

This and other notes are available from <http://www.cs.berkeley.edu/~yozo/cs170.fa05/>

Number Theory Review

Let p denote a prime.

- If $ax = ay \pmod p$ then does it follow that $x = y$?
- Can we solve for x in the equation $ax = b \pmod p$? In particular, every non-zero integer has an inverse in $\mathbb{Z}/p\mathbb{Z}$.
- Give examples where the above two fails in modular arithmetic in m , a non-prime.

Hash Functions

- Suppose we want to look up a student's name given his/her ID. What is the universe U in this case? How many elements are there? Would direct addressing work?
- Now suppose we are just talking about students in this class. What is the universe size now? How would you implement a hash function?
- Now suppose we want to look up a student's ID given his/her name. What is the universe U ? Size of U ? Good hash function?
- Java string hash function (`String.hashCode()`). Up to JDK 1.1 it sampled every n -th character. Now it uses base-31 interpretation of the string.

2-Universal Hash Family

- Given a hash function h , can we choose distinct inputs x_1 and x_2 so that they hash to the same spot? What about three elements x_1, x_2, x_3 ? Up to how many elements can hash to the same spot? Minimal value of this number (over all hash functions)?
- Suppose the hash function returns a uniformly random value. What is the probability that two distinct elements x and y collide?
- Example of 2-universal hash function: $h_{a,b}(x) = (ax + b \pmod p) \pmod m$, with $a \neq 0$ and $p > m$ a prime. Can we use $a = 0$? Why can't we just use $h'_{a,b}(x) = ax + b \pmod m$, even if m is prime?
- Another example from lecture: break x into s -bit fragments x_1, x_2, \dots, x_r . Let $h(x) = a_1x_1 + a_2x_2 + \dots + a_rx_r \pmod p$.

More Questions

1. Suppose you had a hash function h that evenly distributes the input. Given a random sequence of inputs x_1, x_2, \dots, x_n , how big does n has to be on average before we get a collision?
2. Can a hash family (not necessarily universal) have a probability of collision less than $1/m$ for all pairs x, y such that $x \neq y$?
3. When does $x \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse?

4. Another example. Suppose $M = 2^r$ and $m = 2^s$. Then we can interpret elements in U as a r -bit vector, and likewise table indices as a s -bit vector. Let $h(x) = Ax$ where A is a $s \times r$ random 0-1 matrix (we are considering modulo-2 arithmetic here). Show that these hash functions form a 2-universal hash family.