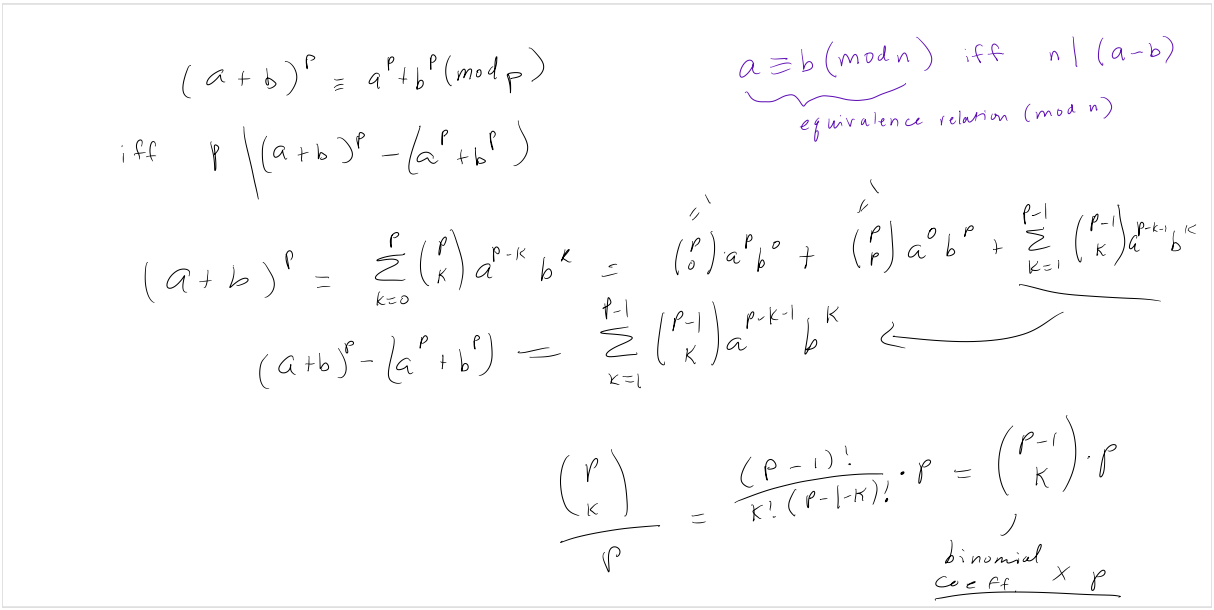
CSCI 5421 - Homework 2
Kelsey Neis, neis@umn.edu

