INSTRUCTIONS

- Duration: 50 minutes
- This test has 4 problems for a total of 100 points.
- This test has 5 pages including this one.
- Read all the questions carefully before starting to work.
- For problems with several parts indicate clearly which part of it you are answering.
- You should give complete arguments and explanations for all your claims and calculations; answers without justifications will not be marked.
- You may write on the backs of pages if you run out of space.
- Attempt to answer all questions for partial credit.
- This is a closed-book examination. None of the following are allowed: documents, cheat sheets or electronic devices of any kind (including calculators, cell phones, etc.)

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points:</td>
<td>20</td>
<td>30</td>
<td>30</td>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>Score:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PROBLEM 1 (20 points)

Suppose that \( n \in \mathbb{Z}_{>0} \) has 77 positive divisors. How many of these divisors can be primes?

\textbf{Answer:} Let \( n = p_1^{a_1} \cdots p_k^{a_k}, a_i \geq 1 \) be the prime decomposition of the positive integer \( n \).

We know that the number of positive divisors of \( n \) is \( \tau(n) = 77 \) and it is also given by

\[ \tau(n) = (a_1 + 1)\cdots(a_k + 1) = 77. \]

The positive divisors of 77 are \( \{1, 7, 11, 77\} \).

Suppose \( a_1 + 1 = 77 \). Then \( a_i = 0 \) for all \( i \geq 2 \). Thus \( n = p_1^{76} \).

Suppose \( a_1 + 1 = 11 \). Then \( (a_2 + 1)\cdots(a_k + 1) = 7 \) which implies \( a_2 = 6 \) and \( a_i = 0 \) for all \( i \geq 3 \). Thus \( n = p_1^6 p_2^6 \).

Suppose \( a_1 + 1 = 7 \). Then \( (a_2 + 1)\cdots(a_k + 1) = 11 \) which implies \( a_2 = 10 \) and \( a_i = 0 \) for all \( i \geq 3 \). Thus \( n = p_1^6 p_2^{10} \).

Suppose \( a_1 + 1 = 1 \). Hence \( a_1 = 0 \) which contradicts \( a_1 \geq 1 \).

Thus \( n \) has either 1 or 2 prime factors.

PROBLEM 2 (30 points)

(a) (5pts) State the definition of a primitive root modulo \( N \), where \( N \) is a positive integer.

\textbf{Answer:} Let \( N \) be a positive integer. A primitive root modulo \( N \) is an integer \( r \) such that \( (r,N) = 1 \) and \( \text{ord}_N r = \phi(N) \), where \( \phi \) is the Euler \( \phi \)-function.

(b) (5pts) How many incongruent primitive roots modulo 13 are there?

\textbf{Answer:} We have \( \phi(13) = 12 = 2^2 \cdot 3 \). We compute \( \phi(12) = \phi(4)\phi(3) = 2 \cdot 2 = 4 \). Therefore there are 4 incongruent primitive roots mod 13.

(c) (10pts) Show that 2 is a primitive root modulo 13.

\textbf{Answer:} The order of any integer \( a \) modulo 13 is a positive divisor of \( \phi(13) = 12 \), which are \( \{1, 2, 3, 6, 12\} \). We have
\[
2^1 \equiv 1, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8 \pmod{13}
\]
and also
\[
2^6 \equiv (2^3)^2 \equiv 8^2 \equiv 64 \equiv 12 \pmod{13}.
\]
Since all the previous numbers are \( \not\equiv 1 \pmod{13} \) we conclude that \( \text{ord}_{13} 2 = 12 \), that is 2 a primitive root mod 13.

(d) (10pts) Determine with proof a maximal set of incongruent primitive roots modulo 13.

\textbf{Answer:} From (c) we know that 2 is a primitive root mod 13, then \( 2^i \) for \( 1 \leq i \leq \phi(13) = 12 \) forms a reduced residue system. Therefore, we can obtain all the incongruent primitive roots as the powers \( 2^i \), where \( 1 \leq i \leq 12 \), satisfying \( \text{ord}_{13} 2^i = 12 \). We know that
\[
\text{ord}_{13} 2^i = \frac{\text{ord}_{13} 2}{(\text{ord}_{13} 2, i)},
\]
which in our setting reads
\[
12 = \frac{12}{(12, i)} \iff (12, i) = 1.
\]
The values of \( i \) in the interval \( 1 \leq i \leq 12 \) satisfying \( (12, i) = 1 \) are \( i = 1, 5, 7, 11 \). Therefore, the integers \( 2^i \) for \( i = 1, 5, 7, 11 \) are 6 incongruent primitive roots. By part (b) this is a maximal list.
PROBLEM 3 (30 points)

