Discrete Mathematics
Exercise sheet 6
Solutions for exploratory & additional exercises
April 2021

Exploratory problems:

Problem 1.

A number n ∈Z is divisible by m∈Z if there exists k∈Z such that:

$$mk = n$$

If such a k exists, then we say that "m divides n" and denote this m|n

a)

For all a∈Z: a*1 = a

Hence for all a∈Z a|a

b)

For all a∈Z: 1*a = a

Hence for all a∈Z 1|a

c)

False.

For example there is no k ∈Z such that

2*k = 1

And hence the statement does not hold for all a∈Z.

Infact it only holds for a = -1 and a = 1.

d)

False.

For example there is no k ∈Z such that

0*k = 1

And hence the statement does not hold for all a∈Z.

Under the definition of divisibility we are using it only holds for a = 0.

e)

For all a∈Z: a*0 = 0

Hence for all a∈Z a|0

f)

False.

For example let a = 1 and b = 5. Now

a*5 = b and hence a|b

but there is no k ∈Z such that

5*k = 1

And hence the statement does not hold for all a, b∈Z.

Infact it only holds for a and b such that |a| = |b|.

g)

If a|b and a|c then

a*n = b and a*m = c therefore

a*n + a*m = b + c = a*(n + m) and hence a k exists such that

ak = b + c and hence

a|b+c

h)

If a|b and b|c then

a*n = b and b*m = c and hence

(a*n)*m = c and hence a k exists such that

a*k = c

and therefore

a|c

i)

if a|b and b|a then

$$an = b \wedge bm = a \leftrightarrow bmn = b \leftrightarrow mn = 1 \leftrightarrow n = m = 1 \vee n = m = -1 \rightarrow a = b \vee a = -b$$

Problem 2.

The divisors of 98 are 1, 2, 7, 14 and 98.

The divisors of 105 are 1, 3, 5, 7, 15, 21, 35 and 105

The gcd is 7.

Problem 3.

a)

Let $c \in Z$ be such that c|a and c|b and therefore there exists some k, $m \in Z$ such that ck = a and cm=b. Then

$$b - na = cm - nck = c(m - nk)$$

And hence c|b-na for all common divisors of b and a.

b)

It should be obvious that the greatest common divisor of 2 numbers depends only upon the numbers, and therefore gcd(2331, 2037) = gcd(2037, 2331).

Now using part a we know that every common divisor of 2331 and 2037 is also a divisor of 2331-2037, and hence the greatest common divisor of 2331 and 2037 is also a divisor of 2331-2037, and hence also the greatest common divisor of 2037 and 2331-2037

Therefore gcd(2331,2037) = gcd(2037,2331-2037) = gcd(2037,294)

c)

gcd(2331, 2037) = gcd(2037, 294) = gcd(294, 2037-6*294) = gcd(273, 294) =

gcd(273, 21) = gcd(21, 273 – 13*21) = gcd(21, 0)

d)

By the result in problem 1 part a) we know that every integer divides itself, and hence it should be clear that the greatest divisor of any non-zero integer is itself, since if b > a and a is not 0 there can be no integer n such that bn = a.

By the result in problem 1 part e) we know that every integer divides 0.

And hence all divisors of any integer a are common divisors of a and 0.

Hence the greatest common divisor of a > 0 and 0 must be the greatest divisor of a, which is a. In otherwords gcd(a, 0) = a

e)

By part c we know gcd(2331,2037) = gcd(21, 0)

And by part d we know gcd(21,0) = 21

Problem 4

a)

If we add 2 to the value of x we have the following function

3*3 -2y = 1 in which case y clearly needs to be 4 since 9 – 8 = 1, and hence if we were to add 2 to x we must add 3 to y.

This should be obvious considering that the coefficient of x is 3 and the coefficient of y is -2.

b)

All the integer solutions are of the form

x = 2n + 1, y = 3n + 1, n∈Z

3*(2n + 1) – 2*(3n + 1) = 6n + 3 – 6n -2 = 1 for all n∈Z

Additional problems:

Problem 1.

