MATH 433 Spring 2024

Sample problems for the final exam

Any problem may be altered or replaced by a different one!

Problem 1. The number 63000 has how many positive divisors?

Problem 2. Solve a system of congruences (find all solutions):

$$\begin{cases} x \equiv 2 \bmod 5, \\ x \equiv 3 \bmod 6, \\ x \equiv 6 \bmod 7. \end{cases}$$

Problem 3. Find all integer solutions of a system

$$\begin{cases} 2x + 5y - z = 1, \\ x - 2y + 3z = 2. \end{cases}$$

[Hint: Eliminate one of the variables.]

Problem 4. You receive a message that was encrypted using the RSA system with public key $(55, 27)$, where 55 is the base and 27 is the exponent. The encrypted message, in two blocks, is 4/7. Find the private key and decrypt the message.

Problem 5. Let $\pi = (1\,2)(2\,3)(3\,4)(4\,5)(5\,6)$, $\sigma = (1\,2\,3)(2\,3\,4)(3\,4\,5)(4\,5\,6)$. Find the order and the sign of the following permutations: π, σ, $\pi\sigma$, and $\sigma\pi$.

Problem 6. For any positive integer n let $n\mathbb{Z}$ denote the set of all integers divisible by n.
(i) Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under addition? Does it form a group?
(ii) Does the set $3\mathbb{Z} \cup 4\mathbb{Z} \cup 7\mathbb{Z}$ form a semigroup under multiplication? Does it form a group?

Problem 7. Given a group G, an element $c \in G$ is called *central* if it commutes with any element of the group: $cg = gc$ for all $g \in G$. The set of all central elements, denoted $C(G)$, is called the *center* of G. Prove that $C(G)$ is a normal subgroup of G.

Problem 8. Find a direct product of cyclic groups that is isomorphic to G_{16} (multiplicative group of all invertible congruence classes modulo 16).

Problem 9. Complete the following Cayley table of a group of order 9:

$*$	A	B	C	D	E	F	G	H	I
A	I								F
B		F						G	
C			H				E		
D				G		A			
E					E				
F				A		B			
G			E				A		
H		G						D	
I	F								C

Problem 10. A linear binary coding function f is defined by a generator matrix

$$G = \begin{pmatrix} 0 & \square & 0 & 1 & 1 & 0 & 1 \\ 1 & \square & 0 & 1 & 1 & 1 & 0 \\ 0 & \square & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

with some entries missing. Fill in the missing entries so that f can detect as many errors as possible. Explain.

Problem 11. Find all prime numbers p such that a polynomial $x^4 - x^3 + x^2 - x + 1$ is divisible by $x + 2$ in $\mathbb{Z}_p[x]$.

Problem 12. Factorise the polynomial $p(x) = x^4 - 2x^3 - x^2 - 2x + 1$ into irreducible factors over the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

[Hint: use the substitution $y = x + x^{-1}$.]