A DUALITY THEOREM FOR LINEAR CONGRUENCES

H.P. WILLIAMS
Department of Business Studies, University of Edinburgh, U.K.

Received 2 June 1981
Revised 20 August 1982

An analogous duality theorem to that for Linear Programming is presented for systems of linear congruences. It is pointed out that such a system of linear congruences is a relaxation of an Integer Programming model (for which the duality theorem does not hold). Algorithms are presented for both the resulting primal and dual problems. These algorithms serve to give a constructive proof of the duality theorem.

1. Introduction

Given a set of linear congruences

$$\sum_{j=1}^{n} a_{ij}x_j \equiv r_i \pmod{b_i}, \quad i=1,2,\ldots,m, \tag{1.1}$$

we seek information about the possible values for another linear expression

$$\sum_{j=1}^{n} c_j x_j \tag{1.2}$$

where a_{ij}, b_i, c_j, r_i are integers and x_j integer variables (allowed to be positive, zero or negative).

Assuming the congruences (1.1) have a solution they will have an infinite set of solutions. Each solution will give rise to a value for (1.2). Our interest is in the class of values for (1.2). These values will be characterised by a *modulus* b_0 and a *residue* r_0, i.e.

$$\sum_{j=1}^{n} c_j x_j \equiv r_0 \pmod{b_0}. \tag{1.3}$$

An algorithm for finding the modulus and residue will be described in Section 4.

The main interest, however, lies in showing that the modulus and residue can also be obtained by solving a *dual* problem. This dual problem involves finding integer multipliers to apply to the congruences in (1.1) in order to deduce (1.3).

Clearly the motivation for this result lies in trying to find an analogy to the Duality Theorem for Linear Programming (LP). This problem we consider here is a relaxation of an Integer Programming (IP) problem. Unlike IP itself this relaxa-

0166-218X/84/$3.00 © 1984, Elsevier Science Publishers B.V. (North-Holland)

tion has a beautifully simple dual. In order to provide further motivation we describe the LP duality result in a similar form. Although well known this result is restated in an intuitive form in order to clarify the analogy.

2. The linear programming analogy

Given a set of linear constraints

$$\sum_{j=1}^{n} a_{ij}x_j \leq b_i, \quad i=1,2,\ldots,m, \tag{2.1}$$

we seek information about the possible values for another linear expression (the objective function)

$$\sum_{j=1}^{n} c_j x_j \tag{2.2}$$

where a_{ij}, b_i, c_j, are real numbers and x_j non-negative continuous variables.

Assuming the constraints have a feasible solution each solution to (2.1) will give rise to a value for (2.2). These values for (2.2) will all be less-than-or-equal to some value (possibly ∞), i.e.

$$\sum_{j=1}^{n} c_j x_j \leq z. \tag{2.3}$$

The general *primal* LP problem is to find (i) the value of z (maximum of the objective function) and (ii) values for x_j which make (2.2) attain this maximum (so long as $z \neq \infty$), i.e.

(P$_1$) maximise $z_{\text{P}} = \sum_{j=1}^{n} c_j x_j$

such that $\sum_{j=1}^{n} a_{ij}x_j \leq b_i, \quad i=1,2,\ldots,m$

where x_j are non-negative continuous variables.

The duality theorem of LP gives rise to an alternative way of finding z. It shows that so long as z is not ∞ a set of suitable (non-negative) multipliers y_i can be found to apply to the constraints (2.1) so as to deduce (2.3). The non-negative multipliers y_i come from this solution to the *dual* LP problem:

(D$_1$) minimise $z_{\text{D}} = \sum_{i=1}^{n} b_i y_i$

such that $\sum_{i=1}^{m} a_{ij} y_i \geq c_j, \quad j=1,2,\ldots,n.$

It is straightforward to show that $z_{\text{P}} \leq z_{\text{D}}$ (the Weak Duality Theorem). Of greater significance is the result that $z_{\text{P}} = z_{\text{D}}$ (the Strong Duality Theorem).

3. The duality theorem for linear congruences

We define the following homogeneous *primal* problem
Find the maximum integer M_P such that:

$$(P_2) \qquad \forall x_j\left[\sum_{i=1}^{n} a_{ij}x_j \equiv 0 \pmod{b_i},\ i=1,2,\dots,m \rightarrow \sum_{j=1}^{n} c_jx_j \equiv 0 \pmod{M_P}\right]$$

where a_{ij}, b_i, c_j are given integers. x_j are (positive or negative) integer variables.

