COMP2711H Tutorial 8

Yuchen Mao

Department of Computer Science and Engineering,
Hong Kong University of Science and Technology

1 Extended Euclidean Algorithm

Example 1.1. Calculate the greastest common divisor d of $a = 2445$ and $b = 652$. Which integers s and t make $as + bt = d$?

i	r_i	q_i	s_i	t_i
0	2445		1	0
1	652	3	0	1
2	489	1	1	-3
3	163	3	-1	4
4	0			

so we have that $163 = (-1)2554 + (4)652$.

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i q_i \\ r_i &= as_i + bt_i \\ s_{i+1} &= s_{i-1} - q_i s_i \\ r_{i+1} &= r_{i-1} - q_i r_i \end{aligned}$$

2 Fermat's Little Theorem

Exercise 1. What is the value of $9^{794} \mod 73$?

Exercise 2. What is the value of $34^{70} \mod 73$?

Exercise 3. Prove that $(2^{70} + 3^{70}) \mod 13 = 0$.

Reference

1. `http://www.oxfordmathcenter.com/drupal7/node/204`

2. `http://people.brandeis.edu/~jbellaic/nt/ex2sol.pdf`

3. `http://db.math.ust.hk/notes_download/elementary/number/ne_N1.pdf`