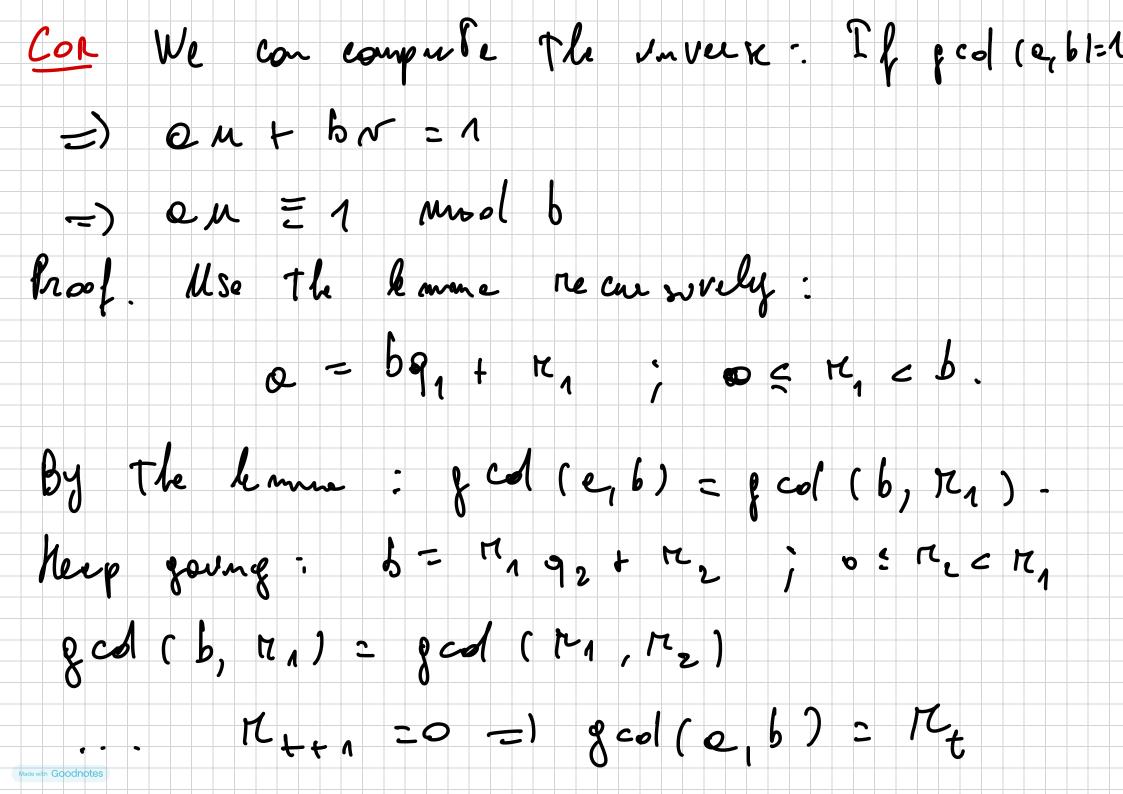


Mooluler enthmetic over 1/2 = 40,1,.., m-16 look: (Zn,+) Ns e Grove. Smportoubly, 3 en Inverse: VacIn, 3 bc Ins. t. @ +b = 0 mod h. Look et !. I sheel: (In, .), NT in most a group for every m. LEMMA If god Ce, m1>1, Then a wo not under la ble mod m. Proof. Assure not: a vs unvertible, so 7 both s.t. e.b = 1 mool m. But then: ab=1+9m for 9>0

Then & col (e, n) obvioles eb - 0, m, em! thus it durvoles 1, so gal (e, b) = 1 -5 = 14 Zn = 1 e = Zn: e souvertuble mod m !.

