

**PROBLEMS SET 9**  
**DUE TUESDAY, DECEMBER 8**

1.– Show that the characteristic of an integral domain is either a prime number or 0.

2.– Let  $p$  be an odd prime number. An element  $x$  in  $\mathbb{Z}_p^*$  is called a *square* if there exists an element  $y$  in  $\mathbb{Z}_p^*$  such that  $x = y^2$ .

a.– Write down a complete list of squares for  $p = 3, 5, 7$ . Can you guess a formula for the number of squares in  $\mathbb{Z}_p^*$ ?

b.– Prove your conjecture

c.– Write  $p = 2k + 1$  (with  $k$  an integer since  $p$  is odd). Show that if  $x \in \mathbb{Z}_p^*$  is a square, then  $x^k = \bar{1}$ .

d.– Deduce that  $-\bar{1}$  is not a square if  $p \equiv 3 \pmod{4}$ .