2. Euclid's algorithm and bank accounts

What is the best was to find the inverse k of 15 modulo 26? Otherways put, what is the best way of finding an integer k such that the equation

$$15 \times k \equiv 1 \mod 26 \mod \tag{2.1}$$

holds? One possibility is to run through the numbers $0, 1, 2, \ldots, 25$

$$\begin{aligned} 15 \times 0 &\equiv 0 \mod 26 \\ 15 \times 1 &\equiv 1 \mod 26 \\ 15 \times 2 &\equiv 4 \mod 26 \\ 15 \times 3 &\equiv 19 \mod 26 \\ 15 \times 4 &\equiv 8 \mod 26 \\ &\vdots \end{aligned}$$

until we find a k satisfying equation (2.1). We'll describe an alternative method which is better in two respects. The alternative method will be more efficient, particularly when applied to finding inverses module a number significantly larger than 26. Secondly, the alternative method provides mathematical insight into inverses in clock arithmetic.

2.1 Euclidean algorithm

The *greatest common divisor* of two integers m and n is defined to be the smallest positive integer d such that both m and n are integer multiples of d. We denote this greatest common divisor by $gcd(m,n)$. For example, $gcd(30,36) = 6$.

The alternative method begins by using a procedure known as the *Euclidean algorithm* to find the greatest common divisor of 15 and 26. Clearly we don't really need any algorithm to determine $gcd(15,26) = 1$. But we can use the inner workings of the Euclidean algorithm to find a solution k to (2.1). The easiest way to explain the algorithm is simply to illustrate its use.

To calculate $gcd(108,46)$ we procede as follows.

$$\mathbf{108} = 2.\mathbf{46} + \mathbf{16} \tag{2.2}$$
$$\mathbf{46} = 2.\mathbf{16} + \mathbf{14} \tag{2.3}$$
$$\mathbf{16} = 1.\mathbf{14} + \mathbf{2} \tag{2.4}$$
$$\mathbf{14} = 7.\mathbf{2} + \mathbf{0} \tag{2.5}$$

The algorithm stops when we hit a remainder of 0. The penultimate remainder, namely 2, divides all numbers on the left hand side of the equalities. (In this example we can simply observe this; but a simple inductive argument can be used to prove that the penultimate remainder will divide all numbers on the left of the equalities in every example.) In particular, the penultimate remainder divides both 108 and 46 and is thus a common divisor of the two numbers.

In order to establish that the penultimate remainder is the greatest common divisor of 108 and 46 we start with the penultimate equation (2.4) of the algorithm, and procede to use the subsequent equations in turn, as follows.

$$\mathbf{2} = \mathbf{16} - 1.\mathbf{14} \tag{2.6}$$
$$= \mathbf{16} - 1.(\mathbf{46} - 2.\mathbf{16}) = 3.\mathbf{16} - 1.\mathbf{46} \tag{2.7}$$
$$= 3.(\mathbf{108} - 2.\mathbf{46}) - 1.\mathbf{46} = -3.\mathbf{46} + 3.\mathbf{108} \tag{2.8}$$

This manipulation is summarized by the following exprssion.

$$\mathbf{2} = 3.\mathbf{108} - 3.\mathbf{46} \tag{2.9}$$

In particular, any common divisor of 46 and 108 must devide 2. We conclude that the penultimate remainder, 2, is the *greatest* common divisor.

2.2 Bézout's identity

Note that equation (2.9) is an expression of $gcd(108,46)$ as an integer combination of 108 and 46. An expression of $gcd(m,n)$ as an integer combination $gcd(m,n) = a.m + b.n$ will always arise in this way for any integers m,n and is known as *Bézout's Identity*. The integers a and b are not unique.

