A system of two congruences

The following lemma follows easily from Proposition 2.2.3.

Lemma 1. *Let a and b be integers and let n_1 and n_2 be relatively prime positive integers. Then*

$$a \equiv b \pmod{n_1} \qquad \textit{and} \qquad a \equiv b \pmod{n_2}, \tag{1}$$

if and only if

$$a \equiv b \pmod{n_1 n_2}. \tag{2}$$

Proof. The implication (2) $\Rightarrow$ (1) is clear. Now assume (1). Then $n_1|(b-a)$ and $n_2|(b-a)$. Since n_1 and n_2 be relatively prime, by Proposition 2.2.3 we have $(n_1n_2)|(b-a)$. Hence (2) holds. The lemma is proved. $\square$

Let a_1 and a_2 be integers and let n_1 and n_2 be relatively prime positive integers. Given two congruences

$$x \equiv a_1 \pmod{n_1} \qquad \text{and} \qquad x \equiv a_2 \pmod{n_2}, \tag{3}$$

we want to find an integer c and a positive integer m such that x satisfies (3) if and only if x satisfies

$$x \equiv c \pmod{m}. \tag{4}$$

Since n_1 and n_2 are relatively prime integers, by Proposition 3.3.2 there exist integers b_1 and b_2 such that

$$b_1 n_2 \equiv 1 \pmod{n_1} \qquad \text{and} \qquad b_2 n_1 \equiv 1 \pmod{n_2}. \tag{5}$$

Now assume (3) and proceed to construct c and m. From (3) and (5) we have

$$x \equiv a_1 \pmod{n_1} \qquad \text{and} \qquad b_1 n_2 \equiv 1 \pmod{n_1},$$

and consequently

$$x \equiv a_1 b_1 n_2 \pmod{n_1}.$$

Since clearly

$$0 \equiv a_2 b_2 n_1 \pmod{n_1},$$

we conclude that

$$x \equiv a_1 b_1 n_2 + a_2 b_2 n_1 \pmod{n_1}. \tag{6}$$

Similarly from (3) and (5) we have

$$x \equiv a_2 \pmod{n_2} \qquad \text{and} \qquad b_2 n_1 \equiv 1 \pmod{n_2},$$

and consequently

$$x \equiv a_2 b_2 n_1 \pmod{n_2}.$$

Since also

$$0 \equiv a_1 b_1 n_2 \pmod{n_2},$$

we conclude that

$$x \equiv a_1 b_1 n_2 + a_2 b_2 n_1 \pmod{n_2}. \tag{7}$$

Since n_1 and n_2 are relatively prime integers, Lemma 1 and congruences (6) and (7) yield

$$x \equiv a_1 b_1 n_2 + a_2 b_2 n_1 \pmod{n_1 n_2}. \tag{8}$$

Now set $c = a_1 b_1 n_2 + a_2 b_2 n_1$ and $m = n_1 n_2$. With these c and m we proved that (3) implies (4).

Next we prove that (8) implies (3). Assume (8). Then, by Lemma 1,

$$x \equiv a_1 b_1 n_2 + a_2 b_2 n_1 n_1 \pmod{n_1} \quad \text{and} \quad x \equiv a_1 b_1 n_2 + a_2 b_2 n_1 n_1 \pmod{n_2},$$

Since clearly

$$0 \equiv a_2 b_2 n_1 \pmod{n_1} \qquad \text{and} \qquad 0 \equiv a_1 b_1 n_2 \pmod{n_2},$$

we get

$$x \equiv a_1 b_1 n_2 \pmod{n_1} \qquad \text{and} \qquad x \equiv a_2 b_2 n_1 \pmod{n_2}.$$

Now congruences in (5) imply

$$a_1 \equiv a_1 b_1 n_2 \pmod{n_1} \qquad \text{and} \qquad a_2 \equiv a_2 b_2 n_1 \pmod{n_2}.$$

Therefore,

$$x \equiv a_1 \pmod{n_1} \qquad \text{and} \qquad x \equiv a_2 \pmod{n_2},$$

and (3) is proved.

A system of several congruences

Next we will replace two congruences with r congruences. Here r is a positive integer with $r > 1$. Before proceeding with this proof we prove two lemmas.

