$k_1=1$$

$$k_2=1$$

$$k_{i+1}=2(k_1+k_2+\ldots+k_{i-1})+1\ (i\geq 2)$$

(2) 导出 k_i 的一个二阶递归关系，算出递归关系的一个显式解。

解：(1) NAF 表示的定义为，对于正整数 $k,(k_{n-1},\ldots,k_0)$ 为一种 BSD 表示，其中没有两个连续的 k_i 是非零的，则称它是非相邻形式的表示，即 ±1 的前后只能是 0。

① 当 $i=1$ 时，L_1 中仅有一个系数为 1，即 $k_1=|L_1|=1$

② 当 $i=2$ 时，L_2 中有两个系数，首系数为 1，由于 NAF 性质，则第二个系数必为 0，即为 10，$k_2=|L_2|=1$

③ 当$i=3$时，L_3中有三个系数，前两个为10，第三位可能为1、0、-1三种情况，即$k_3=|L_3|=2k_1+1=3$

④ 当$i=4$时，L_4中有四个系数，前两个系数为10，第三位可能为1、0、-1三种情况；当第三个系数为0时，第四个系数的可能值为$k_3=2k_2+1=3$；当第三个系数为±1时，第四个系数的可能值均为k_2。综上，$k_4=|L_4|=2(k_1+k_2)+1=5$

⑤ 以此类推，假设当$i=m$时，使得$k_m=|L_m|=2(k_1+k_2+...+k_{m-2})+1$等式成立。则当$i=m+1$时，前两个系数为10，当第三位为0时，此时后面的可能值为k_m；当第三位为±1时，此时后面的可能值均为k_{m-1}。综上，$k_{m+1}=|L_{m+1}|=2k_{m-1}+k_m$，将$k_m$代入可使得$k_{m+1}=2(k_1+k_2+...+k_{m-1})+1$成立。

(2) 由上述递归式可知

$$k_{i+1}=2(k_1+k_2+...+k_{i-1})+1 \quad \cdots\cdots ①$$

$$k_i=2(k_1+k_2+...+k_{i-2})+1 \quad \cdots\cdots ②$$

令①$-$②得$k_{i+1}=k_i+2k_{i-1}$，即为所求的二阶递推关系式

$\therefore$ 得$k_{i+1}+k_i=2(k_i+k_{i-1})=2^{i-1}(k_2+k_1)$，又$k_1=k_2=1$，故$k_{i+1}+k_i=2^i, i\geq 2$。

假设C使得$k_{i+1}+C2^{i+1}=-(k_i+C2^i)$，解得$C=-\frac{1}{3}$

即$k_{i+1}-\frac{1}{3}2^{i+1}=-(k_i-\frac{1}{3}2^i)=(-1)^i(k_1-\frac{2}{3})$，化简得显式解为

$$k_{i+1}=\frac{1}{3}((-1)^i+2^{i+1}),\ i\geq 2$$

第五次作业　格(1)

题 1： Let L be the lattice given by the basis

$$B=\{(3,1,-2),(1,-3,5),(4,2,1)\}$$

Which of the following sets of vectors are also bases for L? For those that are, express the new basis in terms of the basis B, i.e., find the change of basis matrix.

a) $B_1=\{(5,13,-13),(0,-4,2),(-7,-13,18)\}$.

b) $B_2=\{(4,-2,3),(6,6,-6),(-2,-4,7)\}$.

解： 用 B 作为行向量构造矩阵 $A=\begin{bmatrix}3 & 1 & -2\\ 1 & -3 & 5\\ 4 & 2 & 1\end{bmatrix}$，计算 $A^{-1}=\begin{bmatrix}\frac{13}{48} & \frac{5}{48} & \frac{1}{48}\\ \frac{-19}{48} & \frac{-11}{48} & \frac{17}{48}\\ \frac{-7}{24} & \frac{1}{24} & \frac{5}{24}\end{bmatrix}$

