复习题中的作业

4. 16. 试给出椭圆曲线群*E*5(1,1)上的所有点。

解，分别以*x*=0，1，2，3，4带入到椭圆曲线*y*2=*x*3+*x*+1 mod 5 求解y得到如下点：

(0, ±1) , (2, ±1), (3, ±1), (4, ±2),

所以*E*5(1,1)={(0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,1), (4,4),*O* }

5.3． 对于RSA算法中两个大素数p，q，试分析如果2p与3q的差值很小，也能被快速分解

证明： 由于(2*p*+3*q*)2=4x2x3*n*+(2*p*-3*q*)2=24*n*+(2*p*-3*q*)2，对24n+*x*2从*x*=1开始搜索满足*y*2=24n+*x*2的*x*取值，如果找到则可通过计算gcd(24n, *x*+*y*)和gcd(24n, *x*-*y*)来分解n，当2p与3q的差值很小时，上述搜索将很快发现满足条件的*x*，所以2p与3q的差值很小时也能被快速分解