Exercise 1 (4 points). 1. Find the greatest common divisor $d$ of 1001 and 312, and then find integers $x$ and $y$ satisfying

$$1001x + 312y = d.$$ 

**Euclid's algorithm:**

$$1001 = 3 \times 312 + 65$$
$$312 = 4 \times 65 + 52$$
$$65 = 1 \times 52 + 13$$
$$52 = 4 \times 13 + 0.$$ 

So $(1001, 312) = 13$.

Now we find $(x, y)$:

$$13 = 65 - 52$$
$$= 65 - (312 - 4 \times 65) = 5 \times 65 - 312$$
$$= 5 \times (1001 - 3 \times 312) - 312$$
$$= 5 \times (1001) - 16 \times 312.$$ 

$$x = 5, \quad y = -16.$$ 

2. Is \overline{77} invertible in $\mathbb{Z}/24\mathbb{Z}$? If yes, give its inverse (Use previous question, think of dividing by $d$...).

\[ 77 = 7 \times 11 \text{ is prime to } 24 = 3 \times 2^3 \text{ so } \overline{77} \text{ is invertible in } \mathbb{Z}/24\mathbb{Z}. \]

Note that $1001 = 13 \times 77$ and $312 = 13 \times 24$ so, by dividing the equality $1001x + 312y = 13$ by 13 we get

$$77x + 24y = 1.$$ 

Mod 24 we have

$$77x \equiv 1 \pmod{24},$$

so $\overline{x} = \overline{5}$ is the inverse of $\overline{77}$ in $\mathbb{Z}/24\mathbb{Z}$. 

Exercise 2 (6 points). Let \( p \) be a prime number.

1. For \( k \) an integer \( 1 \leq k \leq p \), prove the following equality between binomial coefficients:

\[
\binom{p}{k} = \binom{p - 1}{k - 1}.
\]

On one side we have

\[
\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{p!}{(p-k)!k!} \quad \text{possible because } k \neq 0,
\]

On the other side,

\[
\binom{p-1}{k-1} = \frac{(p-1)!}{(p-1-(k-1))!(k-1)!} = \frac{(p-1)!}{(p-k)!k!}.
\]

And we have proved that these numbers are equal.

2. For which values of \( k, 1 \leq k \leq p \), does \( p \) divide \( \binom{p}{k} \)? (Use Question 1).

Does \( p \) divide \( \binom{p}{0} \)?

For \( k = p \), \( \binom{p}{p} = 1 \); for \( k = 0 \), \( \binom{p}{0} = 1 \). So \( p \) does not divide \( \binom{p}{0} \) or \( \binom{p}{p} \).

But, if \( 1 \leq k \leq p-1 \), we just proved that \( p \) divides \( k \times \binom{p}{k} \).

Since \( (p, k) = 1 \) (because \( p \) is prime and \( k < p \)) it implies: \( p \) divides \( \binom{p}{k} \). So \( p \) divides \( \binom{p}{k} \) for \( 1 \leq k \leq p-1 \).

3. Prove that \((x + y)^{37} \equiv x^{37} + y^{37} \mod 37\) for any \( x, y \in \mathbb{Z} \).

Set \( p = 37 \)

\[
(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.
\]

But, \( \mod p \) we just said that \( \binom{p}{k} \equiv 0 \mod p \) if \( 1 \leq k \leq p-1 \).

So \( (x + y)^p = \binom{p}{0} x^p y^0 + \binom{p}{p} x^0 y^p \mod p \)

\[
= x^p + y^0 \mod p \quad \text{and}.
\]
Exercise 3 (7 points). 1. Find the inverse of $2$ in $\mathbb{Z}/7\mathbb{Z}$.

\[ \text{mod } 7 \text{ we have } 1 \equiv 8 \equiv 2 \times 4 \mod 7 \]

So in $\mathbb{Z}/7\mathbb{Z}$

\[ 1 = \bar{2} \times \bar{4} \]

$\bar{4}$ is the inverse of $\bar{2}$.

2. Solve $x^7 + 15x - 57 \equiv 0 \mod 7$. (First transform $x^7 \mod 7$ into something simpler). (You will use Question 1 at some point).

By Fermat's little theorem $x^7 \equiv x \mod 7$ for any $x \in \mathbb{Z}$.

So $x^7 + 15x - 57 \equiv 0 \mod 7$ is equivalent to

$16x \equiv 57 \mod 7$.

Since $16 \equiv 2 \mod 7$

$57 = 7 \times 8 + 1 \equiv 1 \mod 7$, it is also equivalent to

$2x \equiv 1 \mod 7$

That is to say $x \equiv 4 \mod 7$ by question 1.
3. Solve $x^3 \equiv 2 \pmod{5}$. In $\mathbb{Z}/5\mathbb{Z}$:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4 = (-1)</td>
</tr>
</tbody>
</table>

So $x \equiv 3 \pmod{5}$ is our solution.

4. Solve $x^7 + 15x - 57 \equiv 0 \pmod{5}$. (First explain why $x^7 \equiv x^3 \pmod{5}$ for any $x$).

By Fermat's little theorem $x^5 \equiv x \pmod{5}$ for any $x$.

So $x^7 \equiv x^3 \pmod{5}$.

The equation is therefore equivalent to

$x^3 - 2 \equiv 0 \pmod{5}$.

And its solutions are the $x$ such that $x \equiv 3 \pmod{5}$ by Question #3.

5. Is 3 a quadratic residue mod 5? Justify.

$\frac{4}{3^2} = \frac{4}{9} = 4 \equiv -1 \pmod{5}$, so 3 is not a QR mod 5.

$p = 5$ is prime.

6. Bonus Does the equation $x^6 + 15x - 63 = 0$ have a solution in $\mathbb{Z}$? Explain.

If this equation had a solution in $\mathbb{Z}$, then, mod 5, we would have

$x^6 - 3 \equiv 0 \pmod{5}$ in $\mathbb{Z}/5\mathbb{Z}$.

So $x^6 = 3$ in $\mathbb{Z}/5\mathbb{Z}$.

It is impossible by Question #5.

So the equation has no solution.

(Or work mod 2! Even easier...)
Exercise 4 (3 points). 1. Prove that $\sqrt{5}$ does not belong to $\mathbb{Q}$, that is to say, is not a rational number.

(In other words, prove that it can’t be written as a fraction $\frac{m}{n}$ with $m \in \mathbb{Z}$, $n \in \mathbb{N}$ with $n \geq 1$ and $m$ and $n$ relatively prime).

If we could write $\sqrt{5} = \frac{m}{n}$, then $5m^2 = n^2$. So $5$ divides $m^2 = m \times m$.

But $5$ is prime! So $5$ divides $m$.

Hence $m$ can be written $m = 5k$ for a certain $k \in \mathbb{Z}$.

Now $5m^2 = 5^2k^2$ $n^2 = 5k^2$. By the same argument $5$ divides $m$.

It contradicts $(m, n) = 1$.

So $\sqrt{5}$ is not rational.

2. Does the equation $x^2 - x - 1 = 0$ have a solution in $\mathbb{Z}$? in $\mathbb{Q}$?

Its solutions are $\frac{1 \pm \sqrt{5}}{2}$.

So none of them is in $\mathbb{Z}$, and none of them is in $\mathbb{Q}$ by the previous question.