Ve203 Discrete Mathematics (Fall 2022)

Assignment 4

Date Due: See canvas
This assignment has a total of **(28 points)**.
Note: Unless specified otherwise, you must show the details of your work via logical reasoning for each exercise. Simply writing a final result (whether correct or not) will receive **0 point**. **Explain** (briefly) if you claim something is trivial or straightforward. Provide a counterexample if you are trying to disprove something. It is **NOT OK** to write something like "how do we know that blahblahblah is even true…" In addition, be careful that some problems might be ill-defined.

Exercise 4.1 (2 pts) Given $a, b, c \in \mathbb{N} \setminus \{0\}$, show that $a \mid bc$ iff $\left.\dfrac{a}{\gcd(a,b)}\,\right|\, c$.

Exercise 4.2 (4 pts) Show that

(i) (2 pts) There exist infinitely many primes of the form $3n+2$, $n \in \mathbb{N}$.

(ii) (2 pts) There exist infinitely many primes of the form $6n+5$, $n \in \mathbb{N}$.

Exercise 4.3 (4 pts) The numbers $F_n = 2^{2^n} + 1$ are called the *Fermat numbers*.

(i) (2 pts) Show that $\gcd(F_n, F_{n+1}) = 1$, $n \in \mathbb{N}$.

(ii) (2 pts) Use (i) to show that there are infinitely many primes.

(These results are from a letter of Christian Goldbach to Leonhard Euler written in 1730.)

Exercise 4.4 (4 pts) Find all $x, y \in \mathbb{Z}$ such that

(a) $56x + 72y = 39$ (b) $84x - 439y = 156$

Exercise 4.5 (2 pts) Given a group $G = (S, \cdot)$, where S is the underlying set, and $\cdot$ is the groups law. Define a new function

$$\boxtimes : S \times S \to S$$
$$(a, b) \mapsto a \boxtimes b := b \cdot a$$

Show that $(S, \boxtimes)$ is a group.

Exercise 4.6 (4 pts) For $n \in \mathbb{N} \setminus \{0\}$, consider the *greatest common divisor matrix* $S = (s_{ij}) \in M_{n\times n}(\mathbb{N})$ with $s_{ij} = \gcd(i, j)$.

(i) (2 pts) Show that $\det S = \prod_{j=1}^{n} \varphi(j)$ where φ is the Euler totient function.

(ii) (2 pts) Show that S is positive definite, i.e., $x^\top A x > 0$ for all nonzero $x \in \mathbb{R}^n$.

Exercise 4.7 (2 pts) Consider a set $S = \{a, b, c, d, e, f, g\}$ with the following multiplication table for $\cdot : S \times S \to S$,

$\cdot$	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	c	a	e	d	g	f
c	c	a	b	f	g	d	e
d	d	e	f	g	b	c	a
e	e	d	g	b	f	a	c
f	f	g	d	c	a	e	b
g	g	f	e	a	c	b	d

Is $(S, \cdot)$ a group? Explain.

Exercise 4.8 (4 pts) Given a group G, show that

(i) (2 pts) If the order of every nonidentity element of G is 2, then G is Abelian.

(ii) (2 pts) If $a, b \in G$, then $|ab| = |ba|$, i.e., ab and ba have the same order.

Exercise 4.9 (2 pts) For integer $n > 1$, let $\omega \in \mathbb{C}$ be a *primitive nth root of unity*, i.e., $\omega^n = 1$ and $\omega^k \neq 1$ for $1 \le k \le n-1$, show that

$$\sum_{k=0}^{n-1} \omega^{km} = \begin{cases} n, & n \mid m \\ 0, & \text{otherwise} \end{cases}$$

Exrercise 4.1

$a \mid bc \Leftrightarrow (\exists k_1 \in \mathbb{Z})(bc = ak_1)$

suppose $d = \gcd(a, b)$

$a = a_1 d$, $b = b_1 d$.

$\gcd(a_1, b_1) = 1$

$a \mid bc \Rightarrow a_1 \mid b_1 c \Rightarrow a_1 \mid c \Rightarrow \frac{a}{\gcd(a,b)} \mid c$

If $\frac{a}{\gcd(a,b)} \mid c \Rightarrow \frac{a_1 d}{d} \mid c$

$\Rightarrow a_1 \mid c$.