并构造矩阵 $B_1=\begin{bmatrix}5 & 13 & -13\\ 0 & -4 & 2\\ -7 & -13 & 18\end{bmatrix}$ 和 $B_2=\begin{bmatrix}4 & -2 & 3\\ 6 & 6 & -6\\ -2 & -4 & 7\end{bmatrix}$

a) 假设存在过渡矩阵 U_1 使得 B_1 为 L 的一个基，则有 $B_1=U_1A$，即

$$U_1=B_1A^{-1}=\begin{bmatrix}5 & 13 & -13\\ 0 & -4 & 2\\ -7 & -13 & 18\end{bmatrix}\begin{bmatrix}\frac{13}{48} & \frac{5}{48} & \frac{1}{48}\\ \frac{-19}{48} & \frac{-11}{48} & \frac{17}{48}\\ \frac{-7}{24} & \frac{1}{24} & \frac{5}{24}\end{bmatrix}=\begin{bmatrix}0 & -3 & 2\\ 1 & 1 & -1\\ -2 & 3 & -1\end{bmatrix}$$

则 U_1 的行列式为 $\det(U_1)=\begin{vmatrix}0 & -3 & 2\\ 1 & 1 & -1\\ -2 & 3 & -1\end{vmatrix}=1$

$\therefore B_1$ 是格 L 的基

b) 假设存在过渡矩阵 U_2 使得 B_2 为 L 的一个基，则有 $B_2=U_2A$，即

$$U_2=B_2A^{-1}=\begin{bmatrix}4 & -2 & 3\\ 6 & 6 & -6\\ -2 & -4 & 7\end{bmatrix}\begin{bmatrix}\frac{13}{48} & \frac{5}{48} & \frac{1}{48}\\ \frac{-19}{48} & \frac{-11}{48} & \frac{17}{48}\\ \frac{-7}{24} & \frac{1}{24} & \frac{5}{24}\end{bmatrix}=\begin{bmatrix}1 & 1 & 0\\ 1 & -1 & 1\\ -1 & 1 & 0\end{bmatrix}$$

则U_2的行列式为$\det(U_2)=\begin{vmatrix}1 & 1 & 0\\ 1 & -1 & 1\\ -1 & 1 & 0\end{vmatrix}=-2$

∴ B_2不是格L的基

题 2： Let $L\subset\mathbb{R}^m$ be a lattice of dimension n and let $v_1,v_2,...,v_n$ be a basis for L. Note that we are allowing n to be smaller than m. The *Gram matrix of* $v_1,v_2,...,v_n$ is the matrix.

$$Gram\ (v_1,v_2,...,v_n)=(v_i\cdot v_j)_{1\le i,j\le n}$$

a) Let $F(v_1,v_2,...,v_n)$ be the matrix (7.11) described in Proposition (7.20), except that now $F(v_1,v_2,...,v_n)$ is an n-by-m matrix, so it need not be square. Prove that

$$Gram(v_1,v_2,...,v_n)=F(v_1,v_2,...,v_n)F(v_1,v_2,...,v_n)^t$$

Where $F(v_1,v_2,...,v_n)^t$ is the transpose matrix, i.e., the matrix with rows and columns interchanged.

b) Prove that

$$\det(Gram\ (v_1,v_2,...,v_n))=\det(L)^2$$

Where note that $\det(L)$ is the volume of the parallelepiped spanned by any basis for L. (You may find it easier to first do the case $n=m$.)

c) Let $L\subset\mathbb{R}^4$ be the 3-dimensional lattice with basis

$$v_1=(1,0,1,-1),v_2=(1,2,0,4),v_3=(1,-1,2,1)$$

Compute the Gram matrix of this basis and use it to compute $\det(L)$.

d) Let $v_1^*,v_2^*,...,v_n^*$ be the Gram-Schmidt orthogonalized vectors (Theorem 7.13) associated to $v_1,v_2,...,v_n$ Prove that

$$\det(Gram\ (v_1,v_2,...,v_n))=\|v_1^*\|^2\|v_2^*\|^2...\|v_n^*\|^2$$

解：(a) 假设$v_1=(r_{11},r_{12},...,r_{1m})^T,v_2=(r_{21},r_{22},...,r_{2m})^T,...,v_n=(r_{n1},r_{n2},...,r_{nm})^T$

