

Additional Practice: Algebra Weeks 5 – 6

MA180/MA185/MA190

Contents

1	Congruences	1
2	Chinese Remainder Theorem	2
3	Prime factorisation, gcd and lcm	2
4	Fermat's Little Theorem	2
5	Euler's totient function and theorem	3
6	Affine ciphers	3

This sheet provides additional practice problems. This is not marked, nor is it part of the tutorials. Although the solutions are available, try to get the point where you can write a complete answer without looking at them.

1 Congruences

1. Determine whether each congruence has a solution. If it does, state how many distinct solutions there are in $\mathbb{Z}_m$. Justify your answers using the greatest common divisor.
 - (a) $18x \equiv 12 \pmod{30}$;
 - (b) $14x \equiv 9 \pmod{35}$;
 - (c) $21x \equiv 15 \pmod{36}$;
 - (d) $25x \equiv 7 \pmod{40}$.
2. Solve each congruence, finding *all distinct solutions* in $\mathbb{Z}_m$.
 - (a) $14x \equiv 20 \pmod{30}$;
 - (b) $18x \equiv 12 \pmod{42}$;
 - (c) $9x \equiv 17 \pmod{26}$.

Show your use of Euclid's algorithm and Bézout's identity where appropriate.

2 Chinese Remainder Theorem

3. Use the Chinese Remainder Theorem to solve the following systems.

(a)
$$\begin{cases} x \equiv 1 \pmod{4}, \\ x \equiv 3 \pmod{7}; \end{cases}$$

(b)
$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 4 \pmod{7}. \end{cases}$$

For each system, find the smallest non-negative solution and express the complete family of integer solutions.

4. Three alarms repeat at intervals of 4, 7, and 9 minutes, respectively. The first rings at times satisfying $t \equiv 3 \pmod{4}$, the second at times satisfying $t \equiv 1 \pmod{7}$, and the third at times satisfying $t \equiv 5 \pmod{9}$.

- (a) Express the problem as a system of simultaneous congruences.
- (b) Find the first non-negative time at which all three alarms ring together.
- (c) How many minutes pass between consecutive occasions when all three alarms ring together?

3 Prime factorisation, gcd and lcm

5. Using the Fundamental Theorem of Arithmetic:

- (a) Express 756 and 1260 as products of prime powers.
- (b) Calculate $\gcd(756, 1260)$ and $\text{lcm}(756, 1260)$.
- (c) Verify that

$$\gcd(a, b) \text{lcm}(a, b) = ab$$

for these two integers.

- (d) Explain briefly why this identity holds for arbitrary positive integers a, b .

4 Fermat's Little Theorem

6. Use Fermat's Little Theorem to calculate the following. Show how you reduce the exponents before performing the modular arithmetic.

- (a) $7^{2026} \pmod{13}$;
- (b) $3^{1000} \pmod{17}$;
- (c) Suppose p is prime and $p \nmid a$. Prove that

$$a^{p+4} \equiv a^5 \pmod{p}.$$

7. Consider the congruence

$$x^3 \equiv 8 \pmod{11}.$$

- (a) Find the inverse of 3 modulo 10.
- (b) Use Fermat's Little Theorem and your answer to (a) to find a solution.
- (c) Prove that your solution is the unique solution in $\mathbb{Z}_{11}$.

5 Euler's totient function and theorem

8. Let ϕ denote Euler's totient function.

(a) Calculate:

- (i) $\phi(45)$;
- (ii) $\phi(72)$;
- (iii) $\phi(175)$.

(b) List all multiplicatively invertible elements of $\mathbb{Z}_{18}$, and verify that their number equals $\phi(18)$.

(c) Use the multiplicativity of Euler's totient function to explain why

$$\phi(35) = \phi(5)\phi(7).$$

9. Use Euler's Totient Theorem to evaluate each expression.

(a) Find the last two digits of 7^{222} .

(b) Calculate $11^{203} \pmod{100}$.

For both parts, calculate $\phi(100)$, reduce the exponent, and show the remaining modular arithmetic.

6 Affine ciphers

10. Consider the affine cipher

$$f_E(x) \equiv 5x + 8 \pmod{26},$$

where letters are represented by $A = 1, B = 2, \dots, Z = 26$, interpreted as elements of $\mathbb{Z}_{26}$.

(a) Explain why 5 has a multiplicative inverse modulo 26.

(b) Find $5^{-1} \pmod{26}$ using Euclid's algorithm.

(c) Determine the corresponding decryption function $f_D(x)$.