Assignment 3

1. Show that if p is an odd prime then:

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases} \tag{1}$$

Solution. Firstly, we must assume that $p > 3$, as the statement in (1) does not hold otherwise. We can then apply Gauss's Quadratic Reciprocity Law:

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \begin{cases} -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \pmod 4 \\ \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \pmod 4. \end{cases} \tag{2}$$

So now we can observe also that:

$$\left(\frac{p}{3}\right) = \begin{cases} -1 & \text{if } p \equiv 2 \pmod 3 \\ 1 & \text{if } p \equiv 1 \pmod 3. \end{cases} \tag{3}$$

So that $\left(\frac{3}{p}\right)$ is 1 only in those two cases:

(a) If $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$, with the solution $p \equiv 11 \pmod{12}$.

(b) If $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$, with the solution $p \equiv 11 \pmod{12}$.

Finally, we can prove easily that $\left(\frac{3}{p}\right)$ is negative if and only if:

(a) If $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 3$, with the solution $p \equiv 7 \pmod{12}$.

(b) If $p \equiv 1 \pmod 4$ and $p \equiv 2 \pmod 3$, with the solution $p \equiv 5 \pmod{12}$.

2. Let $a, b, c \in \mathbb{Z}$ be integers and p be an odd prime. Prove that the modular equation:

$$(x^2 - ab)(x^2 - ac)(x^2 - bc) \equiv 0 \pmod p. \tag{4}$$

admits always a solution $x \in \mathbb{Z}$.

Solution. If p divides at least one among a, b, c, we can simply choose x to be in the congruence class of zero modulo p.

Otherwise, if p does not divide any of $a, b, c \in \mathbb{N}$, suppose a and b are quadratic residues. Then, there exist coprime integers y and z such that

$$\begin{cases} y^2 \equiv a \pmod{p} \\ z^2 \equiv b \pmod{p}. \end{cases} \tag{5}$$

This implies that $(xy)^2$ is congruent to ab modulo p. More generally, if at least two among a, b, c are quadratic residues, the product of which is also a residue, the equation (4) has a solution.

Conversely, if a and b are not quadratic residues modulo p, a direct consequence of Euler's criterion (corollary) is

$$\begin{cases} -1 \equiv a^{\frac{p-1}{2}} \pmod{p} \\ -1 \equiv b^{\frac{p-1}{2}} \pmod{p}. \end{cases} \tag{6}$$

This implies that $(ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, which, again by Euler's criterion, means that ab is a quadratic residue. Similarly, if at least two among a, b, c are not quadratic residues, the product of which is also a residue, the equation (4) has a solution.

3. Let $n \in \mathbb{Z}$ be an integer. Prove that the integer $n^2 + n + 1$ does not have any divisors of the form $6k - 1$, with $k \in \mathbb{Z}$.

   Solution. Suppose there exists a prime p such that $p \mid n^2 + n + 1$. Then, p must divide $n^3 - 1 = (n-1)(n^2 + n + 1)$.

   Either p divides $n - 1$, in which case it also divides the gcd between $n - 1$ and $n^2 + n + 1$. This implies:

   $$n^2 + n + 1 - (n-1)(n+2) = 3.$$

   Hence, $p \mid 3$, and a prime that divides 3 is necessarily 3.

   Alternatively, if n has multiplicative order 3 in $\mathbb{Z}/p\mathbb{Z}$, it means that $3 \mid (p-1)$, and thus, $p = 6k + 1$ for some $k \geq 1$.

   In summary, a prime divisor of $n^2 + n + 1$ is either 3 or of the form $6k + 1$.

   Therefore, if $m \mid n^2 + n + 1$, then either m is a multiple of 3 and belongs to the congruence class of zero modulo 6, or there exist positive integers k_i for $i = 1, 2, \ldots, r$ such that:

   $$m = \prod_{i=1}^{r} (1 + 6k_i) \equiv 1 \pmod{6}.$$

4. Let $p > 3$ be a prime.

   (a) Prove that the sum of all quadratic residues modulo p is divisible by p, i.e.,

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z}):\ \left(\frac{a}{p}\right)=1} a \equiv\ 0 \pmod{p}. \tag{7}$$

   Solution. Let s be defined as follows:

$$s = \sum_{a \in (\mathbb{Z}/p\mathbb{Z}):\ \left(\frac{a}{p}\right)=1} a. \tag{8}$$

   Since $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group, there exists a primitive root r. The sum expressed in (8) can be rewritten as:

$$s \equiv r^2 + r^4 + \cdots + r^{p-1} \pmod{p}. \tag{9}$$

   Since $p > 3$, r^2 is not the multiplicative identity modulo p. Therefore, $p \nmid (r^2 - 1)$. Multiplying (9) by $r^2 - 1$, we have, thanks to Fermat's Little Theorem:

$$(1 - r^2)s \equiv (1 - r^2)(r^2 + \cdots + r^{p-1}) \equiv r^2 \left(r^{p-1} - 1\right) \pmod{p}. \tag{10}$$

   Therefore, $p \mid s$ since it cannot divide $(1 - r^2)$, as observed earlier.

