THE EUCLIDEAN ALGORITHM

We are to find the greatest common divisor (gcd) of 1905 and 11205. We proceed as follows

$$\begin{aligned}
11205 &= 5 \times 1905 + 1680 &(1)\\
1905 &= 1 \times 1680 + 225 &(2)\\
1680 &= 7 \times 225 + 105 &(3)\\
225 &= 2 \times 105 + 15 &(4)\\
105 &= 7 \times 15 + 0 &(5)
\end{aligned}$$

More precisely, at the k^{th} step of the process we have

$$R_{k-2} = D_k\, R_{k-1} + R_k$$

Then at the $(k+1)^{st}$ step we divide R_{k-1} by R_k and obtain a new remainder R_{k+1}, that is

$$R_{k-1} = D_{k+1}\, R_k + R_{k+1}$$

This process stops when $R_{k+1} = 0$. The conclusion that can be drawn from equations (1)–(5) is that the gcd of 11205 and 1905 is 15. The reasoning is as follows:

$$\begin{aligned}
(5) &\Rightarrow \text{15 divides 105}\\
(4) &\Rightarrow \text{15 divides 225}\\
(3) &\Rightarrow \text{15 divides 1680}\\
(2) &\Rightarrow \text{15 divides 1905}\\
(1) &\Rightarrow \text{15 divides 11205}
\end{aligned}$$

Thus 15 is a common divisor of 11205 and 1905. Conversely, suppose d is any divisor of these two numbers. Reversing the argument, we get

$$\begin{aligned}
(1) &\Rightarrow d \text{ divides 1680}\\
(2) &\Rightarrow d \text{ divides 225}\\
(3) &\Rightarrow d \text{ divides 105}\\
(4) &\Rightarrow d \text{ divides 15}
\end{aligned}$$

and thus 15 must be the greastest common divisor of these two numbers. Actually equations (1)-(5) give a bit more. Indeed we can write

$$\begin{aligned}
15 &= 225 - 2 \times 105 = 225 - 2(1680 - 7 \times 225)\\
&= -2 \times 1680 + 15 \times 225 = -2 \times 1680 + 15(1905 - 1680)\\
&= 15 \times 1905 - 17 \times 1680 = 15 \times 1905 - 17(11205 - 5 \times 1905)
\end{aligned}$$

So finally we get

$$15 = -17 \times 11205 + 100 \times 1905 \tag{6}$$

The point is that our equations (1)-(5) give us constants h (=-17) and k (=100) such that we have

$$15 = h \times 11205 + k \times 1905$$

More generally, given two integers a and b, the process illustrated above, usually referred to as the Euclidean Algorithm, yields not only the greatest common divisor of a and b, call it d for a moment, but it also yields two constants h and k such that

$$\boxed{d = h\,a + k\,b} \tag{7}$$

Remark 1.
Note that equation (6) may also be written in the form

$$15 = (-17 + 1905)11205 + (100 - 11205)1905 = 1888 \times 11205 - 11105 \times 1905$$

More generally, assuming that $a \geq b > 0$, by adding $c\,b$ to h and subtracting $c\,a$ from k (for a suitable choice of c) we can always rewrite (7) in the form

$$d = s\,a - t\,b$$

with $0 \leq s \leq b-1$ and $0 \leq t \leq a-1$. The reason for this is that we can certainly choose c so that $s = h + c\,b$ satisfies the first of these inequalities, this done we get (setting $t = k - ca$)

$$t\,b = s\,a - d < b\,a$$

and this gives the second inequality.

Remark 2.
It is customary to denote the gcd of two numbers a and b by the symbol (a, b). We should note that if

$$d = (a, b) \tag{8}$$

then we have as well

$$1 = \left(\frac{a}{d}, \frac{b}{d}\right) \tag{9}$$

The reason for this is very simple. Indeed, the condition in (8) by the Euclidean algorithm, implies that

$$d = h\,a + k\,b \tag{10}$$

moreover since d is a divisor of both a and b we can write $a = d\,a'$ and $b = d\,b'$. Substituting this in (10) gives

$$d = h\,d\,a' + k\,d\,b'$$

cancelling the common factor d yields

$$1 = ha' + kb'$$

and this clearly implies that the gcd of a' and b' is equal to 1 as asserted.

We should mention that two numbers a and b with $(a, b) = 1$ are said to be "*relatively prime*".

SOLUTIONS TO LINEAR CONGRUENCE EQUATIONS

Our aim is now to show how to solve equations of the form

$$a\,x \equiv b \pmod{m} \tag{11}$$

where a, b and m are given and x is unknown. Equation (11) simply means that for some integer p we have

$$a\,x = b + p\,m \tag{12}$$

or better

$$b = a\,x - p\,m$$

Now clearly this implies that the gcd of a and m must divide b. So unless this is the case, equation (11) cannot possibly have any solutions. This given, let $d = (a, m)$ and set $a = d\,a'$, $b = d\,b'$, and $m = d\,m'$. Substituting this in (12) gives

$$d\,a'\,x = d\,b' + p\,d\,m'$$

cancelling the common factor we finally get

$$a'\,x = b' + p\,m' \tag{13}$$

that is $a'\,x \equiv b' \pmod{m'}$. Now, by Remark 2, we deduce that $(a', m') = 1$. In other words, when (a, m) divides b, we may conclude that equation (11) can be reduced (by dividing out (a, m)) to one of the same form for which a and m are relatively prime. Moreover note that if x is any solution of (13) then the expression

$$x + i\,m' \qquad \text{for } i = 1, 2, \ldots, d-1$$

gives d distinct solutions of (11). We therefore are left to solve (11) when $(a, m) = 1$. However, in this case we have a very nice result, namely:

