UNIVERSITY OF CALIFORNIA
Department of Electrical Engineering
and Computer Sciences
Computer Science Division

CS 282 **Prof. R. Fateman**
Fall 2002

Assignment 3: FFT, Newton Iteration, and GCD problems

Due: Wed, 13 March, 2002

1. Write a paragraph describing your proposed course project. (See me during office hours or other times if you need help.)

2. Write out the 4 by 4 Fourier Transform matrix in $\mathbf{Z}_{17}$ using $\omega = 4$, as well as its inverse.

3. Create a trinary FFT in the following way: First note that idea that a polynomial p(x) with 3^n terms (degree $3^n - 1$) can be decomposed into three parts as

$$p(x) = p_0(x^3) + xp_1(x^3) + x^2p_3(x^3).$$

Here the degree of p_0, p_1 and p_2 are at most $3^{n-1} - 1$. Show how to evaluate $p(x)$ at 3^n points "fast". How fast? You should be able to follow the FFT handout.

4. Use Newton's method to find the first 8 terms of the reciprocal of the power series

$$a(x) = 2 - x^2 + x^3 + 4 * x^4 - 5 * x^5 + x^7 + \cdots$$

5. Given two multivariate polynomials over the integer $f(x_0, x_1, \ldots, x_{v-1})$ and $g(x_0, x_1, \ldots, x_{v-1})$, and the information that the gcd modulo some prime p of $f(x_0, 0, 0, \ldots, 0)$ mod p and $g(x_0, 0, 0, \ldots, 0)$ mod p is a constant, what can you say about the gcd of f and g? What additional conditions on f, g, and p would allow you to conclude that f and g were relatively prime?