Solutions

1.

(i) The units in $\mathbb{Z}_{36}$ are obtained by requiring $(a, 36) = 1$. This yields

$$U(\mathbb{Z}_{36}) = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}.$$  

(ii) We let $x$ be the inverse of 11. Then

$$11x \equiv 1 \pmod{36} \implies 11x = 1 + 36y \implies 11x + 36(-y) = 1.$$  

We run the Euclidean algorithm finding the solution $x = -13, -y = 4$ hence

$$x = -13 \mod 36 = 23 \mod 36.$$  

(iii) We have

$$U(\mathbb{Z}_{10} \times \mathbb{Z}_{30} \times \mathbb{Z}_{60}) = U(\mathbb{Z}_{10}) \times U(\mathbb{Z}_{30}) \times U(\mathbb{Z}_{60}).$$

The number of units in each factor is

$$\phi(10) = \phi(2 \cdot 5) = (2 - 1)(5 - 1) = 4$$  
$$\phi(30) = \phi(2 \cdot 3 \cdot 5) = (2 - 1)(3 - 1)(5 - 1) = 8$$  
$$\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = 2(2 - 1) \cdot (3 - 1) \cdot (5 - 1) = 16$$

hence the number of units in the product is

$$\phi(10) \cdot \phi(30) \cdot \phi(60) = 4 \cdot 8 \cdot 16 = 512.$$  

2.

(i) This part is very similar to proving that the Euler function is multiplicative. We follow the hint. We only need to prove that

$$f : J(nm) \to J(n) \times J(m)$$

is a bijection for gcd$(m, n) = 1$. Since $J(n)$ is the number of elements in $J(n)$, counting elements we conclude

$$J(nm) = J(n) \cdot J(m),$$

or equivalently $J$ is multiplicative.

First, $f$ is well defined. Indeed, for

$$(a, b) \in J(nm) \implies \gcd(a, b, nm) = 1$$

which gives gcd$(a, b, n) = 1$ and gcd$(a, b, m) = 1$, so the image of $f$ does lie in $J(n) \times J(m)$.

To prove $f$ is injective, we assume $f(a, b) = f(a', b')$. Then, by the definition of $f$

$$(a, b) \mod n = (a', b') \mod n \implies n\mid a - a', n\mid b - b'$$

and similarly

$$(a, b) \mod m = (a', b') \mod m \implies m\mid a - a', m\mid b - b'.$$
Thus since \((m, n) = 1\), we find
\[ nm | a - a' \text{ and } nm | b - b' \]
or that \((a, b) = (a', b') \mod mn\). This proves injectivity.

To prove \(f\) is surjective, pick \((a_1, b_1)\) in \(\mathfrak{J}(n)\) and \((a_2, b_2)\) in \(\mathfrak{J}(m)\). By Chinese remainder, we can solve the congruence
\[ a \equiv a_1 \mod n, \ a \equiv a_2 \mod m \]
and similarly
\[ b \equiv b_1 \mod n, \ b \equiv b_2 \mod m. \]
Clearly by definition,
\[ f(a, b) = ((a_1, b_1), (a_2, b_2)) \]
proving surjectivity. There is one detail we still need to worry about: we need to ensure that indeed
\[ \gcd(a, b, nm) = 1, \]
so that the pair \((a, b)\) is in the domain \(\mathfrak{J}(nm)\) of \(f\). Indeed, if \(p\) is a common prime factor of \(\gcd(a, b, nm)\), then \(p\) divides either \(n\) or \(m\). Assume it divides \(n\). Also \(p\) should divide \(a\) and \(b\). Thus
\[ p | n, p | a, p | b. \]
But then
\[ a_1 \equiv a \mod n \implies n | a - a_1 \implies p | a - a_1 \text{ and } p | a \implies p | a_1 \]
and similarly \(p | b_1\). This means \((a_1, b_1, n)\) have the prime \(p\) in common, which contradicts the fact that \((a_1, b_1, n)\) is in the set \(\mathfrak{J}(n)\) for which the \(\gcd\) is 1.

