

Show all of your work.

1. What are the elements of \mathbf{Z}_{18}^\times ?

Solution: $\mathbf{Z}_{18}^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}\}$.

2. What is $\phi(45,000)$?

Solution:

$$\begin{aligned}\phi(45,000) &= \phi(2^3 3^2 5^4) = \phi(2^3)\phi(3^2)\phi(5^4) \\ &= (8-4)(9-3)(625-125) = 12,000.\end{aligned}$$

3. a) What are the possible orders of the elements of \mathbf{Z}_{100}^\times ?

Solution: The possible orders are the divisors of $\phi(100) = \phi(4)\phi(25) = 2 \cdot 20$. Thus, the possible orders are 1, 2, 4, 5, 8, 10, 20, 40.

- b) What is the order of $\bar{31}$ in \mathbf{Z}_{100}^\times ?

Solution: Using Maple to calculate, if we wish, we obtain:

$$\begin{aligned}\bar{31}^2 &= \bar{61} \\ \bar{31}^4 &= \bar{21} \\ \bar{31}^5 &= \bar{51} \\ \bar{31}^8 &= \bar{41} \\ \bar{31}^{10} &= \bar{1}.\end{aligned}$$

Since 10 is the smallest of the possible orders that gives $\bar{1}$, the order is 10.

- c) What is the smallest positive integer congruent to $31^{7825234}$ mod 100?

Solution:

$$31^{7825234} = 31^{782523 \cdot 10 + 4} = (31^{10})^{782523} 31^4 \equiv 1^{782523} 31^4 \equiv 21 \pmod{100}$$

Here, we use the fact that 31 has order 10, along with the calculation above of $\bar{31}^4$.

Exam 2 Solutions

4. What is the order of 5^{711862} in \mathbf{Z}_{13}^\times ?

Solution: We first calculate the order of $\bar{5}$. The possible orders are the divisors of $\phi(13) = 12$. We have

$$\bar{5}^2 = \bar{12}$$

$$\bar{5}^3 = \bar{8}$$

$$\bar{5}^4 = \bar{1},$$

so $\bar{5}$ has order 4 in \mathbf{Z}_{13}^\times . Thus, $\bar{5}^{711862}$ has order $\frac{4}{(4,711862)} = 2$.

5. For which primes p is $x^{25} \equiv x \pmod{p}$ for all $x \in \mathbf{Z}$?

Solution: The primes in question satisfy $25 \equiv 1 \pmod{p-1}$, i.e., $(p-1) \mid 24$. This is satisfied by $p = 2, 3, 5, 7, 13$.

6. Find the smallest nonnegative solution for the following congruences.

$$x \equiv 156 \pmod{180}$$

$$x \equiv 6 \pmod{75}$$

$$x \equiv 36 \pmod{48}$$

Solution: We begin by solving the first pair of congruences, i.e.,

$$156 + 180k = 6 + 75l$$

$$150 = 75l - 180k$$

To solve this, we first solve Bezout's identity for 75 and 180:

$$180 = 2 \cdot 75 + 30$$

$$75 = 2 \cdot 30 + 15.$$

Since 15 divides 30, it is the g.c.d., and we back substitute, getting

$$15 = 75 - 2 \cdot 30 = 75 - 2(180 - 2 \cdot 75) = 5 \cdot 75 - 2 \cdot 180$$

We now multiply through by $\frac{150}{15} = 10$, getting

$$150 = 10 \cdot 15 = (10 \cdot 5)75 - (10 \cdot 2)180,$$

so we may take $k = 20$ and $l = 50$. Thus,

$$\begin{aligned} x &\equiv 6 + 75 \cdot 50 \pmod{[180, 75]} = 900 \\ &\equiv 156. \end{aligned}$$

We now solve the pair of congruences

$$x \equiv 156 \pmod{900}$$

$$x \equiv 36 \pmod{48}.$$

Thus, we solve

$$156 + 900k = 36 + 48l$$

$$120 = 48l - 900k.$$

Solving Bezout for 48 and 900, we have

$$900 = 18 \cdot 48 + 36$$

$$48 = 36 + 12.$$

Since 12 divides 36, we may begin back substitution:

$$12 = 48 - 36 = 48 - (900 - 18 \cdot 48) = 19 \cdot 48 - 900.$$

Multiplying through by $\frac{120}{12} = 10$, we have

$$120 = 10 \cdot 12 = (10 \cdot 19)48 - 10 \cdot 900,$$

so we may take $k = 10$ and $l = 190$. Thus,

$$\begin{aligned} x &\equiv 156 + 900 \cdot 10 \pmod{[900, 48]} = 3600 \\ &\equiv 1956. \end{aligned}$$

Thus, the smallest positive solution is 1956.

