Mock exam

a) For integers a, b, we say a divides b"
If there exists in ETL such that b = caThis is withen as a b, or a x b
When this is not true.

het a,b, c et and arrune that a b and a c.

From the definition above this means there exists 3,8 ETL that sality.

beap and ceax.

Let m, n E TL.

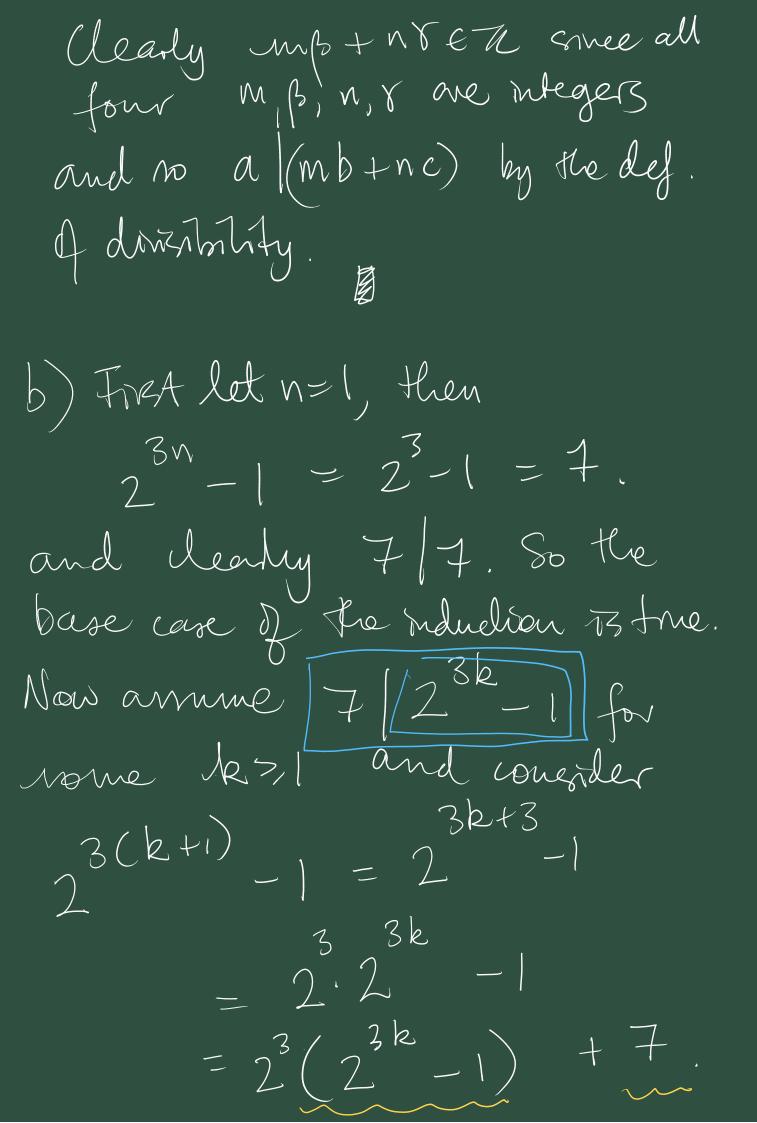
Let $m, n \in \mathbb{Z}$.

replacing

mb+nc = mas + mas, b,c

with $= a(m\beta + nx).$

theabox



Now notice that this last exprension à linear combination 2 2 - 1 and 7, hold Which are divisible by 7. Therefore by result frompatical,