Keeping in mind our initial question of finding $15^{-1} \mod 26$, let us find a Bézout identity for $gcd(26,15)$. We begin with the Euclidean algorithm.

$$\mathbf{26} = 1.\mathbf{15} + \mathbf{11} \tag{2.10}$$
$$\mathbf{15} = 1.\mathbf{11} + \mathbf{4} \tag{2.11}$$
$$\mathbf{11} = 2.\mathbf{4} + \mathbf{3} \tag{2.12}$$
$$\mathbf{4} = 1.\mathbf{3} + \mathbf{1} \tag{2.13}$$
$$\mathbf{3} = 3.\mathbf{1} + \mathbf{0} \tag{2.14}$$

The penultimate remainder is 1 which equals $gcd(26,15)$. We now rewrite the workings of the algorithm, starting from the penultimate equation (2.13).

$$\mathbf{1} = \mathbf{4} - 1.\mathbf{3} \tag{2.15}$$
$$= \mathbf{4} - 1.(\mathbf{11} - 2.\mathbf{4}) = 3.\mathbf{4} - 1.\mathbf{11} \tag{2.16}$$
$$= 3.(\mathbf{15} - 1.\mathbf{11}) - 1.\mathbf{11} = 3.\mathbf{15} - 4.\mathbf{11} \tag{2.17}$$
$$= 3.\mathbf{15} - 4.(\mathbf{26} - 1.\mathbf{15}) = 7.\mathbf{15} - 4.\mathbf{26} \tag{2.18}$$

We thus have the Bézout identity

$$\mathbf{1} = 7.\mathbf{15} - 4.\mathbf{26} \tag{2.19}$$

2.3 Inverses in clock arithmetic

Expressing (2.19) on a 26-hour clock we find

$$7 \times 15 \equiv 1 \mod 26 \tag{2.20}$$

which yields the required inverse.

$$15^{-1} \equiv 7 \mod 26$$

This method of finding the inverse of $n \mod m$ clearly works whenever $gcd(m,n) = 1$. On the other hand, if n has some inverse k modulo m then $nk \equiv 1 \mod m$, which means there exists an integer ℓ for which the following holds.

$$nk = 1 + \ell m \tag{2.21}$$

In this case we must have $gcd(m,n) = 1$. We have just proved the following useful result.

Theorem 2.3.1 The integer n has an inverse on an m-hour clock if, and only if, $gcd(m,n) = 1$.

In particular, none of the integers $0,2,4,6,8,10,12,13,14,16,18,20,22,24$ has an inverse modulo 26.

2.4 Bank account numbers

A bank account is identified by its International Bank Account Number (IBAN). This has the form

GB 82 WEST 123456 98765432

where *GB* is the country code, *WEST* is derived from the owner's name, *123456* is the bank sort code, and *98765432* is the account number. The digits *82* are check digits. The IBAN is converted to an integer by first rearranging it in the form

WEST 123456 98765432 GB 82

and then replacing each letter with two digits according to the scheme $A \sim 10$, $B \sim 11$, $\ldots$, $Z \sim 35$. In the given example we get the following integer.

$$n = 32142829\ 123456\ 98765432\ 1611\ 82$$

The check digits 82 are chosen to ensure

$$n \equiv 1 \mod 97.$$

The check numbers c in this example would have been chosen using the following formula.

$$c \equiv 1 - (32142829\ 123456\ 98765432\ 1611) \times 100 \equiv 82 \mod 97 \tag{2.22}$$

To use the formula we need an efficient method for calculating modulo 97. One handy method uses the observation that $100 \equiv 3 \mod 97$. Suppose for instance that we want to find the value of 31415927 modulo 97. We can procede as follows.

$$\begin{aligned}
31415927 &= 31 \times 10^6 + 41 \times 10^4 + 59 \times 10^2 + 27 && (2.23)\\
&\equiv 31 \times 3^3 + 41 \times 3^2 + 59 \times 3 + 27 \mod 97 && (2.24)\\
&\equiv 93 \times 3^2 + 26 \times 3 + 80 + 27 \mod 97 && (2.25)\\
&\equiv -4 \times 9 - 19 - 17 + 27 \mod 97 && (2.26)\\
&\equiv -45 \mod 97 && (2.27)\\
&\equiv 52\,. && (2.28)
\end{aligned}$$