以$v_1,v_2,...,v_n$作为行向量，则$F(v_1,v_2,...,v_n)=\begin{bmatrix}r_{11} & r_{12} & ... & r_{1m}\\ r_{21} & r_{22} & ... & r_{2m}\\ \vdots & \vdots & \ddots & \vdots\\ r_{n1} & r_{n2} & ... & r_{nm}\end{bmatrix}$

∴ $F(v_1,v_2,...,v_n)F(v_1,v_2,...,v_n)^t=\begin{bmatrix}r_{11} & r_{12} & ... & r_{1m}\\ r_{21} & r_{22} & ... & r_{2m}\\ \vdots & \vdots & \ddots & \vdots\\ r_{n1} & r_{n2} & ... & r_{nm}\end{bmatrix}\begin{bmatrix}r_{11} & r_{21} & ... & r_{n1}\\ r_{12} & r_{22} & ... & r_{n2}\\ \vdots & \vdots & \ddots & \vdots\\ r_{1m} & r_{2m} & ... & r_{nm}\end{bmatrix}$

$$= \begin{bmatrix} \sum_{i=1}^{m} r_{1i}^{\ 2} & \sum_{i=1}^{m} r_{1i}r_{2i} & \cdots & \sum_{i=1}^{m} r_{1i}r_{ni} \\ \sum_{i=1}^{m} r_{2i}r_{1i} & \sum_{i=1}^{m} r_{2i}^{\ 2} & \cdots & \sum_{i=1}^{m} r_{2i}r_{ni} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^{m} r_{ni}r_{1i} & \sum_{i=1}^{m} r_{ni}r_{2i} & \cdots & \sum_{i=1}^{m} r_{ni}^{\ 2} \end{bmatrix}$$

$$= (v_i \cdot v_j)_{1\le i,j\le n} = Gram\ (v_1, v_2, ..., v_n)$$

(b) 由定义可知 $\det(L)^2 = \det(VV^T)$

∵ 根据(a)证出 $Gram\ (v_1, v_2, ..., v_n) = F(v_1, v_2, ..., v_n)F(v_1, v_2, ..., v_n)^t$

∴ $\det(Gram\ (v_1, v_2, ..., v_n)) = \det(F(v_1, v_2, ..., v_n)F(v_1, v_2, ..., v_n)^t)$

$$= \det(v_i \cdot v_j)_{1\le i,j\le n}$$

$$= \det(VV^T)$$

∴ $\det(Gram\ (v_1, v_2, ..., v_n)) = \det(L)^2$

(c) $F(v_1, v_2, v_3) = \begin{bmatrix} 1 & 0 & 1 & -1 \\ 1 & 2 & 0 & 4 \\ 1 & -1 & 2 & 1 \end{bmatrix}$，则 $F(v_1, v_2, v_3)^t = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \\ 1 & 0 & 2 \\ -1 & 4 & 1 \end{bmatrix}$

∴ $Gram\ (v_1, v_2, v_3) = F(v_1, v_2, v_3)F(v_1, v_2, v_3)^t$

$$= \begin{bmatrix} 1 & 0 & 1 & -1 \\ 1 & 2 & 0 & 4 \\ 1 & -1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \\ 1 & 0 & 2 \\ -1 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -3 & 2 \\ -3 & 21 & 3 \\ 2 & 3 & 7 \end{bmatrix}$$

∴ $\det(L) = \sqrt{\det(Gram\ (v_1, v_2, v_3))} = \sqrt{231}$

(d) $v_1^*, v_2^*, ..., v_n^*$ 是由 $v_1, v_2, ..., v_n$ 经过 $Gram-Schmidt$ 正交化得到

∴ $v_1^*, v_2^*, ..., v_n^*$ 是 L 的一组基

∴ $\det(Gram\ (v_1, v_2, ..., v_n)) = \det(L)^2$

$$= \det(F(v_1^*, v_2^*, ..., v_n^*)F(v_1^*, v_2^*, ..., v_n^*)^t)$$

$$= \det(Gram\ (v_1^*, v_2^*, ..., v_n^*))$$

$$= \det(v_i^* \cdot v_j^*)_{1\le i,j\le n}$$

∵ 当 $i \ne j$ 时，$v_i^* \cdot v_j^* = 0$

∴ $\det(Gram\ (v_1, v_2, ..., v_n)) = \det(diag(v_1^{*2}, v_2^{*2}, ..., v_n^{*2}))$

$$= \| v_1^* \|^2 \| v_2^* \|^2 ... \| v_n^* \|^2$$

第六次作业　格(2)

