Ve203 Discrete Mathematics (Spring 2023)

Assignment 7

Date Due: None

Exercise 7.1 Given $p \in \mathbb{P}$, show that

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

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

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

(iv) Use (ii) to show that there are infinitely many composite numbers of the form $n! + 1$.

Exercise 7.2 Given $p \in \mathbb{P}$, consider the polynomial p of degree n given by

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_0, \ldots, a_n \in \mathbb{Z}/p\mathbb{Z}$$

show that p has at most n roots in $\mathbb{Z}/p\mathbb{Z}$. (Hint: factor p and use induction.)

Exercise 7.3 Apply Chinese remainder theorem to show that $a^{561} \equiv a \pmod{561}$ for all $a \in \mathbb{Z}$.

Exercise 7.4 Given $p, q \in \mathbb{P}$, $a \in \mathbb{Z}$, show that

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

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

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

Exercise 7.5 Find prime factors of $F_5 = 2^{2^5} + 1$ by applying Fermat's theorem.

Exercise 7.6 Show that 2077 is not prime by Fermat test.

Exercise 7.7 Sove the following system of linear congruence

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 5 \pmod{6} \\ x &\equiv 6 \pmod{7} \end{aligned}$$

Exercise 7.8

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

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

Exercise 7.9 Given public key $(n, E) = (2077, 97)$, where $2077 = 31 \times 67$.

(i) Encrypt the message 1984 by the encryption function $e(x) = x^E \pmod{n}$.

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

(iii) Decrypt the encrypted message in (i) using Chinese remainder theorem. Is it possible to do the encryption in (i) using Chinese remainder theorem?

Exercise 7.10 Is the group $(\mathbb{Z}/12\mathbb{Z})^\times$ is cyclic? Explain.