Ve203 Discrete Mathematics (Spring 2023)

Assignment 5

Date Due: See canvas

This assignment has a total of **(50 points)**. Exercises with **0 pt** might be

- something that is very basic, but you should know anyway, or
- something that is too technical for this course, or
- ill-posed (i.e., wrong).

Meanwhile, this is not to say that other problems necessarily lack the above features.

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..."

Exercise 5.1 (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 5.2 (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 5.3 (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 5.4 (4 pts) Solve the following linear Diophantine equations (find all integer solutions),

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

Exercise 5.5 (2 pts) Given a group $G = (S, \cdot)$, where S is the underlying set, and $\cdot$ is the groups law. Define a new function

$$\begin{aligned} \boxtimes : S \times S &\to S \\ (a, b) &\mapsto a \boxtimes b := b \cdot a \end{aligned}$$

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

Exercise 5.6 (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

(i) `(1 pt)` Show that $(S, \cdot)$ is not a group.

(ii) `(1 pt)` Use Lagrange's theorem to show that $(S, \cdot)$ is not a group.

Exercise 5.7 (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 5.8 (2 pts) Given a magma M, for each $x \in M$, define

$$\begin{aligned} L_x : M \to M, \qquad & y \mapsto xy \qquad \text{(left multiplication by } x\text{)} \\ R_x : M \to M, \qquad & y \mapsto yx \qquad \text{(right multiplication by } x\text{)} \end{aligned}$$

For $x, y, z \in M$, show that the following are equivalent,

(A) $(xy)z = x(yz)$ (B) $R_z \circ L_x = L_x \circ R_z$ (C) $L_{xy} = L_x \circ L_y$ (D) $R_{yz} = R_z \circ R_y$

Exercise 5.9 (4 pts) Given groups G, G', and $f : G \to G'$ a surjective homomorphism. Show that

(i) (2 pts) G' is cyclic if G is cyclic.

(ii) (2 pts) G' is abelian if G is abelian.

Exercise 5.10 (2 pts) Given group G and a function $f : G \to G$, $x \mapsto x^{-1}$. Show that the following are equivalent,

(A) G is abelian. (B) f is a homomorphism.

Exercise 5.11 (2 pts) Show that $\{1, (12)(34), (13)(24), (14)(23)\}$ is a subgroup of A_4. Is it a normal subgroup?

Exercise 5.12 (2 pts) Given a group G with $|G|$ even, show that G contains an element of order 2.

Exercise 5.13 (4 pts)

(i) (2 pts) Show that a subgroup of index 2 is normal.

(ii) (2 pts) Show that a subgroup of index 3 is not necessarily normal, but might be.

Exercise 5.14 (4 pts) Let G be a group of order p^2, with p prime. Show that

(i) (2 pts) G has at least one subgroup of order p.

(ii) (2 pts) If G contains only one subgroup of order p, then G is cyclic.

Exercise 5.15 (2 pts) The (continuous) Heisenberg group H is the group of 3×3 upper triangular matrices of the form

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, \qquad a, b, c \in \mathbb{R}$$

under the operation of matrix multiplication. Calculate the center of G, and show that it is isomorphic to $\mathbb{R}$ under addition.

Exercise 5.16 (2 pts) Given $a, b, c, d, m \in \mathbb{Z}$, $m > 0$. Show that

(i) (1 pt) If $a \equiv b \pmod{m}$, and $d \mid m$, $d > 0$, then $a \equiv b \pmod{d}$.

(ii) (1 pt) If $a \equiv b \pmod{m}$, and $c > 0$, then $ac \equiv bc \pmod{mc}$

Exercise 5.17 (2 pts) Given $a, x, y, m \in \mathbb{Z}$, $m > 0$. Show that

(i) (1 pt) $ax \equiv ay \pmod{m}$ iff $x \equiv y \left(\bmod \dfrac{m}{\gcd(a,m)}\right)$.

(ii) (1 pt) If $ax \equiv ay \pmod{m}$ and $\gcd(a, m) = 1$, then $x \equiv y \pmod{m}$.

Exercise 5.18 (2 pts) Given $x, y \in \mathbb{Z}$, and positive intergers $m_1, \ldots, m_r$, show that $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$ iff $x \equiv y \pmod{m}$, where $m = \operatorname{lcm}(m_1, m_2, \ldots, m_r)$.

The following exercises are not to be graded

Exercise 5.19* 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) Show that $\det S = \prod_{j=1}^{n} \varphi(j)$ where φ is the Euler totient function.

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

Exercise 5.20* 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 $1 \leq k \leq n-1$, show that

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