The associated *dual* problem is defined as: Find the maximum integer M_D such that:

$$(D_2) \qquad \exists y_i\left[\sum_{i=1}^{m} a_{ij}y_i \equiv c_j \pmod{M_D},\ j=1,2,\dots,n,\ b_iy_i \equiv 0 \pmod{M_D}\right].$$

y_i are (positive or negative) integer variables.

Notice that (P_2), unlike (1.1) and (1.2) deals with homogeneous congruences. The extension to deal with non-homogeneous congruences is discussed in Section 4.

Theorem (a) *Weak Duality. In* (P_2) *and* (D_2) M_D/M_P ('/' stands for 'divides').
(b) *Strong Duality.* $M_D = M_P$.

As in LP weak duality is easy to prove as is done below. Strong duality is a much stronger result and requires a more difficult proof. This is given in Section 4.

Proof of (a) *Weak Duality*

If

$$\sum_{j=1}^{n} a_{ij}x_j \equiv 0 \pmod{b_i}, \quad i=1,2,\dots,m,\ x_j \text{ integer}$$

$$\sum_{i=1}^{m} y_i \sum_{j=1}^{n} a_{ij}x_j \equiv 0 \pmod{q}, \quad y_i \text{ integer where } q = \gcd_i(b_iy_i)$$

('gcd$_i$' stands for 'greatest common divisor'), i.e.

$$\sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ij}y_i \equiv 0 \pmod{\gcd_i(b_iy_i)}.$$

Choose

$$M = \gcd\left(\sum_{i=1}^{m} a_{ij}y_i - c_j,\ j=1,2,\dots,n,\ b_iy_i,\ i=1,2,\dots,m\right).$$

Then $\sum_{j=1}^{n} c_jx_j \equiv 0 \pmod{M}$. But by ($P_2$),

$$\sum_{j=1}^{n} c_jx_j \equiv 0 \pmod{M_P}.$$

Hence M/M_P. In particular M_D/M_P. □

4. An algorithm for the primal problem

We will solve a more general form of the model (P_2) in which there are non-homogeneous congruences.

Find the maximum integer M_P such that

$$(P_2) \qquad \exists r_0 \forall x_j \left[\sum_{j=1}^{n} a_{ij} x_j \equiv r_i \ (\text{mod } b_i),\ i=1,2,\ldots,m \rightarrow \sum_{j=1}^{n} c_j x_j \equiv r_0 \ (\text{mod } M_P) \right].$$

The algorithm described would not be efficient computationally but allows a constructive proof of the duality theorem. It bears an analogy to Fourier-Motzkin elimination for linear inequalities as described by, for example Dantzig [1].

We let $\sum_{j=1}^{n} c_j x_j = z$. The congruences and this equation can be expressed in the form

$$\sum_{j=1}^{n} c_j x_j - z = 0, \tag{4.1}$$

$$\sum_{j=1}^{n} a_{ij} x_j \equiv r_i \ (\text{mod } b_i), \quad i=1,2,\ldots,m, \tag{4.2}$$

$$x_j \equiv 0 \ (\text{mod } 1), \quad j=1,2,\ldots,n. \tag{4.3}$$

It is helpful to include the congruences (4.3) in describing the algorithm.

The algorithm proceeds by successively eliminating each variable between every pair of congruences and every congruence and equation in (4.1), (4.2) and (4.3). The justification for the eliminations follows from results in elementary number theory. These are not given here but can be found in, for example Mathews [3].

Result 1. *Eliminating a variable x_k between two congruences. If*

$$\sum_{j=1}^{n} a_{1j} x_j \equiv r_1 \ (\text{mod } b_1) \tag{4.4}$$

and

$$\sum_{j=1}^{n} a_{2j} x_j \equiv r_2 \ (\text{mod } b_2), \tag{4.5}$$

then if $a_{1k} \neq 0$, $a_{2k} \neq 0$, let L be the lcm (least common multiple) of a_{1k} and a_{2k}.

