Final Exam, 2007

1. **Prove that $6601 = 7 \cdot 23 \cdot 41$ is an absolute pseudoprime.**

2. **Let n be a positive integer. Recall that the value of $\displaystyle\sum_{k=1}^{n} \frac{1}{k}$ 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 $B(x) \sim (\log 2)x$. You may use that $\sum_{p \leq x} 1/p = \log\log x + A + O(1/\log x)$ for some constant A and that $\pi(x) = O(x/\log x)$. (Note: If you end up preferring to replace $> \sqrt{n}$ above with $> \sqrt{x}$, then feel free to do so.)

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.)

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

$$f(x) = a_n \prod_{j=1}^{n} (x - \alpha_j)$$

and

$$w(x) = a_n \prod_{\substack{1 \le j \le n \\ |\alpha_j| > 1}} (x - \alpha_j) \prod_{\substack{1 \le j \le n \\ |\alpha_j| \le 1}} (\alpha_j x - 1).$$

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

6. Hadamard's inequality asserts that

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) \leq \|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\|,$$

where the $\vec{b}_j$ 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

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) = \det\left(\vec{b}_1^*, \ldots, \vec{b}_n^*\right),$$

where the $\vec{b}_j^*$ come from the Gram-Schmidt orthogonalization process and are defined by

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^* \quad \text{(for } 1 \leq i \leq n\text{), and}$$

$$\mu_{ij} = \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*} \quad \text{(for } 1 \leq j < i \leq n\text{).}$$

6. Hadamard's inequality asserts that

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) \leq \|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\|,$$

where the $\vec{b}_j$ 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.

(b) Using part (a), explain why

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right)^2 = \left(\prod_{i=1}^{n} \|\vec{b}_i^*\|\right)^2.$$

You may use here and in the next part that the $\vec{b}_j^*$ are pairwise orthogonal; you do not need to justify this.

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

7. Define what it means for a basis $\vec{b}_1, \ldots, \vec{b}_n$ for a lattice $\mathcal{L}$ 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 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 ≤ 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.

9. Let $\vec{b}_1, \ldots, \vec{b}_n$ be a basis for a lattice $\mathcal{L}$, and let $\vec{b}_1^*, \ldots, \vec{b}_n^*$ be the corresponding vectors obtained from the Gram-Schmidt orthogonalization process. Suppose $\vec{b} \in \mathcal{L}$ with $\vec{b} \neq 0$. Then $\vec{b}$ can be written in the form

$$\vec{b} = u_1\vec{b}_1 + \cdots + u_k\vec{b}_k, \qquad \text{where each } u_j \in \mathbb{Z} \text{ and } u_k \neq 0.$$

Explain why $\|\vec{b}\|^2 \geq \|\vec{b}_k^*\|^2$.

10. We want to make use of Dixon's Factoring Algorithm with the table below to get a nontrivial factor of $n = 26989$. The table contains some random integers a found for which $s(a) = a^2 \bmod n$ has all its prime factors ≤ 11. 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).

row number	random a	factorization of $a^2 \bmod 26989$
1	763	$2^3 \cdot 5^2 \cdot 7 \cdot 11$
2	595	$2^5 \cdot 3^2 \cdot 11$
3	1026	$3 \cdot 5 \cdot 7$
4	830	$3^4 \cdot 5^2 \cdot 7$
5	519	$2^2 \cdot 3^3 \cdot 5 \cdot 7^2$

Comp Exam Problem

We showed in class that if $f(x)$, $g(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ satisfying $f(x) = g(x)h(x)$, then $\|g(x)\| \leq 2^{\deg g}\|f(x)\|$. We did this for a reason. Let $f(x) = x^8 + x^4 + x^2 - 1$. Then

$$f(x) \equiv \left(x^2+1\right)(x+23)(x+80)\left(x^2+22\,x+94\right)\left(x^2+81\,x+94\right)$$

where the factors on the right are irreducible modulo 103. The polynomial $f(x)$ factors as x^2+1 times the product of two different irreducible cubics $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$. Using the factorization of $f(x)$ modulo 103, determine "with justification" which of the factorizations below are the factorizations of $u(x)$ and $v(x)$ modulo 103. You should not try to factor $f(x)$ in $\mathbb{Z}[x]$ for this problem.

$$(x+23)\left(x^2+22\,x+94\right)$$

$$(x+23)\left(x^2+81\,x+94\right)$$

$$(x+80)\left(x^2+22\,x+94\right)$$

$$(x+80)\left(x^2+81\,x+94\right)$$