Solving a Linear Congruence

Solving a Linear Congruence

Frank Rubin

Marist College ACM

March 15, 2021

Linear Congruence

$aX \equiv b \pmod{m}$

m is the *modulus*, a (large) positive integer

X is the unknown value to be found

a is the coefficient of X, an integer constant

b is the scalar term, an integer constant

b is called the *residue* of aX modulo m

Usually $0 < a,b < m$

Linear Congruence

$$aX \equiv b \pmod{m}$$

There is an integer n such that

$$aX - b = mn$$

(Loosely) Two integers are congruent modulo m if they have the same remainder when divided by m.

(Formally) Two integers belong to the same *residue class* modulo m if they differ by a multiple of m.

Carl Friedrich Gauss, *Disquisitiones Arithmeticae,* 1801.

Exhaustive Enumeration

If m is small enough, you can find X simply by trying all possible values up to m-1.

Requires, on average, m/2 trials.

Good for $m < 10^9$. If you are doing this only once, then $m < 10^{12}$.

Strong vs Weak

$5X \equiv 1 \pmod{12}$. Unique solution $X \equiv 5 \pmod{12}$.

$10X \equiv 8 \pmod{12}$. Two solutions $X \equiv 2, 8 \pmod{12}$.

$9X \equiv 3 \pmod{12}$. Three solutions $X \equiv 3, 7, 11 \pmod{12}$.

$8X \equiv 4 \pmod{12}$. Four solutions $X \equiv 2, 5, 8, 11 \pmod{12}$.

$6X \equiv 6 \pmod{12}$. Six solutions $X \equiv 1, 3, 5, 7, 9, 11 \pmod{12}$.

$12X \equiv 0 \pmod{12}$. Twelve solutions. No information.

The number of solutions is gcd(a,m).

Operations

Congruences with the **same modulus** can be added and subtracted, or multiplied by an integer constant.

$$13X \equiv 74 \pmod{97}$$
$$\underline{\quad 7X \equiv 11 \pmod{97}}$$
$$20X \equiv 85 \pmod{97}$$

If a, b and m have a **common factor** you can divide a, b and m by that factor.

$$9X \equiv 3 \pmod{12}$$
$$3X \equiv 1 \pmod{4}$$

If a and m have a common factor that **does not divide** b, then the congruence has no solution.

$$4X \equiv 5 \pmod{16}$$

Reducing the Coefficient

Start with $38X \equiv 55 \pmod{101}$.

Reduce the coefficient by multiplying the congruence by some constant to make the coefficient a little greater than m.

Here, $101/38 = 2.658$. Multiply by $\lceil 2.658 \rceil = 3$.

$3 \times 38X \equiv 3 \times 55 \pmod{101}$,
$114X \equiv 165 \pmod{101}$,
$13X \equiv 64 \pmod{101}$.

Again, $101/13 = 7.769$, so multiply by 8.

$8 \times 13X \equiv 8 \times 64 \pmod{101}$,
$104X \equiv 512 \pmod{101}$,
$3X \equiv 7 \pmod{101}$.

One more iteration gives $X \equiv 36 \pmod{101}$.

Iterations

The expected number of iterations is $\log_{\phi}(a)$, where $\phi = (1+\sqrt{5})/2 = 1.618$ is the Golden Ratio.

Half & Half Rule

Let f be the fractional part of m/a, and let n be the integer part of m/a. Half the time f < .5, and half the time f > .5.

When f < .5, na is closer to m, so multiply the congruence by n and subtract m.

When f > .5, (n+1)a is closer to m, so multiply the congruence by n+1 and subtract it from m.

Half & Half Example

$41X \equiv 90 \pmod{101}$. Here 101/41=2.463.

$82X \equiv 180 \pmod{101}$. Subtract this from multiples of 101.

$101X \equiv 202 \pmod{101}$. Equivalent to 0=0.

Since 101-82=19 and 202-180=22, you get

$19X \equiv 22 \pmod{101}$.

