Number Theory and Cryptography Math UN3020 New York, 2023/02/22

EXERCISE SHEET 6

Linear Congruences

Exercise 1 (12 points.). Show that, for all m > 0, we have

$$gcd(ma, mb) = m \ gcd(a, b)$$
.

Exercise 2 (9 points). Find all the zero-divisors on \mathbb{Z}_{18} . For each zero-divisor, find a non-zero element of \mathbb{Z}_{18} that multiplies to zero with the zero-divisor.

Exercise 3 (15 points). Solve the following linear congruences.

- (a) $131x \equiv 11 \pmod{1979}$.
- (b) $127x \equiv 11 \pmod{1091}$.
- (c) $3x \equiv 12 \pmod{21}$.
- (d) $6x \equiv 12 \pmod{15}$.
- (e) $2x \equiv 7 \pmod{10}$.

Exercise 4 (15 points). Solve the following systems of congruences.

(a)

$$\begin{cases} x \equiv 4 & \pmod{55} \\ x \equiv 11 & \pmod{69} \end{cases}$$

(b)

$$\begin{cases} x \equiv 5 & \pmod{11} \\ x \equiv 7 & \pmod{13} \end{cases}$$

(c)

$$\begin{cases} x \equiv 11 & \pmod{16} \\ x \equiv 16 & \pmod{27} \end{cases}$$

Exercise 5 (9 points). Solve the following system of congruences.

$$\begin{cases} 3x \equiv 6 & \pmod{9} \\ 3x \equiv 2 & \pmod{7} \\ x \equiv 1 & \pmod{5} \end{cases}$$