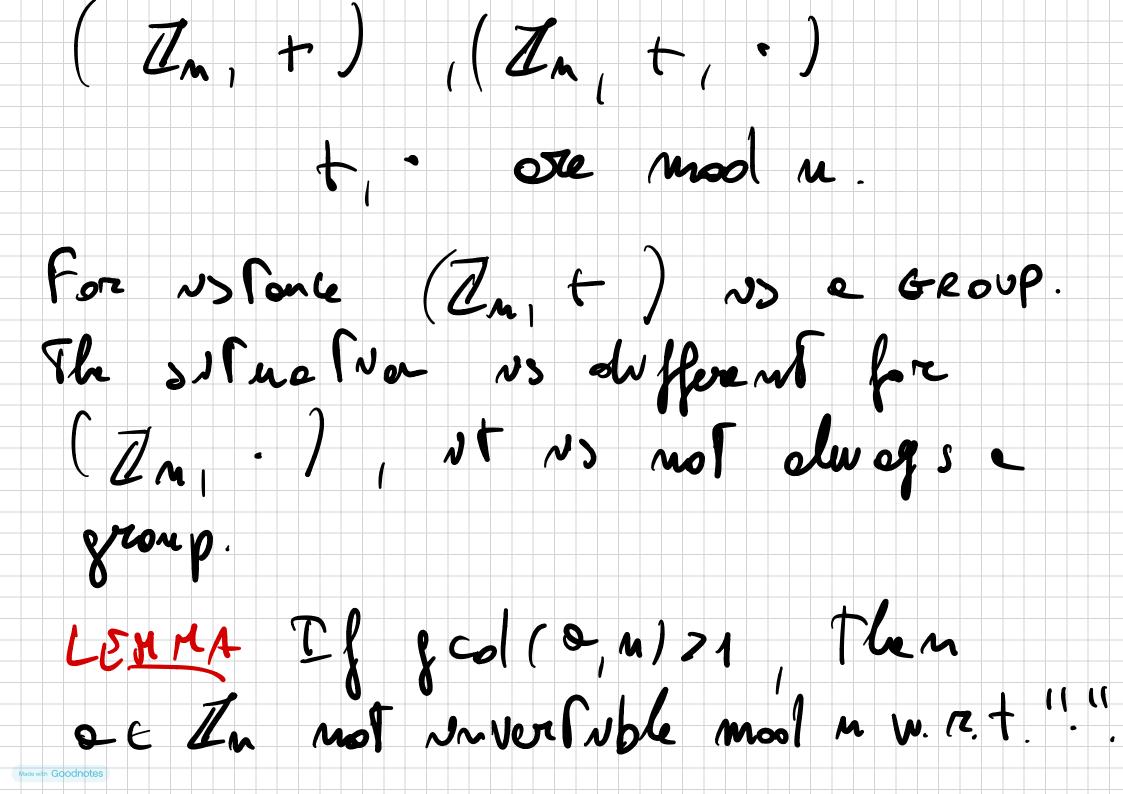
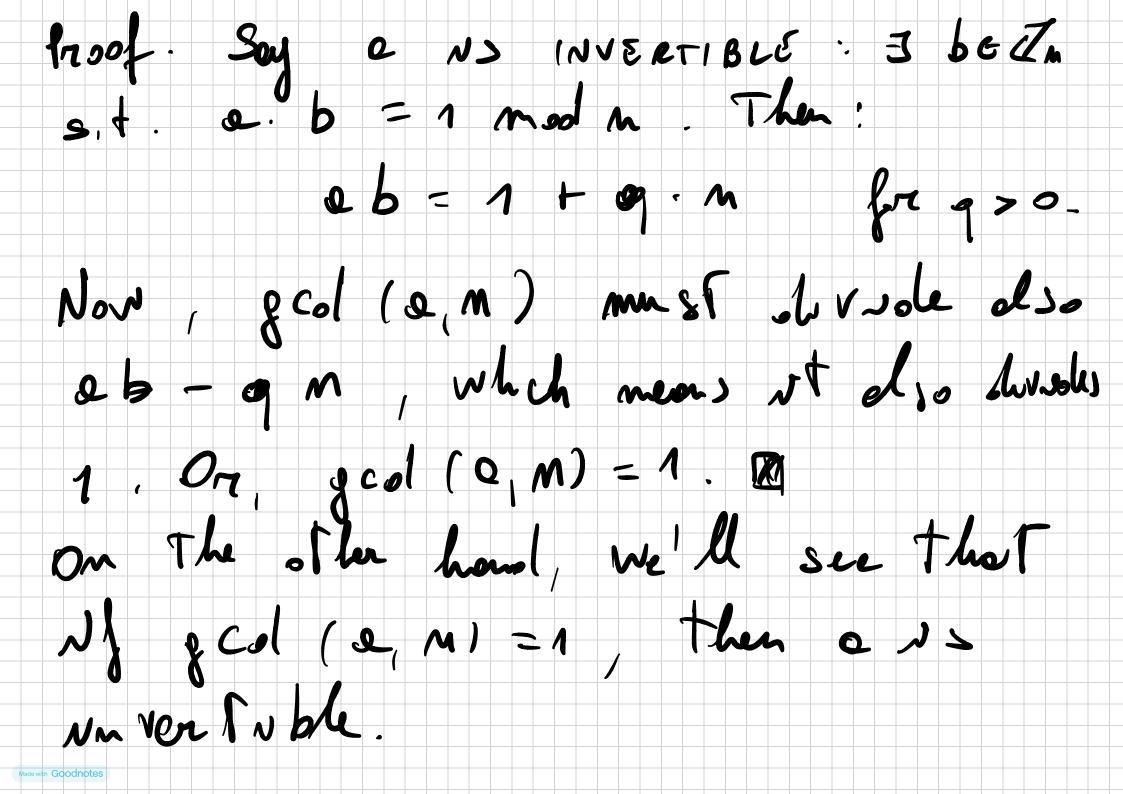
NJ MBER TITTORY We will in Produce some concrete essemptions: FACTORING, DISCRETE LOG, LEXANING WITH ERRORS. Number Thory No Spoul modulor oxilling In = 