31.1
6

Prove if p is prime and 0 < k < p , then p | p-choose-k

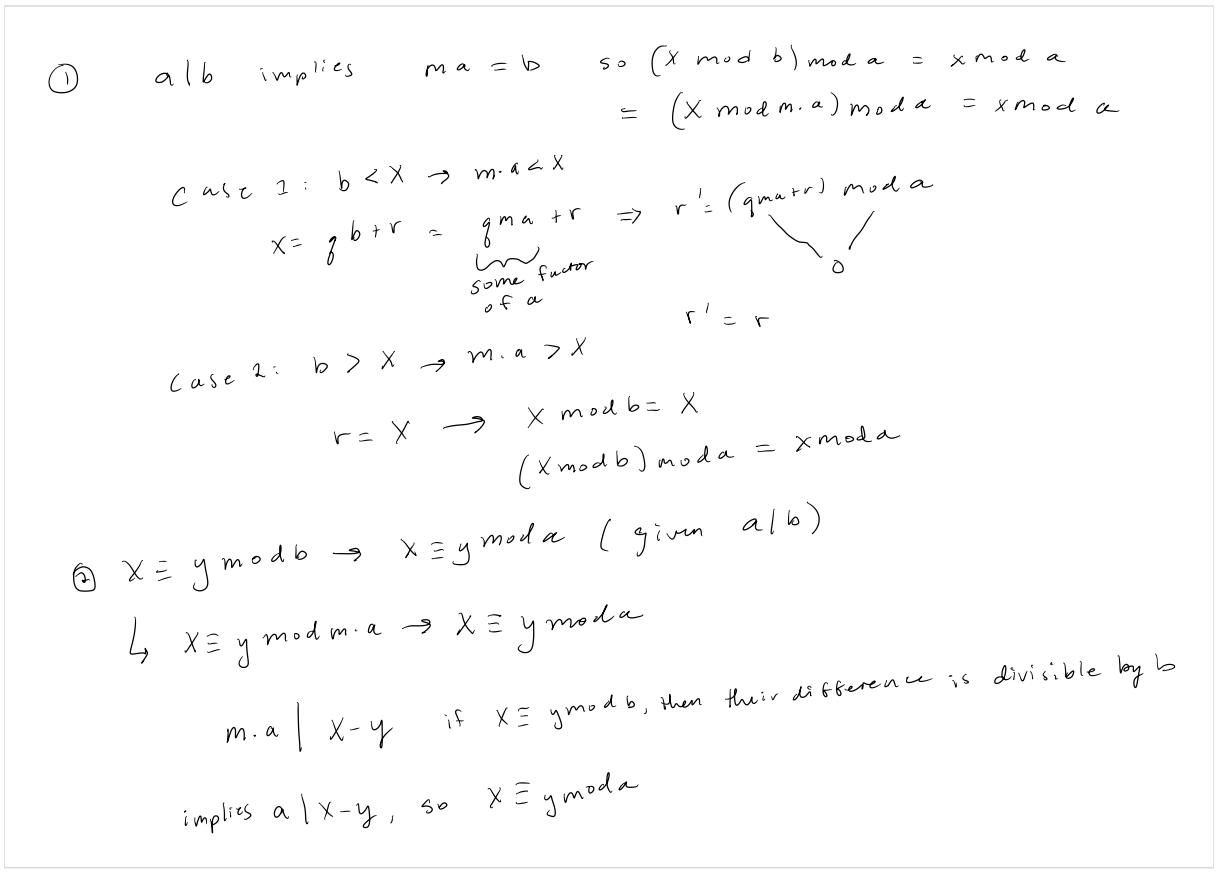
conclude:

$$(a+b)^p \equiv a^p + b^p (mod\, p)$$



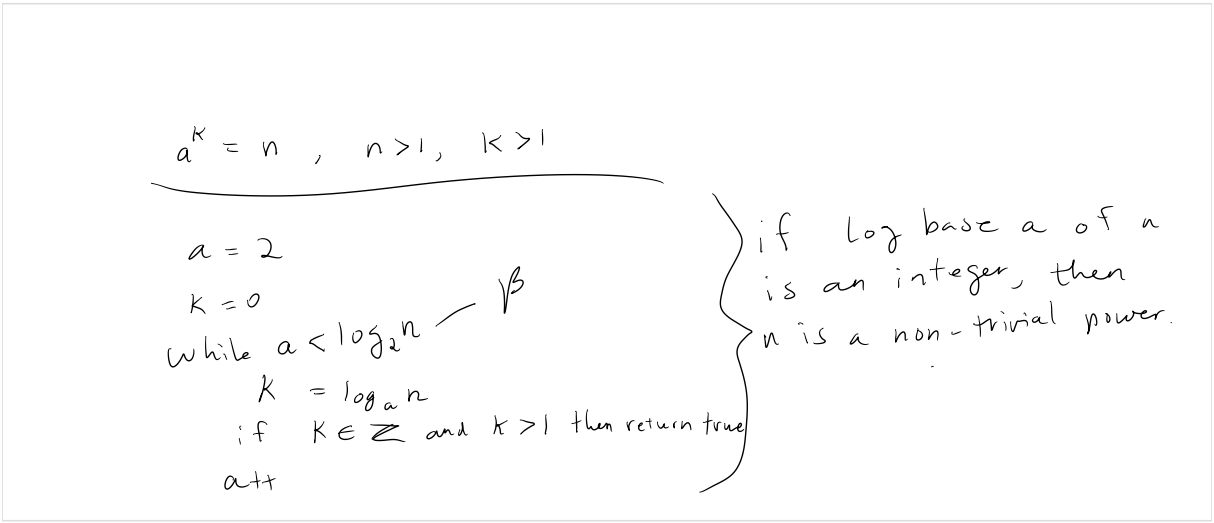
7

1. Prove if a and b are positive integers such that a | b, then (X mod b) mod a = X mod a for any X
2. prove X ≡ y (mod b) implies X ≡y (mod a) for any x and y



