

Additional Practice: Algebra Weeks 5–6

Solutions

MA180/MA185/MA190

Contents

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

1 Congruences

1. The congruence $ax \equiv b \pmod{m}$ has a solution exactly when $\gcd(a, m) \mid b$. If it is solvable, it has $\gcd(a, m)$ distinct solutions in $\mathbb{Z}_m$.
 - (a) $\gcd(18, 30) = 6$ and $6 \mid 12$. Thus there are 6 solutions in $\mathbb{Z}_{30}$.
 - (b) $\gcd(14, 35) = 7$ but $7 \nmid 9$. Thus there is no solution.
 - (c) $\gcd(21, 36) = 3$ and $3 \mid 15$. Thus there are 3 solutions in $\mathbb{Z}_{36}$.
 - (d) $\gcd(25, 40) = 5$ but $5 \nmid 7$. Thus there is no solution.

2. Dividing by the gcd where necessary, and using Bézout's identity to find inverses, gives:

- (a) Since $\gcd(14, 30) = 2$, the congruence becomes

$$7x \equiv 10 \pmod{15}.$$

Euclid's algorithm gives $15 = 2(7) + 1$, so $1 = 15 - 2(7)$ and $7^{-1} \equiv -2 \equiv 13 \pmod{15}$. Hence

$$x \equiv 13(10) \equiv 10 \pmod{15}.$$

The two distinct solutions in $\mathbb{Z}_{30}$ are $x = 10, 25$.

(b) Since $\gcd(18, 42) = 6$, the congruence becomes

$$3x \equiv 2 \pmod{7}.$$

Now $7 = 2(3) + 1$, so $1 = 7 - 2(3)$ and $3^{-1} \equiv -2 \equiv 5 \pmod{7}$. Thus

$$x \equiv 5(2) \equiv 3 \pmod{7}.$$

The six distinct solutions in $\mathbb{Z}_{42}$ are 3, 10, 17, 24, 31, 38.

(c) Since $\gcd(9, 26) = 1$, there is one solution. Euclid's algorithm gives

$$26 = 2(9) + 8, \quad 9 = 8 + 1,$$

and back-substitution gives

$$1 = 9 - (26 - 2(9)) = 3(9) - 26.$$

Thus $9^{-1} \equiv 3 \pmod{26}$, and

$$x \equiv 3(17) \equiv 25 \pmod{26}.$$

2 Chinese Remainder Theorem

3. The moduli in each system are pairwise coprime, so the Chinese Remainder Theorem gives a unique solution modulo their product.

(a) Write $x = 1 + 4k$. The second congruence gives

$$4k \equiv 2 \pmod{7}.$$

Since $4^{-1} \equiv 2 \pmod{7}$, we obtain $k \equiv 4 \pmod{7}$. Consequently,

$$x = 1 + 4(4 + 7n) = 17 + 28n, \quad n \in \mathbb{Z}.$$

The smallest non-negative solution is 17.

(b) Write $x = 2 + 3k$. The congruence modulo 5 gives

$$3k \equiv 1 \pmod{5},$$

so $k \equiv 2 \pmod{5}$. Thus $x = 8 + 15\ell$. The congruence modulo 7 now gives

$$8 + 15\ell \equiv 4 \pmod{7} \implies \ell \equiv 3 \pmod{7}.$$

Therefore

$$x = 8 + 15(3 + 7n) = 53 + 105n, \quad n \in \mathbb{Z}.$$

The smallest non-negative solution is 53.

4. (a) The three alarms ring together when

$$\begin{cases} t \equiv 3 \pmod{4}, \\ t \equiv 1 \pmod{7}, \\ t \equiv 5 \pmod{9}. \end{cases}$$

- (b) Write $t = 3 + 4k$. Reducing modulo 7 gives

$$4k \equiv 5 \pmod{7},$$

so $k \equiv 3 \pmod{7}$. Hence $t = 15 + 28\ell$. Reducing modulo 9 gives

$$15 + 28\ell \equiv 5 \pmod{9} \implies \ell \equiv 8 \pmod{9}.$$

Thus

$$t = 15 + 28(8 + 9n) = 239 + 252n, \quad n \in \mathbb{Z}.$$

The first non-negative time is 239 minutes.

- (c) Since 4, 7, and 9 are pairwise coprime, the common ringing times repeat every $4 \cdot 7 \cdot 9 = 252$ minutes.

