# Cryptology - Week 1 worksheet

These exercises are to introduce material you will need in weeks 3+. This worksheet is on modular arithmetic. These problems are designed to be answered in order as the concepts build on the previous questions.

- If you are already confident in modular arithmetic for arbitrary moduli, you may want to skip ahead to questions 6 and 7.
- If you have not seen these concepts before or are not confident with these concepts, and you do not have time to complete the sheet in this session, please aim to complete it by Friday of Week 3 at the latest at which point we will assume some familiarity with modular arithmetic to do some interesting cryptography (question 7 is a spoiler!).

1. **[One-time pad (OTP)]** Consider the message $m = 1100$, and key $k = 1010$. Calculate the ciphertext (encrypted message) given by $m \oplus k$, where $\oplus$ is the XOR operator.

   Solution: $m \oplus k = 1100 \oplus 1010 = 0110$.

2. **[Introduction to modular arithmetic]** In the OTP, we add strings together bitwise according to truth table logic. Another way we can think of this is by (bitwise) adding together numbers, and seeing what the remainder is when we divide by 2.
   For example, $1 + 1 = 2$, and when we divide this by 2, the remainder is 0; $1 + 0 = 1$ and when we divide this by 2, the remainder is 1.

   We can extend this type of addition to other numbers. For example, let's look at the remainders when we divide by 3. For example

   - $1 + 1 = 2$ and the remainder when we divide by 3 is 2;
   - $1 + 2 = 3$ and the remainder when we divide by 3 is 0;
   - $2 + 2 = 4$ and the remainder when we divide by 3 is 1.

   Calculate the remainder of:

   (a) Compute $10 + 5$ by 4

   (b) Compute $107 + 56$ by 9

(c) Compute $11 + 6$ by 12.

Solution:

(a) 3

(b) 1

(c) 5

This way of addition should already be familiar with you, at least when we're looking at the remainder after division by 12 – this is a new perspective about how we look at time on a 12-hour clock.

To make it easier to talk about this, we will introduce some vocabulary. This type of arithmetic is called **modular arithmetic**; we write $x \bmod y$ to mean the remainder of $x$ after after dividing by (an integer multiple of) $y$. Typically we have $x \bmod y \in \{0, 1, \ldots, y-1\}$, although we can choose an equivalent set of representatives. The "mod" is short for the word "modulo", so sometimes when speaking we say "modulo".

3. [ **Modular arithmetic tricks**] Let's look at the computations from Question 2 again; it was perhaps a bit cumbersome to first add the numbers and then look at the remainder because the numbers got quite big. This time:

   (a) Compute $(10 \bmod 4) + (5 \bmod 4)$

   (b) Compute $(107 \bmod 9) + (56 \bmod 9)$.

   (c) How could you make $(11 + 6) \bmod 12$ even easier to compute?

   Note that we can also subtract!

   (c) Compute $(8 - 12) \bmod 7$

   (d) Compute $(58 - 112) \bmod 7$.

   And multiply!

   (e) Compute $(5 \times 3) \bmod 13$

   (f) Compute $(68 \times 89) \bmod 11$ (remember the tricks from the earlier parts of this question!).

   Solutions:

   (a) $(10 \bmod 4) + (5 \bmod 4) = (2 \bmod 4) + (1 \bmod 4) = 3 \bmod 4$.

   (b) $(107 \bmod 9) + (56 \bmod 9) = (-1 \bmod 9) + (2 \bmod 9) = 1 \bmod 9$. It would also be correct to write $(8 \bmod 9)$ instead of $(-1 \bmod 9)$, but sometimes you might get slightly easier arithmetic by using negative numbers. Note that these are the same $\pmod 9$ since

   $$-1 \bmod 9 = -1 + 9 \bmod 9 = 8 \bmod 9.$$

(c) $(11+6) \bmod 12 = (11 \bmod 12)+(6 \bmod 12) = (-1 \bmod 12)+(6 \bmod 12) = (5 \bmod 12)$.

(c) again (sorry) $(8-12) \bmod 7 = (8 \bmod 7) - (12 \bmod 7) = (1 \bmod 7) - (5 \bmod 7) = -4 \bmod 7 = 3 \bmod 7$.

(d) $(58 - 112) \bmod 7 = 58 \bmod 7 - 112 \bmod 7 = 2 \bmod 7 - 0 \bmod 7 = 2 \bmod 7$.

(e) $(5 \times 3) \bmod 13 = 15 \bmod 13 = 2 \bmod 13$.

(f) $(68 \times 89) \bmod 11 = (68 \bmod 11) \times (89 \bmod 11) = (2 \bmod 11) \times (1 \bmod 11) = 2 \bmod 11$.

4. [**Finding additive inverses**] 0 is a special number for addition because $x + 0 = x$ for any number $x$; we call 0 the **additive identity**. For any number $x$, its **additive inverse** is $-x$ because $x + (-x) = 0$.

   In modular addition, we also have additive inverses. Find the additive inverse of:

   (a) $3 \bmod 7$

   (b) $5 \bmod 9$.

   e.g. for (a) you must find a number $x$ so that $3 + x = 0 \bmod 7$.
   Solutions:

   (a) $-3 \bmod 7 = 4 \bmod 7$.

   (b) $-5 \bmod 9 = 4 \bmod 9$.

5. [**Finding multiplicative inverses**] 1 is a special number for multiplication because $x \times 1 = x$ for any number $x$; we call 1 the **multiplicative identity**. For any non-zero (real) number $x$, its **multiplicative inverse** is $1/x$ because $x \times (1/x) = 1$.

   In modular addition, we also have multiplicative inverses. However they don't always exist!

   Find the multiplicative inverse of:

   (a) Compute the inverse of $6 \pmod{11}$, if it exists.

