CS 235: Algebraic Algorithms, Spring 2021

Discussion 3

Date: Tuesday, February 23, 2021.

Problem 1. Euler's/ Fermat's Little Theorem.

(a) Find 3^{31} mod 7, 2^{35} mod 7.

(b) Solve the congruence $x^{103} \equiv 4 \pmod{11}$.

(c) Suppose that p and q are distinct primes, $a^p \equiv a \pmod{p}$, and $a^q \equiv a \pmod{p}$. Show that $a^{pq} \equiv a \pmod{pq}$.

Problem 2. Prove that an odd integer n is prime if and only if $(n-2)! \equiv 1 \pmod{n}$.

Problem 3. Apply the Extended Euclidean's Algorithm to find the $\gcd(240, 46)$ and two integers s and t such that $240s + 46t = \gcd(240, 46)$.

Recall: Let a, b be integers, with $a \geq b \geq 0$. Using the division with remainder property, define the integers $r_0, r_1, \ldots, r_{\lambda+1}$ and $q_1, \ldots, q_\lambda$ where $\lambda \geq 0$ and integers $s_0, s_1, \ldots, s_{\lambda+1}$ and $t_0, t_1, \ldots, t_{\lambda+1}$ as follow:

$$r_0 := a, \quad s_0 := 1, \quad t_0 := 0,$$

$$r_1 := b, \quad s_1 := 0, \quad t_1 := 1,$$

$$r_{i+1} := r_{i-1} - q_i r_i,$$

$$s_{i+1} := s_{i-1} - q_i s_i,$$

$$t_{i+1} := t_{i-1} - q_i t_i$$

$$\ldots$$

$$(i = 1, 2, \ldots, \lambda)$$

then, for $i = 0, \ldots, \lambda + 1$, we have $as_i + b_t i = r_i$; in particular, $as_\lambda + bt_\lambda = \gcd(a, b)$. See Theorem 4.3 (page 78) for the rest of the properties.