```
[ 4 50m]
```

P=1; 5 13 17 29 37 41 53 61 73 89 97 101 109 113

p = 1 ; 1

P = 3 ; 3 7 11 19 23 31 A3 A7 59 14 71 79 83

[mod 5]

p = 0 ; 5

 $p \equiv 1$; 11 31 41 61 71 101 131 151 181 191

ρ = 3 , 3 13 23 43 53 73 83 103 113 163 173 193

p = 4 , 19 29 59 79 89 109 139 149 179 199

```
[ 4 50m]
                                     41
                                             61 73
                  13
                       17
                             29
                                          53
P = 1 ;
                                  37
                                                           97
                                                               101
                                                                    109 113
             134
                  149
                             173
                                 181
                                      193
                                          194
                        157
 P = 1 ,
                            19
                                                                     83
              3
                        11
                                 23
                                     31
                                          43
                                              47
                                                    59
                                                             41
                                                                 49
 D = 3
             103
                   107
                        124
                             131
                                 139
                                      151
                                          163
                                               167
                                                         191
                                                             199
                                                    179
                                                             P=1 (mod4)
                                                             P = 2 ( Mod 4 )
                                                            P = 3 (mod 4)
 [ Mod 5]
         ; 11 31 41 61 71 101 131 151 181 191
          1 17 37
                                  47 67
                                           97 107 119 139 157 119
```

, 3 13

29 59 79

53 75 85 103 113 163 173 193

89 109 139 149

เหมือหามกรณี

```
p=1 (mod 4) , 5 13 17 29 37 41 53 61 73 89 97
101 109 113 137 149 157 175 181 195 194
```