CAS CS 235: Algebraic Algorithm Spring 2011 Instructor: Leonid Levin

Lecture Notes and Exercises 1

Scriber: Xianrui Meng *Jan. 29, 2012* Teaching Fellow: Xianrui Meng

Exercises #1 (1.10 Victor Shoup): Let $a, b \in \mathcal{Z}$, and $d = gcd(a, b)$. Prove that $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof: (Sketch) Since $d = gcd(a, b)$, we will have $as + bt = d$ (**Thm 1.8**). Also, $d|a$ and $d|b$, so for some $k_1, k_3 \in \mathcal{Z}$, $\frac{a}{d} = k_1$ and $\frac{b}{d} = k_2$. Rewrite $as + bt = d$ as $\frac{a}{d}s + \frac{b}{d}t = 1$, we can conclude that $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Exercises #2 (Euclid's Lemma): If $a|bc$ and $gcd(a, b) = 1$, then $a|c$.

Proof: (Sketch) Since $gcd(a, b) = 1$, $\exists$ some $x, y \in \mathcal{Z}$ such that $ax + by = 1$. $c = 1 \cdot c = (ax + by)c = acx + bcy$. Also, we have $a|ac$ and $a|bc$, then $a|(acx + bcy)$, i.e. $a|c$.

Exercises #3 Suppose we have $x^2 \equiv 1 \pmod{p}$, where p is a prime and $p > 2$. Show that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

Proof: (Sketch) If $x^2 \equiv 1 \pmod{p}$, then we will have $p|(x^2 - 1)$, i.e. $p|(x + 1)(x - 1)$. Since here p is a prime and $p > 2$, we will have $p|(x - 1)$ or $p|(x + 1)$, i.e. $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$

Exercises #4 Let $a, b, n, n' \in \mathcal{Z}$ with $n, n' > 0$ and $n'|n$. Show that $a \equiv b \pmod{n}$ implies $a \equiv b \pmod{n'}$.

Proof: (Sketch) $a \equiv b \pmod{n}$ means $n|(b - a)$. Since $n'|n$ this implies $n'|(b - a)$, hence $a \equiv b \pmod{n'}$.