Theorem: #Formally Little

statement:

If 'p'is a prime and a \$0 mad p. then

(Apan) I= 1

Proof the (using group theory):

i. The multiplicative group Zothas P-1 elements

since it's a finite group the order

amy element divides p-1

about 1 = 1 mod p

minz ---- MK be painwise co-prime integr Ž A B CK WOOD SUF. I = (d.c.) bag rown. a unique solution modulo N= n, ne --For any integers a, a, --- ax the system: the mysted = near 19 M. Euchdean Algoration; # Chinese Remainders Theorem (CRT): Proof a and b be integers on the way X = as mod m2 TO TOX + PT 1-5-12-1-12 + 150 Of the Part - LAN a - bar + 151 D TO THE THE ST Theorem statement. X = a, mdn, (B)

Bezout's Theorem: proof and Example: Theorem statement: Theorem s-whemend: For any integers a and b There exist integery x and y such that: supported was state ged (a,b) = 0x+bx X = a mod ni This is Bezout Identity. when ged (a,b) = 1, the Identity used to find the modular inverse of a mod b' Proof: - Nobom moduloz supinu a don Let a and b' be integers, and apply Euclidean Algorithm: a = bq, + R, b=17,9/2+12 12n-2= 12n-19/ + 12n

12n-1 = 12n 9n+1 40