Parcial # 1

Nombre:

Profesor: Rodrigo De Castro K.

Calificación.

No se permite el uso de celulares. No se permite compartir calculadoras,

1. (12 puntos) Algoritmo de los Productos y Cuadrados Iterados presentado en clase:

Algoritmo para hallar be mod m

ENTRADA: e, b, m (números naturales) Expresar e en base 2, e = $(a_k ... a_1 a_0)_2$ Inicializar

u:= 1

Potencia := b mod m

Para i desde 0 hasta k,

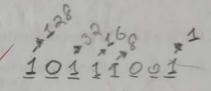
REPETIR:

Si a = 1 entonces

u := (u × Potencia) mod m

Potencia := (Potencia)² mod m

SALIDA: $u \equiv b^e \mod m$, donde u < m



56

36

(i) Expresar el número 185 en base 2: 10111001

68×36=2448

92×36=332

6

(ii) Ejecutar el anterior algoritmo en la siguiente tabla para calcular 6185 mod 124 6 X6=6 (56) ?= 3136 6 x 36 = 256 68

4 Respossta =

