Test: Monday, November 19

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where the elements of the third column have been replaced by asterisks.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

Definition: Let $\vec{b}_1, \ldots, \vec{b}_n$ be a basis for a lattice $\mathcal{L}$ and $\vec{b}_1^*, \ldots, \vec{b}_n^*$ the corresponding basis for $\mathbb{R}^n$ obtained from the Gram-Schmidt orthogonalization process, with μ_{ij} as defined before. Then $\vec{b}_1, \ldots, \vec{b}_n$ is said to be *reduced* if

(i) $|\mu_{ij}| \leq \frac{1}{2} \quad$ for $1 \leq j < i \leq n$

(ii) $\|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\vec{b}_{i-1}^*\|^2 \quad$ for $1 < i \leq n$.

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

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

Problems from Another Final

Definition: Let $\vec{b}_1, \ldots, \vec{b}_n$ be a basis for a lattice $\mathcal{L}$ and $\vec{b}_1^*, \ldots, \vec{b}_n^*$ the corresponding basis for $\mathbb{R}^n$ obtained from the Gram-Schmidt orthogonalization process, with μ_{ij} as defined before. Then $\vec{b}_1, \ldots, \vec{b}_n$ is said to be ***reduced*** if

(i) $|\mu_{ij}| \leq \frac{1}{2} \quad$ for $1 \leq j < i \leq n$

(ii) $\|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\vec{b}_{i-1}^*\|^2 \quad$ for $1 < i \leq n$.

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

Let $\vec{b}_1, \ldots, \vec{b}_n$ be a reduced basis for a lattice $\mathcal{L}$. Prove that if $\vec{b} \in \mathcal{L}$, then $\|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|$.

Online Test Problem

row number	numerator	numerator squared mods 34189
1	185	$2^2 \cdot 3^2$
2	1849	$-1 \cdot 3^2 \cdot 11$
3	5732	$3 \cdot 5 \cdot 13$
4	7581	$-1 \cdot 2^2 \cdot 37$
5	13313	193
6	20894	$-1 \cdot 3 \cdot 5 \cdot 7$
7	55101	$5 \cdot 7^2$
8	75995	$-1 \cdot 2^2 \cdot 11$
9	587066	$3 \cdot 7 \cdot 11$
10	663061	$-1 \cdot 3 \cdot 41$
11	1913188	43
12	15968565	$-1 \cdot 7 \cdot 13$
13	49818883	$2^2 \cdot 67$
14	65787448	$-1 \cdot 3 \cdot 7$
15	1102418051	$2^2 \cdot 3 \cdot 5^2$

Suppose we wish to use the CFRAC algorithm to factor $N = 34189$. In the table below, the first column of the jth row corresponds to the jth numerator of a reduced convergent of the simple continued fraction for $\sqrt{34189}$ for $1 \leq j \leq 15$. Letting $B = 11$ in the algorithm, we choose a_j's from among these numerators so that $s(a_j) = a_j^2 \mod{s} N$ (the residue in $(-N/2, N/2]$) has no prime factor greater than B. Note: We treat -1 as if it is a prime number. For the CFRAC algorithm, we end up attempting to factor N by properly combining information from different rows of the table to produce positive integers x and y such that $\gcd(x-y, N)$ has a good chance of giving us a non-trivial factor of N. For example, using rows 3, 6, and 12, we deduce that

$$\gcd(5732 \cdot 20894 \cdot 15968565 - 3 \cdot 5 \cdot 7 \cdot 13, 34189)$$

would be a good gcd to compute to try to factor N except that the prime divisor 13 appearing in this expression exceeds $B = 11$. Write down three different expressions like the one above (that is, expressions of the form $\gcd(x-y, 34189)$ where x and y are given explicitly but should be written as products as I have done above) that correspond to good gcd computations suggested by the CFRAC algorithm for finding a non-trivial factor of 34189. Note that you should be taking $B = 11$ (so my choice above would be a wrong answer) and you should NOT be doing the gcd computation (i.e., I am not asking for a non-trivial factor of 34189).