7 (2 -1. So we have shown that

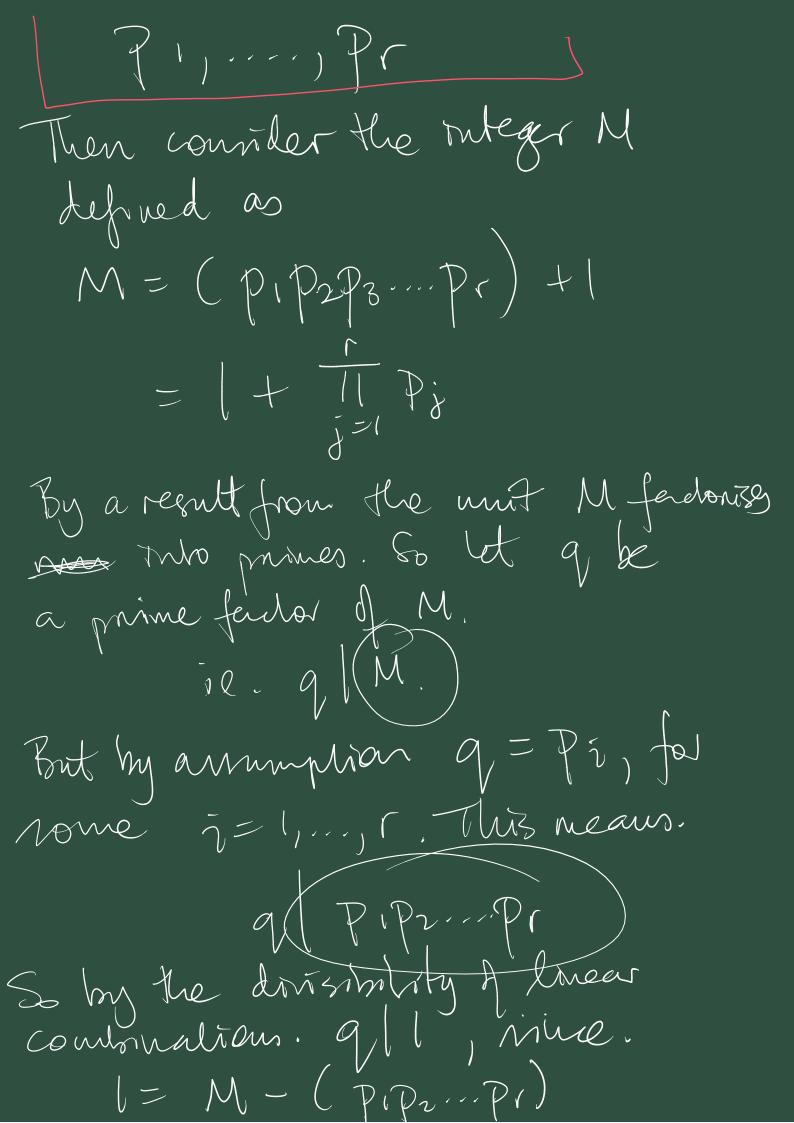
7 (24) => 7 (24) and by induction, Kirs proves fleet

Ynzi 7/230-1. () ged(a,b) It is the greatest common divisor de and b, il. the grantest integer & such that

d (a and d (b. Counter the set L, defrued L= { mathb: mnet} then ged (a,b) in the smallest positive element of L. d) let a b, el Assume ged (a,b)=1 and a/c and b/c. This means there exist & BET.

quel that c = xa, $c = \beta b$. There expres 1, y Ell such that 1= xa+yb = $c = \pi a c + y b c$ $= \pi a \beta b + y b \times a$ $= a b \left(\pi \beta + y \times \right)$

= C = ab \Rightarrow abc. Note the term in the torachet, Mb Ha is cleaty an integer. N B, y, 2 CTC. Norefore able as required a) Endid's proof of infristely many primes. Prof (prof hy coulradiction) Tost arme there are only a forte runher of primes and that they are all losted as.



But this is a contradiction mule (>) no connot double 1. So our mital annuplion itself. must be false, so herefore llere are an infinire munher of mines. (b) Endid's Jemma was crucial for Fundamental Ansthructor. Troof of Euclid's lemana het ab ett. het p be a prime rumber, settestying plab. From Cogit. (AORB) = 7A = 3If pla we are done.

Mense ve con assume (p/a)ie. gcd(p,a) = 1ford p. This means flore exist n, y etc. Such that. V= np+ya. a linear could nation of p and ab with of which are trisime by P. The has Moun. p/a >> p/b. Mondois donvalent to. pla or plb.

Claim: 2+1 is prime => m=2 for nome net. Proof. We will be coultepositive intead. $(A \Rightarrow B) = (B) \Rightarrow (A)$ Commonthe A A B which is the statement. If M # 2 for none nex Han 2 H in

composite. We arrive that me can helyphesed as M = 2.5, for vone odd S > 1 2^{n} , S 2^{n} , S $= (2^{n})^{5} - (-1)^{5}$ $= (2^{n})^{5} - (-1$ => 2 + 1 n vouvositie.

mon thin.

any theger factorisation 2^M + 1. n 2 1 1 > 1 and 21/2 2 1. This proves the contrapositive and herselle orginal result.

