关于 Pollard_Rho 的期望复杂度的证明

设我们要分解 n，$n=n_1n_2(n_1 \leqslant n_2)$，我们构造的序列为 a_i，$a_i\%n_1=b_i$

为 a_i 可近似看为随机序列，根据生日悖论可以推出其出现循环的期望步数为 sqrt(n)，b_i 同理。

因为 $n>n_i$，所以在 b_i 循环之后，a_i 有很大可能没有进入循环，此时 $a_i-a_j=(k_in_1+b_i)-(k_jn_1+b_j)=(k_i-k_j)n_1+(b_i-b_j)=(k_i-k_j)n_1$。于是求 gcd 即可求出 n_1。