40,1,2,--, m-15. Them you can have structures like





This motoveles the flowing slef. In: 1 e e In: {col (a, m) = 1 } # Zm = Y(m) EVLER TOTIENT FUNCTION-Some specul cases:

M=p=a-prume # 27 Zp = 11, ..., p-11, y(p)=p-1

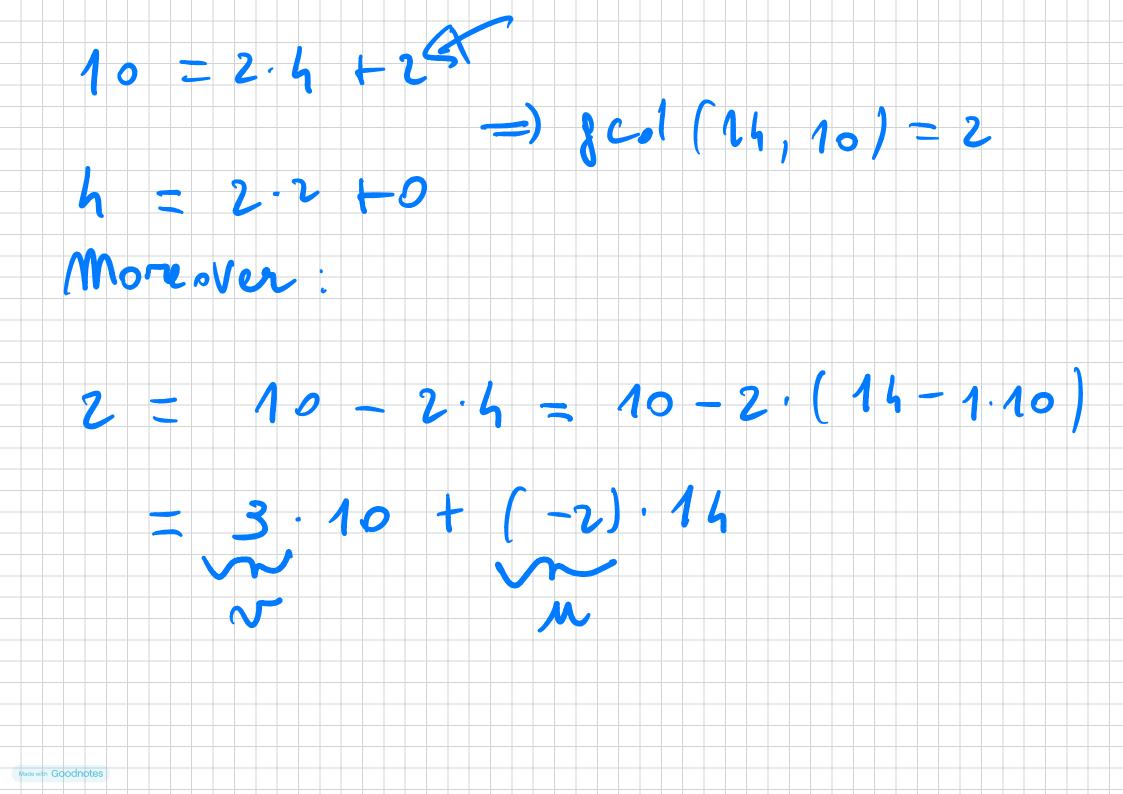