Multiplying (4.4) by L/a_{1k} and (4.5) by L/a_{2k} and subtracting yields

$$\sum_{\substack{j=1 \\ j \neq k}}^{n} a'_j x_j \equiv r' \ (\text{mod } b') \tag{4.6}$$

where

$$a'_j = \frac{L}{a_{1k}} a_{1j} - \frac{L}{a_{2k}} a_{2j}, \qquad r' = \frac{L}{a_{1k}} r_1 - \frac{L}{a_{2k}} r_2,$$

$$b' = \gcd\left(\frac{L}{a_{1k}} b_1, \frac{L}{a_{2k}} b_2 \right).$$

Result 2. *Eliminating a variable x_k between a congruence and an equation.* If

$$\sum_{j=1}^{n} a_{1j}x_j = r_1 \tag{4.7}$$

and

$$\sum_{j=1}^{n} a_{2j}x_j \equiv r_2 \pmod{b_2}, \tag{4.8}$$

then if $a_{1k} \neq 0$, $a_{2k} \neq 0$, let L be the lcm of a_{1k} and a_{2k}.

Multiplying (4.7) by L/a_{1k} and (4.8) by L/a_{2k} and subtracting yields

$$\sum_{\substack{j=1\\ j\neq k}}^{n} a'_j x_j \equiv r' \pmod{b'}$$

where

$$a'_j = \frac{L}{a_{1k}} a_{1j} - \frac{L}{a_{2k}} a_{2j},$$

$$r' = \frac{L}{a_{1k}} r_1 - \frac{L}{a_{2k}} a_{2j},$$

$$b' = \frac{L}{a_{2k}} b_2.$$

The congruences (4.3) ensure that each variable x_j always occurs, with a non-negative coefficient, in at least one congruence. Should it occur in no other congruence it may be ignored.

Once all the variables x_j have been eliminated from the system (4.1), (4.2) and (4.3) we will be left with a series of congruences involving only the variable z. By the Generalised Chinese Remainder Theorem (see e.g. Dickson [2]) these congruences are either (i) incompatible or (ii) can be aggregated into a single congruence.

In case (i) the original congruences (4.2) have no feasible solution. In case (ii) we will produce a single congruence of the form

$$z \equiv r_0 \pmod{M} \tag{4.9}$$

giving the required maximum value of M.

The whole procedure is illustrated by a numerical example. Each elimination of a variable involves taking a linear combination of congruences (and possibly an equation). It is helpful to keep track of these combinations of the original congruences and equation giving rise to each resultant congruence.

A numerical example of the primal algorithm

Find the maximum integer M such that

$$\exists r_0 \forall x_1 x_2 \left[\begin{matrix} 5x_1 + x_2 \equiv 1 \pmod{6} \\ 13x_1 + 7x_2 \equiv 7 \pmod{20} \end{matrix} \rightarrow 2x_1 + 14x_2 \equiv r_0 \pmod{M} \right]$$

We specify each congruence below:

$$\begin{array}{rll}
2x_1+14x_2- & z=0, & \mathrm{R0}\\
5x_1+x_2 & \equiv 1 \pmod{6}, & \mathrm{R1}\\
13x_1+7x_2 & \equiv 7 \pmod{20}, & \mathrm{R2}\\
x_1 & \equiv 0 \pmod{1}, & \mathrm{S1}\\
x_2 & \equiv 0 \pmod{1}. & \mathrm{S2}
\end{array}$$

Eliminating x_1 gives

$$\begin{array}{rll}
-68x_2+5z & \equiv 2 \pmod{12}, & 2\mathrm{R1}-5\mathrm{R0}\\
-168x_2+13z & \equiv 14 \pmod{40}, & 2\mathrm{R2}-13\mathrm{R0}\\
-14x_2+z & \equiv 0 \pmod{2}, & 2\mathrm{S1}-\mathrm{R0}\\
22x_2 & \equiv 22 \pmod{2}, & 5\mathrm{R2}-13\mathrm{R1}\\
x_2 & \equiv 1 \pmod{1}, & \mathrm{R1}-5\mathrm{S1}\\
7x_2 & \equiv 7 \pmod{1}, & \mathrm{R2}-13\mathrm{S1}\\
x_2 & \equiv 0 \pmod{1}. & \mathrm{S2}
\end{array}$$

Simplifying and removing redundant congruences gives

$$\begin{array}{rll}
4x_2+5z & \equiv 2 \pmod{12}, & 2\mathrm{R1}-5\mathrm{R0}\\
32x_2+13z & \equiv 14 \pmod{40}, & 2\mathrm{R2}-13\mathrm{R0}\\
z & \equiv 0 \pmod{2}, & 2\mathrm{S1}-\mathrm{R0}\\
x_2 & \equiv 0 \pmod{1}. & \mathrm{S2}
\end{array}$$