(ii) Clearly,
\[ \mathfrak{J}(p) = \{(a, b) : \gcd(a, b, p) = 1\} = \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(a, b) : \gcd(a, b, p) \neq 1\}. \]
If the \(\gcd\) of \((a, b, p)\) is not 1, it must equal \(p\), hence
\[ \gcd(a, b, p) = p \implies p | a, p | b \implies a = b = p. \]
Thus
\[ \mathfrak{J}(p) = \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(p, p)\} \implies J(p) = p^2 - 1. \]

(iii) We have
\[ J(p_1 \cdots p_\ell) = J(p_1) \cdots J(p_\ell) = (p^2_1 - 1) \cdots (p^2_\ell - 1) \]
using parts (i) and (ii).

3. We solve the system by the method outlined in class, following three steps:
(i) First, we bring the system in normal form. The first congruence is

\[ 2x \equiv 1 \mod 27 \iff x \equiv 14 \mod 27. \]

The second congruence is

\[ 6x \equiv 21 \mod 45 \iff 2x \equiv 7 \mod 15 \iff x \equiv 11 \mod 15. \]

The new system is

\[ x \equiv 14 \mod 27, \ x \equiv 11 \mod 15, \ x \equiv 1 \mod 175. \]

(ii) The moduli are not coprime. We write

\[ 27 = 3^3, 15 = 3 \cdot 5, 175 = 5^2 \cdot 7. \]

The above system rewrites modulo powers of the primes appearing in the above decomposition as

\[ x \equiv 14 \mod 3^3, \ x \equiv 11 \mod 5, \ x \equiv 1 \mod 5^2 \]

\[ x \equiv 1 \mod 7. \]

Keeping only the equations with the highest exponent of primes, we obtain

\[ x \equiv 14 \mod 3^3, \ x \equiv 1 \mod 5^2, \ x \equiv 1 \mod 7. \]

(iii) Now we obtained a system with coprime moduli. We can solve it using fundamental solutions, but it’s easier to first combine the last two equations into \( x \equiv 1 \mod 5^2 \cdot 7 \equiv 1 \mod 175. \) The new system is

\[ x \equiv 14 \mod 27, \ x \equiv 1 \mod 175. \]

In turn, here it’s easier to apply the Euclidean algorithm (or just use trial and error). We write

\[ x = 14 + 27k = 1 + 175\ell \iff 27k + 175(-\ell) = -13 \]

with particular solutions

\[ k = 6, \ell = 1. \]

Substituting, \( x_p = 14 + 27 \cdot 6 = 176 \) is a particular solution, hence by Chinese remainder theorem, we have the general solution

\[ x \equiv 176 \mod 4725. \]

4.

(i) First, we solve the congruence mod 23. Using the “quadratic” formula from Homework 5, we find

\[ x_{1,2} = \frac{7 \pm \sqrt{7^2 - 4 \cdot 2 \cdot 8}}{4} \]
interpreted in $\mathbb{Z}_{23}$. This yields

$$x_{1,2} = \frac{7 \pm \sqrt{-15}}{4}.$$ 

Now,

$$10^2 \equiv -15 \mod 23 \implies \sqrt{-15} = \pm 10 \text{ in } \mathbb{Z}_{23}$$

and the inverse of $4 \mod 23$ is $6$ since $4 \cdot 6 = 1$. Thus

$$x_1 = 6(7 + 10) = 10 \mod 23$$

and

$$x_2 = 6(7 - 10) = 5 \mod 23.$$ 

Second we compute the solution $\mod 23^2$. Let

$$f(x) = 2x^2 - 7x + 8 \implies f'(x) = 4x - 7.$$ 

We have either $x \equiv x_1 \mod 23$ or $x \equiv x_2 \mod 23$.