Half & Half Comparison

Without H&H Rule	With H&H Rule
$135X \equiv 77 \pmod{1009}$	$135X \equiv 77 \pmod{1009}$
$71X \equiv 616 \pmod{1009}$	$64X \equiv 470 \pmod{1009}$
$56X \equiv 159 \pmod{1009}$	$15X \equiv 457 \pmod{1009}$
$55X \equiv 1003 \pmod{1009}$	$4X \equiv 660 \pmod{1009}$
$36X \equiv 895 \pmod{1009}$	$X \equiv 165 \pmod{1009}$
$35X \equiv 730 \pmod{1009}$	
$6X \equiv 990 \pmod{1009}$	
$5X \equiv 825 \pmod{1009}$	
$X \equiv 165 \pmod{1009}$	

Iterations

The expected number of iterations is $\log_{2\phi}(a)$, where $2\phi = 1+\sqrt{5} = 3.236$.

What Went Wrong?

Reducing the coefficient is slow, even using the Half & Half Rule. The problem is that as the coefficient gets smaller, the multiplier gets bigger, so the product is always at least as large as m.

For example, if m is about 10^{100}, when a has been reduced to 10^{50}, $n=\lceil m/a \rceil$ will be about 10^{50}, so na will be the product of two 50-digit numbers, and nb will be the product of a 100-digit number and a 50-digit number.

Laddering

Suppose we had 2 congruences, say

$$1607X \equiv 454 \pmod{35221}$$
$$764X \equiv 1903 \pmod{35221}$$

Instead of multiplying 764 by 46 to get it close to 35221, it could be multiplied by 2 to get it close to 1607.

$$1607X \equiv 454 \pmod{35221}$$
$$\underline{1528X \equiv 3806 \pmod{35221}}$$
$$79X \equiv 31869 \pmod{35221}$$

Getting Started

Let's look at an example using larger numbers.

$$6114257X \equiv 90926 \pmod{28338689}$$

Use the same 0=0 trick we used before.

$$28338689X \equiv 0 \pmod{28338689}$$

Since 28338689/6114257 is about 4.635, multiply by 5 and subtract to get

$$\begin{aligned} 30571285X &\equiv 454630 \pmod{28338689} \\ \underline{28338689X} &\underline{\equiv 0 \pmod{28338689}} \\ 2232596X &\equiv 454630 \pmod{28338689} \end{aligned}$$

Now we can repeat this process using the congruences

$$\begin{aligned} 6114257X &\equiv 90926 \pmod{28338689} \\ 2232596X &\equiv 454630 \pmod{28338689} \end{aligned}$$

Laddering

$$2232596X \equiv 454630 \pmod{28338689}$$

$$6697788X \equiv 1363890 \pmod{28338689}$$

$$\underline{6114257X \equiv 90926 \pmod{28338689}}$$

$$583531X \equiv 1272964 \pmod{28338689}$$

2232596/583531 is 3.826, so multiply by 4.

$$2334124X \equiv 5091856 \pmod{28338689}$$

$$\underline{2232596X \equiv 454630 \pmod{28338689}}$$

$$101528X \equiv 4637226 \pmod{28338689}$$

etc.

This takes the same number of steps, but the multipliers stay small.

That’s Better

This is a BIG speedup, since the multipliers for both na and nb are almost always small.

The modulo reduction of nb (mod m) is also much faster.

This is the BENCHMARK we want to beat.

Continued Fractions

Consider the fraction **.13579**. This is a bit less than 1/7, about 1/7.3643. This can be written as 1/7+ .3643, where the addition is done in the denominator.

Here, .3643 is about 1/2.745, so 1/7+ 1/2+ .745. Since .745 is about 3/4, this is 1/7+ 1/2+ 3 /4.

This can be unrolled as 1/7+ 1/(2+3/4) = 1/7+ 4/11 = 1/(7+4/11) = 1/(81/11) = 11/81, which is **.13580**, a difference of only .00001, so this is an excellent way of approximating fractions.

