1. Mod Madress

1. DEZ BEZ CEZ MEZ DI. DEZ BEZ CEZ MEZ C>0 m>0 C>0 m>0 given lil Cazob (mod cm) Assumption 1.1 a=b(mod m) Assumption (12 Cm/(ca-cb) Congruency: 1.1 1.2 m (ca-b) (Congregation: 1.7 1.3 3KEZ that Drustbility 1.2 1.3 JKEZ Host Divisibility Ca-cb= Kcm a-b= km 14 Or-b= kin Algorithm: 1.1.3 1.4 C(a-b)= Ckm Algorithm: 115 FREZ HOM Mtro]: 1.4 Ca-cb = C. km 1. 1.2 a-b= km 1.5 FREZ than Intro]: 1.6 m a-b divisibility: 1.5 Ca-cb=k·cm 1.4 1.7 OI=6 (mod m) Congruency: 1.6 1.6 cm | ca-cb Drussibility: 2. Ca=cb(mod cm) -> a=b(mod m) 1.7 COECH (mod cm) Direct proof Mule (bicondition (an)) Congruency: 116 : Ca=cb(mod cm) (> a=b(mod m) 2. Ozb(mod m) -> Ca=cb (mod cm) in for any integer a and b and any positive Direct Proof rule Integer could m. Ca=clamselon) if and only 2. GCDs one consier than factoring fa=b(mod m) (a) $gcd(0,12^{73}) = 12^{73}$ (c) gcd(91,434)= gcol (91,434 mod 91) = gcd (91,70) (b) gcd (139,69) = gcd (70, 91 mod 70) = gcd [70,21] = gcol (69. 139 med 69) = gcd (21, 70 med 21) = gcd (21,7) = 9col(69,1) = gcol (1, 69 mod 1) = gcol (7, 21 mod 7) = gcol (7,0) = 900 (110)