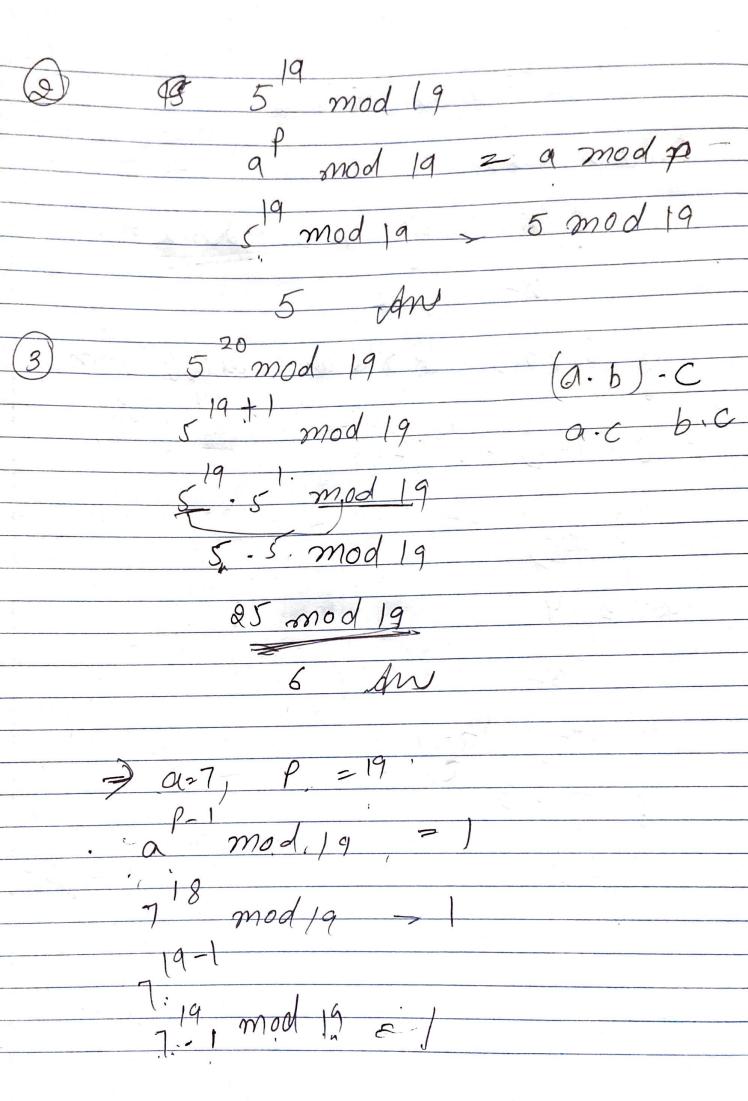


fermat's Theorem Where as a is not divisible by P levoof P2 & J, 2, --- P-13 X = SamodP, 29 modP a(P-V mod P) 51, 2--- P-13(mod p = 5a, 8a (P-1) | mod p = Sa - 1/P-1 mod P P-1)! mod modp = a = . (P-1) a = 1 mod p a = a (mod p) 5" mod 19 mod on a 15 mod19 =



x mod 19 Euler's theorem (n) if n is prime mo if (n) PX Q are muliple of n d (P-1) · d(q/-1)

fn f(q x, mod n) = f(x, x)dn To axi = fr x, modn dn 1 dn Ti=1 dn 1 dn Ti x, modn mod n 1 moo mod 10