

Simple Substitution Ciphers

Here are examples of simple ciphers which use congruences modulo the alphabet size.

Use the numbers 0 to 25 to represent (code) the English alphabet: $0 = A$, $1 = B$, $2 = C$, ..., $25 = Z$.

With this code, we can encipher a message by computing with the numbers corresponding to the letters of the message. Then we use the code to change numbers back to letters.

For example, we can “rotate the alphabet” by k letters. In terms of the numbers, we encipher x by adding k to it modulo 26: $E(x) = x + k \pmod{26}$.

Julius Caesar used this cipher with $k = 3$. Under this cipher, the message

RENAISSANCE

is enciphered as

UHQDLVVDQFH

One deciphers this cipher either by rotating the alphabet backwards by k letters: $D(x) = x - k \pmod{26}$ or by rotating the alphabet forward by $26 - k$ letters: $D(x) = x + (26 - k) \pmod{26}$.

The case $k = 13$ gives the rotate cipher used in some newsgroups. It has the nice property that the deciphering formula is the same as the enciphering formula: $D(x) = x + 13 \pmod{26} = E(x)$.

Another possibility is to multiply the numbers which represent the letters by a constant: $E(x) = kx \pmod{26}$.

Under this cipher with $k = 9$, the message
RENAISSANCE
is enciphered as

XKNAUGGANSK

In order for deciphering to be possible, k and 26 must be relatively prime. When this is so, let $jk \equiv 1 \pmod{26}$. Then the deciphering function is $D(x) = jx \pmod{26}$.

The Chinese Remainder Theorem

Theorem. Let n_1, \dots, n_r be r positive integers relatively prime in pairs. (That is, $\gcd(n_i, n_j) = 1$ whenever $1 \leq i < j \leq r$.) Let a_1, \dots, a_r be any r integers. Then the r congruences

$$x \equiv a_i \pmod{n_i}$$

for $i = 1, \dots, r$ have common solutions. Any two common solutions are congruent modulo

$$n = n_1 \cdots n_r$$

.

The proof gives an algorithm for computing the common solution.

Proof: For $j = 1, \dots, r$, the number n/n_j is an integer and

$$\gcd(n/n_j, n_j) = 1,$$

so there is an integer b_j such that

$$(n/n_j)b_j \equiv 1 \pmod{n_j}.$$

Clearly, $(n/n_j)b_j \equiv 0 \pmod{n_i}$ if $i \neq j$. Let

$$x_0 = \sum_{j=1}^r (n/n_j)b_j a_j.$$

Then

$$x_0 = \sum_{j=1}^r (n/n_j b_j) a_j = \sum_{j=1}^r \delta_{ij} a_j \equiv a_i \pmod{n_i}.$$

Thus there is a common solution x_0 .

If x_1 is another common solution, then $n_i | (x_0 - x_1)$ for each i , so $n | (x_0 - x_1)$ because the moduli are relatively prime in pairs.