MATH 335 Lecture 6

Chris Camano: ccamano@sfsu.edu

September 8, 2022

Let m and n be two positive integers that are relativley prime, this is to say that gcd(m,n)=1
Then :

$$\phi(mn) = \phi(m)\phi(n)$$

Proof. let:

$$A = \{1 \leq a \leq m : gcd(a,n) = 1\}$$

This is equivilant to saying the set of all integers from 1 to m that are relativley prime to m. The cardinality of A is equal to $\phi(m)$

$$B = \{1 \leq b \leq n : gcd(b,n) = 1\}$$

This is equivilant to saying the set of all integers from 1 to n that are relativley prime to n. The cardinality of B is equal to $\phi(n)$

$$C = \{1 \leq c \leq mn : gcd(c,mn) = 1\}$$

This is equivilant to saying the set of all integers from 1 to mn that are relativley prime to mn. The cardinality of C is equal to $\phi(mn)$
Observe the following:

$$|AxB| = |\{(a,b) : a \in A, b \in B\}| = |A||B| = \phi(m)\phi(n)$$

if we can then show that the cardinality of C is equal to the cardinality of the cartesian product then we have proven equivilancy. To prove that two sets have the same cardinality we typically prove that there is a bijection Ψ between the two sets.

If we can show $\exists \quad \Psi : C \mapsto AxB$ then we prove the original problem.

Given integers c and m we know that we can divide one by the other and obtain a remainder by the divison algorithm. such that

$$c = qm + r \quad 0 \leq r < m$$

denote r as $\bar{c_m}$
for $c \in C$

$$\Psi(c) = (\bar{c_m}, \bar{c_n})$$

$0 \leq \bar{c_m} < m$ by definition of remainder , however $\bar{c_m}$ cannot be equal to 0 by the definition of set c so : $1 \leq \bar{c_m} < m$ also $1 \leq \bar{c_n} < n$. We now need to show that $gcd(\bar{c_m}), m = 1, gcd(\bar{c_n}, n = 1))$ to prove they belong to A and B.

if $gcd(\bar{c_m}, = d > 1$ then $d|\bar{c_m}$ and $d|m$ therefore $d|c$. Since d divides m and d divides c then this would imply that gcd(c,m)¿1, but this implies gcd(c,mn)=1 which contradicts the set that c was chosen from, that being C which states that gcd must be equal to 1; We can extend this to n and $\bar{c_n}$ with a symmetric proof.

Injectivity
We now demonstrate that $\Psi(c)$ is injective suppose$c_q, c_2 \in C$ and $\Psi(c_1) = \Psi(c_2)$ we then need to conclude that this implies that c_1 and $c2$ are the same. In other words we need to prove that for each element in the domain there exists a uniuq element in the codomain.

$$\Psi(c_1) = (\bar{c_{1,m}}, \bar{c_{1,n}}) \quad \Psi(c_2) = (\bar{c_{2,m}}, \bar{c_{2,n}})$$
$$c_1 = mq_1 + \bar{c_{1,m}} \quad c_2 = mq_2 + \bar{c_{2,m}}$$

we need to now show that c_1 and c_2 are the same. Let us start by subtracting these two expressions: When assuming that the remainders are the same this gives

$$c_1 - c_2 = m(q_1 - q_2)$$
$$m|c_1 - c_2$$

likewise:

$$c_1 - c_2 = n(q_1^* - q_2^*)$$
$$n|c_1 - c_2$$

By definition m and n are relativley prime. Since gcd(m,n)=1 then $mn|c_1 - c_2$ By construction we have:

$$1 \leq c_1 < mn \quad 1 \leq c_2 < mn$$

The only time that this is true is if the difference is equal to zero since otherwise the difference of the two chosen c will be less than mn. therefore we have proven injectivity and that $c_1 = c_2$

Surjectivity
To show that Ψ is surjective we start with an element in the codomain and create a corresponding element in the domain. Take:

$$(a,b) \in AB \quad 1 \leq a \leq m, gcd(a,m) = 1 \quad 1 \leq b \leq mgcd(b,m) = 1$$

We must now construct $c \in C, q \leq c \leq mn, gcd(c, mn = 1)$
Such that

$$\Psi(c) = (a,b)$$

Since gcd(m,n)=1 then we can express 1 as a linear combination of m,n as such:

$$\exists \quad t, u \in \mathbb{Z} : mu + nt = 1$$

What would the word munt mean ? mean runt?
Let z= an(t)+bmu. This is some linear combination using the coefficients of the gcd of c and the integers a,b.

Conjecture: z mod m =a .

$$z = a(1 - mu) + bmu = (bu - au)m + a$$

so we have $\bar{z_m} = a$ and $\bar{z_n} = b$, however we now need to determine the size of z.

Now we let c to be equal to the remainder we get when we divide z by mn. so:

$$0 \leq c < mn$$

$$z = qmn + c$$

since z mod m is equal to a then if divide c by m we get remainder a since qmn must be equal to zero which implies that c is the term needed to satisfy $\bar{z_m} = a$ likewise for b Finally we need to show tha c is in c the only criterion missing is that gcd(c,mn)=1. If we can prove that gcd(z,mn)=1 then we can show that gcd(c,mn)=1 by the property that gcd(a,b)=gcd(b,r) when a=bq+r,

To show that consider the following:

$$gcd(a,m) = gcd(c,m) = 1 \quad gcd(b,n) = gcd(c,n) = 1 \therefore gcd(c, mn = 1)$$

And we have proven surjectivity

$\square$

Equivilance realtions and equivilance classes

An equivilance relation on a set X is a subset R as follows:

$$R \subset X \times X$$

such that

1. $(x,x) \in R \quad \forall x \in X$ (Reflexivity)
2. $(x,y) \in R \iff (y,x) \in R$ (Symmetric)
3. if $(x,y) \in R$ and $(y,z) \in R$ then $(x,z) \in R$ (Transitivity)

Instead of denoting $(x,y) \in R$ we write $x\ y$. with this new notation:

1. x∼ $xx \iff$ y
3. xand ythen x