- When $x \equiv x_1 \mod 23$, we write

$$x = 10 + 23t.$$ 

We have

$$f(10) = 138 = 23 \cdot 6, \text{ and } f'(10) = 33.$$ 

Using Taylor

$$f(x) = f(10) + 23t f'(10) \mod 23^2 = 23(6 + 33t) \equiv 0 \mod 23^2$$

$$\implies 6 + 33t \equiv 0 \mod 23 \implies t \equiv 4 \mod 23 \implies x = 10 + 23t \equiv 10 + 23 \cdot 4 \mod 23^2$$

$$\implies x \equiv 102 \mod 23^2.$$ 

- The second case $x \equiv x_2 \mod 23$ is similar. We have

$$x = 5 + 23t.$$ 

We have $f(5) = 23, f'(5) = 13$. By Taylor

$$f(5 + 23t) = f(5) + 23t \cdot f'(5) = 23(1 + 13t) \equiv 0 \mod 23^2 \implies 1 + 13t \equiv 0 \mod 23$$

$$\implies t \equiv 7 \mod 23 \implies x = 5 + 23t \equiv 5 + 23 \cdot 7 \mod 23^2$$

$$\implies x \equiv 166 \mod 23^2.$$ 

There are two solutions, namely $102$ and $166 \mod 23^2$.

(ii) We split the system into two equations

$$4x^5 - x^2 - 4 \equiv 0 \mod 8,$$

$$4x^5 - x^2 - 4 \equiv 0 \mod 3.$$
Since the modulus is small, the last equation can be solved by trial and error and the solution is
\[ x \equiv 2 \mod 3. \]

For the first equation, let
\[ f(x) = 4x^5 - x^2 - 4, f'(x) = 20x^4 - 2x, f''(x) = 80x^3 - 2. \]

We solve the congruence mod 2. By trial and error, we must have \( x \equiv 0 \mod 2 \). From here, we write \( x = 2t \) and use Taylor to conclude
\[ f(x) = f(0) + 2tf'(0) + (2t)^2 f''(0)/2 \mod 8 \equiv -4 - 4t^2 \mod 8 \equiv 0 \mod 8 \]
\[ \implies t \equiv 1 \mod 2 \implies x \equiv 2 \mod 4. \]

Thus putting things together
\[ x \equiv 2 \mod 3, x \equiv 2 \mod 4 \implies x \equiv 2 \mod 12. \]

5.A.

(i) We have 221 = 13 \cdot 17 and \( \phi(13) = 12, \phi(17) = 16 \). Thus for \( (a, 221) = 1 \), we have
\[ a^{12} \equiv 1 \mod 13, \]
\[ a^{16} \equiv 1 \mod 17 \]
by Fermat’s theorem. In particular
\[ 3^{8031} = 3^{8028} \cdot 3^3 = (3^{669})^{12} \cdot 3^3 \equiv 3^3 \mod 13 \equiv 1 \mod 13. \]

Similarly,
\[ 3^{8031} = 3^{8032} \cdot 3^{-1} = (3^{502})^{16} \cdot 3^{-1} \equiv 3^{-1} \mod 17 \equiv 6 \mod 17. \]

We assemble the two congruences together using the Chinese remainder theorem. We need to solve
\[ x \equiv 1 \mod 13, x \equiv 6 \mod 17. \]

We could find the fundamental solutions, or we can search for solutions by trial and error. A third option is to just solve
\[ x = 1 + 13k = 6 + 17\ell \implies 13k + 17(-\ell) = 5 \]
using the Euclidean algorithm. A particular solution is
\[ k = 5 \cdot 4, \ell = 5 \cdot 3 \]
so \( x_p = 1 + 13 \cdot 5 \cdot 4 = 261 \) is a particular solution of the congruence. By uniqueness
\[ x \equiv 261 \mod 221 \equiv 40 \mod 221 \]
which gives
\[ 3^{8031} \equiv 40 \mod 221. \]
(ii) We have $\phi(221) = \phi(13 \cdot 17) = (13 - 1)(17 - 1) = 192$ so by Euler $a^{192} \equiv 1 \mod 221$.