Lemma 2. *Let $n_1, n_2, \ldots, n_r$ and s be positive integers. If $\gcd(n_j, s) = 1$ for all $j = 1, 2, \ldots, r$, then*

$$\gcd(n_1 n_2 \cdots n_r, s) = 1.$$

Proof. The contrapositive is easier to prove. Assume that $\gcd(n_1 n_2 \cdots n_r, s) > 1$. Then there exists a prime p such that

$$p \mid \gcd(n_1 n_2 \cdots n_r, s).$$

Since p divides a common divisor of $n_1 n_2 \cdots n_r$ and s, we conclude that

$$p \mid (n_1 n_2 \cdots n_r) \qquad \text{and} \qquad p \mid s.$$

By Proposition 2.2.8 there exists $k \in \{1, 2, \ldots, r\}$ such that $p \mid n_k$. Hence, $p \mid \gcd(n_k, s)$ and consequently $\gcd(n_k, s) > 1$. Thus, there exists $k \in \{1, 2, \ldots, r\}$ such that $\gcd(n_k, s) > 1$. □

Lemma 3. *Let a and b be integers and let $n_1, n_2, \ldots, n_r$ be positive integers each two of which are relatively prime. Then*

$$a \equiv b \pmod{n_1}, \quad a \equiv b \pmod{n_2}, \quad \ldots, \quad a \equiv b \pmod{n_r},$$

if and only if

$$a \equiv b \pmod{n_1 n_2 \cdots n_r}.$$

Let $a_1, a_2, \ldots, a_r$ be integers and let $n_1, n_2, \ldots, n_r$ be positive integers each two of which are relatively prime. That is $\gcd(n_j, n_k) = 1$ whenever $j \neq k$ and $j, k \in \{1, 2, \ldots, r\}$. Given r congruences

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_r \pmod{n_r}, \tag{9}$$

we want to find an integer c and a positive integer m such that x satisfies (9) if and only if x satisfies

$$x \equiv c \pmod{m}. \tag{10}$$

We introduce the following notation

$$m = n_1 n_2 \cdots n_r, \qquad m_j = \frac{m}{n_j}, \quad j = 1, 2, \ldots, r.$$

That is, m is the product of all integers $n_1, n_2, \ldots, n_r$ and m_j is the product of $r - 1$ integers; namely the integer n_j is skipped in this product. Let j be an arbitrary integer in $\{1, 2, \ldots, r\}$. Then, by definition $m = m_j n_j$. Since $\gcd(n_j, n_k) = 1$ for all $k \in \{1, 2, \ldots, r\}$ such that $k \neq j$, by Lemma 2 we have that

$$\gcd(m_j, n_j) = 1.$$

By the definition of m_j we have

$$n_k \,|\, m_j \quad \text{for all} \quad k \in \{1, 2, \ldots, r\} \quad \text{such that} \quad k \neq j.$$

We proceed similarly as in the case of two congruences. Since n_j and m_j are relatively prime integers, by Proposition 3.3.2 there exist integers b_j such that

$$b_j m_j \equiv 1 \pmod{n_j} \tag{11}$$

Now assume (9) and proceed to construct c and m. From (9) and (11) we have

$$x \equiv a_j \pmod{n_j} \qquad \text{and} \qquad b_j m_j \equiv 1 \pmod{n_j},$$

and consequently

$$x \equiv a_j b_j m_j \pmod{n_j}$$

For $k \in \{1, 2, \ldots, r\}$ such that $k \neq j$ we have $n_j \,|\, m_k$. Therefore

$$0 \equiv a_k b_k m_k \pmod{n_j}, \qquad k \in \{1, 2, \ldots, r\}, \quad k \neq j.$$

The last displayed relations contain r congruences. Adding these r congruences we get

$$x \equiv a_1 b_1 m_1 + a_2 b_2 m_2 + \cdots + a_r b_r m_r \pmod{n_j}.$$

Now set $c = a_1 b_1 m_1 + a_2 b_2 m_2 + \cdots + a_r b_r m_r$. Thus we proved

$$x \equiv c \pmod{n_j}.$$

Since $j \in \{1, 2, \ldots, r\}$ was arbitrary we have

$$x \equiv c \pmod{n_j} \qquad \text{for all} \qquad j \in \{1, 2, \ldots, r\}.$$

Now Lemma 3 implies

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

This proves that (9) implies (10).

A proof that (10) implies (9) is left as an exercise.