   (b) Use the previous statement to show that also the sum of all non-quadratic residue mod p is divisible by p, i.e.,

$$\sum_{b \in (\mathbb{Z}/p\mathbb{Z}):\ \left(\frac{a}{p}\right)=-1} b \equiv\ 0 \pmod{p}. \tag{11}$$

   Solution. The proof relies on the previous case, with s' being the sum defined in (11). It is clear that

$$\frac{p(p-1)}{2} = 1 + 2 + \cdots + p - 1 = s + s'. \tag{12}$$

   But, from the previous point, we have $p \mid s$ and the term on the left side of (12). Therefore, we get:

$$\sum_{b \in (\mathbb{Z}/p\mathbb{Z}):\ \left(\frac{a}{p}\right)=-1} b = s' = \frac{p(p-1)}{2} - p \equiv 0 \pmod{p}. \tag{13}$$

5. Consider the quadratic congruence

$$aX^2 + bX + c \equiv 0 \pmod{p} \tag{14}$$

where p is prime and a, b, and c are integers with a not divisible by p.

(a) Let $p = 2$. Determine which quadratic congruences have solutions.

Solution. So, by assumption, a is odd, and the equation (14) becomes, by Fermat's Little Theorem,

$$(1 + b)X + c \equiv 0 \pmod{p}. \tag{15}$$

So, if b is odd and c is odd, there are no solutions. This is because we would have $(1 + b)X + c \equiv 2X + 1$, which is always odd.

If b is odd but c is even, the equation (15) is always satisfied.

If b is even, on the other hand, the equation becomes $X + c \equiv 0 \pmod{p}$, which always has solutions.

(b) Let p be an odd prime and set $d = b^2 - 4ac$. Show that the congruence (14) is equivalent to the congruence

$$Y^2 \equiv d \pmod{p} \tag{16}$$

where $Y = 2aX + b$. Determine the number of incongruent solutions $\pmod{p}$ of (14).

Solution. We start by multiplying (14) by $4a$, without altering the equation since a is coprime with p, and $\mathbb{Z}/p\mathbb{Z}$ is, in particular, an integral domain:

$$0 \equiv 4a^2X^2 + 4abX + 4ac \equiv (2aX + b)^2 - (b^2 - 4ac) \pmod{p}. \tag{17}$$

Therefore, thanks to (17), the equation can be rewritten as follows:

$$(2aX + b)^2 \equiv d \pmod{p}, \tag{18}$$

which is equivalent to saying that a solution exists if and only if d is a quadratic residue modulo p, as in (16).

To find the number of solutions, we can rely on (16), as we have shown it to be equivalent to solving (14).

Clearly, if $d \equiv 0 \pmod{p}$, there is a single solution corresponding to the zero residue class.

On the other hand, if d is not a quadratic residue modulo p, there is no solution.

Finally, if d is a quadratic residue modulo p, there are two incongruent solutions.

6. (a) Find a primitive root of the prime 19.

   Solution. Let g be a primitive root, then $g = 3$. To prove this, let's observe that if o is the multiplicative order of g, then $o \mid 18$. We want to prove that $o = 18$.

$$\begin{aligned}
3^2 &\equiv 9 \pmod{19} \\
3^3 &\equiv 27 \equiv 8 \pmod{19} \\
3^6 &\equiv \left(3^3\right)^2 \equiv 8^2 \equiv 7 \pmod{19} \\
3^9 &\equiv \left(3^3\right)^3 \equiv 8^3 \equiv 7 \cdot 8 \equiv -1 \pmod{19}.
\end{aligned}$$

   Hence, we have found a primitive root.

   (b) Find all solutions of $x^6 \equiv 6 \pmod{19}$.

   Solution. Since 3 is a primitive root, observe that $3^8 \equiv 6 \pmod{19}$, and for $k \in \mathbb{N}$ such that $3^k \equiv x \pmod{19}$, the equation can be rewritten as

$$x^6 \equiv 3^8 \pmod{19} \iff 6k \equiv 8 \pmod{18},$$

   which has no solution since 6 is a divisor of zero modulo 18.