8

- for any k> o, n is a kth power if there exists a such that a^k=n
- n>1 is a non-trivial power if it is a kth power for k>1
- Show how to determine whether a β-bit integer n is a nontrivial power in time polynomial in β

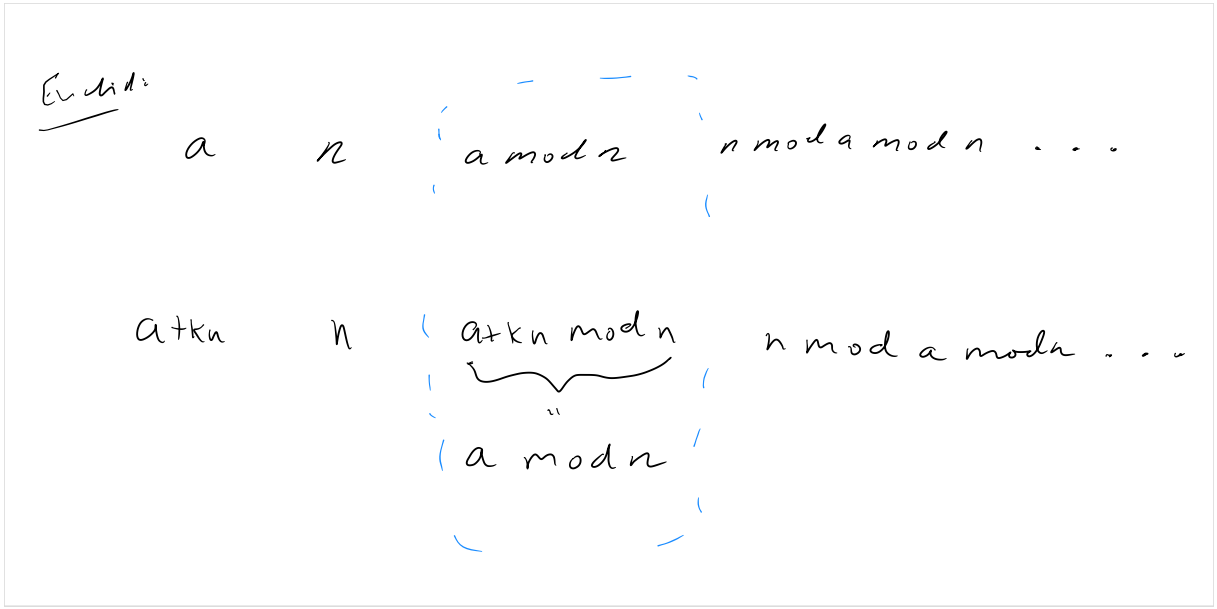


$\log_2 n$ is the ceiling for the checks needed to determine whether n is a non-trivial power, because 2 is the smallest non-trivial power.