Suppose we wish to use the CFRAC algorithm to factor $N = 34189$. In the table below, the first column of the jth row corresponds to the jth numerator of a reduced convergent of the simple continued fraction for $\sqrt{34189}$ for $1 \leq j \leq 15$. Letting $B = 11$ in the algorithm, we choose a_j's from among these numerators so that $s(a_j) = a_j^2$ mods N (the residue in $(-N/2, N/2]$) has no prime factor greater than B. Note: We treat -1 as if it is a prime number. For the CFRAC algorithm, we end up attempting to factor N by properly combining information from different rows of the table to produce positive integers x and y such that $\gcd(x - y, N)$ has a good chance of giving us a non-trivial factor of N. For example, using rows 3, 6, and 12, we deduce that

$$\gcd(5732 \cdot 20894 \cdot 15968565 - 3 \cdot 5 \cdot 7 \cdot 13, 34189)$$

would be a good gcd to compute to try to factor N except that the prime divisor 13 appearing in this expression exceeds $B = 11$. Write down three different expressions like the one above (that is, expressions of the form $\gcd(x - y, 34189)$ where x and y are given explicitly but should be written as products as

$(-N/2, N/2])$ has no prime factor greater than B. Note: We treat -1 as if it is a prime number. For the CFRAC algorithm, we end up attempting to factor N by properly combining information from different rows of the table to produce positive integers x and y such that $\gcd(x-y, N)$ has a good chance of giving us a non-trivial factor of N. For example, using rows 3, 6, and 12, we deduce that

$$\gcd(5732 \cdot 20894 \cdot 15968565 - 3 \cdot 5 \cdot 7 \cdot 13, 34189)$$

would be a good gcd to compute to try to factor N except that the prime divisor 13 appearing in this expression exceeds $B = 11$. Write down three different expressions like the one above (that is, expressions of the form $\gcd(x - y, 34189)$ where x and y are given explicitly but should be written as products as I have done above) that correspond to good gcd computations suggested by the CFRAC algorithm for finding a non-trivial factor of 34189. Note that you should be taking $B = 11$ (so my choice above would be a wrong answer) and you should NOT be doing the gcd computation (i.e., I am not asking for a non-trivial factor of 34189).

row number	numerator	numerator squared mods 34189
1	185	$2^2 \cdot 3^2$
2	1849	$-1 \cdot 3^2 \cdot 11$
3	5732	$3 \cdot 5 \cdot 13$
4	7581	$-1 \cdot 2^2 \cdot 37$
5	13313	193
6	20894	$-1 \cdot 3 \cdot 5 \cdot 7$
7	55101	$5 \cdot 7^2$
8	75995	$-1 \cdot 2^2 \cdot 11$
9	587066	$3 \cdot 7 \cdot 11$
10	663061	$-1 \cdot 3 \cdot 41$
11	1913188	43
12	15968565	$-1 \cdot 7 \cdot 13$
13	49818883	$2^2 \cdot 67$
14	65787448	$-1 \cdot 3 \cdot 7$
15	1102418051	$2^2 \cdot 3 \cdot 5^2$

row number	numerator	numerator squared mods 34189
1	185	$2^2 \cdot 3^2$
2	1849	$-1 \cdot 3^2 \cdot 11$
~~3~~	~~5732~~	~~$3 \cdot 5 \cdot 13$~~
~~4~~	~~7581~~	~~$-1 \cdot 2^2 \cdot 37$~~
~~5~~	~~13313~~	~~193~~
6	20894	$-1 \cdot 3 \cdot 5 \cdot 7$
7	55101	$5 \cdot 7^2$
8	75995	$-1 \cdot 2^2 \cdot 11$
9	587066	$3 \cdot 7 \cdot 11$
~~10~~	~~663061~~	~~$-1 \cdot 3 \cdot 41$~~
~~11~~	~~1913188~~	~~43~~
~~12~~	~~15968565~~	~~$-1 \cdot 7 \cdot 13$~~
~~13~~	~~49818883~~	~~$2^2 \cdot 67$~~
14	65787448	$-1 \cdot 3 \cdot 7$
15	1102418051	$2^2 \cdot 3 \cdot 5^2$