Theorem 1 *Let $(a, m) = 1$ and let h, k be derived from the Euclidean Algorithm so that we have*

$$1 = h\,a + k\,m \tag{14}$$

then the equation

$$a\,x \equiv b \pmod{m} \tag{15}$$

has the unique solution

$$x \equiv h\,b \pmod{m} \tag{16}$$

Proof

Multiplying (15) by h we derive

$$h\,a\,x \equiv (1 - k\,m)\,x \equiv h\,b \pmod{m}$$

or, which is the same

$$x \equiv h\,b \pmod{m}$$

This shows that the solution of (15), if it exists, must be given by (16) as asserted. Conversely, substituting this value of x in (16) (and using (14) again) we get

$$a\,x \equiv a\,h\,b \equiv (1 - km)\;b \equiv b \pmod{m}.$$

Thus (16) does indeed give a solution. This completes the proof.

Remark 3.
Note that we may have

$$a\,x \equiv a\,y \pmod{m} \tag{17}$$

without necessarily having

$$x \equiv y \pmod{m}$$

For instance,

$$2 \times 5 \equiv 2 \times 2 \pmod{6}$$

yet we do not have

$$5 \equiv 2 \pmod{6}$$

The reason for this is that we cannot "cancel" common factors in modular arithmetic, since our "numbers" do not always have "inverses". Nevertheless, in case $(a, m) = 1$ then cancellation is possible in (17). Indeed, in this case we are able to find an integer a' such that

$$a\,a' \equiv 1 \pmod{m} \tag{18}$$

this integer is precisely the solution of the equation

$$a\,x \equiv 1 \pmod{m}$$

which we now know how to solve. Using this integer we deduce from (17) that

$$a'\,a\,x \equiv a'\,a\,y \pmod{m}$$

that is (using (18))

$$x \equiv y \pmod{m}$$

which is precisely what we wanted to conclude.

We can see then that the integer h in the expression

$$1 = h\,a + k\,m,$$

given by the Euclidean Algorithm, is precisely the (mod m) "*inverse*" of a.

Example
Let us suppose we are given to solve the equation

$$127\,x \equiv 22 \pmod{747} \tag{19}$$

Note that since we do have $15 = (11205, 1905)$, upon division by 15 we get as well that $1 = (747, 127)$. So this equation can be solved. In fact, upon dividing (6) by 15 we get

$$1 = 100 \times 127 - 17 \times 747$$

and thus the solution of (19) is given by

$$x \equiv 100 \times 22 \equiv 2200 \equiv 706 \pmod{747}$$

and indeed we see that

$$127 \times 706 \equiv 120 \times 747 + 22 \equiv 22 \pmod{747}$$

THE CHINESE REMAINDER THEOREM

The following result is very useful in those situations where we need to reduce congruence equations with composit modulus to equations with prime modulus.

Theorem 2 . *If $m_1, m_2, \ldots, m_k$ are relatively prime then the system of congruences*

$$x \equiv a_i \pmod{m_i} \quad i = 1, 2, \ldots, k \tag{20}$$

has a unique solution modulo

$$m = m_1\, m_2\, \cdots m_k$$

Proof. Set

$$M_i = m/m_i$$

Now clearly m_i and M_i have no common factor. Thus using the Euclidean algorithm we can construct x_i, p_i so that

$$1 = x_i\, M_i + p_i\, m_i$$

Note then that (20) gives

$$\begin{aligned} x = 1\, x &= (x_i\, M_i + p_i\, m_i)\, a_i \\ &\equiv x_i\, M_i\, a_i \pmod{m_i} \end{aligned}$$

Note that for any i we have as well

$$x_i\, M_i\, a_i \equiv (x_i\, M_i + p_i\, m_i)\, a_i \pmod{m_i}$$

Thus we see that the expression

$$x \equiv \sum_{i=1}^{k} x_i M_i a_i \pmod{m} \tag{21}$$

should be the common solution of the equations in (20). And this is easily verified. Uniqueness of the solution follows immediately from the fact that the multiple condition

$$x \equiv 0 \pmod{m_i} \quad i = 1, 2, \ldots, k$$

when the m_i are relatively prime, is equivalent to the single condition

$$x \equiv 0 \pmod{m}.$$

Exercises:

1. Find the greatest common divisors of
   (a) 3108 and 3948
   (b) 1147 and 2491
2. Use the Euclidean Algorithm to find h and k in
   $$(a, b) = ha + kb$$
   for both pairs a, b given in problem 1.
3. Use the Euclidean Algorithm to solve the equations
   (a) $19x \equiv 25 \pmod{221}$
   (b) $1147x \equiv 455 \pmod{2491}$
4. Find a common solution (mod 5423) to the equations
   $$x \equiv 5 \ (\text{mod } 11)$$
   $$x \equiv 12 \ (\text{mod } 17)$$
   $$x \equiv 23 \ (\text{mod } 29)$$