31.2

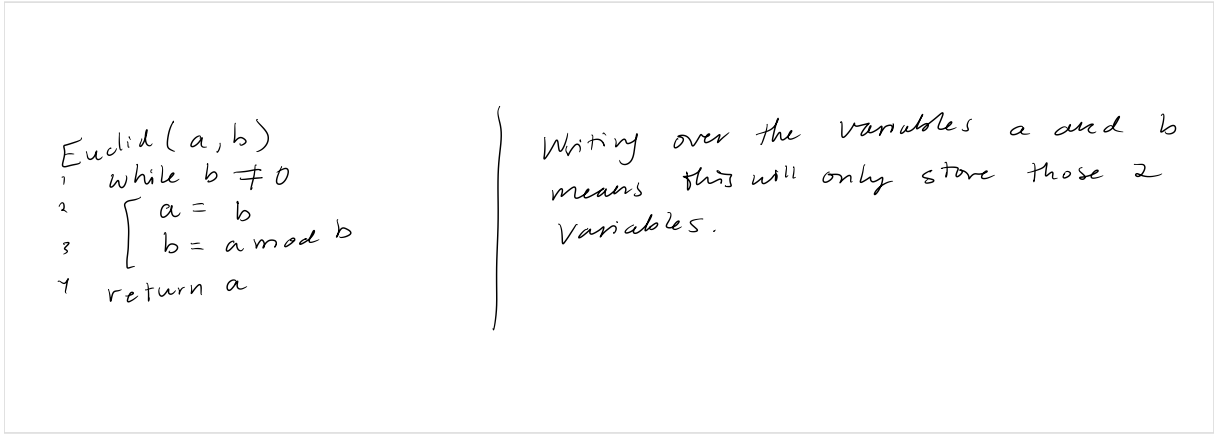
3

prove that for all integers **a, k, n** , **gcd (a, n**) = **gcd (a + kn, n**)



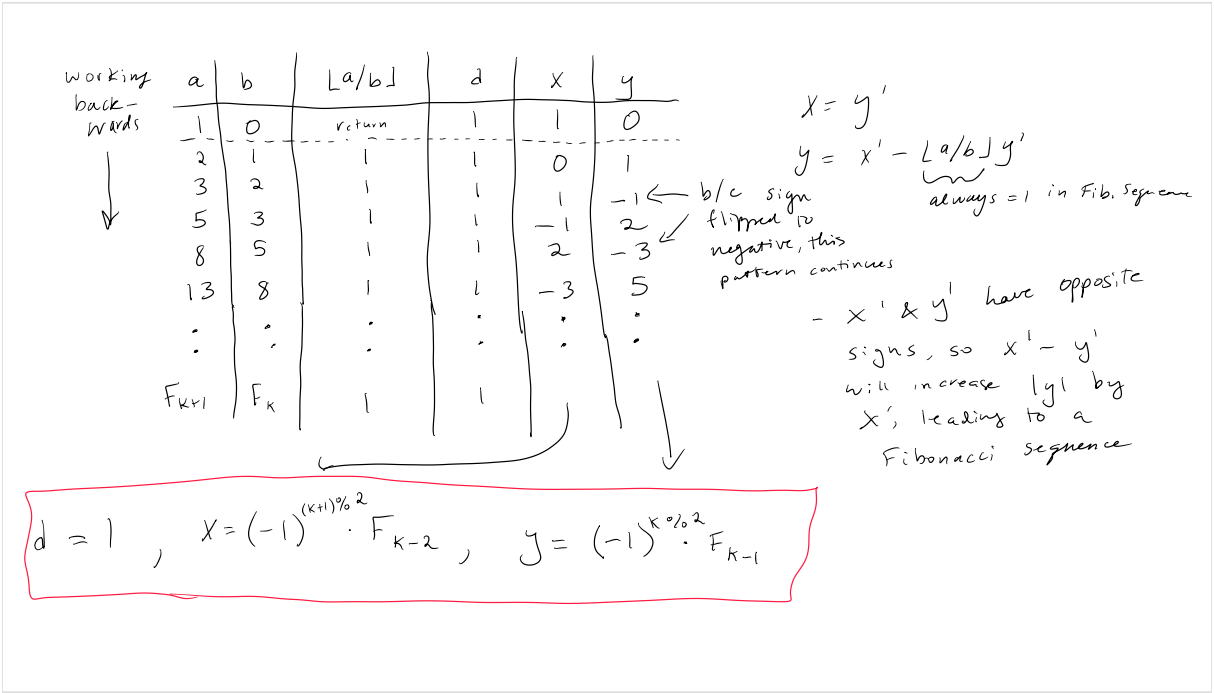
Following Euclid's method of finding the gcd, we see that **a + kn mod n** simplifies down to **a mod n**, because **kn** is 0 **mod n**. In other words, **a** + **kn** is equivalent to **a** (mod n).

