Cryptography

Modular arithmetic

We can use the notation

$$y = a \pmod{p}$$

to represent the remainder after division.

> **Example**
>
> For example, if $p = 4$ and $a = 11$. Then
>
> $$a \pmod{p}$$
>
> is
>
> $$11 \pmod{4}.$$
>
> This means the remainder when 11 is divided by 4.
> As 4 goes into 11 two times with three left over
>
> $$11 \equiv 3 \pmod{4}.$$

Exercises

1. Compute
    a. $5 \pmod{3}$
    b. $13 \pmod{7}$
    c. $18 \pmod{4}$

Exponents under modular arithmetic

We can perform arithmetic operations (e.g. addition, multiplication, powers) under modular arithmetic. Examples are multiplication

$$ab \pmod{4}$$

and exponentiation

$$a^x \pmod{p}.$$

> **Note**
>
> Suppose $a = 3$, $x = 2$ and $p = 7$. Then
>
> $$a^x = 3^2 = 9.$$
>
> So
>
> $$9 \equiv 2 \pmod{7}.$$

Exercises

Compute

1. $4 \times 3 \pmod{4}$
2. $5^2 \pmod{4}$
3. $(2^3)^2 \pmod{5}$
4. $(2^2)^3 \pmod{5}$.

> **Note**
>
> Did you get the same answer for (3) and (4)?
> This is because in general
>
> $$(a^b)^c \sim (a^c)^b \pmod{p}$$

A Caesar cipher

Using a cipher to encrypt a message requires replacing letters with letters, symbols or numbers.

Consider the cipher

Letter	Encryption
a	b
c	d
l	r
u	p
b	q

Letter	Encryption
s	t
t	m

Example

The word *tub* would be encrypted as *mpq*.
Using the table, the letter t is replaced by m, u is replaced by p etc.

Can you use the cipher to

1. encrypt the message *tall*?
2. decrypt the word *dbrdprpt*?

Warning

These types of fixed ciphers are not useful in modern encryption as they can be cracked using frequency analysis (with enough examples of words, use the known frequencies of letters in the english languages to crack the cipher).

A hash function is similar to a cipher in that letters in a message are represented by some other symbols. However, the output of hash functions is designed so that they cannot be cracked using frequency analysis.

The discrete log problem

Cracking Diffie-Hellman requires a computer to solve the discrete logarithm problem

$$a^x \mod p = q.$$

Suppose $a = 2$, $p = 7$ and $q = 5$.

The discrete log problem takes the form

$$2^x \mod 11 = 10.$$

Usually, when confronted with a difficult problem, we might consider an easier problem first. Here are some examples:

Try to solve the following problems for x:

1. $$2x = 10$$

   .

2. Now try $2^x = 10$.

`Does this second equation have a solution if we restrict  $x$ to being an integer?`

3. Now consider introducing modular arithmetic. Try to solve

$$2x \pmod{11} = 10$$

- did you find a solution?
- is there more than one?

> **Hint**
>
> a. Try inspection (guessing): for example is 0 a solution? If so, substituting yields
>
> $$0 \pmod{11} \neq 10.$$
>
> Hence 0 is not a solution.
>
> b. Could you sketch a graph of the function
>
> $$y(x) = 2x \pmod{11}.$$

4. Finally, let's consider the problem

$$2^x \pmod{11} = 10.$$

> **Hint**
>
> Diffie-Hellmann works because there is not a nice way to solve this problem.
> Try using the app to have a look at the graph and find a solution by inspection!