Feremat's Little Theoriem 1 por 15

Proof:

It posis prime and a is an integer not divisible by p, then sall = 10 (mod p) to furtheremore, for every integer a we have,

 $a^{b} = a \pmod{p}$

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

Example:

Find 7^{222} mod 41By Feremat's Little theoriem, we know that $7^{11-1} \equiv 1 \pmod{11}$ and $7^{10} \equiv 1 \pmod{11}$ and $7^{10} \equiv 1 \pmod{11}$

fore every positive integer k thereforce, $7^{222} = 7^{22 \cdot 10 + 2} \cdot 7 = 1 \cdot 49 = 5 \pmod{11}$

50, 7 222 mod 11 =5 all offil 240mo197 Does Fermat's theoriem hold the trive for prise and sa = only of the wib ou so repetin preve not emmanentoruis P=5, a=2 restants little thorown is useful in comp a = a (mod p) the memainderes thought = $\frac{5-1}{9}$ and $\frac{5}{9}$ powers of integers. $\frac{5}{9}$ bom $\frac{5}{9}$ $\frac{5}{9}$ $\frac{1}{9}$ $\frac{5}{9}$ $\frac{1}{9}$ $\frac{1}{9}$ Example:

Example:

LE born cer build

Att word 11 36 = $\frac{1}{2}$ (model 13) althir extremes at year $11^{2} \equiv 1 \mod 13$ (reg born) $\pm = 1$ for $-2^{2} \equiv 1 \mod 13$ (replaced by born) $-2^{12} \equiv 1 \mod 13$ (replaced by born) $-2^{4\times3} \equiv 1 \mod 13$ (replaced by born)

find an inverse of 101 modulo 4620 to show that gcd (101, 4620)=1 Nous 46200=45×10415mi sons sonott => 101 = 1×75426dt + se toAt. without > 文文 \$ 2 X26+23 Hood pring the !! => 26 = 1×23+30 ablair o rd D= od=> 232= 7×3it2 ola abulono ow. > 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) = 1 and
a/bc then a/c

e find an inverse of 201 mod \$ 620

HoploAssume ged (a,b) = 1 and albe

· since ged (a,b) = 1 by Bezout's theorem

there are integers is and it such

that sa+tb=12+x+= 10+x

· Multiplying both sides of the equation by a yields sactible=cos

· we conclude alc since = sac + tbc = c

=> 3 = 1×2+1

=> 2 = 2 XI

god (101, 4260) = 1.

Bezow 's Theorem:

Townor: It aspec are bositive int such that ded (asp) = I and