4



6

Since the sequence of Fibonacci numbers starts with 0, 1, 1 is the gcd of any adjacent Fibonacci numbers. So, the first d', x', y' triple would be d' = 1, X '= 1, y' = 0. Interestingly, x and y follow a sort of Fibonacci sequence as well, alternating positive and negative



Because floor(a/ b) is always one for the fibonacci sequence, the x and y values are a result of summing up previous x and y values, forming another Fibonacci sequence, which is 3 behind for **a** and 2 behind for **b.** Assuming F_1 is the first row in the table, x is negative on the even indexes and y is negative on the odd indexes, hence (-1) ^ k +1 % 2 and (-1) ^ k % 2

31.3

1

$(\mathbb{Z}_4, +_4)$:

$\{0, 1, 2, 3\}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_5^*, \cdot_5)$

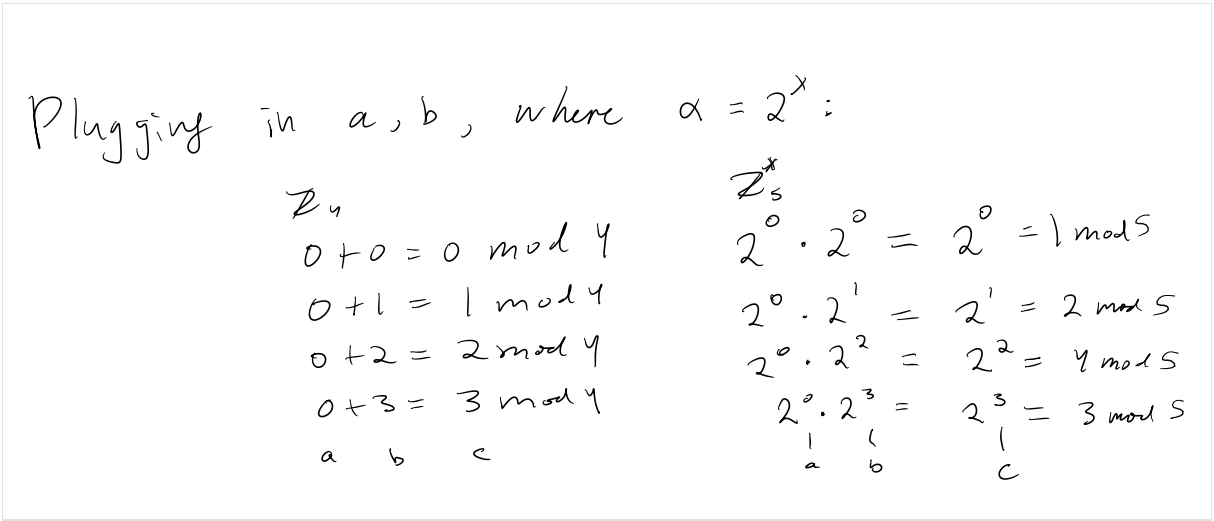
$\{1, 2, 3, 4\}$

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

We need to find the order of Z* and we do this by finding the first instance of the identity, 1. Evidently, the order is 2, since 2, 3 is the first inverse pair. Where we look at the abelian group for 2^x mod 5 we see it is cyclic:

