Algorithms Core 15-750 PROBLEM SET # 5 Spring 1999

DUE: 1:00PM Wednesday April 7 1999

1 Another GCD Algorithm

Consider the following variant of Euclid's GCD algorithm.

Procedure $GCD(a, b)$

1. If $a = 0$ then return b
2. If $b = 0$ then return a
3. If a is even then $GCD(a/2, b)$
4. If b is even then $GCD(a, b/2)$
5. If a and b are both odd then $GCD(\frac{a+b}{2}, \frac{a-b}{2})$

Problem 1.1 *Show that this algorithm correctly computes the GCD of a and b if either a or b is odd.*

Problem 1.2 *Show that this algorithm computes the GCD of a and b in time polynomial in the length of a and b.*

2 Randomized Algorithm for Square Roots

Suppose that p is an odd prime and a is a quadratic residue mod p, i.e., there exists an integer b such that $b^2 \equiv a \pmod{p}$.

Consider the following randomized algorithm for finding $\pm b$

Procedure $SquareRoot(a, p)$

1. Randomly pick $0 \leq \alpha, \beta < p$ and set $f(x) = \alpha x + \beta$
2. Compute $g(x) = GCD(f(x)^{\frac{p-1}{2}} + 1, x^2 - a)$, the polynomial GCD over the field Z_p. We assume that $g(x)$ is monic, the leading coefficient is one.
3. If $g(x) = x^2 - a$ or 1 then $SquareRoot(a, p)$
   else return the constant coefficient of $g(x)$.

end

Through a collection for subproblems we shall show that $SquareRoot(a, p)$ is a polynomial time randomized algorithm which correctly compute a square root of a modulo p.

2.1 Timing

The only non-constant time step is 2.,assuming that we can generate random number in unit time.

Problem 2.1 *Show how to compute $g(x)$ in time polynomial in* $\log p$.

2.2 Correctness

To see correctness we shall think of this algorithm in a very different way. In particular, we will view $f(x)$ as an element in the quotient ring $R = Z_p[x]/(x^2 - a)Z_p[x]$. Since is a quadratic residue module p the polynomial $x^2 - a$ is reducible over Z_p, i.e., $x^2 - a = (x - b)(x + b)$.

Problem 2.2 *Show that the ring $Z_p \times Z_p$(the direct product of Z_p with itself) is isomorphic to the ring $R = Z_p[x]/(x^2 - a)Z_p[x]$. If ϕ is the isomorphism from $Z_p \times Z_p$ to R. What is $\phi(1,1)$, $\phi(0,0)$, $\phi(1,0)$, and $\phi(0,1)$*

Problem 2.3 *Thinking of the polynomial $f(x)$ from line 1 as an element of R. Show that $f(x)$ is uniformly generated from R.*

Problem 2.4 *Thinking of the polynomial $h(x) = f(x)^{\frac{p-1}{2}}$ as an element of $Z_p \times Z_p$. Enumerate the different values that $h(x)$ could be with their probabilities.*