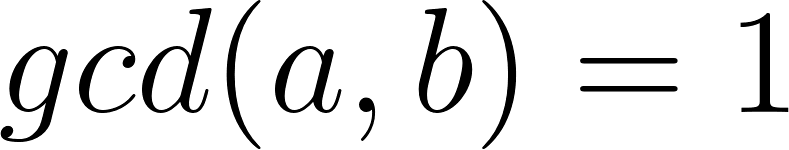
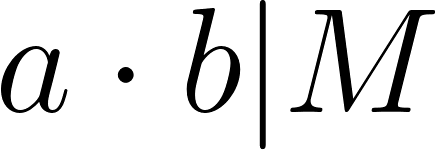
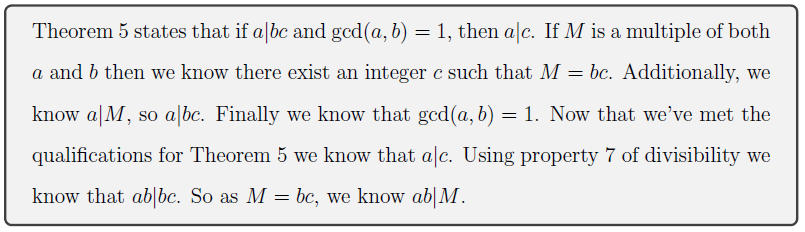
**Homework 2**

**Instructions:** Do as many of the problems as you like, but make sure to complete at least **three**. Then the whole class will create a solution jointly (write below, or create a separate file; either is OK). One problem can have multiple solutions, so if your solution is different than the one already posted and you’d like to share yours with others, feel free to add yours. Make sure to separate different solutions to minimize confusion.

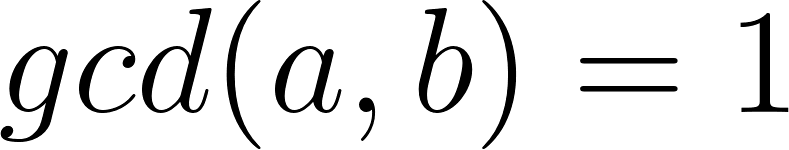
1. Show that if *a* and *b* divide *M* and [](https://www.codecogs.com/eqnedit.php?latex=gcd(a%2Cb)%3D1#0), then [](https://www.codecogs.com/eqnedit.php?latex=a%5Ccdot%20b%20%7C%20M#0).



Proof: Since M| b and M|a we have that, for some integers n and p

M = ap

M= bn.

Further, [](https://www.codecogs.com/eqnedit.php?latex=gcd(a%2Cb)%3D1#0), so there exist integers x, y such that ax+by = 1.

Multiplying both sides by M,

M = Max + Mby

= (bn)ax + (ap)by

= ab(nx + py).

We have shown that if a|M and b|M and gcd(a,b)=1, then ab|M.

1. a. Prove that [](https://www.codecogs.com/eqnedit.php?latex=%5Csqrt%7B3%7D#0) is irrational.

We will use a proof by contradiction. Assume where (so the fraction is in simplest form). Then

