Arithmetic Algorithms 2014: HW1

Taylor Lee

Febuary 14, 2014

Problem 2

Part A:

A pair (a,b) creates a good permutation is this context if and only if $\gcd(a,n) = \gcd(a-1,n) = 1$.

It is clear that any affine transformation, $f : \mathbb{Z}_n \to \mathbb{Z}_n$ where

$$x \mapsto a\,x + b \pmod{n}$$

is a bijection if only if a has an inverse in $\mathbb{Z}_n$. For if we let $y = a\,x + b \pmod{n}$, then $a\,x = y - b \pmod{n}$ and hence $x = a^{-1}\big(y - b\big) \pmod{n}$ if and only if $\exists a^{-1} \in \mathbb{Z}_n$. Next, in order to be a good permutation, $g(x) = x - f(x) \pmod{n}$ must also be a bijection, as this is equivalent to each shift g being unique. If g is bijective, then for any $d \in \mathbb{Z}_n$ there must be a solution $x \in z\,z_n$ to the equation:

$$x - a\,x - b \equiv c \pmod{n}$$

We will add b to both sides and multiply by -1 in order to put this congruence into a more desirable form:

$$(a-1)\,x \equiv b - c \pmod{n}$$

Here again, we can see that no matter the b, if given a c, only when $a-1$ has an inverse $(\text{mod } n)$ can we ensure that a solution $x \in \mathbb{Z}_n$ will exist. Hence, our initial statement as to what pairs (a,b) create a good permutation is correct.

Part B:

How many of these 'good' pairs (a,b) exist, given $n \in \mathbb{Z}^+$? Let us first consider when n is a prime p. In this case, the number of invertible elements in $\mathbb{Z}_p = p-1$, as all other integers are coprime with p, except for the additive identity, 0. Hence, for prime p, there are $p(p-1) = p^2 - p$ possible pairs, as there are p possible b and $p-1$ possible a.

We can now consider prime powers, or permutations of $\mathbb{Z}_{p^k}$. The only elements of this ring which don't have inverses are those which have p as a divisor and 0. Hence, for $\mathbb{Z}_{p^k}$, we can start with 0 and add p to it repeatedly in order to iterate over all of the elements of $\mathbb{Z}_{p^k}$ which do not have inverses, and we can see that since there are p^k elements in this ring, and since we are incrementing by p, there are p^{k-1} elements which do not have inverses, and hence $p^k - p^{k-1}$ elements in $\mathbb{Z}_{p^k}$ which could be a and ensure that our affine transformation is bijective and hence a permutation. However, as we have shown above, $a-1$ must also be invertible in $\mathbb{Z}_{p^k}$. This means that our count for the number non-invertible elements in $\mathbb{Z}_{p^k}$ must double. Thus, the number of elements in $\mathbb{Z}_{p^k}$ which could be a and satisfy our conditions for a good permutation are:

$$p^k - 2p^{k-1} = p^{k-1}(p-2) = (2p^k - 2p^{k-1}) - p^k = 2\varphi(p^k) - p^k.$$

We can multiply this number by p^k, on behalf of the initial shift b, in order to get the total number of pairs (a,b) in $\mathbb{Z}_{p^k}$ which correspond to good permutations.

This result can be generalized to any $n \in \mathbb{Z}^+$ with the Chinese Remainder Theorem, since if

$$n = p_1^{k_1} \times \cdots \times p_i^{k_i}$$

Where each p_j is distinct, then we have two isomorphic rings:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_h^{k_h}}.$$

And hence our most general formula for pairs (a,b) is

$$\#_{a,b}(n) = n \prod_{p|n} \left[2\varphi(p_i^{k_i}) - p_i^{k_i} \right]$$

Where k_j is the multiplicity of p_j in n.