(f cd (e, m) = 1.) ? $\# Z_{M} = Q(n); e.s. m = p.q$ $q(m) = (p-1) \cdot (q-1)$ Zp = Zp \ 404 = 41, ..., p-11. (Zp,) No ecroup. We went effectent elsouthurs for compating sey over ([n + ,): |n| = 20(8 bus)

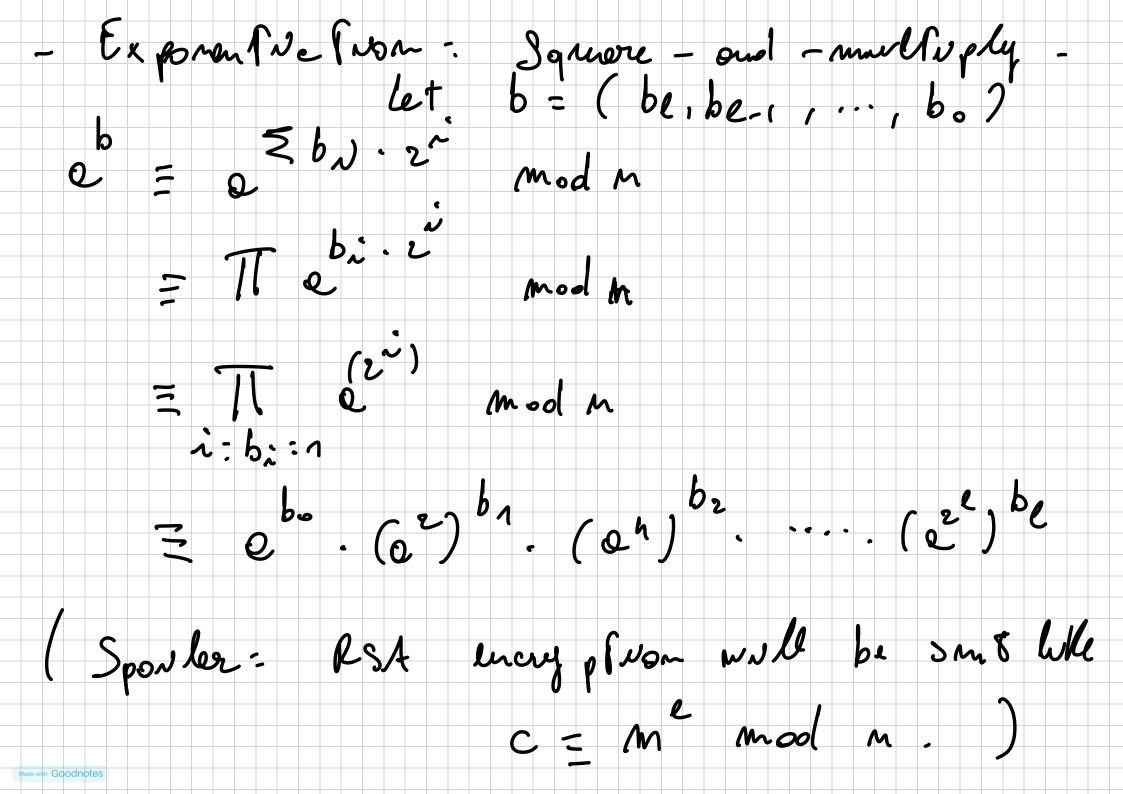
- Adolf Non and multiplice I vou ou trevol. - Inverse? Exponentvetion a mod n? Inverse. Externed Enchower Algorithm. Lenne Let a, 6 s.t. a > b > o. Then g cd (a, b) = & col (b, a max (b). Proof. Because the common durisors between (e,b) ere The seme es (b, a mod b), sombe e = 9b + e moolb; 9 = Le/61 THM. Guver 2 2 6 >0, va con compuse agrad (a, b) un poly-Tune. Also, ve con find untegers w, N, S.T. ent b N = gcd (o,b)