and

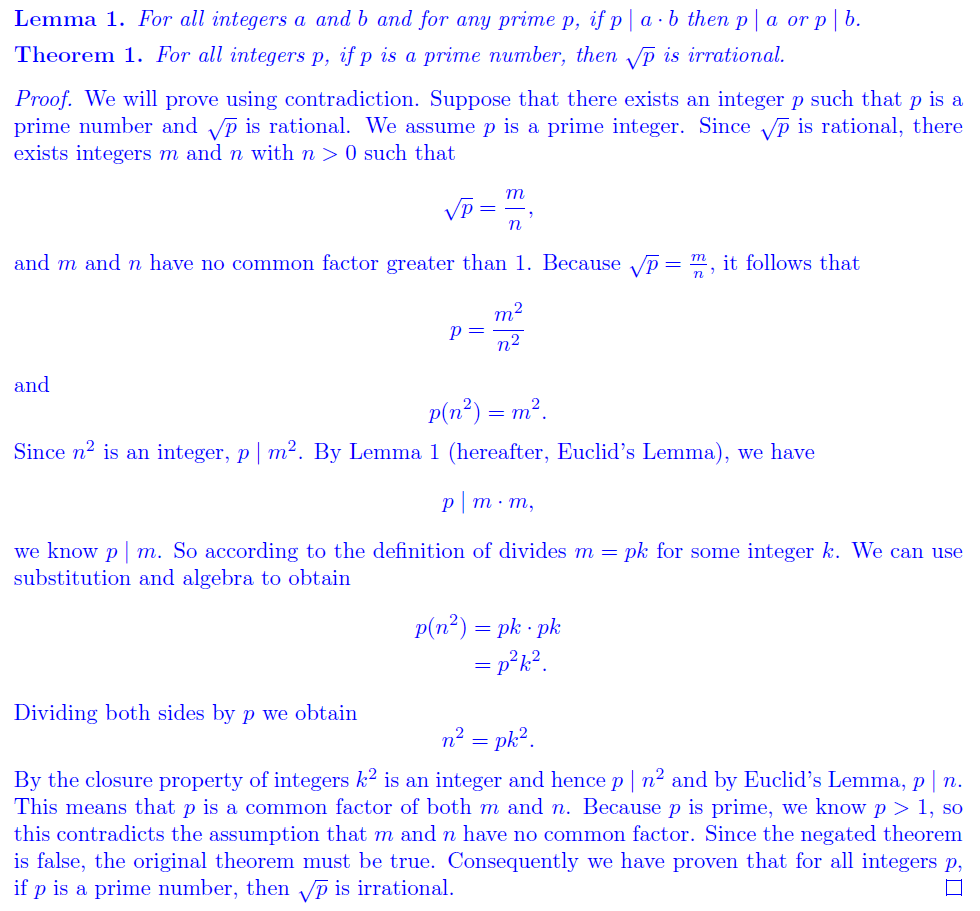
Note that which we claim implies . The proof is by contradiction. Assume 3 does not divide Then or Thus, or which contradicts

Thus for some Then

so thus

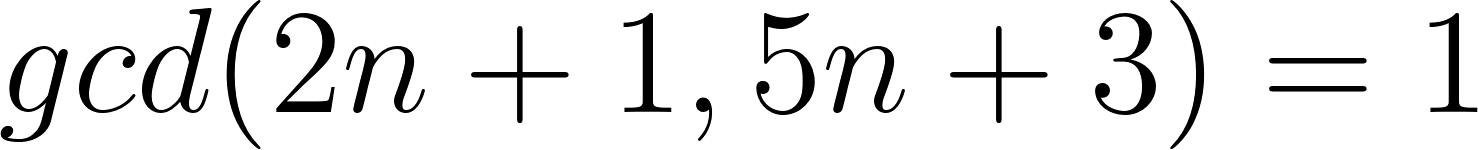
Using the previous proof,

But then and contradicting our assumption that



b. You likely also saw that [](https://www.codecogs.com/eqnedit.php?latex=%5Csqrt%7B2%7D#0) is irrational in MTH 210. So, it feels like we can make a general statement. Come up with at least two different generalizations of the statement “[](https://www.codecogs.com/eqnedit.php?latex=%5Csqrt%7B2%7D#0) is irrational.” No need to write full proofs, but give some good reasonings for why the generalizations would be true.

* is irrational for prime.
* is irrational for all where
* is irrational for odd.
* is irrational for square-free
* is irrational for odd.
* is irrational for prime and *r* odd.