m=p.oj wwith populaes_ But we'll see Y(m) = (p-1) (q-1) # In Will show This lose 2.) We ore sometimes to 1 some obserge of weathy spore Trons over In or It for pretty lorge mor p (l.s. 1p1 JS 2048-buls) Some Mary Lery: Aslow Tron and multi-

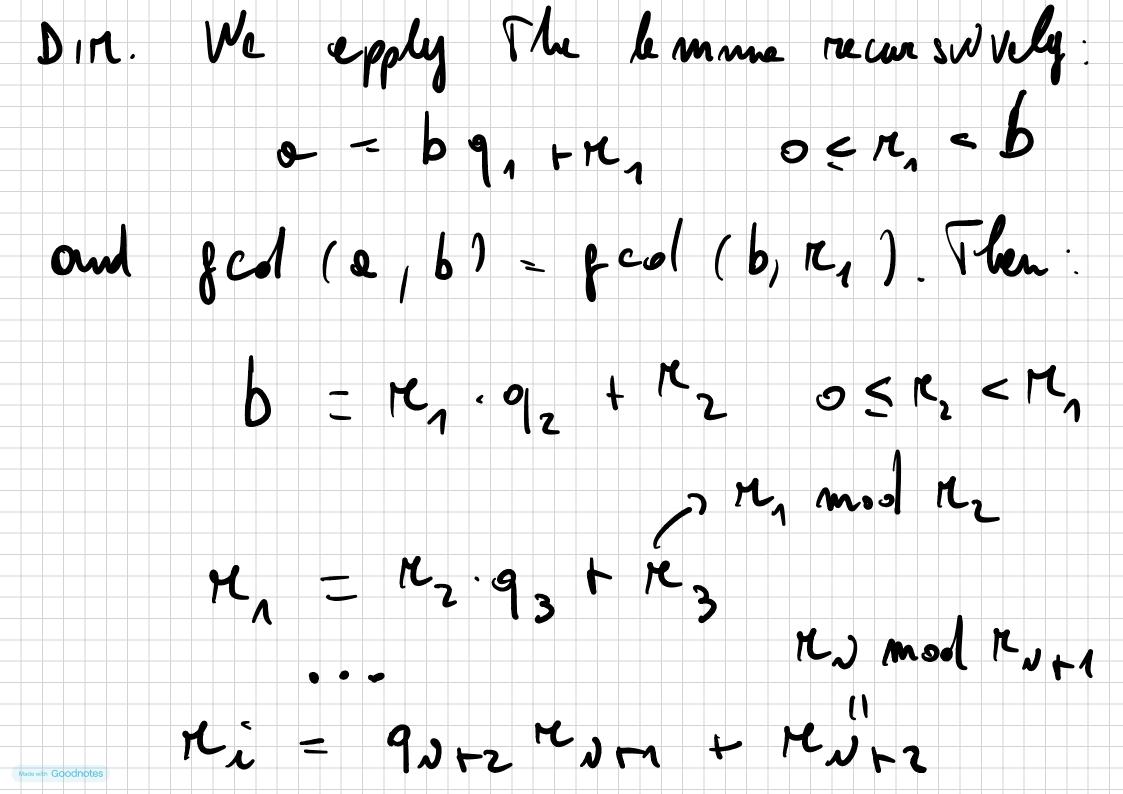
plu colision con be stone in polynomial Ve mon slow, slot she unverse con olso be compulied un polynomial sume. This is possible whing the EXTENDED

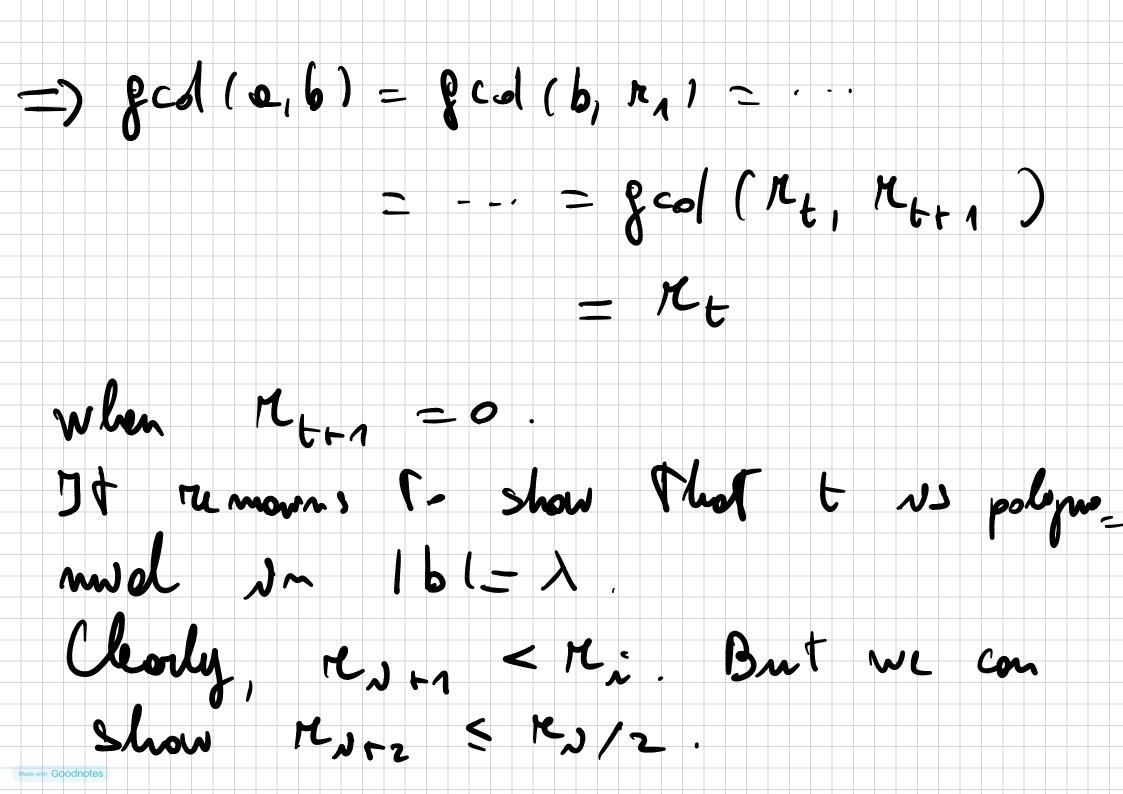
