Tutorial 6 (with solution)

Modulo

Question 1: Divisibility by 9

Let x be an n-digit number. Prove that

$$x \equiv a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \pmod 9,$$

where a_i is the $(i+1)$-th digit of x.

- Example 1:
  - Suppose $x = 6213$. $x \bmod 9 = 6 + 2 + 1 + 3 \bmod 9 = 3$.

- Example 2:
  - Suppose $x = 7218$. Since the digit sum (mod 9) $= 7 + 2 + 1 + 8 \pmod 9 = 0$, x must be divisible by 9.

Q.1 (solution)

An n-digit number x can be represented by

$$x = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0.$$

Since $10 \equiv 1 \bmod 9$,

$$10^i \equiv 1 \bmod 9, \text{ for any integer } i.$$

Then ,

$$x \equiv a_{n-1}\times 1 + a_{n-2}\times 1 + \cdots + a_1\times 1 + a_0\times 1 \pmod 9.$$
$$\equiv a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \pmod 9.$$

Q.E.D

Question 2: Diophantine Equation

- Solve the equation

$$98x + 35y = 14,$$

where x and y are integers.

Q.2 (solution)

98	35		
1	0	98	a
0	1	35	b
1	-2	28	c = a – 2b
-1	3	7	d = b – c

- First, find gcd(98,35).
- By extended Euclidean algorithm,
$$98(-1) + 35(3) = 7.$$
- Multiplying both sides by 2, we obtain
$$98(-2) + 35(6) = 14.$$
- Therefore, $x_0 = -2, y_0 = 6$ is a particular solution.
- Dividing both sides by 7, we obtain
$$14(-2) + 5(6) = 2.$$
- It can be seen that
$$14(-2 - 5t) + 5(6 + 14t) = 2.$$
- The general solution is
$$x = -2 - 5t, y = 6 + 14t,$$
where t is an integer.

Question 3: Repeat-and-Multiply

a) Use the Repeat-and-Multiply method to compute $3^{94} \bmod 17$.

b) Use Fermat's Little Theorem to compute $40^{110} \bmod 37$.

Q.3(a) (solution)

- $3^2 \equiv 9 \pmod{17}$
- $3^4 \equiv (9)^2 \equiv 81 \equiv 13 \equiv -4 \pmod{17}$
- $3^8 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$
- $3^{16} \equiv (-1)^2 \equiv 1 \pmod{17}$
- $3^{32} \equiv 1 \pmod{17}$
- $3^{64} \equiv 1 \pmod{17}$
- Therefore, $3^{94} \equiv 3^{64}3^{16}3^{8}3^{4}3^{2}$

$$\equiv (1)(1)(-1)(-4)(9)$$

$$\equiv 36 \equiv 2 \pmod{17}$$

Q.3(b) (solution)

- First, note that
$$40^{110} \equiv 3^{110} \bmod 37.$$
- Since 37 is a prime, we can use Fermat's Little Theorem, which implies $3^{36} \equiv 1 \bmod 37$.
- Hence,
$$40^{110} \equiv 3^{110} \equiv 3^{36\times 3}3^2 \equiv 9 \pmod{37}.$$

Question 4: Fermat's Little Theorem

- Solve $x^{103} \equiv 4 \bmod 11$.

Q.4 (solution)

- By Fermat's Little Theorem, $x^{10} \equiv 1 \bmod 11$.
- Therefore, $x^{103} \equiv x^3 \bmod 11$.
- We only need to solve $x^3 \equiv 4 \bmod 11$.
- If we try all values from $x = 1$ through $x = 10$, we find that

$$x \equiv 5 \bmod 11.$$