题1：利用 LLL 算法对三维格的一组基底 $v_1=\{20,16,3\}, v_2=\{15,0,10\}, v_3=\{0,18,9\}$ 实施约化，得到 LLL 约化基。

解：① $v_1=(20,16,3), v_2=(15,0,10), v_3=(0,18,9)$

令 $v_1^*=v_1$，$|u_{21}|=\dfrac{|v_2v_1^*|}{\|v_1^*\|^2}=\dfrac{330}{665}\approx 0.496<\dfrac{1}{2}$，满足尺度约化，无需约减

判断 $\|v_2^*\|^2\geq(\dfrac{3}{4}-u_{21}{}^2)\|v_1^*\|^2$ (或 $\|v_2\|^2\geq\dfrac{3}{4}\|v_1\|^2$)是否成立

又∵ $\|v_2\|^2=325<\dfrac{3}{4}\|v_1\|^2$，不满足 *Lov'asz* 条件，需要交换 v_1 和 v_2

② $v_1=(15,0,10), v_2=(20,16,3), v_3=(0,18,9)$

令 $v_1^*=v_1$，$|u_{21}|=\dfrac{|v_2v_1^*|}{\|v_1^*\|^2}=\dfrac{330}{325}\approx 1.015>\dfrac{1}{2}$，不满足尺度约化，则需约减

∴ $v_2=v_2-\lceil u_{21}\rfloor v_1=(20,16,3)-(15,0,10)=(5,16,-7)$

（**注：**⌈ ⌋是四舍五入取整符号）

∴ $|u_{21}|=\dfrac{|v_2v_1^*|}{\|v_1^*\|^2}=\dfrac{5}{325}\approx 0.015<\dfrac{1}{2}$, 满足尺度约化，无需约减

又∵ $\|v_2\|^2=330>\dfrac{3}{4}\|v_1\|^2$, 满足 *Lov'asz* 条件

③ $v_1=(15,0,10), v_2=(5,16,-7), v_3=(0,18,9)$

令 $v_1^*=v_1$，则 $v_2^*=v_2-u_{21}v_1^*=(5,16,-7)-\dfrac{5}{325}(15,0,10)=(\dfrac{62}{13},16,-\dfrac{93}{13})$

∵ $|u_{31}|=\dfrac{|v_3v_1^*|}{\|v_1^*\|^2}=\dfrac{18}{65}<\dfrac{1}{2}$，$|u_{32}|=\dfrac{|v_3v_2^*|}{\|v_2^*\|^2}\approx\dfrac{223.7}{329.9}>\dfrac{1}{2}$

∴ 不满足尺度约化，则需约减

∴ $v_3=v_3-\lceil u_{32}\rfloor v_2-\lceil u_{31}\rfloor v_1=(0,18,9)-(5,16,-7)=(-5,2,16)$

④ $v_1=(15,0,10), v_2=(5,16,-7), v_3=(-5,2,16)$

∴ $|u_{31}|=\dfrac{|v_3v_1^*|}{\|v_1^*\|^2}=\dfrac{17}{65}<\dfrac{1}{2}$，$|u_{32}|=\dfrac{|v_3v_2^*|}{\|v_2^*\|^2}\approx\dfrac{|-106.3|}{329.9}<\dfrac{1}{2}$

∴满足尺度约化，无需约减

∵ $v_3^*=v_3-u_{32}v_2^*-u_{31}v_1^*\Rightarrow v_3^*+u_{32}v_2^*=v_3-u_{31}v_1^*$

∴ $\|v_3^*+u_{32}v_2^*\|^2=\|v_3-u_{31}v_1^*\|^2=\|(-5,2,16)-\dfrac{17}{65}(15,0,10)\|^2\approx 262.72$