SUCLIDEAN ALGORITHM. LEMMA Let e, b s.t. a > b > o. Then gcd (a,b) = fcol (b, a mool b). Proof. We have a = q.b + a mod b worh 9 = L @/b J.

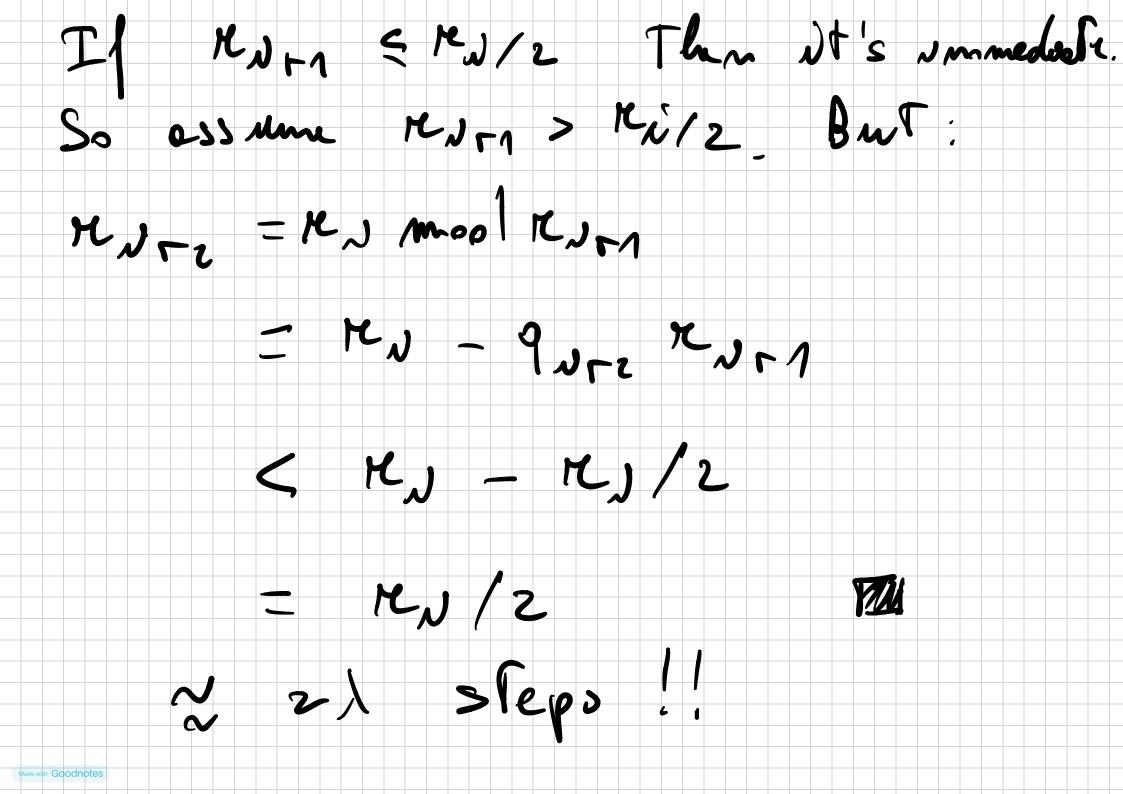
Now: a Common duvisor of e and b No also e ownsor of a mood b = Q - 9 