Homework 11

Question 1

5.39. Solve the discrete logarithm problem $10^x = 106$ in the finite field $\mathbb{F}_{811}$ by finding a collision among the random powers 10^i and $106 \cdot 10^i$ that are listed in Table 5.17.

i	g^i	$h \cdot g^i$
116	96	444
497	326	494
225	757	764
233	517	465
677	787	700
622	523	290

i	g^i	$h \cdot g^i$
519	291	28
286	239	193
298	358	642
500	789	101
272	24	111
307	748	621

i	g^i	$h \cdot g^i$
791	496	672
385	437	95
178	527	714
471	117	237
42	448	450
258	413	795

i	g^i	$h \cdot g^i$
406	801	562
745	194	289
234	304	595
556	252	760
326	649	670
399	263	304

Table 5.17: Data for Exercise 5.39, $g = 10$, $h = 106$, $p = 811$

Question 2

5.40. Table 5.18 gives some of the computations for the solution of the discrete logarithm problem

$$11^t = 41387 \quad \text{in } \mathbb{F}_{81799} \tag{5.62}$$

using Pollard's ρ method. (It is similar to Table 5.11 in Example 5.52.) Use the data in Table 5.18 to solve (5.62).

i	x_i	y_i	α_i	β_i	γ_i	δ_i
0	1	1	0	0	0	0
1	11	121	1	0	2	0
2	121	14641	2	0	4	0
3	1331	42876	3	0	12	2
4	14641	7150	4	0	25	4
			$\vdots$			
151	4862	33573	40876	45662	29798	73363
152	23112	53431	81754	9527	37394	48058
153	8835	23112	81755	9527	67780	28637
154	15386	15386	81756	9527	67782	28637

Table 5.18: Computations to solve $11^t = 41387$ in $\mathbb{F}_{81799}$ for Exercise 5.40

Question 3

This exercise describe Pollard-ρ-factorization algorithm.

$N = pq$ where p and q are odd primes

Let $f(x) = x^2+1 \mod N$.

Let $x_0 = y_0 = 2$

For $i = 1, 2, \ldots$

(a) compute $x_i = f(x_{i-1})$

(b) Compute $y_i = f(f(y_{i-1}))$

(c) Compute $g_i = \gcd(|x_i - y_i|, N)$.

If $g_i \neq 1$, returned g_i as the prime divisor of N.

(1) For each of the following cases, compute the smallest k such that $g_k \neq 1$ and the ratio $k/\sqrt{N}$.

(A) $N = 8051$

(B) $N = 10403$

(C) $N = 9409613$

(2) Let p be the smallest prime divisor of N. Suppose that the function f is random, show that the algorithm factors N in $O(\sqrt{p})$ steps.