VE203 Discrete Math
Spring 2022 — Worksheet 6

April 16, 2022

Exercise 6.1 Modular Arithmetic

Find each of these values.

a) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

b) $(457 \bmod 23 \cdot 182 \bmod 23) \bmod 23$

Exercise 6.2 Fermat's (Little) Theorem

Show that $2^{11,213} - 1$ is not divisible by 11 .

Exercise 6.3 Euler's Theorem

1. Compute $\varphi\left(p^2\right)$ where p is a prime.
2. Compute $\varphi(pq)$ where both p and q are primes.

Exercise 6.4 Congruences

Find all solutions of the congruence $12x \equiv 27 (\mathrm{mod} 18)$.

Exercise 6.5 Solving Congruences

What are the solutions of the linear congruence $101x \equiv 583 (\mathrm{mod} 4620)$?

Exercise 6.6 Fast Modular Exponentiation

$$2^{2021} \bmod 2021$$

Exercise 6.7 Chinese Remainder Theorem

Solve the following system of linear congruence

$$\begin{aligned} x &\equiv 6 \pmod{11} \\ x &\equiv 13 \pmod{16} \\ x &\equiv 9 \pmod{21} \\ x &\equiv 19 \pmod{25} \end{aligned}$$

Exercise 6.8 RSA

In an RSA procedure, the public key is chosen as $(n, E) = (2077, 97)$, i.e., the encryption function e is given by

$$e(x) = x^{97} \pmod{2077}$$

(Note that $2077 = 31 \times 67$.)

Compute the private key D, where $D = E^{-1}(\mathrm{mod}\,\varphi(n))$. Decrypt the message 279 , that is, find x if $y = e(x) = 279(\mathrm{mod}\,2077)$.

Reference

1. Rosen, Kenneth H., and Kamala Krithivasan. Discrete mathematics and its applications: with combinatorics and graph theory. Tata McGraw-Hill Education, 2012.

2. Fraleigh, John B. A first course in abstract algebra. Pearson Education India, 2003.