Example

Look again at $6114257X \equiv 90926 \pmod{28338689}$.

A good approximation of 6114257/28338689 is 241/1117, so multiply 6114257 by 1117 and 28338689 by 241.

$$\begin{aligned} 6829625069X &\equiv 101564342 \pmod{28338689} \\ \underline{6829624049X} &\underline{\equiv \quad 0 \pmod{28338689}} \\ 1020X &\equiv 101564342 \pmod{28338689} \\ 1020X &\equiv \ 16548275 \pmod{28338689} \end{aligned}$$

Here, the coefficient 6114257 was reduced to 1020, a factor of 5994. So this method can reduce the number of steps substantially.

How Many Terms?

Unfortunately, this does not give a large (or any) improvement unless the approximation is very close.

One **Rule of Thumb** for getting a good approximation is to stop just before a term with a large denominator. For example, $1/1_+ 1/2_+ 1/4_+ 1/2_+ 1/18_+ \ldots$ Stop just before the 1/18 term, hence $1/1_+ 1/2_+ 1/4_+ 1/2$.

This Many Terms

Here is a **precise calculation**.

Let the coefficients be a_1 and a_2, and let their exact ratio be $r=a_1/a_2$. We want to approximate r by a fraction n/d, namely $a_1/a_2 = n/d$, or $da_1 = na_2$. For the best approximation, we minimize $|da_1 - na_2|$. Replace a_1 by ra_2 to get $|dra_2 - na_2|$. Divide through by a_2. The goal is to minimize $|dr - n|$.

The Rule of Thumb works better!

If r is large, say $r>2^{16}$, it may be better to use one round of Half & Half.

This Many Terms

Here is a precise calculation.

Let the coefficients be a_1 and a_2, and let their exact ratio be $r=a_1/a_2$. We want to approximate r by a fraction n/d, namely $a_1/a_2 = n/d$, or $da_1 = na_2$. For the best approximation, we minimize $|da_1 - na_2|$. Replace a_1 by ra_2 to get $|dra_2 - na_2|$. Divide through by a_2. The goal is to minimize $|dr - n|$.

The Rule of Thumb works better!

If r is large, say $r>2^{16}$, it may be better to use one round of Half & Half.

Descent

Let's look at the congruences a different way.

$$\mathbf{a_1X_1 \equiv b_1 \pmod{m_1}}$$

The congruence $7X_1 \equiv 3 \pmod{17}$ means that $7X_1 = 3 + 17X_2$. Now let's flip this. $17X_2 = 7X_1 - 3$, so $17X_2 \equiv -3 \pmod 7$, which is $3X_2 \equiv 4 \pmod 7$.

Notice that the numbers are smaller. Flip this again, $3X_2 = 4 + 7X_3$, or $7X_3 = 3X_2 - 4$, so that $7X_3 \equiv -4 \pmod 3$, which is $X_3 \equiv 2 \pmod 3$.

Back-substitution

Any solution to $X_3 \equiv 2 \pmod 3$ will work, so choose $X_3 = 2$.

From $3X_2 = 4 + 7X_3$ we get $3X_2 = 18$, so $X_2 = 6$.

From $7X_1 = 3 + 17X_2$ we get $7X_1 = 105$, so $X_1 = 15$.

To verify $7X_1 \equiv 3 \pmod{17}$, we have $7 \times 15 = 105$, and $105 = 17 \times 6 + 3$.

Formulas

Descent

$$a_i = m_{i-1} \bmod a_{i-1}$$
$$b_i = -b_{i-1} \bmod a_{i-1}$$
$$m_i = a_{i-1}$$

Ascent

$$x_i = (m_i x_{i+1} + b_i) / a_i$$

Pros & Cons

Advantages

Works for all moduli, not just primes.

All numbers get smaller.

Disadvantages

Requires a separate back-substitution phase.

Numbers get larger.

Results

The Continued Fraction method is the fastest.