LINEAR CONGRUENCES AND LINEAR DIOPHANTINE EQUATIONS

MATH 422, CSUSM. SPRING 2009. AITKEN

This document discusses methods and results related to solving linear congruences and linear Diophantine equations.

1. Linear Congruences: Simple Case

In what follows assume m is a positive integer. Here x is an unknown, and a, c and m are fixed. In this section we will consider the case where a and m are coprime (the "simple case").

Theorem 1. *If* $\gcd(a, m) = 1$ *then the equation*

$$ax \equiv c \mod m$$

has the unique solution $x \equiv a^{-1}c$ *modulo* m*.*

Proof. Existence: It is easy to see that $x = a^{-1}c$ does work: substitute and simplify. Recall that a^{-1} exists since $\gcd(a, m) = 1$.

Uniqueness: Suppose that x_1 is any solution. Then $ax_1 \equiv c$ modulo m. Multiply both sides by a^{-1} and simplify. Thus $x_1 \equiv a^{-1}c$ modulo m. This shows that $x_1 \equiv x_0 \mod m$. □

Exercise 1. Solve $7x \equiv 11 \mod 9$ by finding an inverse for 7.

Exercise 2. Solve $3x + 3 \equiv x + 5 \mod 11$.

Exercise 3. Use the Euclidean algorithm to find the inverse to 297 modulo 349. Use this to solve $297x \equiv 3$ modulo 349.

y

Remark. We only have uniqueness modulo m. There are actually an infinite number of solutions in $\mathbb{Z}$ given by the formula $x = a^{-1}c + km$ where $k \in \mathbb{Z}$.

Another method is to use the cancellation law. With this method you do not have to actually compute a^{-1}, you just need to know it exists. In this method you try to rewrite the right hand side c as a multiple of a.

Theorem 2. *If* $\gcd(a, m) = 1$ *then the equation*

$$ax \equiv ab \mod m$$

has the same solutions as

$$x \equiv b \mod m$$

Proof. This is a consequence of the following theorem where $d = a$. □

Date: March 2, 2009.

Theorem 3. *If* $\gcd(d, m) = 1$*, and if* d *divides* a *and* c*, then*

$$ax \equiv c \mod m$$

has the same solutions as

$$(a/d)x \equiv (c/d) \mod m.$$

Proof. Suppose that x_0 solves the first congruence. Multiply both sides by d^{-1} (which exists since it is prime to m):

$$d^{-1}ax \equiv d^{-1}c \mod m$$

Rewrite a as $d(a/d)$ and c as $c(c/d)$.

$$d^{-1}d(a/d)x \equiv d^{-1}d(c/d) \mod m.$$

Now simply. This shows that x_0 satisfies the second congruence.

Conversely, suppose that x_0 solves the second congruences. Multiple both sides of the congruence (with $x = x_0$) by d and simplify. This shows that x_0 satisfies the first congruence. □

Remark. Observe that the modulus does not change in this case.

Exercise 4. Solve $6x \equiv 18 \bmod 31$ without finding the inverse of 6. Solve $5x \equiv 4 \bmod 21$ without finding the inverse of 5.

2. Linear Congruences: Nonsimple Case

Now we consider the case where a is not relatively prime to m. Here we must reduce the modulus. First we consider a result that describes how to reduce the modulus.

Theorem 4. *Suppose* d *divides* a, c, m*. Then*

$$ax \equiv c \mod m$$

has the same solutions as

$$(a/d)x \equiv (c/d) \mod (m/d).$$

Proof. Suppose that x_0 solves the first congruence.

$$ax \equiv c \mod m.$$

Then $m \mid (ax_0 - c)$. So $ax_0 - c = ml$ for some $l \in \mathbb{Z}$. Dividing by d gives us that $(a/d)x_0 - (c/d) = (m/d)l$. In other words, m/d divides $(a/d)x_0 - (c/d)$. Thus x_0 solves the second congruence.

Conversely, if x_0 solves the second congruence, then m/d divides $(a/d)x_0 - (c/d)$. So $(a/d)x_0 - (c/d) = (m/d)l$ for some $l \in \mathbb{Z}$. Multiply by d. So $ax_0 - c = ml$. Thus $m \mid (ax_0 - c)$. Hence x_0 solves the first congruence. □

Just because the two congruences above have the same solutions, does not mean that they have the same *number* of solutions relative to their respective moduli. This is described in the following:

Theorem 5. *Suppose d divides a, c, m. Then every solution of*

$$(a/d)x \equiv (c/d) \mod (m/d)$$

corresponds to d distinct solutions (modulo m) of

$$ax \equiv c \mod m.$$

In particular, the second congruence has d times the number of solutions as the first congruence.