(iii) We have seen above that
$$a^{12} \equiv 1 \mod 13,$$
$$a^{16} \equiv 1 \mod 17.$$ by Fermat’s theorem. Thus
$$a^{48} = (a^{12})^4 \equiv 1 \mod 13,$$
$$a^{48} = (a^{16})^3 \equiv 1 \mod 17.$$ Therefore by the Chinese remainder theorem, the uniqueness of solutions claim, we find
$$a^{48} \equiv 1 \mod 221.$$

5.B.

(i) Since $\{a_1, \ldots, a_{p-1}\}$ is a reduced residue system, their remainders mod $p$ give the set $\{1, 2, \ldots, p-1\}$. It follows that
$$a_1 + \ldots + a_{p-1} = 1 + 2 + \ldots + (p-1) = \frac{p(p-1)}{2} = p \cdot \frac{p-1}{2} \equiv 0 \mod p.$$

(ii) The $p-1$ numbers $\frac{(p-1)!}{k}$ for $1 \leq k \leq p-1$ are clearly coprime to $p$, since $p$ is prime and it does not appear in the factorization of $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$.

We need to show only that the $p-1$ numbers $\frac{(p-1)!}{k}$ for $1 \leq k \leq p-1$ are distinct modulo $p$. Then they would be a reduced residue system mod $p$. Assume otherwise, so that for $k \neq \ell$ we have
$$\frac{(p-1)!}{k} \equiv \frac{(p-1)!}{\ell} \mod p \implies (p-1)!\ell \equiv (p-1)!k \mod p$$ after multiplying by $k\ell$. But $(p-1)! = -1 \mod p$ by Wilson, hence the above becomes
$$-\ell = -k \mod p \implies \ell = k \mod p \implies k = \ell$$ using that $1 \leq k, \ell \leq p-1$. This completes the proof.

(iii) Using parts (i) and (ii), we have that
$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \mod p \implies \sum_{k=1}^{p-1} \frac{(p-1)!}{k} = pX,$$ for some $X$. This rewrites as
$$pX = (p-1)! \sum_{k=1}^{p-1} = (p-1)! \cdot \frac{a}{b}.$$ Multiplying by $b$ we obtain that
$$(p-1)!a = pbX \implies p|(p-1)!a \implies p|a$$ since $(p-1)! \equiv -1 \mod p$ is coprime with $p$.

5.C.
(i) If \( x \neq 0 \) then \( x \) is a unit, hence an inverse exists. If \( x^{-1} = 1 \) or \( x^{-1} = -1 \) we obtain \( x = \pm 1 \) which is not allowed. Thus \( x^{-1} \in \mathbb{Z}_p \setminus \{0, \pm 1\} \).

If \( x^{-1} = x \) in \( \mathbb{Z}_p \) it follows that \( x^2 = 1 \) after multiplying by \( x \). By Lagrange (or any other argument) this equation has at most two solutions. Since \( \pm 1 \) are solutions already, there cannot be any others, so in particular there no solutions in \( \mathbb{Z}_p \setminus \{\pm 1\} \). Thus \( x \neq x^{-1} \).

(ii) The elements in the set \( \mathbb{Z}_p \setminus \{0, \pm 1\} \) can be grouped in pairs \((x, x^{-1})\), and the product of elements in each pair is 1. Thus the product of all elements in \( \mathbb{Z}_p \setminus \{0, \pm 1\} \) is 1 in \( \mathbb{Z}_p \).

(iii) Now, \((p - 1)!\) is the product of all elements in \( \mathbb{Z}_p \setminus \{0, \pm 1\} \) together with 1 and \(-1\). By part (ii), the elements not equal to \( \pm 1 \) multiply to 1 in \( \mathbb{Z}_p \), hence this gives the value \(-1\) for \((p - 1)!\) in \( \mathbb{Z}_p \).