Daniel Frey

CS 4920-001

Assignment 2

2/14/17

**Problem 1: Dice**

1. Typical die; entropy value for one event:

Typical die; entropy value for four events:

1. Modified dice (1-4 occupy one side, 5 occupies two sides); entropy value for one event:

Modified dice (1-4 occupy one side, 5 occupies two sides); entropy value for four events:

1. You can maximize entropy by having each side represent a unique number.
2. To minimize entropy, you would have each side would have the same number.

**Problem 2: Balls in a Bin**

5 red, 3 yellow, 4 green; pick ball put back

1. Entropy value for one event:

1. Entropy value for five events:

1. Add two yellow balls; entropy value for one event:

1. Adding one green ball to the bin will maximize the entropy.

**Problem 3: GCD**

1. Determine gcd(24140, 16762) = 34
2. Determine gcd(4655,12075) = gcd(12075,4655) = 35
3. Determine gcd(4278,8602) = gcd(8602,4278) = 46

**Problem 4: Proofs**

1. a ≡ b (mod n) implies b ≡ a (mod n)

If a, b ∈ Z and a ≡ b (mod n), then a − b = k · n for some k ∈ Z, and so b − a = (−k) · n, so that b ≡ a (mod n).

1. a ≡ b (mod n) and b ≡ c (mod n) imply a ≡ c (mod n)

If a, b, c ∈ Z, with a ≡ b (mod n) and b ≡ c (mod n), then a − b = k · n and b − c = j · n, for some k, j ∈ Z, so that a − c = a − b + b − c = (k + j) · n, and a ≡ c (mod n).

1. [(a mod n) - (b mod n)] mod n = (a - b) mod n

let a=hn-(a mod n),b=kn-(b mod n) and h,k ∈ Z  
R.H.S:

(a-b) mod n=[ a-b-(h+k)n] mod n

=[hn- a mod n )+(kn+b mod n)-hn -kn]mod n

=(a mod n- b mod n) mod n=L.H.S

1. [(a mod n) × (b mod n)] mod n = (a × b) mod n

let a mod n = h, a = kn + h, b = jn + g

ab = (kn + h)(jn + g)

ab = kjn2 + hjn + ghn + hg

= ab − hg = (kjn + hj + gh)n

= (ab) mod n = (hg) mod n.

**Problem 5: Proofs**

1. For two consecutive integers n and n+1, gcd(n,n+1)=1

d/n and d/n+1 so d/n+1-n, therefore d/1 and d is equal to +or - 1

1. Given two integers a and b, prove that Euclidean algorithm, described in Section 2.2, yields the greatest common divisor gcd(a,b)

Show that if a = bq + r, then an integer d is a common divisor of a and b if, and only if, d is a common divisor of b and r.

Let d be a common divisor of a and b, then d|a and d|b. Thus d|(a − bq), which means d|r, since r = a − bq.

Therefore, d is a common divisor of b and r.

Now suppose d is a common divisor of b and r. Then d|b and d|r.

Therefore, d|(bq +r), so d|a.

Therefore, d must be a common divisor of a and b.

Therefore, the set of common divisors of a and b are the same as the set of common divisors of b and r.

It follows that d is the greatest common divisor of a and b if and only if d is the greatest common divisor of b and r