Eliminating x_2 gives

$$\begin{array}{rll}
27z & \equiv 2 \pmod{8}, & 8(2\mathrm{R1}-5\mathrm{R0})-(2\mathrm{R2}-13\mathrm{R0})\\
5z & \equiv 2 \pmod{4}, & (2\mathrm{R1}-5\mathrm{R0})-4\mathrm{S2}\\
13z & \equiv 14 \pmod{8}, & (2\mathrm{R2}-13\mathrm{R0})-32\mathrm{S2}\\
z & \equiv 0 \pmod{2}. & 2\mathrm{S1}-\mathrm{R0}
\end{array}$$

Simplifying

$$\begin{array}{rll}
3z & \equiv 2 \pmod{8}, & -2\mathrm{R2}+16\mathrm{R1}-14\mathrm{R0}\\
z & \equiv 2 \pmod{4}, & 2\mathrm{R1}-5\mathrm{R0}-4\mathrm{S2}\\
5z & \equiv 6 \pmod{8}, & 2\mathrm{R2}+13\mathrm{R0}-32\mathrm{S2}\\
z & \equiv 0 \pmod{2}. & 2\mathrm{S1}-\mathrm{R0}
\end{array}$$

In this case the aggregation of these final congruences is trivial since the first and third are equivalent and imply the second and fourth. Multiplying the first congruence by 3 produces

$$z\equiv 6 \pmod{8}. \qquad -6\mathrm{R2}+48\mathrm{R1}-42\mathrm{R0}$$

This shows that the required maximum value of M (this modulus) is 8 and the corresponding residue r_0 is 2.

The multiples of the original congruence giving rise to this final congruence are (modulus 8)

$$2\text{R}2-2\text{R}0,$$

i.e. by taking 2R2 we can deduce the form of the expression $2x_1+14x_2$.

$$2(13x_1+7x_2\equiv 7 \pmod{20})$$

gives

$$26x_1+14x_2\equiv 14 \pmod{40}.$$

Dividing by 8 gives

$$2x_1+14x_2\equiv 6 \pmod 8.$$

Alternatively multiplying the third of the four congruences above by 5 produces the same multipliers (modulus 8).

Notice that the residues r_i, $i=1,2,\dots,m$ in (P2′) play no part in the elimination procedure. Their only roles are (i) to determine whether there is or is not a feasible solution and (ii) to determine the final residue $r_0\equiv z \pmod M$. Assuming therefore that the r_i are such as to allow a feasible solution the multipliers of the congruences and equation will be the same whatever values of r_i are taken. In particular those arising from the homogeneous model (P2) (which must always be feasible) will be applicable also in the non-homogeneous case.

5. Proof of (b) strong duality

Suppose we solve (P_2) using the algorithm of Section 4 and Setting $z=\sum_{j=1}^{n} c_jx_j$. (P_2) has a feasible solution (in particular $x_j=0$, $j=1,2,\dots,n$). Therefore after eliminating all x_j we will be able to aggregate the resultant congruences in z into a single congruence. This congruence will be expressible in the form

$$z\equiv 0 \pmod{M_\text{P}} \tag{5.1}$$

This congruence will result from subtracting the equation from some integer linear combination of the original congruences. Let the multipliers in this combination be y_i (of the congruences in (4.2) with $r_i=0$) and u_j (of the congruences in (4.3)). Therefore

$$\sum_{i=1}^{m} a_{ij}y_i+u_j\equiv c_j \pmod{M_\text{P}}, \quad j=1,2,\dots,n,$$

$$\gcd_{\substack{i=1,2,\dots,m\\ j=1,2,\dots,n}} (b_iy_i,u_j)=M_\text{P}.$$

Hence M_P/u_j, $j=1,2,\dots,n$. Therefore

$$\sum_{i=1}^{m} a_{ij}y_i \equiv c_j \ (\mathrm{mod}\, M_P), \quad j=1,2,\dots,n, \tag{5.2}$$

$$b_i y_i \equiv 0 \ (\mathrm{mod}\, M_P), \quad i=1,2,\dots,m. \tag{5.3}$$

The dual model (D_2) involves finding the maximum modulus M_D such that (5.2) and (5.3) hold. Therefore $M_P \le M_D$. But by the weak duality theorem M_D/M_P. Therefore $M_D = M_P$. □

6. A characterisation of the greatest common divisor

The well known result that the gcd of a set of integers is expressible as a linear combination of these integers (usually proved by the Euclidean Algorithm) is a result of the duality theorem given in Section 3. This is stated in the form of the following corollary.

