```
#Guanshi He
#ECE404 Hw03
#He_Field.py

import os
import math

n = raw_input('Please enter the number n: ')
flag = 0
root = math.sqrt(float(n))
#print "root = ", root
root = int(root)

fo = open("output.txt","wb")
if (n == 2):
	fo.writelines("field")
	print("field")
else:
	print int(root)
	for i in range(2,root + 1):

		if (int(n) % i) == 0:
			flag = 1
			break
	if flag == 1:
		print "ring"
		fo.writelines("ring")
	else:
		print "field"
		fo.writelines("field")
fo.close()


##############################################
# output
##############################################
# -bash-4.1$ python He_Field.py
# Please enter the number n: 8
# ring
# -bash-4.1$ more output.txt
# ring
# Please enter the number n: 7
# field
# -bash-4.1$ more output.txt
# field

##############################################
#Answers to the Theory Problems
# 1
```

```
# With respect to modulo addition does the set of remainders Z17 form a group.
#
# 2
# Euclid's Algorithm
#   gcd(1056,348)
# = gcd( 348, 12)
# = gcd(  12,  0)
# Therefore, gcd(1056,348) = 12
# Stein's Algorithm
#   gcd(1056,348)
# = gcd( 528,174)
# = gcd( 264, 87)
# = gcd( 132, 87)
# = gcd(  66, 87)
# = gcd(  33, 87)
# = gcd(  54, 33)
# = gcd(  27, 33)
# = gcd(   6, 27)
# = gcd(   3, 27)
# = gcd(  24,  3)
# = gcd(  12,  3)
# = gcd(   6,  3)
# = gcd(   3,  3)
# = gcd(   0,  3)
#  3*2*2 = 12
# Therefore,gcd(1056,348) = 12
#
# 3
# compute the multiplicative inverse of 21 in Z34
#   gcd(21,34)
# = gcd(34,21)|| 21 = 1*21 - 0*34
# = gcd(21,13)|| 13 = 1*34 - 1*21
# = gcd(13,8)  || 8 = 1*21 - 1*(1*34 - 1*21) = 2*21 - 1*34
# = gcd(8,5)    || 5 = 1*13 - 1*8 = (1*34 - 1*21) - (2*21 - 1*34) = 2*34 - 3*21
# = gcd(5,3)    || 3 = 1*8 - 1*5 = (2*21 - 1*34) - (2*34 - 3*21) = 5*21 - 3*34
# = gcd(3,2)    || 2 = 1*5 - 1*3 = (2*34 - 3*21) - (5*21 - 3*34) = 5*34 - 8*21
# = gcd(2,1)    || 1 = 1*3 - 1*2 = (5*21 - 3*34) - (5*34 - 8*21) = 13*21 - 8*34
# Therefore, the MI of 21 is 13 in Z34
#
# 4
# 2,4,6,8,10,12
# These elements do not possess multiplicative inverse since they are even number.
#
# 5
#    gcd(12,42) = 6
#  12 * -10 + 42 *  3 = 6
#  12 *  -3 + 42 *  1 = 6
#  12 *   4 + 42 * -1 = 6
#    gcd(2,3) = 1
```

```
#  3 * 1 - 2 * 1 = 1
#  3 * 3 - 2 * 4 = 1
#  3 * 5 - 2 * 7 = 1
#
# 6
# a. y = 12
# b. y = 3
# c. y = 4
```