且 $\frac{3}{4}\|v_2^*\|^2=\frac{3}{4}\|(\frac{62}{13},16,-\frac{93}{13})\|^2\approx 247.43$，所以 $\|v_3^*+u_{32}v_2^*\|^2>\frac{3}{4}\|v_2^*\|^2$

即 $\|v_3^*\|^2>(\frac{3}{4}-u_{32}{}^2)\|v_2^*\|^2$，满足 *Lov'asz* 条件

∴ 综上，$v_1=(15,0,10),v_2=(5,16,-7),v_3=(-5,2,16)$

附 3：LLL 算法例题 Python 参考代码（个人巩固练习，仅供参考）

参 考 文 献

[1] Stinson D , 斯廷森, 冯登国. 密码学原理与实践[M]. 电子工业出版社, 2009.

[2] Hoffstein J , Pipher J C , Silverman J H . An Introduction to Mathematical Cryptography (Google eBook) [M]// An Introduction to Mathematical Cryptography. Springer Publishing Company, Incorporated, 2008.

[3] 以及参考了班上几位同学的作业解答

附 录

1. 计算椭圆曲线点数 python 参考代码

```
x = 0
y = 0
while x<31:
    c = ((x*x*x)+2*x+7)%31
    while y<30:
        if((y*y)%31)==c:
            print('当 x =',x,'时， x^3+2x+7(mod31)= ',c,'， y =',y)
        y=y+1
    y=0
    x = x + 1
```

2. 椭圆曲线中的点加运算 python 参考代码

```
y=0
x=0
x1=17
y1=26
x2=2
y2=9
F=31
while y<F: #求 P+P
    if ((2*y1)*y)%F == 1:
        z =(y*(3*x1*x1+2))%F
        A = (z*z-2*x1)%F
        B = (z*(x1-A)-y1)%F
        print('P+P = ',A,B)
    y=y+1
while x<F: #求 P+Q
    if ((x2-x1)*x)%F == 1:
        z =(x*(y2-y1))%F
        C = (z*z-x1-x2)%F
        D = (z*(x1-C)-y1)%F
        print('P+Q = ',C,D)
    x=x+1
```

3. LLL 算法例子 python 参考代码

```
k = 2
v1 = [20,16,3]
```

```
v2 = [15,0,10]
v3 = [0,18,9]
v2_star = list(v2)
def Change(x,y):
    e = list(x)
    x = list(y)
    y = e
    return x,y
while k<3:
    a = 0
    b = 0
    c = 0
    sum_v1 = 0
    sum_v2 = 0
    sum_v3 = 0
    sum_v2_star = 0
    sum_v3_star = 0
    for i in range(3):
        a = a + v2[i] * v1[i]
        sum_v1 = sum_v1 + v1[i] * v1[i]
    u21 = a / sum_v1
    print('u21 =',u21)
    if (abs(u21) <= 0.5):   # 判断是否满足尺度约化
        for i in range(3):
            v2_star[i] = v2[i] - u21 * v1[i]
            sum_v2_star = sum_v2_star + v2_star[i] * v2_star[i]
        if (sum_v2_star >=(0.75-u21*u21)* sum_v1):# 判断是否满足 Lovasz 条件
            for i in range(3):
                b = b + v3[i] * v1[i]
                c = c + v3[i] * v2_star[i]
            u31 = b / sum_v1
            u32 = c / sum_v2_star
            print('u31 =', u31)
            print('u32 =', u32)
            if (abs(u31) <= 0.5 and abs(u32) <= 0.5):
                for i in range(3):
                    sum_v3 = sum_v3 + (v3[i] - u31*v1[i]) * (v3[i] - u31*v1[i])
                if (sum_v3 >= 0.75 * sum_v2_star):
                    k = k + 1
                    print('v1=', v1)
                    print('v2=', v2)
                    print('v3=', v3)
                else:
                    (v2,v3) =Change(v2,v3)
```

```
            else:
                for i in range(3):
                    v3[i] = v3[i] - int(u32 + 0.5) * v2[i]-int(u31 + 0.5) * v1[i]
        else:
            (v1,v2) = Change(v1,v2)
    else:
        for i in range(3):
            v2[i] = v2[i] - int(u21 + 0.5) * v1[i]
```