50, 7²²² mod 11 = 5 11 2/11 2 1+2 mod 11 - 5 Does Fermat's theoriem hold the trive for p=5 and a=2117 1 gd shistrib ou so moralmi finana not anomonalipani one of the medit ensprismen out Ore 16 = 1 mod 5 . comportini to Example: Example: LE born 229 brit if word is I the (mod 13) at the strong of 11'2 = 1 mod 13 (12 born) 1 = 1-17 -22 = 1 mod 1300 (11 bom) = = = + bus $-2^{4x3} = 1 \mod 13$ (14 box) 1 = 1 enorginal = + mod +3 27 = 1 mod 13 = (2)23 - 4 = 7 - 43 = 2 (mog 7) =

of Proof bom tot to seravin no bride Assume ged (a,b) = 1 and albe · since ged (a,b) = 1 by Bezout's theorem there are integers is and I such that sa+tb) = 12+x = = = = = = · Multiplying both sides of the equation by c yields sacttber=con · we conclude alc , since sac + tbc = c >3=1×2+1 god (101, 1260) = 1 Bezon ? Theorem:

Townson That dog (orp): T common That dog (orp): T conquer interpretations

. find an inverse of 101 modulo 4620 First have to use Euclidian algorithm to show that gcd (101, 4620)=1 1000 46200 = 45 \$ 10 4 15 m and => 101 = 1 ×75 +26 - + 50 +5 Nt. withours \$175 \$2 x26+23 Had priphithum. > 26 = 1×23+83 abloin 5 Hd D= od=> 230= 7×3it2 ola ebulonos ev. >> 3 = 1×2+1 ⇒ 2 = 2 X1 gcd (101, 4260) = 1

Bezout's Theorem:

Lemma: If a,b,c aree positive integers
such that gcd (a,b) = I and
a/be then alc

Feremat's Little Theorem

Proof:
If p is prime and a is an integer not divisible by p, then $a^{-1} \equiv 1 \pmod{p}$ furtheremore, for every integer a we have, $a^p \equiv a \pmod{p}$

Feremat's Little thoriem is useful in computing the remainderes modulo p of large powers of integers.

Example:

find 7^{22} mod 11By Feremat's Little theoriem, we know that $7^{1-1} \equiv 1 \pmod{11}$ and $7^{10} \equiv 1 \pmod{11}$ and 50; $7^{10} \equiv 1 \pmod{11}$ and 11)

fore every positive integers $1 \pmod{11}$

fore every positive integers K thereforce, $7^{222} = 7^{22 \cdot 10 + 2}$ $= (7^{10})^{22} \cdot 7 = 1^{22} \cdot 49 = 5 \pmod{11}$