$\Rightarrow a_1 \mid b_1 c$

$\Rightarrow a_1 d \mid b_1 d c$

$\Rightarrow a \mid bc$

Therefore, the statement is proved.

Exrercise 4.2

(i) We prove this theorem by proof of contradiction. let $p_1 \cdots p_n$ be a list of finite prime numbers of the form $3n+2$. Let $N = 3p_1 \cdots p_n - 1 = 3(p_1 \cdots p_n - 1) + 2$

If N is prime, it is not one of p_1 through p_n, and we get a new prime out of the list.

If N is not a prime, it is the product of primes. Since $3 \nmid N$, these primes are all of the form $3k+1$ or $3k+2$.

Since for all integers k_1, k_2, $(3k_1+1)(3k_2+1) = 3(k_1k_2+k_1+k_2)+1$, the product of primes from $3k+1$ will also have that form, it must therefore have a factor q of the form $3k+2$. Since none of the p_i devide N, this q is not one of $p_1 \cdots p_n$.

In both cases, we have found a prime not on our original list. Since n was arbitrary, we have found a prime not on our original list.

Therefore, in either cases, we find a new prime out of our original list.

(ii) Let $N = 6p_1 \cdots p_n - 1 = 6(p_1 \cdots p_n - 1) + 5$

If N is prime, it is not in the list.

If N is not prime, it muse have prime factors, since $6 \nmid N$, the factors are of the form of $6k+1 / 6k+3 / 6k+5$

$(6k_1+1)(6k_2+1) = 6(6k_1k_2+k_1+k_2)+1$

$(6k_1+3)(6k_2+3) = 6(6k_1k_2+k_1+k_2+1)+3$

$(6k_1+1)(6k_2+3) = 6(6k_1k_2+k_1+k_2)+3$

Therefore, there must be a factor p of the form $6k+5$, and this factor does not belong to $p_1 \cdots p_n$ since $p_k (1 \le k \le n) \nmid N$. Therefore we find a new prime out of the list.

Excercise 4.3

$F_n = 2^{2^n} + 1$

(i) $\gcd(F_n, F_{n+1})$

$F_n = 2^{2^n} + 1$, $F_{n+1} = 2^{2^{n+1}} + 1$

$F_{n+1} = (F_n - 1)^2 + 1 = F_n^2 - 2F_n + 2$.

$\gcd(F_n, F_n^2 - 2F_n + 2)$

$= \gcd(F_n, (F_n - 2)F_n + 2)$

$= \gcd(F_n, 2)$

since $F_n > 2$ and F_n is always odd

$\gcd(F_n, 2) = 1$

(ii) We first prove that any two distinct Fermat numbers are relatively prime.

Let F_m and F_n be two distinct Fermat number, without loss of generality let $m > n$. we assume that $\gcd(F_m, F_n) = d$, then

then we have $F_m = 2 + F_0 \cdots F_{m-1}$,

$d \mid F_n$ and $d \mid F_m$

$d \mid F_n \Rightarrow d \mid F_0 \cdots F_n F_{n+1} \cdots F_{m-1}$

then $d \mid F_m - F_0 \cdots F_{m-1} \Rightarrow d \mid 2$, all Fermat number odd so $d = 1$.

There are infinitely many distinct Fermat numbers, each of which is divisible by an odd prime, and since any two Fermat numbers are relativoly prime, these odd primes must all be distinct. Thus, there are infinitely many primes.

Excercise 4.4

(a) $56x + 72y = 39$

Since $2 \mid 56x + 72y$, $2 \nmid 39$

There will be no (x, y) that satisfies the requirement.

(b) $84x - 439y = 156$

$439 = 84 \times 5 + 19$

$84 = 19 \times 4 + 8$

$19 = 8 \times 2 + 3$

$8 = 3 \times 2 + 2$

$3 = 2 \times 1 + 1$

$\gcd(84, 439) = 1$

Back Tracing

$1 = 3 - 2 \times 1$

$= 3 - (8 - 3 \times 2)$

$= 3 \times 3 - 8$

$= (19 - 8 \times 2) \times 3 - 8$

$= 19 \times 3 - 8 \times 7$

$= 19 \times 3 - (84 - 19 \times 4) \times 7$

$= 19 \times 31 - 84 \times 7$

$= (439 - 84 \times 5) \times 31 - 84 \times 7$

$= 439 \times 31 - 84 \times 155 - 84 \times 7$

$= 439 \times 31 - 84 \times 162$

$= 84 \times (-162) + (-31) \times (-439)$

When $x_0 = -162 \cdot 156$ $\quad 84(-162 \cdot 156) - 439(-31 \cdot 156) = 156$