b. Sumborly, a common showsor of a mile oral b also shribles a = 9b+e mod b 12 THM Grom e > b >0 me con compresse gcol (a, b) um poly-tume. Also, Con Compuse M, v s.t. am + bv &col (a,b) =

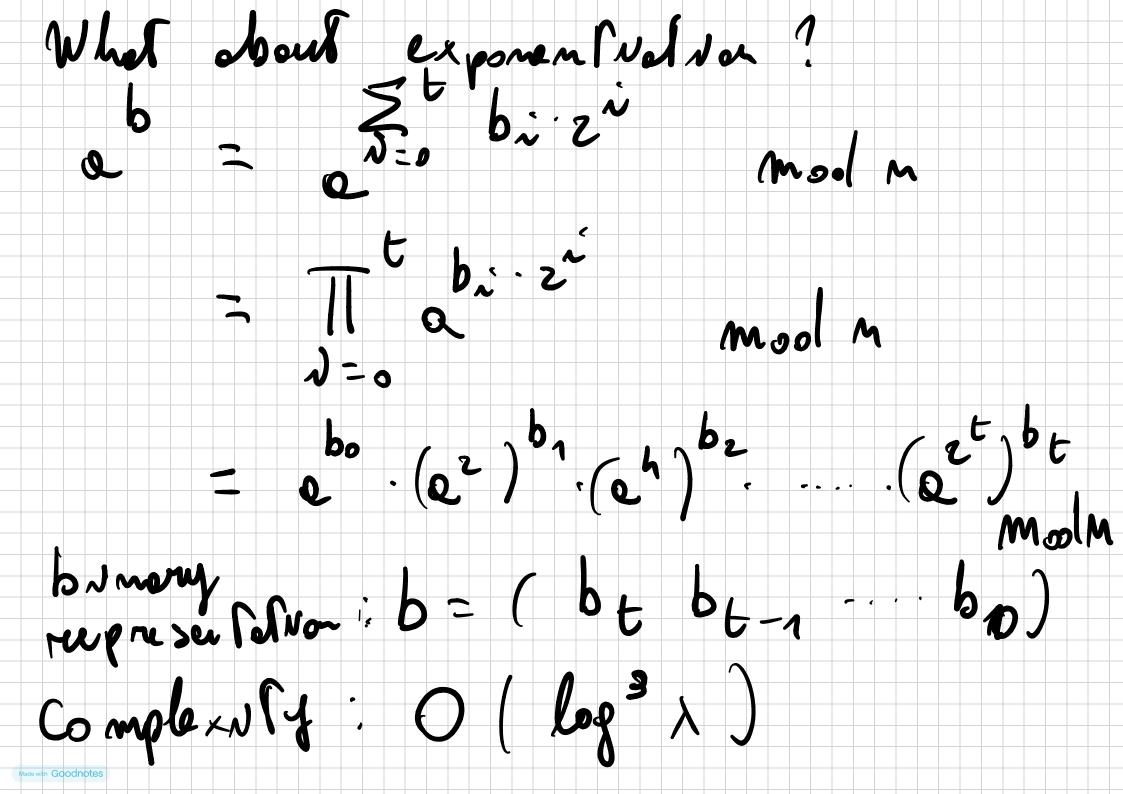