Proof. Let x_0 be a solution to the first equation. We can assume that x_0 is chosen so that $0 \leq x_0 < m/d$. This is a solution modulo m/d and really corresponds to an infinite number of solutions $x = x_0 + k(m/d)$ where $k \in \mathbb{Z}$. Observe that $0 \leq x_0 + k(m/d) < m$ if and only if k is in the range $0, 1, \ldots, d-1$. Thus $x = x_0 + k(m/d)$ describes d distinct solutions. □

Exercise 5. Use the above to find all six solutions to $12x \equiv 24 \bmod 30$.

Now we can prove the main theorem:

Theorem 6. *Consider the congruence*

$$ax \equiv c \mod m$$

and let $g = \gcd(a, m)$. If $g \nmid c$ then this congruence has no solutions. If $g \mid c$ then it has exactly g solutions modulo m.

Remark. Observe that when $g = 1$ we recover the uniqueness result of the previous section.

Proof. First consider the case where $g \nmid c$, and suppose a solution $x = x_0$ exists. Then m divides $ax_0 - c$. Thus $ax_0 - c = ml$ for some $l \in \mathbb{Z}$. This means $c = ax_0 - ml$. Since g divides the right hand side, it must divide c, a contradiction.

Now suppose $g \mid c$. By Theorem 4 we need to solve

$$(a/g)x \equiv (c/g) \mod (m/g)$$

By the following lemma, a/g and m/g are relatively prime. Thus there is exactly one solution modulo m/g. By Theorem 5 there are $g \cdot 1$ solutions to the original congruence modulo m. □

Exercise 6. Use Bezout's identity to prove the following:

Lemma 7. *Let $g = \gcd(a, b)$ where $b \neq 0$. Then a/g and b/g are relatively prime.*

Exercise 7. How many solutions does $34x + 1 \equiv 18 \bmod 85$ have? How many solutions does $34x + 1 \equiv 20 \bmod 170$ have?

3. Linear Diophantine Equations: two variables

Thus far we have been considering congruences (using $\equiv$). Now we will consider true equations (using $=$) where we look only for integer solutions. Such equations are called *Diophantine equations* in honor of the Greek mathematician Diophantus. Diophantine equations are much harder than equations where we allow real solutions. Fortunately, the linear case is not too bad.

Since one variable linear equations are very easy, we start with two variables:

$$ax + by = c$$

where we assume $a, b, c \in \mathbb{Z}$ with a and b nonzero.

To solve this, first solve the congruence $ax \equiv c \bmod |b|$. If there are any solutions, there will be an infinite number of them given by the formula $x_0 + kb/g$ where $g = \gcd(a, b)$. Now use the equation to solve for y. This method is justified by the following theorem and corollary.

Theorem 8. *Let $a, b, c \in \mathbb{Z}$ with a and b nonzero. If (x_0, y_0) is a solution to*

$$ax + by = c$$

then x_0 is a solution to the associated congruence

$$ax \equiv c \bmod m$$

where $m = |b|$.

Conversely, if x_0 is a solution to the above congruence, then there is a y_0 such that (x_0, y_0) is a solution to the above Diophantine equation.

Proof. For the first claim, observe that b divides $(ax_0 - c)$. Thus m divides $(ax_0 - c)$.

For the second claim. Since x_0 solve the congruence, $m \mid (ax_0 - c)$. Thus $ax_0 - c$ is a multiple of b. Hence $ax_0 - c = y_0 b$ for some $y_0 \in \mathbb{Z}$. Thus (x_0, y_0) solves the Diophantine equation. □

Corollary 9. *Let $a, b, c \in \mathbb{Z}$ with a and b nonzero. Let $g = \gcd(a, b)$. Then*

$$ax + by = c$$

has integer solutions if and only if $g \mid c$. If it has a solution (x_0, y_0) then the general solution is of the form

$$x = x_0 + (a/g)k, \qquad y = y_0 - (b/g)k$$

One consequence of the above corollary is that if you find one solution, one can find the general solution.

Proof of corollary. By the above theorem, the equation has a solution if and only if the congruence $ax \equiv c \bmod |b|$ has a solution. By Theorem 6 this occurs if and only if $g \mid c$.

