Math 1580 – Problem Set 8. Due Friday Nov. 11, 4pm

Problem 1. The Miller-Rabin primality test is an example of a Monte Carlo or probabilistic algorithm. This problem concerns such algorithms more generally. Let S be a set, let A be a property of interest, and suppose that for $m \in S$, we have $\mathbb{P}(m \text{ has property } A) = \delta$. Suppose that a Monte Carlo algorithm applied to m and a random number r satisfy

(a) If the algorithm returns 'Yes', then m definitely has the property A.

(b) If m has property A, then the probability that the algorithm returns 'Yes' is at least p.

In other words,

$$\mathbb{P}(m \text{ has property } A \mid \text{algorithm returns 'Yes'}) = 1$$

$$\mathbb{P}(\text{algorithm returns 'Yes'} \mid m \text{ has property } A) \geq p.$$

Suppose that we run the algorithm N times on the number m, and suppose that the algorithm returns 'No' every single time. Derive a lower bound, in terms of δ, p, and N, for the probability that m does not have property A.

Problem 2. Here is a description of Pollard's ρ algorithm for finding a factor of an integer N. Set

$$f(x) = x^2 + c, \quad c \neq 0, -2$$

though just about any integer polynomial will do.

(1) Set $x_0 = y_0 = 2$.

(2) For $i = 1, 2, \ldots$, do the following:

  (a) Set $x_i \equiv f(x_{i-1}) \pmod{N}$, $y_i \equiv f\big(f(y_{i-1})\big) \pmod{N}$.

  (b) Let $d = \gcd(|x_i - y_i|, N)$.

  (c) If $1 < d < N$ return d. If $d = N$, return failure. Otherwise if $d = 1$, continue.

Use the results about the abstract Pollard ρ method stated in class to show that the expected running time to produce a factor of N is $\mathcal{O}(\sqrt{p})$, where p is the smallest prime factor of N. (Hint: think about $S = \mathbb{Z}/p\mathbb{Z}$.)

Problem 3. The following table lists some computations for the solution of the discrete logarithm problem

$$7^k = 3018 \quad \text{in } \mathbb{F}_{7963} \tag{1}$$

using Pollard's ρ method. Extend the table until you find a collision (it shouldn't take too long) and then solve (**??**).

i	x_i	x_{2i}	α_i	β_i	α_{2i}	β_{2i}
0	1	1	0	0	0	0
1	7	49	1	0	2	0
2	49	2401	2	0	4	0
3	343	6167	3	0	6	0
4	2401	1399	4	0	7	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
87	1329	1494	6736	7647	3148	3904
88	1340	1539	6737	7647	3150	3904
89	1417	4767	6738	7647	6302	7808
90	1956	1329	6739	7647	4642	7655