Cor Compule In polynomial Time w, N S. T. 1 = gcd(e, m) = e. m+m.v => 0.16 = 1 mool m u vs the vm verse. Example: 0=14, b=10. Then: 14=1.10+4

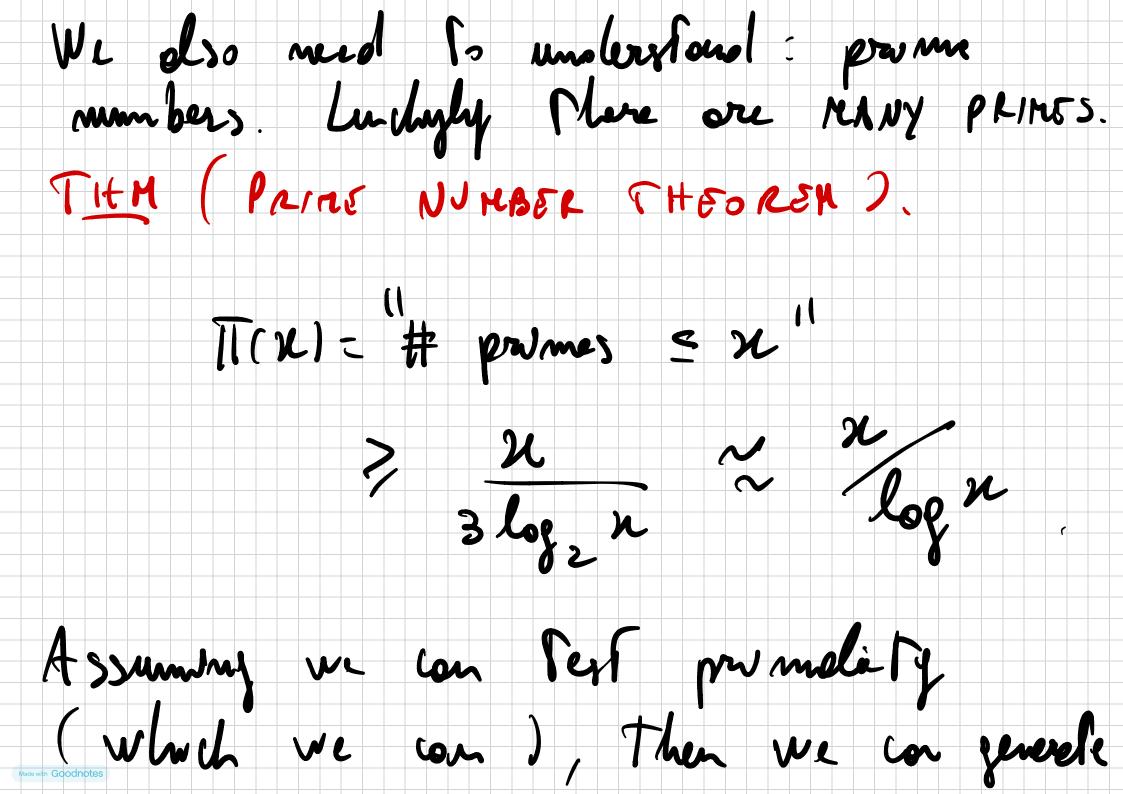


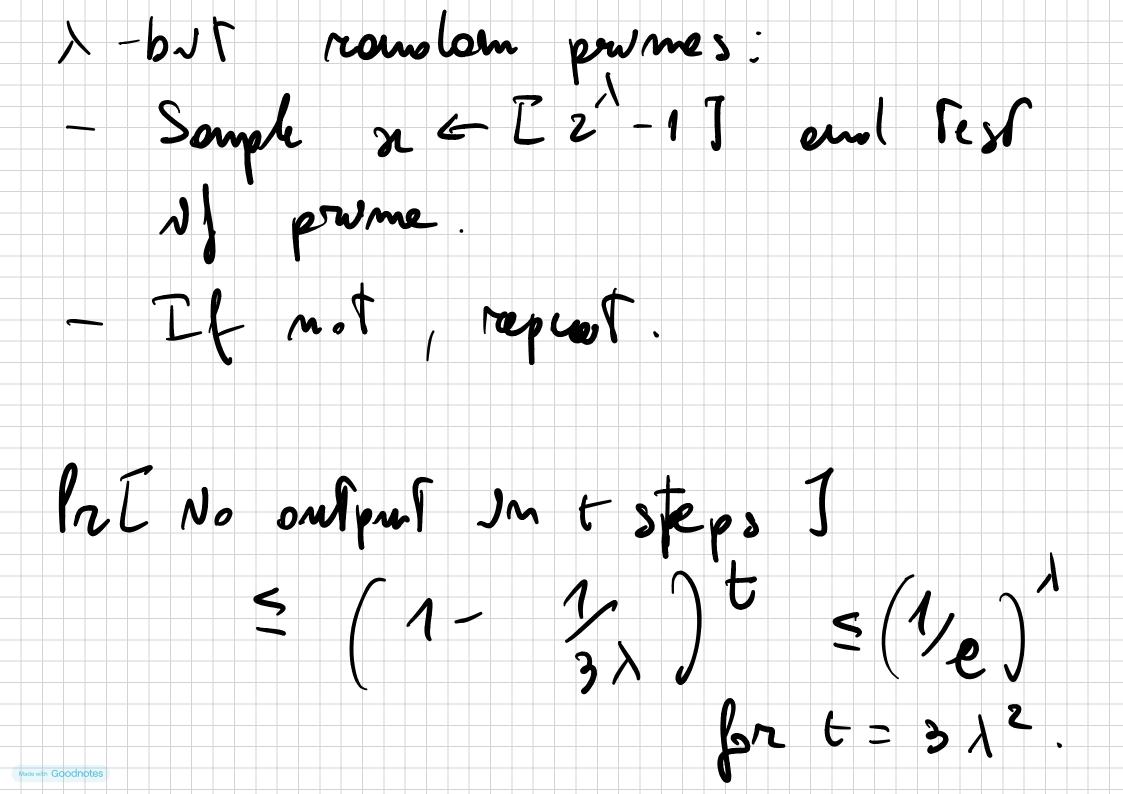


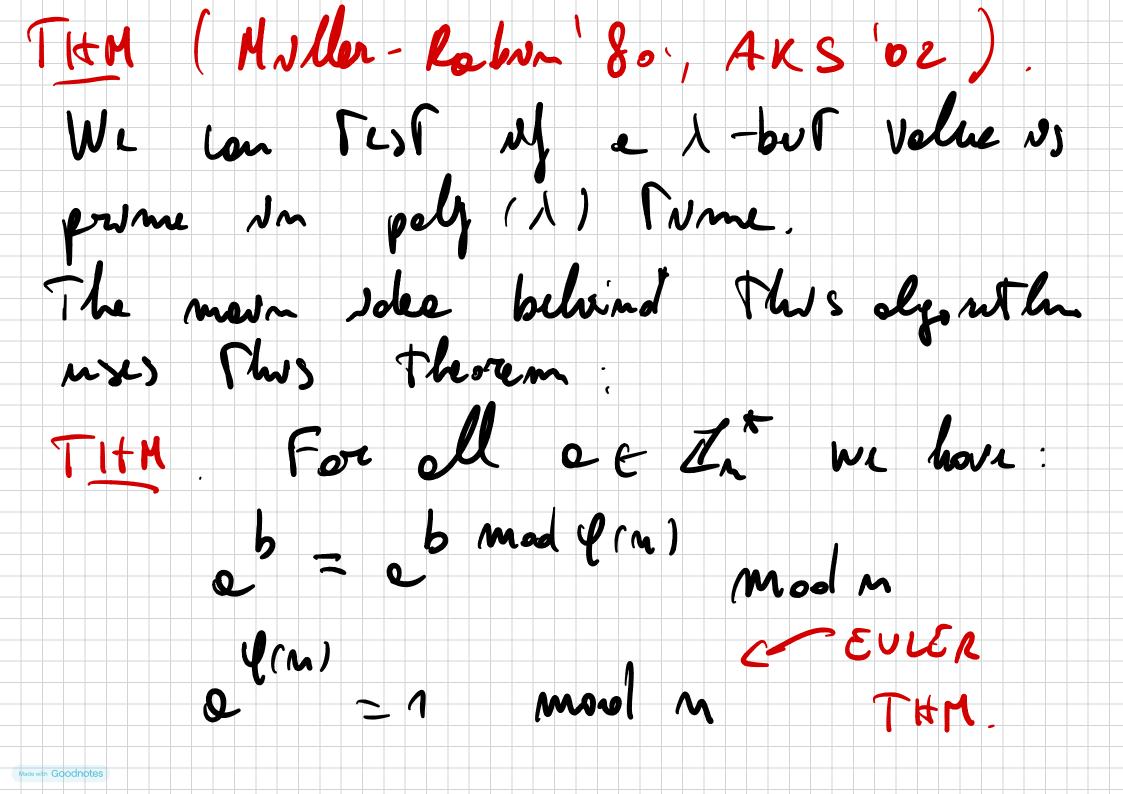


