MATH 521A: Abstract Algebra
Preparation for Exam 1

1. Use induction to prove that \( n^3 < n! \) for all \( n \geq 6 \).

2. Let \( m \in \mathbb{N} \). Use the division algorithm to prove that there is no integer \( n \) with \( m < n < m + 1 \).

3. Let \( a, b, n \in \mathbb{Z} \) with \( n > 1 \). Suppose we apply the division algorithm three times to get \( a = q_1 n + 1 \), \( b = q_2 n + r_2 \), \( ab = q_3 n + r_3 \). Prove that \( r_2 = r_3 \).

4. Let \( S \) be a set with a well-ordering \( < \), and for each \( x \in S \) the proposition \( P(x) \) may be true or false. Suppose that \( c \in S \) is the smallest counterexample, i.e. \( P(c) \) is false, but for all \( x \in S \) with \( x < c \), \( P(x) \) is true. Suppose that with these hypotheses we are able to derive a contradiction. Prove that \( P(x) \) holds for all \( x \in S \), using the well-ordering of \( S \).

5. Prove that \( 5 \mid (3^{2n} - 2^{2n}) \) for all \( n \in \mathbb{N} \).

6. Use the Euclidean Algorithm to find \( \gcd(1492, 1776) \) and to express that \( \gcd \) as a linear combination of \( 1492, 1776 \).

7. Suppose \( a, b, q, r \in \mathbb{Z} \) with \( b > 0 \) and \( a = bq + r \). Prove that \( \gcd(a, b) = \gcd(b, r) \).

8. Let \( a, b, c \in \mathbb{Z} \) with \( a \neq 0 \). Suppose \( a \mid bc \). Prove that \( a \mid \gcd(a, b)c \).

9. Let \( a, b \in \mathbb{N} \). Suppose that \( \gcd(a, b) = 1 \). Without using the FTA, prove that \( \gcd(a^2, b^2) = 1 \).

10. Express 7,938,000 as a product of primes.

11. Let \( p \) be a positive prime, \( n \in \mathbb{Z} \) with \( n > 1 \). Use the Fundamental Theorem of Arithmetic to prove that there do not exist \( a, b \in \mathbb{N} \) with \( a^n = pb^n \). [Note: this proves that \( \sqrt{p} \notin \mathbb{Q} \).]

12. Let \( a, x, y, n \in \mathbb{N} \) with \( \gcd(a, n) = 1 \). Suppose \( ax \equiv ay \pmod{n} \). Prove that \( x \equiv y \pmod{n} \).

13. Let \( a, b, n \in \mathbb{N} \) with \( \gcd(a, n) = 1 \). Prove that \( ax \equiv b \pmod{n} \) has a solution \( x \). Also, prove that any two solutions are congruent modulo \( n \).

14. Suppose \( a, b, m, n \in \mathbb{N} \) and \( \gcd(m, n) = 1 \). Prove that the system \( \{x \equiv a \pmod{m}, x \equiv b \pmod{n}\} \) has a solution \( x \). Also, prove that any two solutions are congruent modulo \( mn \).

15. Prove that any natural number is congruent to its units digit, modulo 10.

16. Prove that \( n^3 \equiv n \pmod{6} \), for all \( n \in \mathbb{N} \).

17. Working in \( \mathbb{Z}_{27} \), find the multiplicative inverse of \([8]\), and use this to solve the modular equation \( [8] \odot [x] = [15] \).

18. Working in \( \mathbb{Z}_n \), prove that the following holds for all \( a, b, c, d \):

\[
([a] \oplus [b]) \odot ([c] \oplus [d]) = ([a] \odot [c]) \oplus ([a] \odot [d]) \oplus ([b] \odot [c]) \oplus ([b] \odot [d])
\]

19. Let \([a] \in \mathbb{Z}_n \). Prove that exactly one of the following holds:

(i) \([a] = [0] \); or
(ii) \([a] \) is a unit; or
(iii) \([a] \) is a zero divisor.

20. Let \( n \in \mathbb{Z} \) with \( n > 1 \). Prove that \( n \) is prime if and only if there are no zero divisors in \( \mathbb{Z}_n \).