

Exercise 2, Discrete Mathematics for Bioinformatics

Sascha Meiers, Martin Seeger

Winter term 2011/2012

2.1 Modulo Arithmetic

a) We show that $\langle a \rangle \subset \langle d \rangle$.

Since $d = \gcd(a, n)$, there is a $k \in \mathbb{N}$ such that $a = kd$. Hence, if $v \in \langle a \rangle$, i.e. $v = ai \pmod n$, then $v = dki \pmod n$ which implies that $v \in \langle d \rangle$.

b) We show that $\langle a \rangle \supset \langle d \rangle$.

Any element v of $\langle d \rangle$ can be written as $v = di \pmod n$ (*). On the other hand, $v \in \langle a \rangle$ iff $v = aj \pmod n$.

We now use Bezout's lemma to find x, y , such that $ax + ny = d$. This is inserted into (*) to yield

$$v = di \pmod n = (ax + ny)i \pmod n = axi \pmod n.$$

In other words, $v \in \langle a \rangle$. \square

2.2 Hashing

x

2.3 Hashing

x

2.4 Expected value

x