General Instructions: Answer as many of the following as you can in the time allotted. Only your 8 best scores will count toward your exam grade. Do not use notes, books, calculators, computers, cell phones or notes on bathroom stalls. Show all work. Put your name on the top of each page you turn in and number the problems with your answers. There is no need to turn in the questions with your answers.

1. Prove that 6601 = 7 · 23 · 41 is an absolute pseudoprime.

2. Let \( n \) be a positive integer. Recall that the value of \( \sum_{k=1}^{n} \frac{1}{k} \) can be estimated by comparing it’s value to an integral. By making such a comparison, explain why

\[
\sum_{k=1}^{n} \frac{1}{k} \leq 1 + \log n.
\]

As usual, \( \log n \) refers to the natural logarithm of \( n \).

3. Let \( B(x) \) denote the number of natural numbers \( n \leq x \) with a prime factor \( > \sqrt n \). Prove that \( B(x) \sim \prod_{\alpha_j > 1} \left( \frac{1}{\alpha_j} \right) \log x \).

4. Let \( n \) be a positive integer. Suppose \( n - 1 = FR \) where all the prime factors of \( F \) are known and \( \gcd(F, R) = 1 \). Suppose further that there exists an integer \( a \) such that \( a^{n-1} \equiv 1 \pmod{n} \) and for all primes \( p \) dividing \( F \) we have \( \gcd(a^{(n-1)/p} - 1, n) = 1 \).

(a) What does the Proth, Pocklington, Lehmer Test allow us to conclude? In other words, the above is everything except the last sentence of the Proth, Pocklington, Lehmer Test that we stated in class. What is the last sentence? (I don’t care about the exact wording but do want the precise meaning of whatever you write.)

(b) Prove the Proth, Pocklington, Lehmer Test.

5. Let

\[
f(x) = a_n \prod_{j=1}^{n} (x - \alpha_j) \quad \text{and} \quad w(x) = a_n \prod_{1 \leq j \leq n} (x - \alpha_j) \prod_{1 \leq j \leq n} (\alpha_j x - 1).
\]

Recall that \( \tilde{f}(x) = x^n f(1/x) \) and \( \tilde{w}(x) = x^n w(1/x) \). Using (do not prove) \( w(x)\tilde{w}(x) = f(x)\tilde{f}(x) \), explain why \( M(f) \leq \|f\| \) (where \( M(f) \) is the Mahler measure of \( f \)).

6. Hadamard’s inequality asserts that

\[
\det(b_1, \ldots, b_n) \leq \|b_1\| \|b_2\| \cdots \|b_n\|.
\]
where the $b_j$ correspond to column vectors in $\mathbb{R}^n$. The proof of Hadamard’s inequality we gave in class can be broken up into three parts. After (b) and (c) below, the above inequality should be clear.

(a) Give a brief explanation as to why
\[
\det (b_1, \ldots, b_n) = \det \left( b_1^*, \ldots, b_n^* \right),
\]
where the $b_j^*$ come from the Gram-Schmidt orthogonalization process and are defined by
\[
b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \quad (\text{for } 1 \leq i \leq n), \quad \mu_{ij} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*} \quad (\text{for } 1 \leq j < i \leq n).
\]

(b) Using part (a), explain why
\[
\det (b_1, \ldots, b_n)^2 = \left( \prod_{i=1}^{n} \| b_i^* \| \right)^2.
\]
You may use here and in the next part that the $b_j^*$ are pairwise orthogonal; you do not need to justify this.

(c) Explain why $\| b_i^* \| \leq \| b_i \|$ for each $i \in \{1, 2, \ldots, n\}$.

7. Define what it means for a basis $b_1, \ldots, b_n$ for a lattice $L$ to be reduced.

8. Let $f(x) = x^5 + x + 1$. Suppose we want to factor $f(x)$ modulo 2. Working modulo 2, we compute a certain matrix $A$ and then $B = A - I$. The result of this computation is (in the field of arithmetic modulo 2)
\[
B = A - I = \begin{pmatrix} 0 & 0 & 0 & * & 0 \\ 0 & 1 & 0 & * & 0 \\ 0 & 1 & 1 & * & 0 \\ 0 & 0 & 0 & * & 1 \\ 0 & 0 & 1 & * & 0 \end{pmatrix},
\]
where by some freakish accident the elements of the fourth column have been replaced by asterisks. Using Berlekamp’s algorithm and what has been stated here, find a polynomial $g(x)$ of degree $\leq 4$ such that when $\gcd(f(x), g(x))$ is computed modulo 2, the result is a non-trivial factor of $f(x)$ modulo 2. You do not need to justify the entries in $B$ above, but you should indicate what the fourth column is and clarify how you obtain it. You may want to check other columns given with your approach to see if you are computing $B$ correctly. You should also indicate $g(x)$ explicitly and explain how you obtain $g(x)$ from $B$.

9. Let $b_1, \ldots, b_n$ be a basis for a lattice $L$ and suppose $b_1^*, \ldots, b_n^*$ are the corresponding vectors obtained from the Gram-Schmidt orthogonalization process. Suppose $b \in L$ with $b \neq 0$. Then $b$ can be written in the form
\[
b = u_1 b_1 + \cdots + u_k b_k,
\]
where each $u_j \in \mathbb{Z}$ and $u_k \neq 0$.

Explain why $\| b \|^2 \geq \| b_k^* \|^2$. 

10. Given \( n = 26989 \), we want to use Dixon’s Factoring Algorithm and the following tabulated information to find a nontrivial factor of \( n \). The table only includes random integers \( a \) found for which \( s(a) = a^2 \mod n \) has all its prime factors \( \leq 11 \). You do not need to come up with a factor of \( n \), but use Dixon’s Factoring Algorithm to reduce coming up with a factor of \( n \) to the computation of \( \gcd(x - y, n) \) where you tell me precisely what the values of \( x \) and \( y \) are (each should involve a product of specific numbers - you do not need to expand products). It is possible that the \( x \) and \( y \) you choose will not produce a factorization of \( n \); in the algorithm one might need to try more than one choice of \( x \) and \( y \). You need only give me one reasonable choice for \( x \) and \( y \).

<table>
<thead>
<tr>
<th>row number</th>
<th>random ( a \in [500, 1200] )</th>
<th>factorization of ( a^2 \mod 26989 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>763</td>
<td>( 2^3 \cdot 5^2 \cdot 7 \cdot 11 )</td>
</tr>
<tr>
<td>2</td>
<td>595</td>
<td>( 2^5 \cdot 3^2 \cdot 11 )</td>
</tr>
<tr>
<td>3</td>
<td>1026</td>
<td>( 3 \cdot 5 \cdot 7 )</td>
</tr>
<tr>
<td>4</td>
<td>830</td>
<td>( 3^4 \cdot 5^2 \cdot 7 )</td>
</tr>
<tr>
<td>5</td>
<td>519</td>
<td>( 2^2 \cdot 3^3 \cdot 5 \cdot 7^2 )</td>
</tr>
</tbody>
</table>