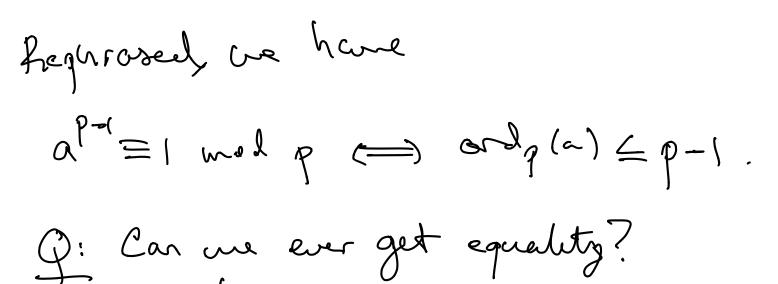
Generators mal p

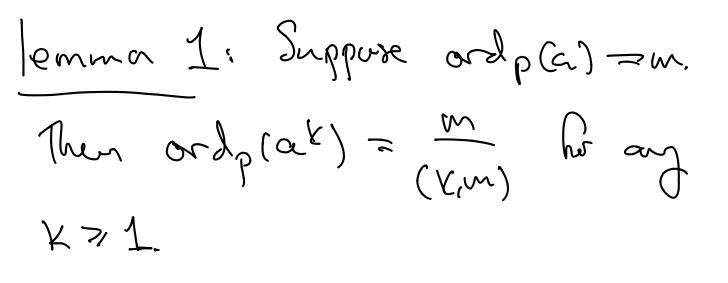
Fernal's little the Say, if $a \neq 0 \mod p$. then $a^{p-1} \equiv 1 \mod p$. hecall from week 5 discussion:

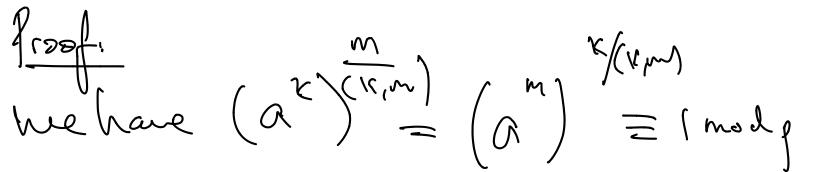
A: Yes!

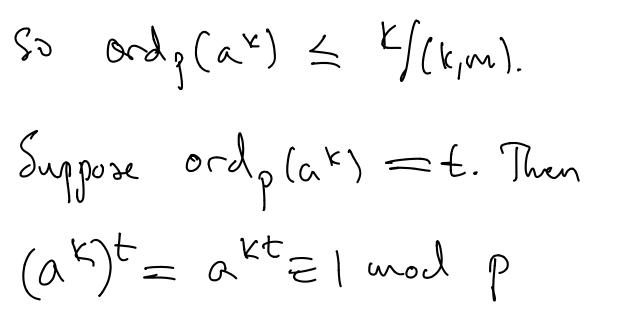


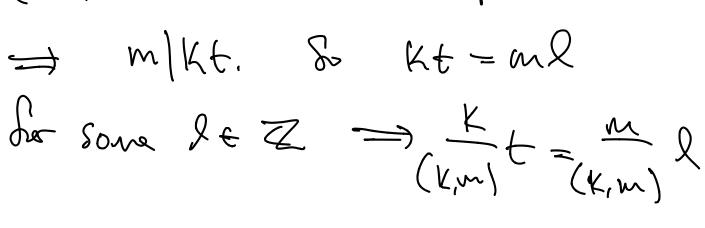
Def: if ordp(a) =p1 then a ic called a generator and p (or primitre rost mal p).

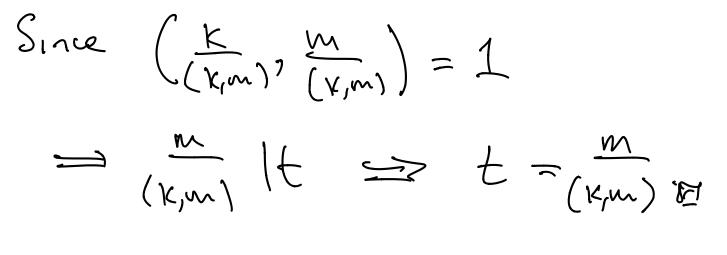
Thur: thur are $\varphi(p-1)$ generators mod pi hur pold prime.





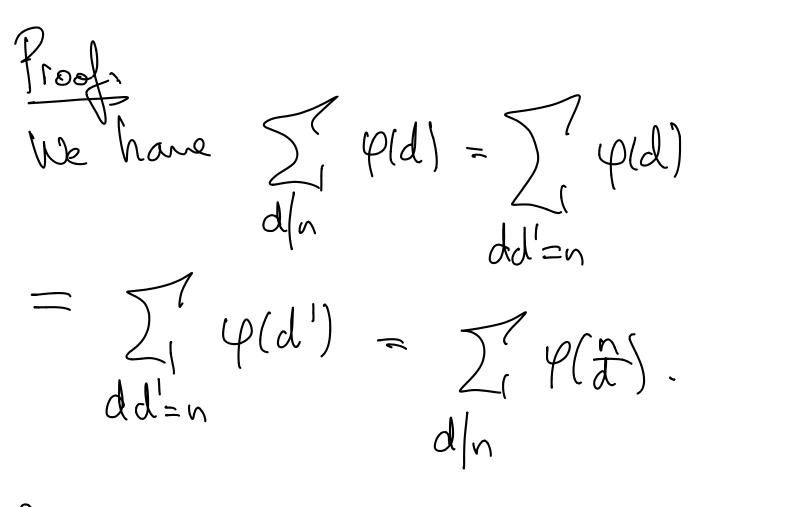






Corollang. Ordp(at) = ordp(a) $(K, ord_2(\alpha)) = 1.$

 $\frac{|e_{mmn} 2: \sum_{i} \varphi(d) = n}{d_{i}n}$



By def, $\varphi(z) = \# \{1 \le k \le z, (k,z) = 1\}$ note for any MEN, that $(m,n) = d \rightleftharpoons (\frac{m}{d}, \frac{n}{d}) = 1$

So this says $\varphi(x) = \# \{1 \le m \le n \le n\}, \ (m,n) = d\}.$

i.e.
$$\varphi(\mathfrak{A}) = \# \{ \text{intrapers with gcd}(mn) = d \}$$

Each M Satrifies $(m,n) = d$ for
Some $l \leq d \leq n$, so fulls into one of
the set little above. Summing up the
Sizes of each set then supp
 $h = \sum_{i=1}^{n} \varphi(\mathfrak{A})$ as desired

Lemma 3: If there is an element of andre d mail p, there are exciently (p(d) elements of arber d.

Proof. An element a of order of

is a root of X-(mod p. This has $\leq d$ roots, and the pours 1,a, a², --, a^{d-1} are d'dubret roots because a here order p, so there we all the voster By Icmaa 2, the pairs with order d are those with exponent aetahely prive to d, of which there are y(d) A

Theorem 1. Thue are $\varphi(p-1)$ generating mod f. Any demat a hes arder Proof:

d for some d|p-1. Let = # Jelements of order d? Nd(p)

be here $p-r = \sum_{i} N_{p}(d) \leq \sum_{i} \psi(d) = p-r$ dp-r dp-r

 $N_{p}(p-1) \neq 0$ \ge $Np(p-i) = \varphi(p-i) hy$ \Rightarrow lenna 30

What about mod n?

Turns out: there is a growthe

mod n =) N= 2,4,9k,2plc

her podd prime.

.