$y_0 = -31 \cdot 156$

$x = -162 \cdot 156 + 439r, \quad y = -31 \cdot 156 + 84r$

Exercise 4.5

1° We need to prove that $(a \boxtimes b) \boxtimes c = a \boxtimes (b \boxtimes c)$

$(a \boxtimes b) \boxtimes c = (b \cdot a) \boxtimes c = c \cdot (b \cdot a)$

$a \boxtimes (b \boxtimes c) = a \boxtimes (c \cdot b) = (c \cdot b) \cdot a = c \cdot (b \cdot a)$

2° Suppose $\mathbb{1}$ is an identity element in the set S.

$\mathbb{1} \boxtimes a = a \cdot \mathbb{1} = a$.

$a \boxtimes \mathbb{1} = \mathbb{1} \cdot a = a$

3° $\forall a \in S$ a^{-1} is the inverse in G.

Then $a^{-1} \boxtimes a = a \cdot a^{-1} = \mathbb{1}$.

for any element in S we can find it's inverse.

Therefore, $(S, \boxtimes)$ is a group.

Exrercise 4.6

(i)

Assume a matrix $A=(a_{i,j})$ such that there exists a function ψ

$$a_{i,j}=\sum_{k|i,k|j}\psi(k) \text{ for all } i,j.$$

Then $\det A=\psi(1)\cdots\psi(n)$

To see this, consider the matrix $B=b_{i,j}$ such that $b_{i,j}=1$ if $i|j$ and $b_{i,j}=0$ otherwise. , B is upper-triangular matrix whose diagonal is $(\psi(1),\cdots,\psi(n))$.

Let C be the diagonal matrix whose diagonal is $(\psi(1)\cdots\psi(n))$

By matric product computation, we show that

$A=B^tCB$ hence $\det A=(\det B)^2\cdot\det C=\psi(1)\cdots\psi(n)$

Since $m=\sum_{k|m}\phi(k)$, $a_{i,j}=\gcd(i,j)=\sum_{k|\gcd(i,j)}\phi(k)$

$$=\sum_{k|i,k|j}\phi(k)$$

And then we find that

$$\det A=\phi(1)\cdots\phi(n)$$

ii) Create $A \in Mat(n \times n, \mathbb{R})$, $A = (a_{ij})$

$$a_{ij} = \begin{cases} \sqrt{p(j)} & j \geq i \\ 0 & \end{cases}$$

Calculate $AA^T =: S$

$$S_{ij} = \sum_k a_{ik} a_{kj} = (i, j)$$

$$x S x^T = (x^T A)(x^T A)^T \geq 0$$

iff $x^T A = 0 \Leftrightarrow x = 0$

So S is positive defined.

Exrercise 4.7

As $(b \cdot c) \cdot d = a \cdot d = d$

$b \cdot (c \cdot d) = b \cdot f = g$

Therefore, it's not a group.

Exrercise 4.8

i) let $G = (S, \cdot)$ identity e.

$\forall a \in S$, if $a \neq e$, then $a^2 = e$

So $\forall\, a, b \neq e$, $(ab)(ba) = a(bb)a = a\,a = e$.

As $ab \in S$. $(ab)(ab) = e$

So $ab = ba$

ii). Assume $|ab| = m$ $\underbrace{ab\,ab \quad ab}_{m \text{ times}} = e$.

Since $\underbrace{ab \cdots ab}_{m} \cdot a = a \Rightarrow \underbrace{baba \cdots ba}_{m} = e$.

Excercise 4-9

when $n | m$, we have

$$\sum_{k=0}^{n-1} w^{km} = w^0 + w^m + w^{2m} + \cdots w^{(n-1)m}$$

$$= 1 + 1 + \cdots 1$$

$$= n.$$

when $n \nmid m$, $|\langle km \rangle| = |\langle d \rangle|$

$$\sum_{k=0}^{n-1} w^{km} = \frac{n}{d} \sum_{k=0}^{d=1} = \frac{n}{d} \sum_{k=0}^{d-1} w^d = \frac{n}{d} \cdot 0 = 0$$