3 Prime factorisation, gcd and lcm

5. (a) The prime factorisations are

$$756 = 2^2 \cdot 3^3 \cdot 7, \quad 1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7.$$

- (b) Taking the smaller exponents for the gcd and the larger exponents for the lcm gives

$$\gcd(756, 1260) = 2^2 \cdot 3^2 \cdot 7 = 252,$$

$$\text{lcm}(756, 1260) = 2^2 \cdot 3^3 \cdot 5 \cdot 7 = 3780.$$

- (c) Indeed,

$$252 \cdot 3780 = 952560 = 756 \cdot 1260.$$

- (d) In general, write $a = \prod p^{\alpha_p}$ and $b = \prod p^{\beta_p}$, where only finitely many exponents are non-zero. In the gcd the exponent of p is $\min(\alpha_p, \beta_p)$, while in the lcm it is $\max(\alpha_p, \beta_p)$. Since

$$\min(\alpha_p, \beta_p) + \max(\alpha_p, \beta_p) = \alpha_p + \beta_p,$$

the product of the gcd and lcm is ab .

4 Fermat's Little Theorem

6. Fermat's Little Theorem states that if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

(a) Since $2026 = 12(168) + 10$,

$$7^{2026} \equiv 7^{10} \pmod{13}.$$

Now $7^2 \equiv 10$, $7^4 \equiv 9$, and $7^8 \equiv 3 \pmod{13}$. Therefore

$$7^{10} \equiv 7^8 \cdot 7^2 \equiv 3(10) \equiv 4 \pmod{13}.$$

(b) Since $1000 = 16(62) + 8$,

$$3^{1000} \equiv 3^8 \pmod{17}.$$

As $3^4 = 81 \equiv 13 \pmod{17}$, we have

$$3^8 \equiv 13^2 = 169 \equiv 16 \pmod{17}.$$

(c) By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Multiplying by a^5 gives

$$a^{p+4} = a^{p-1}a^5 \equiv a^5 \pmod{p}.$$

7. (a) Since $3(7) = 21 \equiv 1 \pmod{10}$, the inverse of 3 modulo 10 is 7.

(b) A solution of $x^3 \equiv 8 \pmod{11}$ cannot be zero modulo 11. By Fermat's Little Theorem, $x^{10} \equiv 1 \pmod{11}$. Raising the congruence to the seventh power gives

$$x^{21} \equiv 8^7 \pmod{11}.$$

Since $x^{21} = x(x^{10})^2 \equiv x \pmod{11}$, it follows that

$$x \equiv 8^7 \equiv (8^4)(8^2)(8) \equiv 4 \cdot 9 \cdot 8 \equiv 2 \pmod{11}.$$

Indeed, $2^3 = 8$.

(c) Every solution must be non-zero, and the preceding argument forces $x \equiv 2 \pmod{11}$. Thus 2 is the unique solution in $\mathbb{Z}_{11}$.

5 Euler's totient function and theorem

8. (a) (i)

$$\phi(45) = \phi(3^2)\phi(5) = 3(3-1)(5-1) = 24.$$

(ii)

$$\phi(72) = \phi(2^3)\phi(3^2) = 2^2(2-1)3(3-1) = 24.$$

(iii)

$$\phi(175) = \phi(5^2)\phi(7) = 5(5-1)(7-1) = 120.$$

(b) The invertible elements of $\mathbb{Z}_{18}$ are precisely those coprime to 18:

$$\{1, 5, 7, 11, 13, 17\}.$$

There are six of them and

$$\phi(18) = \phi(2)\phi(3^2) = (2-1)3(3-1) = 6.$$

(c) Since $\gcd(5, 7) = 1$, multiplicativity gives

$$\phi(35) = \phi(5)\phi(7) = (5-1)(7-1) = 24.$$

9. Since $100 = 2^2 \cdot 5^2$, we have

$$\phi(100) = 2(2-1)5(5-1) = 40.$$

Both 7 and 11 are coprime to 100, so Euler's Totient Theorem applies.

(a) Since $222 = 5(40) + 22$,

$$7^{222} \equiv 7^{22} \pmod{100}.$$

But $7^4 = 2401 \equiv 1 \pmod{100}$, so

$$7^{22} = (7^4)^5 7^2 \equiv 49 \pmod{100}.$$

Thus the last two digits are 49.

(b) Since $203 = 5(40) + 3$,

$$11^{203} \equiv 11^3 = 1331 \equiv 31 \pmod{100}.$$

6 Affine ciphers

10. (a) Since $\gcd(5, 26) = 1$, the element 5 has a multiplicative inverse modulo 26.

(b) Euclid's algorithm gives

$$26 = 5(5) + 1.$$

Thus $1 = 26 - 5(5)$, so

$$5^{-1} \equiv -5 \equiv 21 \pmod{26}.$$

Indeed $5(21) = 105 \equiv 1 \pmod{26}$.

(c) If $y \equiv 5x + 8 \pmod{26}$, then

$$x \equiv 21(y - 8) \equiv 21y + 14 \pmod{26}.$$

Hence the decryption function is

$$f_D(x) \equiv 21x + 14 \pmod{26}.$$