Ve203 Discrete Mathematics (Spring 2022)

Assignment 5

Date Due: 21:00 PM, Tuesday, Apr. 5, 2022
This assignment has a total of **(40 points)**.

Exercise 5.1 (4 pts)
Given $a, b, c, d, m \in \mathbb{Z}$, $m > 0$. Show that

(i) `(2 pts)` If $a \equiv b \pmod{m}$, and $d \mid m$, $d > 0$, then $a \equiv b \pmod{d}$.

(ii) `(2 pts)` If $a \equiv b \pmod{m}$, and $c > 0$, then $ac \equiv bc \pmod{mc}$

Exercise 5.2 (4 pts)
Given $a, x, y, m \in \mathbb{Z}$, $m > 0$. Show that

(i) `(2 pts)` $ax \equiv ay \pmod{m}$ iff $x \equiv y \left(\mod \dfrac{m}{\gcd(a, m)}\right)$.

(ii) `(2 pts)` If $ax \equiv ay \pmod{m}$ and $\gcd(a, m) = 1$, then $x \equiv y \pmod{m}$.

Exercise 5.3 (2 pts)
Given $x, y \in \mathbb{Z}$, and positive intergers $m_1, \ldots, m_r$, show that $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$ iff $x \equiv y \pmod{m}$, where $m = \operatorname{lcm}(m_1, m_2, \ldots, m_r)$.

Exercise 5.4 (6 pts)
Given $p \in \mathbb{P}$, show that

(i) `(2 pts)` $x^2 \equiv 1 \pmod{p}$ iff $x \equiv \pm 1 \pmod{p}$.

(ii) `(2 pts)` (Wilson's theorem) $(p-1)! \equiv -1 \pmod{p}$.

(iii) `(2 pts)` If $p \equiv 3 \pmod{4}$, then $\left(\dfrac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$.

Exercise 5.5 (2 pts)
We know that for all integers a coprime to 561, we have

(i) $a^{3-1} \equiv 1 \pmod{3}$ (ii) $a^{11-1} \equiv 1 \pmod{11}$ (iii) $a^{17-1} \equiv 1 \pmod{17}$

Show that $a^{561} \equiv a \pmod{561}$ for all integers a.

Exercise 5.6 (6 pts)
Given $p, q \in \mathbb{P}$, $a \in \mathbb{Z}$, show that

(i) `(2 pts)` If $a^q \equiv 1 \pmod{p}$, then either $p \equiv 1 \pmod{q}$ or $a \equiv 1 \pmod{p}$.

(ii) `(2 pts)` If $5 \mid a$ and $p \mid a^4 + a^3 + a^2 + a + 1$, then $p \equiv 1 \pmod{5}$.

(iii) `(2 pts)` Use (ii) to show that there are infinitely many primes of the form $10n + 1$, $n \in \mathbb{N}$.

Exercise 5.7 (2 pts)
Find prime factors of $F_5 = 2^{2^5} + 1$ by applying Fermat's theorem.

Exercise 5.8 (2 pts)
Show that 2021 is not prime by Fermat test.

Exercise 5.9 (2 pts)
Sove the following system of linear congruence

$$\begin{aligned} x &\equiv 2 \pmod{4} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 0 \pmod{11} \\ x &\equiv 8 \pmod{15} \end{aligned}$$

Exercise 5.10 (4 pts)

(i) `(2 pts)` Show that $6x \equiv 2 \pmod{3}$ has no solutions.

(ii) `(2 pts)` Show that $6x \equiv 2 \pmod{5}$ has infinitely many solutions.

Exercise 5.11 (6 pts)
Given public key $(n, E) = (323, 95)$, where $323 = 17 \times 19$.

(i) `(2 pts)` Encrypt the message 233 by the encryption function $e(x) = x^E \pmod{n}$.

(ii) `(2 pts)` Compute the private key $D = E^{-1} \pmod{\varphi(n)}$.

(iii) `(2 pts)` Decrypt the encrypted message in (i).