Base case:

$13^0 - 6^0 = 1 - 1 = 0 = 7*0$

$13^1 - 6^1 = 13 - 6 = 7 = 7*1$

Since it is true for some n lets assume it true for n and show that it holds for n + 1

$13^n - 6^n = 7*m$

$13^{n+1} - 6^{n+1} = 13*13^n - 6*6^n = (6 + 7)* 13^n - 6*6^n = 7*13^n + 6*13^n - 6*6^n$

$= 7*13^n + 6*(13^n - 6^n) = 7*13^n + 6*7*m = 7*(13^n + 6*m)$

Since a k = $(13^n + 6*m)$ exists such that $7*k = 13^{n+1} - 6^{n+1}$ we conclude $7|13^{n+1} - 6^{n+1}$

And therefore by induction $7|13^n - 6^n$ for all n∈Z

Problem 2.

a)

$$3^3 \equiv 27 \ \equiv 1 \, mod \, 13$$

$$3^{19} \equiv 3 * (3^3)^6 \ \equiv \ 3 * \ 1^6 \equiv \ 3 \, mod \, 13$$

b)

$$4^3 \equiv 64 \equiv 10 \, mod \, 27$$

$$(10)^3 \equiv 1000 \ \equiv 1 \, mod \, 27$$

$$4^{12} \equiv (10)^3 * 10 \equiv 10 \, mod \, 27$$

c)

$$12 \ \equiv \ -3 \, mod \, 15$$

$$12^{27} \equiv (((-3)^3)^3)^3 \ \equiv ((-27)^3)^3 \equiv ((3)^3)^3 \equiv (27)^3 \equiv (12)^3 \ \equiv (-3)^3 \ \equiv \ -27 \ \equiv \ 3 \, mod \, 15$$

d)

$146^2 \equiv 1$ mod 21

Problem 3.

a)

If n|a-b then we say a ≡ b mod n

Since a ≡ b mod n by definition n|a – b and hence nk = a – b for some k∈Z and therefore

$a^2 - b^2 = (a - b)(a + b) = nk(a + b)$ from which we see that n is a factor of $a^2 - b^2$, and hence n| $a^2 - b^2$ and hence $a^2 \equiv b^2$ mod n.

b)

9 mod 7 = 2 and 16 mod 7 = 2 therefore 9 ≡ 16 mod 7

However 3 mod 7 = 3 and 4 mod 7 = 4.

Therefore this is proven false by counterexample.

Problem 4.

$$n^8 - 2n^6 + n^4 = n^4(n^4 - 2n^2 + 1) = n^4(n^2 - 1)^2 = n^4((n+1)(n-1))^2$$
$$= n^2(n(n+1)(n-1))^2$$

Lets denote $n^8 - 2n^6 + n^4$ = k

Now we observe that 3 consecutive numbers are factors of (n(n+1)(n-1)) and given 3 consecutive numbers 1 is always divisible by 3, and hence (n(n+1)(n-1)) is divisible by 3. Hence $(n(n+1)(n-1))^2$ is divisible by $3^2 = 9$ and since it is a factor of k , k too is divisible by 9.

Further we observe that n^4 is a factor k, and since any even number is divisible by 2 if n were to be even it would be divisible by 2, and hence n^4 would be divisible by $2^4 = 16$ and since it is a factor of k, k too would be divisible by 16. If n were odd however we observe that n + 1 and n – 1 would both be even, and hence their product would be divisible by 4, and hence $((n + 1)(n - 1))^2$ would be divisible by 16, and since it is a factor of k, k too would be divisible by 16.

Therefore regardless of how n is chosen k has 9 and 16 as its factors, and hence has their product as its factor, and 9*16 = 144.

Therefore regardless of how n is chosen k is divisible by 144.