2^x_5	2^0	2^1	2^2	2^3	2^4
	1	2	4	3	1

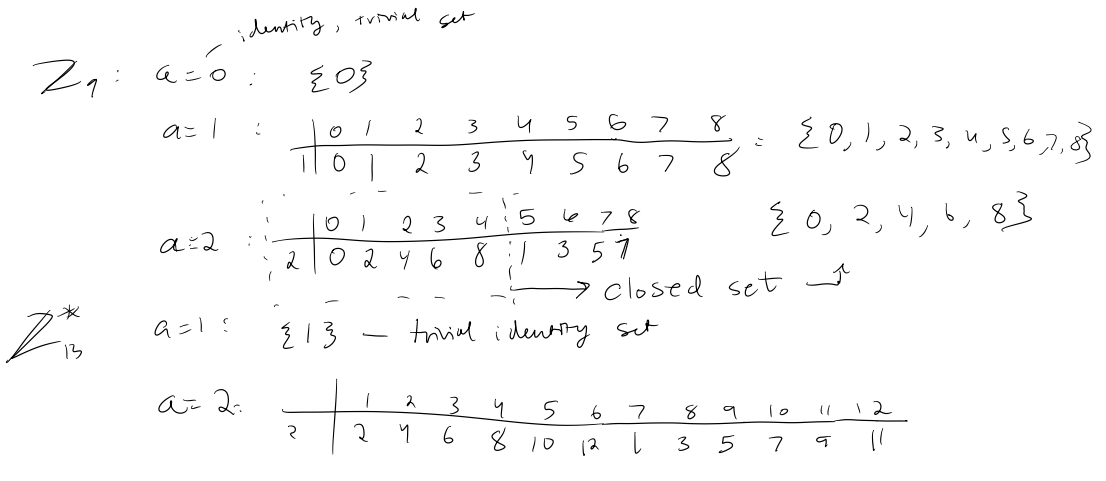
So, this is a good candidate for alpha



Assuming that the a, b, and c refer to the same number on both sides, x= 2 ^ x and these groups are indeed isomorphic.

2

To generate subgroups, multiply a by each member of Z until the end of the cycle mod n

