Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, KONSTANTIN ZIEGLER

5. Assignment: Pollard's ϱ method and polynomial-time reductions

(Due: Thursday, 03 December 2009, 23^{59})

Exercise 5.1 (An example of Pollard's ϱ method). (8 points)

(i) Complete the table below, which represents a run of Pollard's ϱ algorithm for $N = 100181$ and the initial value $x_0 = 399$, up to $i = 6$. $\boxed{3}$

i	x_i rem N	x_i rem 17	y_i rem N	y_i rem 17	gcd$(x_i - y_i, N)$
0	399	8	399	8	100181
1	...	...	...	...	...

(ii) The smallest prime divisor of N is 17. Describe the idea of the algorithm by looking at x_i rem 17 and y_i rem 17 and in particular, why we stopped at $i = 6$. $\boxed{3}$

(iii) Complete the factorization of N using Pollard's ϱ algorithm. $\boxed{2}$

Exercise 5.2 (Polynomial-time reduction). (6 points)

Consider the following two decision problems

- `Primes`: On input of an integer x, decide whether x is a prime.
- `Factor`: On input of two integers k, x, decide whether x has a factor at most k.

(i) Reduce one problem to the other and use the appropriate notation. $\boxed{2}$

(ii) How can you use an efficient algorithm for `Factor` to actually factor an integer? $\boxed{2}$

(iii) In (i), suppose there was a reduction in the other direction as well. What would that imply? Is such a reduction likely to exist? $\boxed{2}$