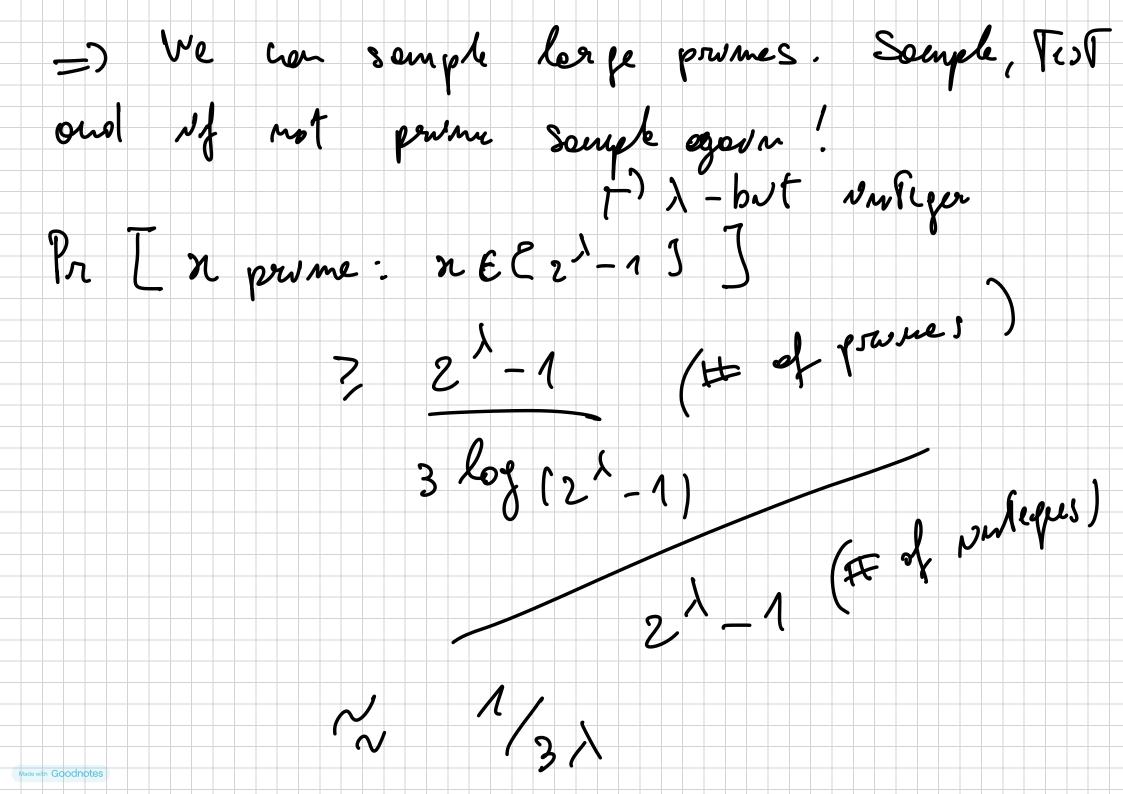
It's polynomial from because Mitz < 171/2 Y n' = 0,1, ..., t-2-Clearly, rest, 2 ri. If rest, 2 rs/2 we one done. So assume rest > rest, 7 rs/2, but There But Then: test = re: mool rest = re: - 92+2 resta < 12 - MD/2 - MD/2. # of sleps: 2 2 1 Nowhere 1 2 1 51

Made with Goodnotes

Exemple: a:14; b=10. Then: 1h=10·1+4; 10=2·4+2~) 12t=2 i h = 2 · 2 + 0 / 2 + 1 = 0 =) 800 (14,10) = 2 To get u, v: 2 = 10 - 2 - 4 = 10 - 2 (14 - 10) - 3-10 + (-2) - 14 $\mu = -2$; $\sigma = 3$



Deorge Non: Cd mod m) Few more thongs: Prime numbers. How do we guerelle large primes. THAT There are supposed rough primes and Idee: Pack e Kondom p and Test vf p NS prome. THU WE can lest sof pour poly- Forme.



la I faic offer t steps 3 5 (1 - 1) Made with Goodnotes