CS 812
Spring 2024
Homework #2

Due Wednesday, March 20, 2024

Rules for Homework. See Homework 1.

1. A 1996 paper by Farris (see link next to this homework) deals with rotational symmetries of curves given in parametric form by

$$f(t) = \sum_{n \in \mathbf{Z}} a_n e^{int},$$

with a_n real. We will assume that $a_0 = 0$, the a_i are real, and all but finitely many of them are 0. The author's main theorem (p. 187) implies a criterion for such a curve to have a nontrivial rotational symmetry: there is a number $m > 1$ and a $u \in \mathbf{Z}_m^*$ such that every n with a nonzero a_n is congruent to u mod m.

   a) Find a computable upper bound on the largest m that could work. This implies that there is an algorithm to decide nontrivial symmetry.

   b) Is there a polynomial time algorithm for this? (Remember that we want polynomial in total bit length.)

2. [Logarithms in algorithms.] Many algorithms have bounds like $2 \ln^2 n$ (for ERH based prime testing) or $\sqrt{\phi(r)} \log_2 n$ (AKS). It is usually assumed without justification that these bounds can be efficiently computed.

   a) Let n and b be positive integers, with $1 < b \leq n$. Show that $\lfloor \log_b n \rfloor$ can be computed using $O(\lg n)^2$ bops, with ordinary arithmetic.

   b) Show that $\lfloor \ln n \rfloor$ is computable. [Hint: It is known that $e = 2.71828...$ is transcendental. That is, it is not the root of any polynomial equation with rational coefficients.]

   c) Show that $\ln n$ can be approximated with absolute error ≤ 1 in time polynomial in $\lg n$. [Hint: You can use the Maclaurin series for $\ln(1 + x)$, provided that x is small. Figure out how to reduce to this case.]

3. Background to this problem: In machine cryptography, permutations of the 26 Roman letters were hard wired into electrical devices called rotors. For technical reasons, it was desired to use a permutation σ for which the "shifts" $i - \sigma(i)$ were all distinct mod 26. Call a permutation *good* if that is the case.

   a) Consider the affine transformations on $\mathbf{Z}_n$ defined by

   $$x \mapsto ax + b$$

   Give a formula for the number of pairs (a, b) for which the above transformation is a good permutation on $\mathbf{Z}_n$. (Hint: consider primes, then prime powers, and finally general n using the Chinese remainder theorem.)

   b) Estimate this number as a function of n.

   c) (*) Find other "easy" ways to make good permutations on $\mathbf{Z}_n$. A desirable property of such constructions is that the set of permutations you can make is large.

4. In class we discussed methods for finding square roots mod p^k, when p is an odd prime. This exercise deals with $p = 2$ (which is needed for the quadratic sieve).

   a) Let f be a monic polynomial in $\mathbf{Z}[X]$. Suppose that $f(x_0) \equiv 0 \pmod{2^m}$, $2^n || f'(x_0)$, and $m > 2n$. Give an efficient algorithm that constructs a solution to $f(x) \equiv 0 \pmod{2^{2m-2n}}$. Note that by hypothesis, $2m - 2n > m$. [Hint: Pick an appropriate j, and then use the Taylor series for $f(x_0 + x_1 2^j)$ to get a congruence you can solve for x_1.]

   This actually holds for any prime p, but we only need it for $p = 2$.

   b) Let $k \geq 3$. Find explicit formulas for four different square roots of 1 in $\mathbf{Z}_{2^k}^*$. Conclude that this group is not cyclic. Under what conditions is $a \in (\mathbf{Z}_{2^k}^*)^2$?

   c) Using the result of a), show how to compute square roots in $\mathbf{Z}_{2^k}^*$ using $O(k^2)$ bops. [Hint: When $m > 2n$, the sequence defined by $k_i = 2k_{i-1} - 2n$, with $k_0 = m$, grows exponentially.]

   Note: The quadratic formula involves division by 2, so it can't be used directly to solve the quadratic $x^2 + bx + c \equiv 0 \pmod{2^k}$. Gauss found the following elegant substitute. Multiply the congruence by 4 and rearrange to get

   $$(2x + b)^2 \equiv b^2 - 4c \pmod{2^{k+2}}.$$

   The solutions to the original congruence are found by solving $2x + b \equiv y \pmod{2^{k+2}}$, where y runs over the solutions to $y^2 \equiv b^2 - 4c \pmod{2^{k+2}}$.