

(1) 1. 3

- (1) 1. $p = 15$ のとき ($15 = 1111_2$ より). 2乗算4回, 乗算4回
2. 160bit のとき, 半分の60bitに1を加えて,
2乗算160回, 乗算80回
3. 2.と同様にして,
2乗算160回, 乗算80回
4. 1024bit のとき, 半分の512bitに1を加えて,
2乗算1024回, 乗算512回

(2) 2. $80M_{160} + 160 \times 0.8 M_{160} = 208 M_{160}$

3. $80 \times 6^2 \times M_{160} + 160 \times 6^2 \times 0.8 \times M_{160} = 17488 M_{160}$

4. $512 \times 6^2 \times M_{160} + 1024 \times 6^2 \times 0.8 \times M_{160} = 47923.2 M_{160}$