Problem 5.

First break the number into its prime factors, and then observe that if p is a prime then 1/p of all numbers are divisible by it, and then if p is a divisor of x then 1/p of the numbers less than x are also divisible by p and hence not relatively prime to x. And therefore if x can be factorized by primes p_1 ... p_n then the number of numbers less than x that are relatively prime to it can be calculated by removing all the numbers that have the same prime factors in the following manner:

$\varphi(x) = x*(1- 1/p_1)*...*(1-1/p_n)$

a)

$\varphi(200) = \varphi(5^2\ 2^3) = 200*(1-1/2)*(1-1/5) = 200*0.5*0.8 = 80$

b)

φ(121) = 110

c)

φ(635) = 504

d)

φ(1010) = 400

e)

φ(2021) = 1932

Problem 6.

Let there be a sequence of 5 numbers a, a+1, a+2, a+3, a+4 where a is an odd prime number.

This means a+1 and a+3 must be even, while a+2 and a+4 are odd.

Every third number is divisible by 3. Since a is prime a is either 3, or not divisible by 3.

If a is 3, then a + 2 = 5, and 2 + 4 = 7 which is a triplet prime.

If a is not 3, and since a is an odd prime number it is therefore also not divisible by 3, then either a + 1 is divisible by 3, in which case a + 4 = a + 1 + 3 is also divisible by 3, which means a+4 is not a prime and hence we do not have a triplet prime, or a + 2 is divisible by 3 in which case we also do not have a triplet prime.

Therefore unless a is 3 a triplet prime is not possible, and hence the only triplet prime is 3, 5 and 7.

Problem 7.

a)

Each fibonacci number is the sum of the two previous fibonacci numbers. Let f_n and f_{n-1} be fibonacci numbers then $f_n = f_{n-1} + f_{n-2}$

Recall that gcd(a+b, b) = gcd(a, b) and observe that since $f_n = f_{n-1} + f_{n-2}$ it must be that:

$\gcd(f_n, f_{n-1}) = \gcd(f_{n-1} + f_{n-2}, f_{n-1}) = \gcd(f_{n-1}, f_{n-2})$ and since $f_{n-1} = f_{n-2} + f_{n-3}$ we can repeat this n-2 times until we reach $\gcd(f_2, f_1) = \gcd(1, 1) = 1$ and hence the gcd of any 2 consecutive fibonacci numbers is 1.

b)

As shown in part a) it takes n – 2 steps.

c)

Let us prove by induction that F_n and F_{n-1} are the smallest numbers for which euclids algorithm takes n-2 steps.

base case:

Let n = 3 then f_n = 2 and f_{n-1} = 1 and a = b = 1, and it takes euclid 1 step to compute for f_n and f_{n-1} while it takes 0 steps to compute for a = b.

Step:

Let us assume that for some n F_n and F_{n-1} are the smallest numbers a > b for which euclids algorithm takes n-2 steps.

Now let us consider n + 1. Let c > d be integers for which euclids algorithm takes n – 1 steps. Then when we take the first step of the algorithm we have gcd(c, d) = gcd(d, c-d) and we know that gcd(d, c-d) takes n-2 steps, and furthermore we know d and c-d must be the smallest integers taking n-2 steps, since c and d were the smallest integers taking n-1 steps. But since we also know F_n and F_{n-1} are the smallest numbers a > b for which euclids algorithm takes n-2 steps we conclude that F_n = d and F_{n-1} = c-d and:

$F_{n+1} = F_n + F_{n-1} = d + c - d = c$

And therefore the smallest integers requiring n-1 steps are F_{n+1} and F_n and hence we have proven by induction that for all n the smallest integers for which euclids algorithm requires n-2 steps is F_n and F_{n-1}

Therefore also for any integest a, b such that $b \leq a < F_n$ euclids algorithm takes more steps to compute gcd(F_n, F_{n-1}) than gcd(a, b).