Corollary (to the Duality Theorem). *$\exists x_j$ $\sum_{j=1}^{n} c_j x_j = M$ where $M = \mathrm{gcd}_j(c_j)$.*

Proof. From the duality theorem

$$\forall x_j \quad \sum_{j=1}^{n} c_j x_j \equiv 0 \ (\mathrm{mod}\, M_D)$$

where $M_D =$ maximum M such that

$$0 \equiv c_j \ (\mathrm{mod}\, M_D), \quad j=1,2,\dots,n,$$

i.e. $M_D = \mathrm{gcd}_j(c_j)$.

Since $M_D =$ maximum M such that

$$\forall x_j \quad \sum_{j=1}^{n} c_j x_j \equiv 0 \ (\mathrm{mod}\, M),$$

$$\exists x_j', x_j'' \text{ such that } \sum_{j=1}^{n} c_j x_j' - \sum_{j=1}^{n} c_j x_j'' = M_D,$$

i.e. $\sum_{j=1}^{n} c_j(x_j' - x_j'') = M_D$.

Taking $x_j = x_j' - x_j''$, $j=1,2,\dots,n$ proves the corollary. □

7. An algorithm for the dual problem

Although the multipliers for the congruences in the primal problem can be obtained through this primal algorithm they can also be obtained by solving the dual problem directly. An algorithm for this is described and then illustrated by the dual of the numerical example above.

We express problem (D_2) in the form: Find the maximum integer M such that $\exists y_i$

$$\sum_{i=1}^{m} a_{ij} y_i \equiv c_j \pmod{M}, \quad j = 1, 2, \ldots, n, \tag{7.1}$$

$$\sum_{i=1}^{m} b_i y_i \equiv 0 \pmod{M}, \quad i = 1, 2, \ldots, m. \tag{7.2}$$

The algorithm proceeds by successively eliminating each variable between every pair of congruences using Result 1 given in Section 4. In this case, however, (4.4) and (4.5) have the same modulus M (which is a variable rather than a constant). Since L/a_{1k} and L/a_{2k} must be coprime the modulus derived in congruence (4.6) is also M.

When all variables have been eliminated from the system (7.1) and (7.2) we will be left with a series of congruences of the form:

$$0 \equiv d_i \pmod{M}, \quad i = 1, 2, \ldots, l \tag{7.3}$$

where the d_i are integer constants. This maximum value of M will clearly be $\gcd_i(d_i)$, $i = 1, 2, \ldots, l$.

In illustrating the whole procedure by the dual of the numerical example in Section 4, it is again helpful to keep track of the multiples of the original congruence giving rise to the congruences in 6.3.

A numerical example of the dual algorithm

Find the maximum integer M such

$$\exists y_1 y_2 \quad \begin{bmatrix} 5y_1 + 13y_2 \equiv 2 \pmod{M} \\ y_1 + 7y_2 \equiv 14 \pmod{M} \\ 6y_1 \qquad \equiv 0 \pmod{M} \\ 20y_2 \equiv 0 \pmod{M} \end{bmatrix}$$

Specifying and naming each congruence

$$\begin{array}{ll} 5y_1 + 13y_2 \equiv 2 \pmod{M}, & \text{T1} \\ y_1 + 7y_2 \equiv 14 \pmod{M}, & \text{T2} \\ 6y_1 \qquad \equiv 0 \pmod{M}, & \text{U1} \\ 20y_2 \equiv 0 \pmod{M}. & \text{U2} \end{array}$$

Eliminating y_1 gives:

$$\begin{array}{ll} 22y_2 \equiv 68 \pmod{M}, & 5\text{T2} - \text{T1} \\ 78y_2 \equiv 12 \pmod{M}, & 6\text{T1} - 5\text{U1} \\ 42y_2 \equiv 84 \pmod{M}, & 6\text{T2} - \text{U1} \\ 20y_2 \equiv 0 \pmod{M}. & \text{U2} \end{array}$$