1. Show that [](https://www.codecogs.com/eqnedit.php?latex=gcd(2n%2B1%2C5n%2B3)%3D1#0) for every *n*.

Applying the Euclidean algorithm we see:

Continuing with the algorithm in the next step with as the dividend and as the divisor, we find

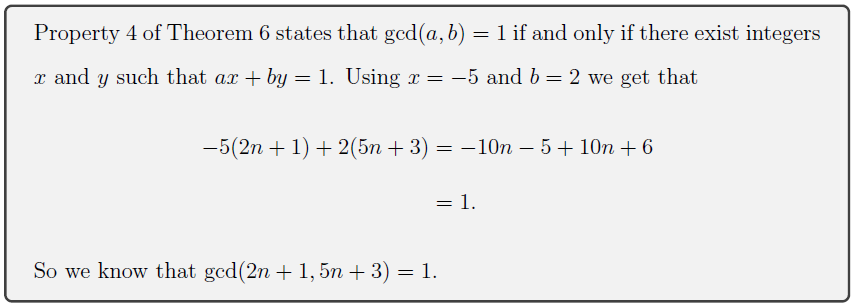
If , we are done with the algorithm, with being the last non-zero remainder as the gcd. If then we continue the algorithm one more step:

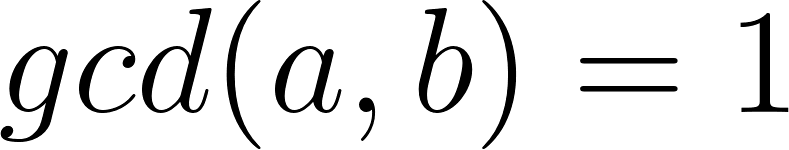
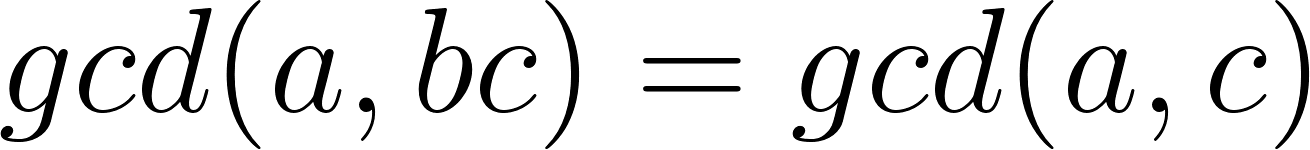
Once we reach this step, in the next step, the remainder will be 0 and hence 1, the last non-zero remainder will be the gcd.

If divides and , then dividesSimilarly,divides the difference between and , which is 1. Therefore, which means.

If we can show that there exist integers *x* and *y* so that the proof will be complete. By rearranging, we find

Since *n* is arbitrary, we need and We can solve this system of equations by substitution or by elimination to find as a solution. Therefore,



1. Show that if [](https://www.codecogs.com/eqnedit.php?latex=gcd(a%2Cb)%3D1#0), then [](https://www.codecogs.com/eqnedit.php?latex=gcd(a%2Cbc)%3Dgcd(a%2Cc)#0).

We will show the equality by showing that and if and only if and Because then the factors are the same, and so the largest factors are also the same.

The forward direction is obvious. So assume and We need to show Since and as well. So, by Theorem 5 of the handout, since and which is what we wanted to show.

Let gcd(a , bc) = d, which means there exist integers x\_1 and y\_1 such that ax\_1 + bcy\_1 = d. (1)

Let gcd(a,c)=f. Then f divides the left hand side of (1) and hence f|d.

Now we show d|f. Since gcd(a,b)=1, there exists integers x and y such that ax+by = 1. Multiplying both sides by f gives

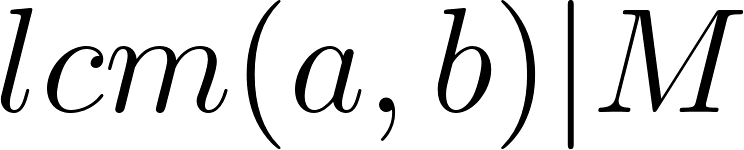
fax + fby = f (2)

Now f=gcd(a,c) is a linear combination of a and c, say ax\_2+cy\_2=f. By substituting that in place of the second f in equation (2) and by rearranging, we find

fax + (ax\_2 + cy\_2)by = f

a(fx + x\_2) + bc(yy\_2) = f.

Now we see that f is a linear combination of a and bc, and, thus, d|f. Since d|f and f|d, d=**±** f, but gcd’s are only positive integers, so we conclude that d = f.

