

6.10

Assume $k = \prod_i^n p_i^{\alpha_i}$

Construct vector $\mathbf{x} = (x_i)_i$ which is k-size

Here then we can pick a_i, b_i from $p_i^{\alpha_i}$

And $x_i = a_j * i + b_j \bmod p_j^{\alpha_j}$ for every $j \in [n]$

Using the chinese remainder therorem, $x_i = \sum_j^n (a_j * i + b_j) * \frac{k}{p_j^{\alpha_j}} * (\frac{p_j^{\alpha_j}}{k} \bmod p_j^{\alpha_j}) \bmod k$

Since $0 \leq x_i \leq k-1$, x_i can be determined by above equation.

And k^2 choose all $a_1, b_1, a_2, b_2 \dots$, it is next step to generate k^2 .

Next, prove for $x_i = x_j$ and for all $0 \leq w, z \leq k-1$, there is unique choice of a_i, b_i for all i , which $x_i = w, x_j = z$.

Let $w_j = w \bmod p_j^{\alpha_j}$, and $z_j = z \bmod p_j^{\alpha_j}$, where $w_j = a_j * m + b_j$ and $z_j = a_j * n + b_j$.

Then a_j and b_j can be unique.

Finally, for a certain i and j, each vector generated a_i, b_i for all i , which has relation to w, z in No. i position with No. j coordinates.

So, k^2 where each pair of these values appears only once. ****