7. You found a note from Alice to Bob with the following *"the answer to the ultimate question of life is m+25. In fact, I used your RSA public key to get $E(m) = 17$"*. You know that Bob's RSA-public key is $(n, e) = (39, 13)$.

   (a) Give in detail a method to break the code (no calculations required yet).

   Solution. The idea is as follows: $n = 3 \cdot 13$ is a composite number with $\phi(n) = 24$, and we use the relation $d^{-1} \equiv e = 13 \pmod{24}$. From this, it's easily derived that $d = 13$. At this point, we can perform the decryption.

$$m \equiv (E(m))^d \equiv 17^{13} \equiv 17 \pmod{24}.$$

(b) What is the answer to the ultimate question of life?
Solution. The answer is $17 + 25 = 42$.

8. (a) Prove that 22 is a square $\pmod{449}$.
Solution.
Using Euler's criterion, we know that:

$$\left(\frac{22}{449}\right) = 1 \iff 22^{\frac{449-1}{2}} = 22^{224} \equiv 1 \pmod{p}. \qquad (19)$$

So, converting the number 224 to binary, we obtain $224_{10} = 11100000$:

$$\begin{aligned} 224 =& 2 \cdot 112 + 0 \\ 112 =& 2 \cdot 56 + 0 \\ 56 =& 2 \cdot 28 + 0 \\ 28 =& 2 \cdot 14 + 0 \\ 14 =& 2 \cdot 7 + 0 \\ 7 =& 2 \cdot 3 + 1 \\ 3 =& 2 \cdot 1 + 1 \\ 1 =& 2 \cdot 0 + 1. \end{aligned}$$

Now we can proceed with the calculation of the power:

$$\begin{aligned} 22^{224} \equiv& 22^{2^7} \cdot 22^{2^6} \cdot 22^{2^5} \pmod{449} \\ 22^2 \equiv& 484 \equiv 35 \pmod{449} \\ 22^3 \equiv& 22 \cdot 35 \equiv 770 \equiv 321 \pmod{449} \\ 22^4 \equiv& 321 \cdot 22 \equiv 7062 \equiv 327 \pmod{449} \\ 22^5 \equiv& 22 \cdot 327 \equiv 7194 \equiv 10 \pmod{449} \\ 22^{2^4} \equiv& 22^16 \equiv 22^{3 \cdot 5} \cdot 22 \equiv 10^3 \cdot 22 \equiv 102 \cdot 449 \cdot -1 \pmod{449} \\ 22^{2^5} \equiv& (-1)^2 \equiv 1 \pmod{449} \\ 22^{2^6} \equiv& 22^{2^7} \equiv 1 \pmod{449}. \end{aligned}$$

Hence, the thesis is $22^{224} \equiv 1 \pmod{449}$: 22 is a square modulo 449.

(b) Find a square root of 22 $\pmod{449}$.
Solution. Let's choose a random $z = 1$ and evaluate and let be α a root of 22, we want to solve:

$$(1+1\alpha)^{224} = u + v\alpha \pmod{449}.$$

To solve this problem, we'll use the binary representation, as done previously:

$$\begin{aligned}
(1+\alpha)^2 &\equiv 23 + 2\alpha \pmod{449} \\
(1+\alpha)^4 &\equiv (23+2\alpha)^2 \equiv 168 + 92\alpha \pmod{449} \\
(1+\alpha)^8 &\equiv (168+92\alpha)^2 \equiv 259 + 380\alpha \pmod{449} \\
(1+\alpha)^{16} &\equiv (259+380\alpha)^2 \equiv 305 + 178\alpha \pmod{449} \\
(1+\alpha)^{32} &\equiv (305+178\alpha)^2 \equiv 282 + 371\alpha \pmod{449} \\
(1+\alpha)^{64} &\equiv (282+371\alpha)^2 \equiv 97 + 10\alpha \pmod{449} \\
(1+\alpha)^{128} &\equiv (97+10\alpha)^2 \equiv 384 + 144\alpha \pmod{449} \\
(1+\alpha)^{96} &\equiv (97+10\alpha)(282+371\alpha) \equiv 316 + 193\alpha \pmod{449} \\
(1+\alpha)^{224} &\equiv (316+193\alpha)(384+144\alpha) \equiv 182\alpha \pmod{449}.
\end{aligned}$$

We found $u = 0$ and $v = 182$. Using the Euclidean division, it's easy to invert v modulo 449, obtaining $v' \equiv v^{-1} \equiv 412$. Now, we know that the modulo 443 roots of 22 are two among 0, 37, and 412. Clearly, the first one is to be excluded: the roots are the modular class of 37 and 412.