   (b) Compute the inverse of $6 \pmod 9$, if it exists.

   (c) Which $a \pmod 5$ have an inverse?

   (d) Which $a \pmod 6$ have an inverse?

   Solutions:

   (a) $6 \times 2 = 12 = 1 \pmod{11}$, so $2 \pmod{11}$ is the (multiplicative) inverse of $6 \pmod{11}$.

(b) There is no multiplicative inverse of 6 (mod 9). We can prove this by computing $6x \pmod 9$ for every $x \pmod 9$, and see that there is no $x$ such that $6x = 1 \pmod 9$:

$$\begin{aligned}
6 \times 0 &= 0 \pmod 9,\\
6 \times 1 &= 6 \pmod 9,\\
6 \times 2 &= 6 \times 1 + 6 = 3 \pmod 9,\\
6 \times 3 &= 6 \times 2 + 6 = 3 + 60 \pmod 9,\\
6 \times 4 &= 6 \times 3 + 6 = 0 + 6 = 6 \pmod 9,\\
6 \times 5 &= 6 \times 4 + 6 = 6 + 6 = 3 \pmod 9,\\
6 \times 6 &= 6 \times 5 + 6 = 3 + 6 = 0 \pmod 9
\end{aligned}$$

6. **[Euclid's algorithm in disguise]** In the previous question, we calculated inverses and it was perhaps somewhat tedious. In this question we're going to use a method that we'll study later in the course to find the inverse of 9 mod 13.

   (a) We'll start by writing $13 = 9m_2 + r_2$, for positive integers $m_2, r_2$. What are $m_2$ and $r_2$? (The subscripts in the notation are to fit in with the future presentation in the lecture.)

   (b) Now write $9 = r_2m_3 + r_3$, for positive integers $m_3, r_3$. What are $m_3$ and $r_3$?

   (c) Now write $r_2 = r_3m_4 + r_4$, for positive integers $m_4, r_4$. What are $m_4$ and $r_4$?

   Spoiler: hopefully you've now found that $r_4 = 0$, so we'll stop collecting these numbers.

   Now let's rewrite $r_3$ in terms of the numbers we found:

$$r_3 = 9 - r_2m_3 = 9 - (13 - 9m_2)m_3$$

   (d) Tidy up this mess to get an equation of the form $r_3 = 9a + 13b$. Now read off the inverse of 9 mod 13.

   (e) Repeat this process to find the inverse of 10 mod 117,

   (a) Applying division-with-remainder: 13 divided by 9 is '1 remainder 4', which algebraically looks like $13 = 9 \times 1 + 4$. So $m_2 = 1$ and $r_2 = 4$.

   (b) $m_3 = 2$ and $r_3 = 1$.

   (c) $m_4 = 4$ and $r_4 = 0$.

(d)

$$\begin{aligned} r_3 = 1 &= 9 - r_2 m_3 && \text{by (b)} \\ &= 9 - (13 - 9m_2)m_3 && \text{plugging in equation (a) for } r_2 \\ &= (1 + m_2 m_3)9 - m_3 13 && \text{rearranging to the form } a9 + b13 \\ &= 3 \times 9 - 2 \times 13 && \text{plugging in } m_2, m_3. \end{aligned}$$

Now reducing the equation

$$1 = 3 \times 9 - 2 \times 13$$

mod 13 gives

$$1 \equiv 3 \times 9 \bmod 13,$$

so the inverse of 9 mod 13 is 3 mod 13.

(e) To calculate the inverse of 10 mod 117, we first compute the gcd (=1!) of 10 and 117 using Euclid's algorithm.

$$\begin{aligned} 117 &= 10 \cdot 11 + 7 \\ 10 &= 7 \cdot 1 + 3 \\ 7 &= 3 \cdot 2 + 1, \end{aligned}$$

and then use the above equations to find $a$ and $b$ such that $10a + 117b = 1$:

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - (10 - 7 \cdot 1) \cdot 2 \\ &= 3 \cdot 7 - 2 \cdot 10 \\ &= 3 \cdot (117 - 11 \cdot 10) - 2 \cdot 10 \\ &= 3 \cdot 117 - 35 \cdot 10. \end{aligned}$$

Reducing mod 117 gives that the multiplicative inverse of 10 mod 117 is $-35$ mod 117.

7. **[Diffie-Hellman key exchange in disguise]** In this question, we'll calculate a shared secret. This is a discussion question so work with a partner. (If you prefer to work on your own, you can also just define two characters Alice and Bob to play the parts of you and a partner). We'll be working mod11.

   (a) First, each pick a non-zero element mod11; let's call it $s$ and keep it secret from your partner.

   (b) Calculate $x = 2^s \bmod 11$. Remember that whilst you're computing this product, at any stage you can reduce it mod11 – depending on how comfortable you are with powers of 2, this may or may not be useful.

(c) Tell your partner $x$. Each of you calculate $x^s \bmod 11$ for your own secret $s$.

(a) Alice: $s_A = 3 \bmod 11$. Bob: $s_B = 4 \bmod 11$.

(b) Alice: $x_A = 2^3 = 8 \bmod 11$. Bob: $x_B = 2^4 = 5 \pmod{11}$.

(c) Alice:

$$x_B^{s_A} = 5^3 = (5 \bmod 11)\cdot(25 \bmod 11) = (5 \bmod 11)\cdot(3 \bmod 11) = 4 \bmod 11.$$

Bob:

$$\begin{aligned} x_A^{s_B} &= 8^4 = (-3 \bmod 11)^4 = (-3 \bmod 11)^2 \cdot (-3 \bmod 11)^2 \\ &= (9 \bmod 11)^2 = (-2 \bmod 11)^2 = 4 \bmod 11. \end{aligned}$$