Euler's phi function

Definition 13. Euler's phi function $\phi(n)$ denotes the number of integers in $\{1, 2, ..., n\}$ that are relatively prime to n.

In other words, $\phi(n)$ counts how many residues are invertible modulo n.

If the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.

Why is this true?

- Why is the formula "obvious" if $n = p^k$ is a prime power?
- On the other hand, for composite n, say $n = ab$, we have: $\boxed{\phi(ab) = \phi(a)\phi(b) \text{ if } \gcd(a,b) = 1}$
  This is a consequence of the Chinese remainder theorem. (Review if necessary! We'll use it later but will only review it briefly then.)

The above formula follows from combining these two observations. Can you fill in the details?

Example 14. Compute $\phi(35)$.

Solution. $\phi(35) = \phi(5 \cdot 7) = \phi(5)\phi(7) = 4 \cdot 6 = 24$

Example 15. Compute $\phi(100)$.

Solution. $\phi(100) = \phi(2^2 \cdot 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$

[Alternatively: $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = (2^2 - 2^1) \cdot (5^2 - 5^1) = 40$]

Historical examples of symmetric encryption

Alice wants to send a secret message to Bob.

What Alice sends will be transmitted through an unsecure medium (like the internet), meaning that others can read it. However, it is important to Alice and Bob that noone else can understand it.

The original message is referred to as the **plaintext** m. What Alice actually sends is called the **ciphertext** c (the encrypted message).

Symmetric encryption algorithms rely on a secret key k (from some **key space**) shared by Alice and Bob (but unknown to anyone else).

Our ultimate goal will be to secure messaging against both:

- eavesdropping (goal: **confidentiality**)
- tampering (goal: **integrity** as well as **authenticity**)

  The symmetric encryption approach, by itself, cannot fully protect against tampering. For instance, an attacker can collect previously sent messages, resend them, or use them to replace new messages. (You could preface each message with something like a time stamp to address these issues. But that's getting ahead of ourselves; and there are better ways.)

Armin Straub
straub@southalabama.edu

Shift cipher

The alphabet for our messages will be $A, B, ..., Z$, which we will identify with $0, 1, ..., 25$.

So, for instance, C is identified with the number 2.

Example 16. (shift cipher) A key is an integer $k \in \{0, 1, ..., 25\}$. Encryption works character by character using

$$E_k: \quad x \mapsto x + k \pmod{26}$$

Obviously, the decryption D_k works as $x \mapsto x - k \pmod{26}$.

The **key space** is $\{0, 1, ..., 25\}$. It has size 26. [Well, $k = 0$ is a terrible key. Maybe we should exclude it.]

For instance. If $k = 1$, then the message $HELLO$ is encrypted as $IFMMP$.

If $k = 2$, then the message $HELLO$ is encrypted as $JGNNQ$.

Historic comment. Caesar encrypted some private messages with a shift cipher (typically using $k = 3$). The shift cipher is therefore also often called Caesar's cipher.

While completely insecure today, it was fairly secure at the time (with many of his enemies being illiterate).

Modern comment. Many message boards on the internet "encrypt" things like spoilers or solutions using a shift cipher with $k = 13$. This is called ROT13. What's special about the choice $k = 13$?

Solution. Since $-13 \equiv 13 \pmod{26}$, for ROT13, encryption and decryption are the same!

Example 17. (affine cipher) A slight upgrade to the shift cipher, we encrypt each character as

$$E_{(a,b)}: \quad x \mapsto ax + b \pmod{26}.$$

How does the decryption work? How large is the key space?

Solution. Each character x is decrypted via $x \mapsto a^{-1}(x - b) \pmod{26}$.

The key is $k = (a, b)$. Since a has to be invertible modulo 26, there are $\phi(26) = \phi(2 \cdot 13) = 26\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{13}\right) = 12$ possibilities for a. There are 26 possibilities for b. Hence, the key space has size $12 \cdot 26 = 312$.

Vigenere cipher (vector shift cipher)

See Section 2.3 of our book for a full description of the Vigenere cipher.

This cipher was long believed by many (until early 20th) to be secure against ciphertext only attacks (more on the classification of attacks shortly).

Example 18. Let us encrypt $HOLIDAY$ using a Vigenere cipher with key BAD (i.e. $1, 0, 3$).

	H	O	L	I	D	A	Y
$+$	B	A	D	B	A	D	B
$=$	I	O	O	J	D	D	Z

Hence, the ciphertext is $IOOJDDZ$.

An encrypted message

Example 19. (bonus challenge!) You find a post-it with the following message:

$$GPLQA \quad VJG \quad YGGMGPF$$

Can you make any sense of it?

Send me an email until 1/16 to collect a bonus point for deciphering the message!

Armin Straub
straub@southalabama.edu