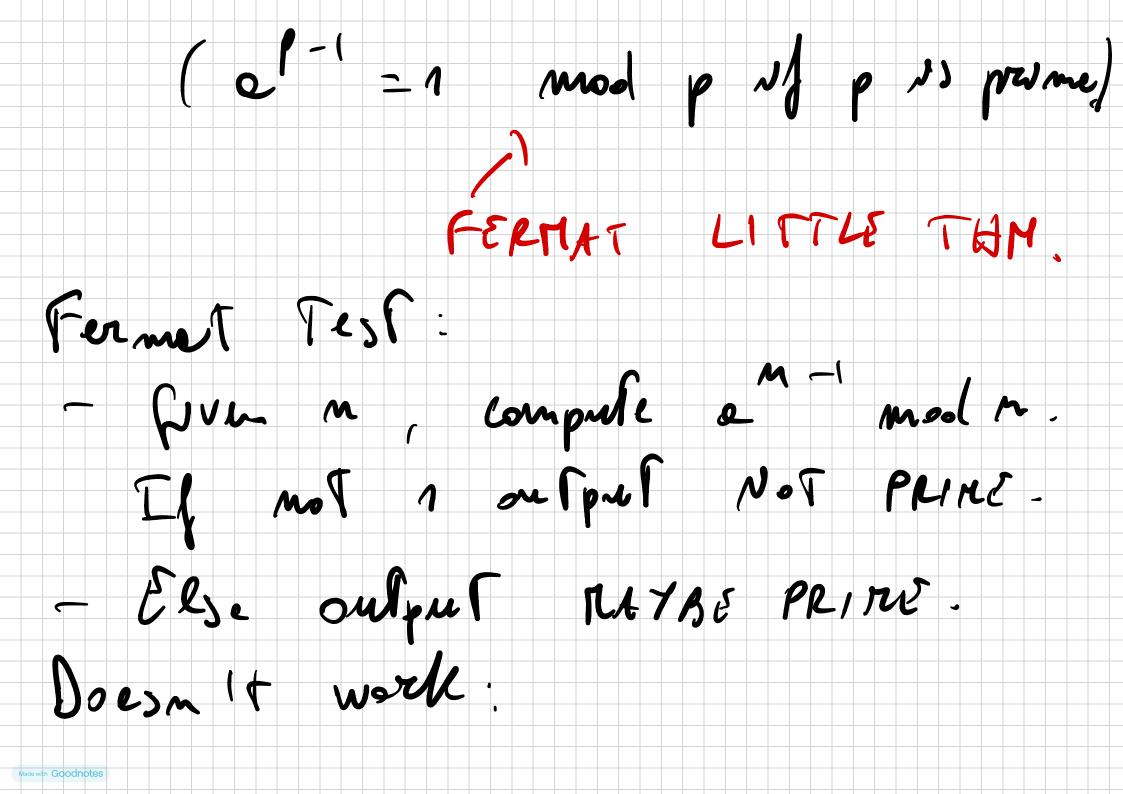




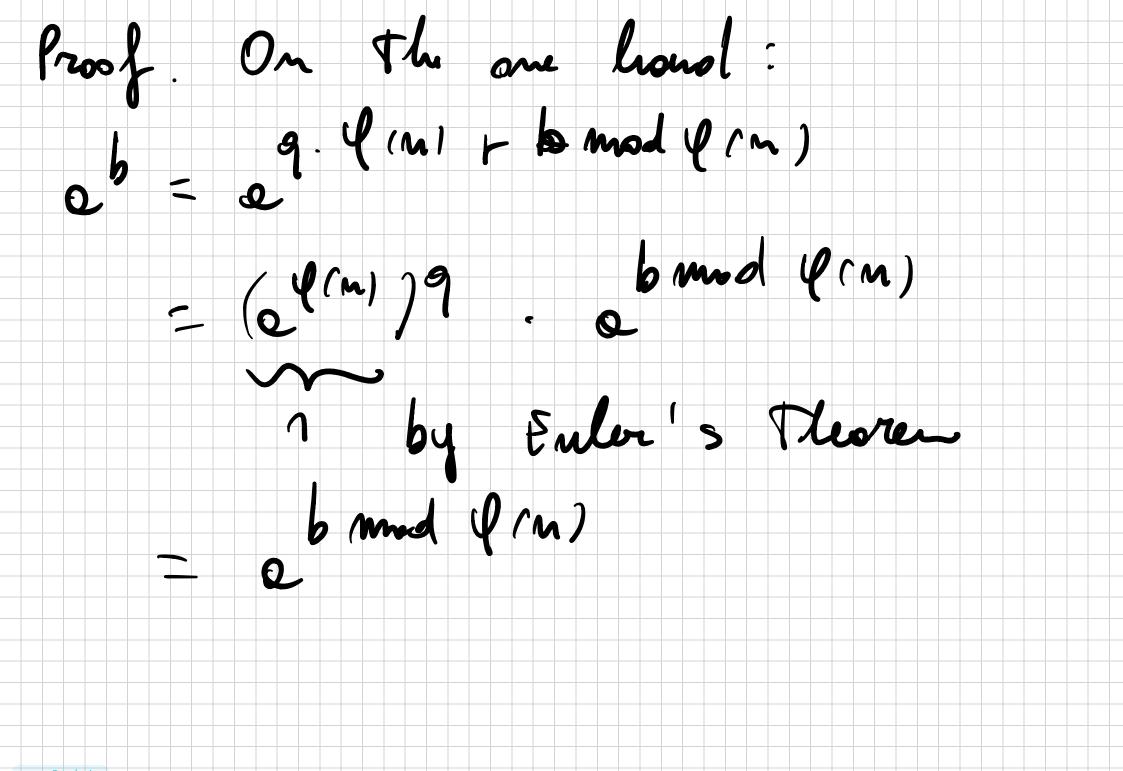








ore mot prime s. t. _ Cheru 2 -1 mool m (FERRAT LIARS) There ore most. en = 1 mool n He E In (CAPMICHABE NUMBERS)



Made with Goodnotes