(a) (15pts) Show, without using the explicit factorization of 1729, but using the following congruences instead, that 1729 is composite

\[ 2^{18} \equiv 1065 \pmod{1729} \quad \text{and} \quad 2^{36} \equiv 1 \pmod{1729}. \]

Answer: Let \( x = 2^{18} \). We have \( x^2 = 2^{36} \equiv 1 \pmod{1729} \), hence if 1729 is a prime we also have \( x \equiv \pm1 \pmod{1729} \). This means \( x = 2^{18} \equiv 1065 \equiv \pm1 \pmod{1729} \), which is impossible. We conclude that 1729 is composite.

(c) (10pts) Let \( p \) be a prime. Let \( a \in \mathbb{Z} \) satisfy \( (a, p) = 1 \) and have order \( d \) modulo \( p \). Show that the integers \( a^i \) for \( i = 1, \ldots, d-1 \) are distinct mod \( p \).

Answer: Suppose that \( a^i \equiv a^j \pmod{p} \). Then \( a^{i-j} \equiv 1 \pmod{p} \) since \( a^{-1} \) exists because \( (a, p) = 1 \). Thus \( i \equiv j \pmod{\text{ord}_p a = d} \) and since \( i, j \) are in the interval \([1, d-1]\) we necessarily have \( i = j \), as desired.

(d) (5pts) Let \( m > 0 \) and \( r \) be a primitive root modulo \( m \). State the definition of \( \text{ind}_r a \), the index of \( a \) with respect to \( r \), where \( a \) is an integer coprime to \( m \). Determine \( \text{ind}_2 12 \) when \( m = 13 \).

Answer: The index of \( a \) coprime to \( m \) with respect to \( r \) is the least positive integer \( y \) such that \( r^y \equiv a \pmod{m} \). From the calculations in Problem 2 (c) we see that \( y = 6 \) is the smallest positive exponent for which \( 2^y \equiv 12 \pmod{13} \), therefore \( \text{ind}_2 12 = 6 \).
PROBLEM 4 (20 points)

Let \( p \) be a prime such that \( p = 2q + 1 \), where \( q \) is an odd prime, and \( a \) be an integer satisfying \( 1 < a < p - 1 \).

In this exercise you will show that \( p - a^2 \) is a primitive root mod \( p \).

(a) (2pts) Show that \( \text{ord}_p(-a^2) = 1, 2, q, \) or \( 2q \).

Answer: We know from class that \( \text{ord}_p(-a^2) \mid \phi(p) = p-1 = 2q \). The positive divisors of \( 2q \) are \( 1, 2, q \) and \( 2q \), as desired.

(b) (8pts) Show that \( (-a^2)^2 \not\equiv 1 \pmod{p} \).

Answer: Suppose \( a^4 \equiv 1 \pmod{p} \). Thus \( \text{ord}_p(a) \) divides both \( 4 \) and \( \phi(p) = p-1 = 2q \). Hence, \( \text{ord}_p(a) \) divides \( \gcd(4, 2q) = 2 \). In other words, \( a^2 \equiv 1 \pmod{p} \). Thus \( a \equiv 1 \pmod{p} \) or \( a \equiv -1 \pmod{p} \) because \( p \) is prime, contradicting \( 1 < a < p - 1 \).

(c) (7pts) Show that \( (-a^2)^q \not\equiv 1 \pmod{p} \).

Answer: Suppose \( (-a^2)^q \equiv 1 \pmod{p} \). Then \( (-1)^q a^{2q} \equiv 1 \pmod{p} \).

By FLT, \( a^{2q} \equiv 1 \pmod{p} \). On the other hand, since \( q \) is odd, \( (-1)^q = -1 \).

Thus, \( -1 \equiv 1 \pmod{p} \), a contradiction.

(d) (3pts) Use parts (a), (b) and (c) to conclude that \( p - a^2 \) is a primitive root mod \( p \).

Answer: Note that \( p - a^2 \equiv -a^2 \pmod{p} \), hence \( p - a^2 \) is a primitive root if \( \text{ord}_p(p - a^2) = \text{ord}_p(-a^2) = \phi(p) = p-1 = 2q \). From (a) we have \( \text{ord}_p(-a^2) = 1, 2, q, \) or \( 2q \). From (b) it follows that \( \text{ord}_p(-a^2) \neq 1, 2 \) and from (c) it follows \( \text{ord}_p(-a^2) \neq q \). Therefore, \( \text{ord}_p(-a^2) = 2q \), as desired.