- This problemset has *one* question. The programming problems may be harder, or require more time, than their point value suggests.
- Please send the solutions to `gawry1+EDSCourse2014@gmail.com`
- The deadline is 08.06.2014 anywhere on Earth.

(80) 1. We want to construct a family of universal hash functions. We assume that the numbers that we are hashing consist of w bits and we want to hash them into ℓ bits. Then it turns out that a nice family is

$$\mathcal{H} = \{H_a : a \in [1, 2^w) \text{ and } a \text{ is odd}\}.$$

where $H_a = \left\lfloor \frac{a \cdot x}{2^{w-\ell}} \right\rfloor \bmod 2^\ell$. Observe that H_a simply takes a range of bits from $a \cdot x$.

(a) Why such functions might be better than $a \cdot x \bmod p$, where p is a prime?

(b) Prove that, for any $\ell \in [1, w]$ and distinct $x, y \in [0, 2^w)$, if we choose a function $H_a \in \mathcal{H}$ uniformly at random, then the chance that $H_a(x) = H_b(y)$ is at most $\frac{1}{2^{\ell-1}}$.
Hint: Take $x < y$ and try to count all odd $a \in [0, 2^w)$ such that $H_a(x) = H_a(y)$. First bound the difference $|a \cdot x \bmod 2^w - a \cdot y \bmod 2^w|$. Then denote $z = y - x$ and look at the expression $a \cdot z \bmod 2^w$. Notice that the bound on the difference implies that the value of the expression belongs to one of two continguous intervals, each of length $2^{w-\ell}$ (so far everything holds even if we allow even a's). Now write $z = z'2^s$ with z' odd. Think what happens when $s = 0$. This special case is enough for (large) partial credit.

(c) Use the previous bound to show that for any set of n integers $S \subseteq [0, 2^w)$, if we choose a function $H_a \in \mathcal{H}$ uniformly at random, then the chance that H_a is injective (i.e., assigns different outputs to different inputs) on S is at least $1 - \frac{n^2}{2^\ell}$.