1. Prove that if *M* is a multiple of *a* and *b*, then [](https://www.codecogs.com/eqnedit.php?latex=lcm(a%2Cb)%7CM#0). (Hint: One way to do this uses Division algorithm and contradiction. Another way uses the relationship between lcm and gcd, and Euclid’s lemma. There are possibly other ways too.) \*\*\*Hindsight: This is what happens when I generalize a definition but then steal statements from other sources that only apply to the restricted definition. This claim is true only for both *a* and *b* positive. If one of them is zero, *M* will have to be 0, along with lcm, leading to 0 | 0 claim, which we did not define. Actually, it looks like I stole this statement from the same source that I got the definition from. Ah well. They weren’t too careful either.

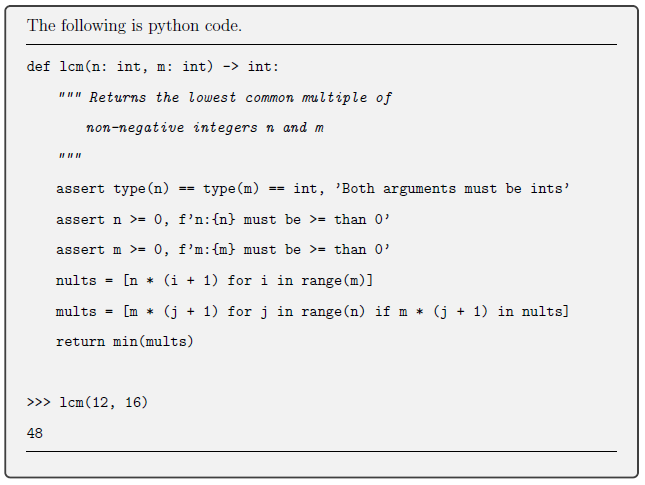
Suppose lcm does not divide *M.* Then by the Division Algorithm, there exist and such that Then *a* divides *r* because it divides both *M* and lcm. Similarly, *b* divides *r.* This means *r*  is a common multiple of *a* and *b,* and hence But this contradicts that *r* is a reminder after dividing by

Let Then from we have Since *a* divides *M,*  for some *k.* Then Since *b* divides *M,*  divides But so by Theorem 5 (Not Euclid’s lemma, oops, sorry, mixed up the two), divides *k,* so say Then Since this proves that divides *M.*

1. (For those who have completed MTH 350) Look up the definitions of a prime element in a commutative ring, and an irreducible element in an integral domain. Since these words are different, the terms should not imply each other. Figure out in which cases one implies the other. Briefly summarize.

No solution provided for this problem. So here’s my sloppy summary.   
Primes in a general commutative ring are essentially defined by generalizing the property in Euclid’s lemma. In principal ideal domains, we can think of prime elements corresponding to prime ideals and can have a bunch of the number theory results generalize to these domains, such as the Fundamental Theorem of Arithmetic. Irreducibility generalizes the definition of prime as not being able to factor into other non-unit numbers. We can define this concept in an integral domain. In a unique factorization domain prime is equivalent to being irreducible.

1. Write a code to find lcm of any two given positive integers. Then use lcm to find the gcd of the two integers. \*\*\*Note: The way we defined lcm (a bit sloppily, I admit), for any non-zero *a.* We need to consider that in our lcm code.



* def lcm(a, b):
  + if a<0 or b<0:
    - return lcm(abs(a), abs(b))
  + if a == 0 or b == 0:
    - return 0
  + else:
    - larger = max(a, b)
    - multiple = larger
    - while not (m % a == 0 and m % b == 0):
      * multiple += larger
    - return multiple
* def gcd(a, b):
  + if a == 0 or b == 0:
    - return 0
  + else: return a\*b/lcm(a,b)

def lcm(a,b):

if b==0:

if a==0:

return('undefined')

else: return 0

else:

if a==0: return 0

else:

k=1

b=abs(b)

while b\*k%a!=0:

k=k+1

return b\*k

def gcd(a,b):

if b==0:  
 if a==0:  
 return(‘undefined’)  
 else: return 0

else:

if a==0: return 0

else: return a\*b/lcm(a,b)