宿題

以下の暗号数理に関する5題から、3題を選択して答えよ。
参考にした文献等は必ず明記すること。

(1) フェルマーの小定理および中国人剰余定理に関して調べ、異なる素数p,qに対して、
gcd(m,pq)=1となる整数は、$m^{(p-1)(q-1)} = 1 \bmod pq$ を満たすことを証明せよ。

(2) 高速な素因数分解アルゴリズムである数体篩法に関して調べよ。

(3) Shorの量子計算機を用いた素因数分解法に関して調べよ。

(4)グレブナー基底を計算するBuchbergerアルゴリズムに関して調べよ。

(5)格子基底簡約を行なうLenstra-Lenstra-Lovászアルゴリズムに関して調べよ。