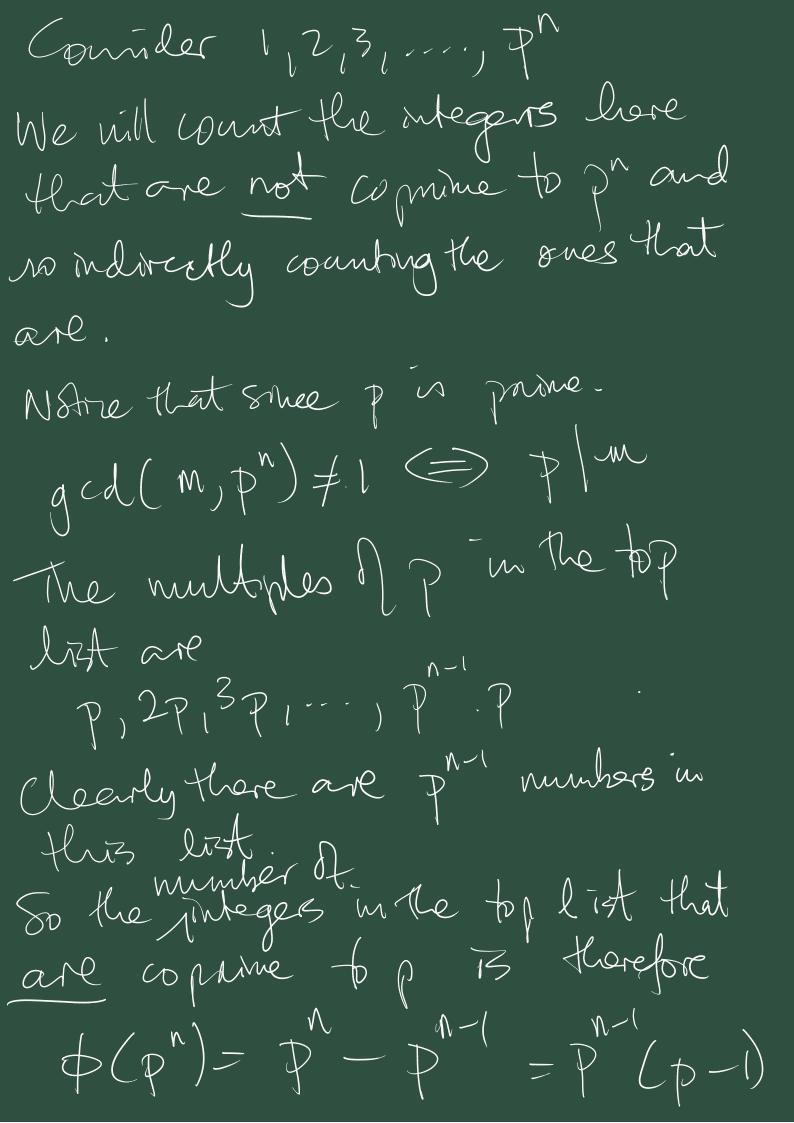
Q3(a).For a natural number n>0 and integers a, b we say "a in congress to be modulo n'' written a $\equiv b$ (mod n) iff. $n \mid a - b$. And futher, a = b (mod n) iff a,b. leave the same small at positive. remainder after division by n. 11. If a=9, n+1, 0 < 1, 52 < n b=92N+12 $a = b \pmod{n}$ b) Posnts show + and. fitwell. with covernenge modulon. Assume $a \equiv a'$, $b \equiv b'$ (mod n).

Clown 1. $a + b \equiv a' + b'$ (mod n) 2. $ab \equiv a'b' \pmod{n}$. Profs We have to whow. and n(a+b) - (a+b).

And n(ab - a'b').

We can armue (n(a-a')and(n(b-b')a)(a+b) - (a+b) = (a+b) = (a-a') + (b-b')Seronlly. (ab - a'b' =) (a - a') (b - b') (2a'b' + ab' + a'b)= (a-a')(b-b')+b'(a-a')+ a'(b-b').

Notice that work final RHS are lon. combs. A a-a' and b-b' and no are divisible by n, by the Ansimity of linear combinations result. toefre n (axb) - (a' +b') and n lab - a'b' as recurred. (c). For a possitive integer 121 o(n) is defined as. $\phi(n) = number of j Sneli that$ $l \leq j \leq N$ and gcd(j, n) = l. Moreorer $\phi(n) = |U(n)| = | - |U(n)|.$ Clarm. For a prime ?. $\phi(p^n) = p^{n-1}(p-1)$. Vrost:



want a (mod n) a exists iff ged(a, n)=1. And Berout's Identity 12 1 4 4 5 m = 1 $(=) na = -yn+1 \equiv |\text{mod } n|$ $n \equiv a^{-1} \text{ (mod } n)$ $n \equiv a^{-1} \text{ (mod } n)$

$$a^{5} - b^{5}$$

$$= (a - b) \sum_{j=0}^{5-1} a^{-1} b^{j}$$

$$= (a - b) \left(a^{5-1} + a^{5-2} b + a^{5-2} b^{5-1} \right)$$

$$+ ... + a b^{5-2} + b^{5-1}$$