7. Find all solutions of $\bar{x}^2 \equiv \bar{1}$ in

a) \mathbf{Z}_{512}

Solution: Since $512 = 2^9$, a power of 2, the solutions are $\bar{1}, \overline{2^8 - 1}, \overline{2^8 + 1}, \overline{-1}$, or $\bar{1}, \overline{255}, \overline{257}, \overline{-1}$.

b) \mathbf{Z}_{75}

Solution: Here, $75 = 3 \cdot 5^2$ is divisible by two primes, so we use the Chinese Remainder Theorem. The solutions satisfy

$$x^2 \equiv 1 \pmod{3}$$

$$x^2 \equiv 1 \pmod{25}.$$

Since both 3 and 25 are powers of odd primes, the solutions satisfy

$$x \equiv \pm 1 \pmod{3}$$

$$x \equiv \pm 1 \pmod{25}.$$

Exam 2 Solutions

Thus, there are four different cases:

Case 1: $x \equiv 1 \pmod{3}$ and $x \equiv 1 \pmod{25}$. Here, $x = 1$ satisfies these congruences. By the uniqueness part of the Chinese Remainder Theorem, $x \equiv 1 \pmod{75}$.

Case 2: $x \equiv 1 \pmod{3}$ and $x \equiv -1 \pmod{25}$. We solve this below by the Chinese Remainder Theorem.

Case 3: $x \equiv -1 \pmod{3}$ and $x \equiv 1 \pmod{25}$. We solve this below by the Chinese Remainder Theorem.

Case 4: $x \equiv -1 \pmod{3}$ and $x \equiv -1 \pmod{25}$. Here, $x = -1$ satisfies these congruences, so the uniqueness part of the Chinese Remainder Theorem gives $x \equiv -1 \pmod{75}$.

Cases 2 and 3 amount to solving

$$\begin{aligned}x &\equiv a_1 \pmod{3} \\x &\equiv a_2 \pmod{25},\end{aligned}$$

for suitable a_1, a_2 . By the first form of the Chinese Remainder Theorem, this means $x \equiv a_1x_1 + a_2x_2 \pmod{75}$, where

$$x_1 \equiv 1 \pmod{3} \text{ and } x_1 \equiv 0 \pmod{25}, \text{ and}$$

$$x_2 \equiv 0 \pmod{3} \text{ and } x_2 \equiv 1 \pmod{25}.$$

We can solve for x_1 and x_2 by Bezout's identity:

$$\begin{aligned}25 &= 8 \cdot 3 + 1, \text{ so} \\1 &= 25 - 3 \cdot 8.\end{aligned}$$

Thus, we can take $x_1 = 25$ and $x_2 = -3 \cdot 8 = -24$. In Case 2, this gives

$$\begin{aligned}x &\equiv 1 \cdot 25 + (-1) \cdot (-24) \pmod{75} \\&\equiv 49.\end{aligned}$$

In Case 3, this gives

$$\begin{aligned}x &\equiv -1 \cdot 25 + 1 \cdot (-24) \pmod{75} \\&\equiv 26.\end{aligned}$$

c) \mathbf{Z}_{400}

Solution: Here, $400 = 2^4 5^2$. Again we use the Chinese Remainder Theorem, but this time one of the factors is a power of 2. The solutions satisfy

$$x^2 \equiv 1 \pmod{16}$$

$$x^2 \equiv 1 \pmod{25},$$

so

$$x \equiv 1, 7, 9, -1 \pmod{16}$$

$$x \equiv \pm 1 \pmod{25}.$$

Since there are four solutions mod 16 and two solutions mod 25, the Chinese Remainder Theorem gives 8 solutions:

Case 1: $x \equiv 1 \pmod{16}$ and $x \equiv 1 \pmod{25}$.

Case 2: $x \equiv 1 \pmod{16}$ and $x \equiv -1 \pmod{25}$.

Case 3: $x \equiv 7 \pmod{16}$ and $x \equiv 1 \pmod{25}$.

Case 4: $x \equiv 7 \pmod{16}$ and $x \equiv -1 \pmod{25}$.

Case 5: $x \equiv 9 \pmod{16}$ and $x \equiv 1 \pmod{25}$.

Case 6: $x \equiv 9 \pmod{16}$ and $x \equiv -1 \pmod{25}$.

Case 7: $x \equiv -1 \pmod{16}$ and $x \equiv 1 \pmod{25}$.

Case 8: $x \equiv -1 \pmod{16}$ and $x \equiv -1 \pmod{25}$.

We apply the Chinese Remainder Theorem as in the last example. The same kind of calculation gives $x_1 = -7 \cdot 25$ and $x_2 = 11 \cdot 16$. The solutions in cases 1–8 are

$$x \equiv 1, 49, 151, 199, 201, 249, 351, -1 \pmod{400},$$

respectively.

8. Use the fact that $3837^2 \equiv 1 \pmod{13837}$ to factor 13837.

Solution: We have $3837^2 - 1 \equiv 0 \pmod{13837}$, so

$$13837 \mid (3837^2 - 1) = 3836 \cdot 3838.$$

Maple gives $(13837, 3836) = 137$ and $(13837, 3838) = 101$. Finally, $137 \cdot 101 = 13837$, so the factorization is obtained.