Now suppose that (x_0, y_0) is a solution (so $g \mid c$). The possible values of x are given by the congruence $ax \equiv c \bmod |b|$ which can be rewritten as the congruence $(a/g)x \equiv (c/g) \bmod |b|/g$. This has a unique solution x_0 modulo $|b|/g$. So the general solution is of the form $x = x_0 + k|b|/g$ where $k \in \mathbb{Z}$. We can remove the absolute value sign, and obtain the same set of possible x.

For any $x = x_0 + kb/g$, the corresponding y is given by solving

$$a(x_0 + kb/g) + by = c.$$

This yields

$$y = (c - ax_0)/b - k(a/g) = y_0 - k(a/g).$$

□

Exercise 8. Find the general solution of equation $6x + 8y = 100$.

Often we want only positive solutions to $ax + by = c$. In this case, take the general solution

$$x = x_0 + (a/g)k, \qquad y = y_0 - (b/g)k$$

and set $x \geq 0$ and $y \geq 0$. Now solve for k. This will give the range of possible k. Now for each integer value of k, you get a positive solution.

Exercise 9. Find the solutions of equation $6x + 8y = 100$ such that x and y are natural numbers.

3.1. **Another method.** The Euclidean algorithm provides another method for finding a solution to the equation $ax+by = c$. Technically the Euclidean algorithm gives a solution to $ax + by = g$ where $g = \gcd(a, b)$ (by finding a linear combination). However, once a solution is found giving g a linear combination, a solution yielding c as a linear combination is simply obtained by multiplying the equation by c/g. Recall that g must divide c for solutions to exist, so c/g will be an integer in any situation where solutions exist. Once one solution is found, the general solution is given by the formula of Corollary 9.

Exercise 10. Solve $297x + 349y = 3$ using the Euclidean algorithm. Then find the general solution.

4. Linear Diophantine Equations: Three Variables

Now consider the Diophantine equation

$$ax + by + cz = d$$

where $a, b, c, d \in \mathbb{Z}$ with a, b, c nonzero.

If there is a solution, then any common divisor of a, b, c will also divide d. Thus the greatest common divisor divides d. We will see that this is also a sufficient condition: the equation has a solution if and only if the greatest common divisor of a, b, c divides d.

From now on suppose that the greatest common divisor of a, b, c divides d. First we solve $ax + by = g$ where g is the greatest common divisor of a and b. Suppose (x_0, y_0) is such a solution. Next solve $gw + cz = d$. This has a solution since the greatest common divisor of g and c divides a, b, c, and by assumption must divide d as well. Let (w_0, Z_0) be such a solution. Observe that

$$d = gw_0 + cz_0 = (ax_0 + by_0)w_0 + cz_0 = a(x_0w_0) + b(y_0w_0) + cz_0$$

Thus we get a solution to the original equation.

This discussion establishes the following

Theorem 10. *Let $a, b, c, d \in \mathbb{Z}$ with a, b, c nonzero. The Diophantine equation*

$$ax + by + cz = d$$

has a solution if and only if d is a multiple of the greatest common divisor of a, b, c.

The above method and theorem extends to four or more variables.

Exercise 11. Find a solution to $6x + 15y + 10z = 2$.

5. Additional Problems

Exercise 12. Find the smallest postive rational number that can be written in the form $x/30 + y/36$ where x, y are integers.

Exercise 13. Suppose you have a piece of paper with 31 parallel horizontal lines colored blue dividing the paper into 32 strips of equal height. Assume that there are also 21 parallel horizontal lines colored red dividing the paper into 22 strips of equal height. Suppose the piece of paper is 10 inches high. What is the shortest distance between two lines?

Exercise 14. Find all positive solution to $15x + 7y = 210$.

Exercise 15. Find all positive solution to $221x + 91y = 1053$.

Exercise 16. Find all integral solution to $(6x + 15y)(8x + 7y) = 129$.

Exercise 17. A farmer buys 120 head of livestock from \$8000. Horses cost 100 dollars, cows 60 dollars, and sheep 30 dollars. The farmer buys at least one of each type. What is the least number of sheep the farmer could have bought?

Exercise 18. A child has \$4.55 in change consisting of dimes and quarters. How many possibilities are there?

Prof. Wayne Aitken, Cal. State, San Marcos, CA 92096, USA
E-mail address: `waitken@csusm.edu`