Cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

5. Assignment: Pollard’s $\varrho$ method and polynomial-time reductions
(Due: Thursday, 03 December 2009, 23:59)

Exercise 5.1 (An example of Pollard’s $\varrho$ method). (8 points)

(i) Complete the table below, which represents a run of Pollard’s $\varrho$ algorithm for $N = 100181$ and the initial value $x_0 = 399$, up to $i = 6$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$x_i \text{ rem } N$</th>
<th>$y_i \text{ rem } N$</th>
<th>$\gcd(x_i - y_i, N)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>399</td>
<td>8</td>
<td>100181</td>
</tr>
<tr>
<td>1</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
</tr>
</tbody>
</table>

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

(iii) Complete the factorization of $N$ using Pollard’s $\varrho$ algorithm.

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.

(ii) How can you use an efficient algorithm for Factor to actually factor an integer?

(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?