Eliminating y_2 gives

$$\begin{aligned}
0 &\equiv 2520 \pmod{M}, && 39(5\mathrm{T}2-\mathrm{T}1)-11(6\mathrm{T}1-5\mathrm{U}1)\\
0 &\equiv 504 \pmod{M}, && 21(5\mathrm{T}2-\mathrm{T}1)-11(6\mathrm{T}2-\mathrm{U}1)\\
0 &\equiv 680 \pmod{M}, && 10(5\mathrm{T}2-\mathrm{T}1)-11\mathrm{U}2\\
0 &\equiv 1008 \pmod{M}, && 13(6\mathrm{T}2-\mathrm{U}1)-7(6\mathrm{T}1-5\mathrm{U}1)\\
0 &\equiv 120 \pmod{M}, && 10(\mathrm{T}2-\mathrm{SU}1)-39\mathrm{U}2\\
0 &\equiv 840 \pmod{M}. && 10\,(6\mathrm{T}2-\mathrm{U}1)-21\mathrm{U}2
\end{aligned}$$

The gcd of the 6 residues in the congruences above is 8 in accordance with the strong duality theorem. If M is set to 8 the congruences can be solved for y_1 and y_2. A convenient method is to work backwards deducing y_2 and then y_1. The general form of y_1 and y_2 can be given in terms of two integer parameters k_1 and k_2

$$y_1 = 4k_1 + 8k_2, \qquad y_2 = 2 + 4k_1.$$

Notice that the general dual problem (D_2) is of the form “Find the maximum M such that $\exists y_i$”. Therefore corresponding to the maximum M there exists one or more solutions y_i such as those above. The primal problem (P_2) is, however, of the form “Find the maximum M such that $\forall x_j$”. Hence the correspondence between the maximum value of M and *specific* values for x_j is not so direct. It is, however, possible to identify a specific set of values for x_j which can be regarded as the corresponding primal solution. An appropriate set of x_j, $j=1,2,\ldots,n$ is such that

$$\sum_{j=1}^{n} a_{ij}x_j \equiv 0 \pmod{b_i}, \quad i=1,2,\ldots,m,$$

$$\sum_{j=1}^{n} c_j x_j = M_{\mathrm{P}}.$$

This set of values can itself be regarded as a set of multipliers for the congruences of the dual problem. They therefore arise from creating a dual of the dual problem. This problem is defined and shown to be equivalent to the primal problem.

8. The dual of the dual

Suppose the congruences (7.1) and (7.2) hold for a particular set of y_i with $M=M_{\mathrm{D}}$. Choose a set of multipliers x_j, $j=1,2,\ldots,n$ for the congruences (7.1) and w_i, $i=1,2,\ldots,m$ for the congruences (7.2) such that

$$\sum_{j=1}^{n} a_{ij}x_j - b_i w_i = 0, \quad i=1,2,\ldots,m. \tag{8.1}$$

Adding the congruences (7.1) and (7.2) in these multiples shows

$$\sum_{j=1}^{n} c_j x_j \equiv 0 \pmod{M_{\mathrm{D}}}. \tag{8.2}$$

If (8.1) is rewritten as

$$\sum_{j=1}^{n} a_{ij}x_j \equiv 0 \pmod{b_i}, \tag{8.3}$$

then we have shown that any set of x_j, $j=1,2,\dots,n$ which satisfy (8.3) also satisfy (8.2). The problem of finding the maximum modulus M is the primal problem.

A numerical example of the primal solution

Consider the final congruences obtained in solving the numerical example of the dual problem in Section 7. 8 is the gcd of the residues in these final congruences. We can by the well known result (already shown to be a corrollary of the duality theorem) find a linear combination of these numbers to total 8. In particular:

$$2520\times 0+504\times 27+680\times(-20)+1008\times 0+120\times 0+840\times 0=8$$

This enables us to derive the congruence $0\equiv 8 \pmod{M}$ as a linear combination of the original congruences in the dual problem. It is:

$$-367\mathrm{T1}+53\mathrm{T2}-29\mathrm{U1}+220\mathrm{U2}$$

The multipliers give the homogeneous primal solution $x_1=-367$, $x_2=53$. It can be verified that

$$5x_1+x_2\equiv 0 \pmod{6},$$

$$13x_2+7x_2\equiv 0 \pmod{20},$$

and that $2x_1+14x_2=8$.

References

[1] G.B. Dantzig, Linear Programming and Extensions (Princeton Univ. Press, Princeton, NJ, 1963).

[2] L.E. Dickson, History of the Theory of Numbers, Vol. II (Carnegie Institute, Washington, 1920).

[3] G.B. Mathews, Theory of Numbers, Part I (Deighton Bell, Cambridge, 1892).