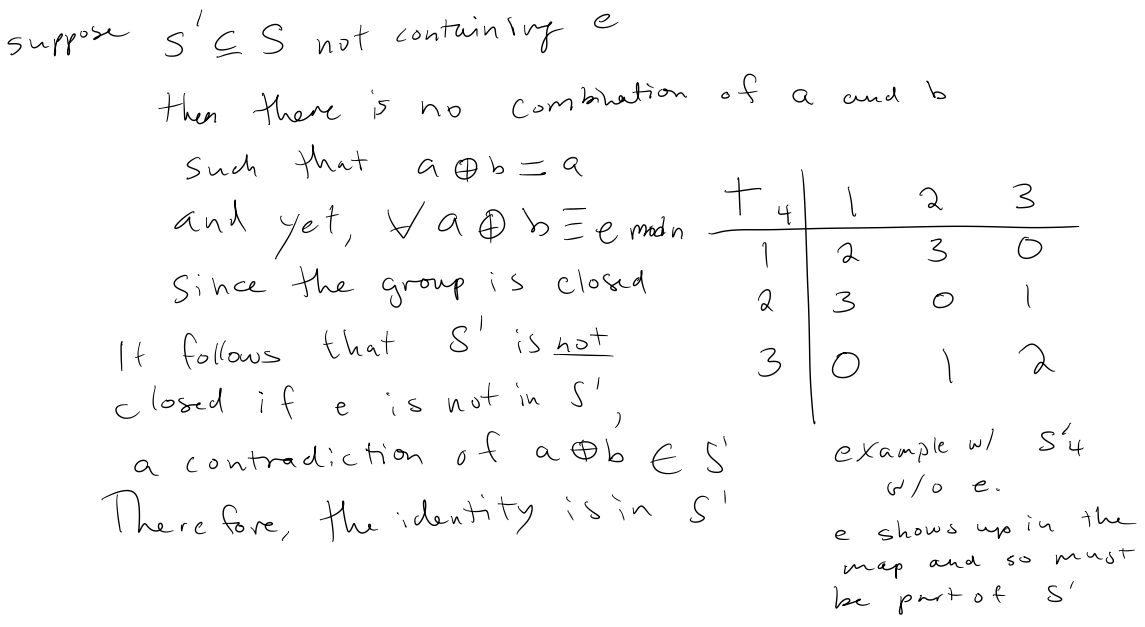


12

↳ {1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12}

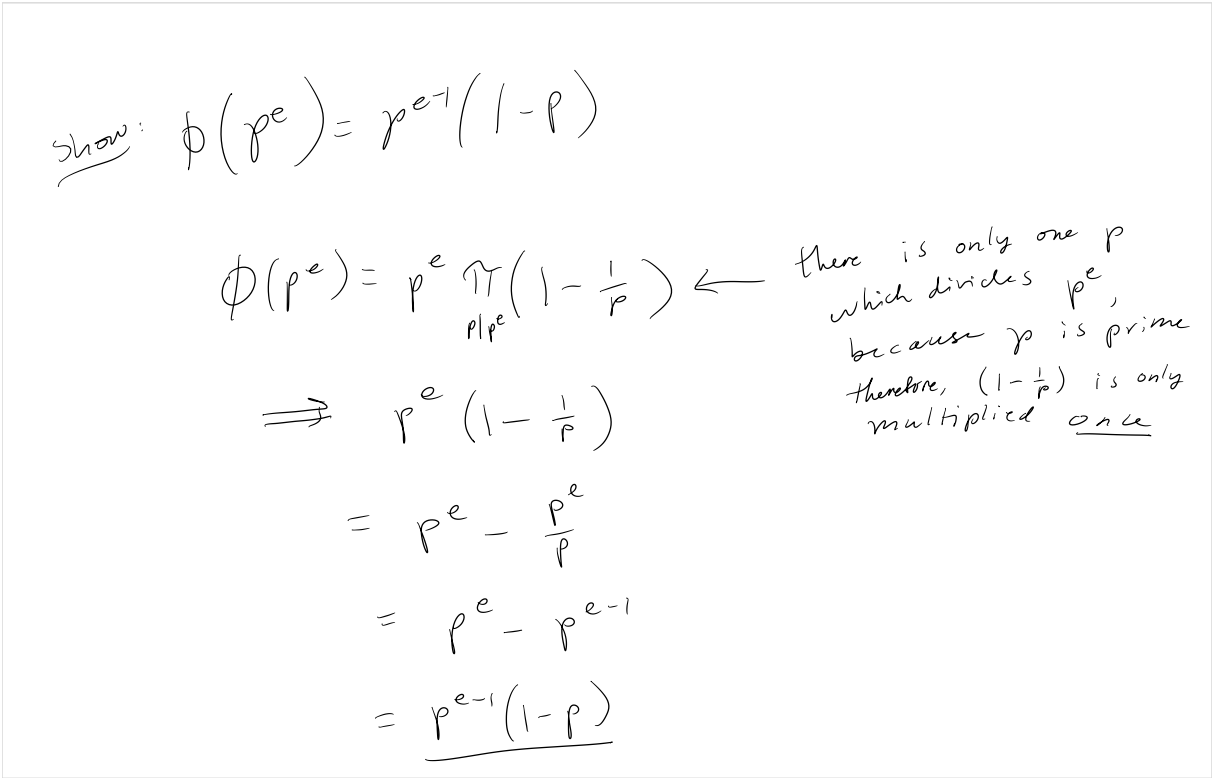
3

For S' to be a subgroup, it must be closed under the binary operation. Since that is part of the presupposition of the theorem, the first requirement is met. Secondly, there needs to be an identity. This also follows from the fact that s' is closed, because if it did not contain the identity, then it wouldn't be closed



The last requirement is that the operations must be associative. If S is an Abelian group, then the binary operations in S are associative. Since S' is a subset of S, it follows that S' meets this requirement.

4



5

If Z* is closed under a binary operation, then performing that operation against all members

of the group for any a∋Z* will yield numbers within that group.

How can we be sure the resulting group is distinct?

By the property of Abelian groups that the map of the binary operation for It has no zero divisors. Therefore, every distinct number mapped by f(x) yields a distinct number mod n.

It follows from the fact that the group is closed and only yields distinct values from binary operations that f(x) will result in a permutation of Z*