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 $x^{103} \equiv 4 \pmod{11}$.

$\alpha^{p-1} \equiv 1 \pmod{p}$

$\hookrightarrow x \in \mathbb{Z}_{11}$

(a) $3^6 \equiv 1 \pmod 7$

$$3^{31} = \underbrace{(3^6)}_{\equiv 1}{}^5 \cdot 3^1 \equiv \underbrace{3^1}_{3} \pmod 7$$

$$3^{31} \bmod 7 = 3$$

$$\underbrace{2^{35}}_{(2^6)^5 \cdot 2^5} \bmod 7 = 4$$

(b) $x^{10} \equiv 1 \pmod{11}$

$$x^{103} = \underbrace{(x^{10})}_{1}{}^{10} \cdot x^3 \equiv x^3 \pmod{11}$$

$$x^3 \equiv 4 \pmod{11} \rightarrow 5^3 \equiv 4 \pmod{11}$$

Sol: $x \equiv 5 \pmod{11}$

(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 $(n-2)! \equiv 1 \pmod{n}$.

"$\Rightarrow$": n is an odd prime

$$(n-1)! \equiv -1 \pmod{n}$$

$$\Rightarrow (n-1)(n-2)! \equiv -1 \pmod{n}$$

Since $n-1 \equiv -1 \pmod{n}$ (*)

$$\Rightarrow (-1)(n-2)! \equiv (-1) \pmod{n}$$

$$\Rightarrow (n-2)! \equiv 1 \pmod{n}$$

"$\Leftarrow$": $(n-2)! \equiv 1 \pmod{n}$

$$(n-1)(n-2)! \equiv (n-1) \pmod{n}$$

$$(n-1)! \equiv (-1) \pmod{n}$$

By Wilson's, n is prime

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:

set up
$$\begin{cases} r_0 := a, & s_0 := 1, \quad t_0 := 0, \\ r_1 := b, & s_1 := 0, \quad t_1 := 1, \end{cases}$$

iteration
$$\begin{cases} r_{i+1} := r_{i-1} - q_i r_i, & (*) \\ s_{i+1} := s_{i-1} - q_i s_i, \\ t_{i+1} := t_{i-1} - q_i t_i \end{cases}$$

$$\ldots$$

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

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.

i	q_i	r_i		
0	N/A	240	1	0
1	N/A	46	0	1
2	5	10	1	-5
3	4	6	-4	21
4	1	4	5	-26
5	1	2	-9	47
6	2	0	23	-120

$\frac{46}{|23|} = 2, \frac{240}{|-120|} = 2$

useful for checking correctness

$\gcd(240, 46) = 2$, $s = -9$, $t = 47$