Test: Monday, November 19

Final Exam, 2007

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.

6. Hadamard's inequality asserts that

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

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

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

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

6. Hadamard's inequality asserts that

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

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 $\|\vec{b}_i^*\| \le \|\vec{b}_i\|$ for each $i \in \{1, 2, \ldots, n\}$.

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 $\|g(x)\| \le 2^{\deg g}\|f(x)\|$. 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.

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

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

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

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

Problems from Another Final

Let $f(x) = x^4 + 4x^2 + x - 1$. To factor $f(x)$ modulo 3 using Berlekamp's algorithm, we compute a certain matrix A as in class and then $B = A - I$. The result of this computation is (in the field of arithmetic mod 3)

$$B = A - I = \begin{pmatrix} 0 & 0 & * & 2 \\ 0 & 2 & * & 0 \\ 0 & 0 & * & 1 \\ 0 & 1 & * & 0 \end{pmatrix},$$

where the elements of the third column have been replaced by asterisks.

(a) Compute the third column of the matrix $B = A - I$.

(b) Find a basis for the null space of B. Justify that the basis you found is a basis. Don't forget that you are working in the field of arithmetic modulo 3.

(a) Compute the third column of the matrix $B = A - I$.

(b) Find a basis for the null space of B. Justify that the basis you found is a basis. Don't forget that you are working in the field of arithmetic modulo 3.

(c) Explain why $f(x)$ has exactly two irreducible factors mod 3.

(d) Using Berlekamp's algorithm and what has been stated here, find a polynomial $g(x)$ of degree ≤ 3 such that when

$$\prod_{s=0}^{2} \gcd(g(x) - s, f(x))$$

is computed modulo 3, the result is a non-trivial factorization of $f(x)$ modulo 3.

(e) Factor $f(x)$ modulo 3 as a product of monic irreducible polynomials modulo 3.

(f) Explain why $f(x)$ is irreducible in $\mathbb{Z}[x]$.

(a) Compute the third column of the matrix $B = A - I$.

(b) Find a basis for the null space of B. Justify that the basis you found is a basis. Don't forget that you are working in the field of arithmetic modulo 3.

(c) Explain why $f(x)$ has exactly two irreducible factors mod 3.

(d) Using Berlekamp's algorithm and what has been stated here, find a polynomial $g(x)$ of degree ≤ 3 such that when

$$\prod_{s=0}^{2} \gcd(g(x) - s, f(x))$$

is computed modulo 3, the result is a non-trivial factorization of $f(x)$ modulo 3.

(e) Factor $f(x)$ modulo 3 as a product of monic irreducible polynomials modulo 3.

(f) Explain why $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Problems from Another Final

Let $\vec{b}_1^*, \vec{b}_2^*, \vec{b}_3^*$, and $\vec{b}_4^*$ be the result of applying the Gram-Schmidt orthogonalization process to a basis $\vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_4$ for a lattice $\mathcal{L}$ in $\mathbb{Q}^4$. Suppose

$$\langle -2, 2, 7, -2\rangle = 2\vec{b}_1^* + \vec{b}_3^* + \vec{b}_4^*,$$
$$\langle 0, 4, 7, 4\rangle = \vec{b}_2^* + \vec{b}_3^* + \vec{b}_4^*,$$

and

$$\langle -1, 1, 7, -1\rangle = \vec{b}_1^* + \vec{b}_3^* + \vec{b}_4^*.$$

What is the value of

$$\|\vec{b}_1^*\|^2 + \|\vec{b}_2^*\|^2 + \|\vec{b}_3^*\|^2 + \|\vec{b}_4^*\|^2\,?$$

Justify that your work gives the correct answer. In particular, you should be using a property of $\vec{b}_1^*, \vec{b}_2^*, \vec{b}_3^*, \vec{b}_4^*$, and you should be telling me what property this is and where you are using it.

Problems from Another Final

(a) Let n and b be integers > 1. Define what it means for an integer n to be a strong pseudoprime to the base b?

(b) Prove that no integer $n > 1$ is a strong pseudoprime to every base b with $1 < b \leq n$ and $\gcd(b, n) = 1$.

(c) Is 25 a strong pseudoprime to the base 7 ? Justify your answer.

Problems from Another Final

(a) Let n and b be integers > 1. Define what it means for an integer n to be a strong pseudoprime to the base b?

(b) Prove that no integer $n > 1$ is a strong pseudoprime to every base b with $1 < b \leq n$ and $\gcd(b, n) = 1$.

(c) Is 25 a strong pseudoprime to the base 7 ? Justify your answer.