CSE 1400 Applied Discrete Mathematics
Modular Numbers

Department of Computer Sciences

College of Engineering

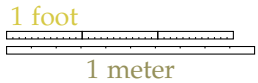
Florida Tech

Fall 2011

Abstract

Conversion Between Units

Pretend you'd like to covert one foot (12 inches) into its equivalent length in meters. You know one foot goes into one meter about 3 times with a remainder of about 3 inches. The empirical approach to convert feet to meters is to lay the foot-long ruler along a meter stick as many times as it will go; in this case 3 times.



There will be a tiny piece ▭ left over, not covered, on the meter stick. Call the length of this tiny piece r and note that r is some fraction of a foot.

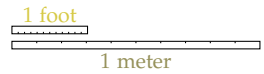
To compute r, lay it along the foot-long ruler and measure that about three r's almost covers a foot, so that $r \approx 0.3333\cdots$ feet and 1 meter is approximately $3.3333\cdots$ feet.

The conversion between units is

$$1\,\text{meter} \approx 3.2808\,\text{feet}$$

$$1\,\text{foot} \approx 0.3048\,\text{meters}$$

The Euclidean algorithm compute these approximations.



One meter is approximately three feet.

$$1 \text{ meter } = 3 \text{ feet } + r \text{ feet}$$

where r is some fractional part of one foot. Three, the number of time a foot goes into a meter is called the quotient, and r is called the remainder or residue.

But there is still a tiny piece ▫ left over, not covered, on the foot-long ruler. Call the length of this tiny piece r_1, and let's also rename r, the first fraction of a foot, by calling it r_0 from now on.

To compute the length r_1, lay it along the fractional foot

$$r_0 = \text{▭} \approx \frac{1}{3}$$

and measure that two of these smaller remainder $r_1 =$ ▫ almost cover $r_0 =$ ▭, but by a little too much.

We can continue this process until:

- Some multiple of a tiny remainder exactly covers the previous one.
- The approximation computed is accurate enough for its intended purpose.

Let's stop at this step and note what we've discovered.

$$1 \text{ meter} = (3 + r_0) \text{ feet}$$

$$1 \text{ foot} = (3r_0 + r_1) \text{ feet}$$

$$r_0 \text{ feet} = (2r_1 - r_2) \text{ feet}$$

We make a truncation error by ignoring the value of r_2, effectively setting its value to 0, but we gain a conversion factors to change meters into feet and vice versa. That is, we have

$$r_1 \text{ feet } \approx \frac{r_0}{2} \text{ feet}$$

$$1 \text{ foot } \approx (3r_0 + \frac{r_0}{2}) = \frac{7r_0}{2} \text{ feet}$$

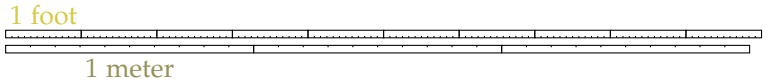
$$r_0 \text{ feet} \approx 2/7 \text{ feet}$$

$$1 \text{ meter } \approx (3 + \frac{2}{7}) \text{ feet}$$

Or, 1 meter is about $23/7 = 3.28571428571$ feet. Let us declare that $3 + 2/7 = 23/7 \approx 3.2857$ feet is "good enough for our uses" as an approximation to 1 meter.

Recall from above, 1 meter is approximately 3.2808 feet.

In practice we would like to have a ruler $1/7$ of a foot-long so we subdivide 1 foot evenly into 7 parts and 1 meter (almost) evenly into 23 parts. Here's how we can CONSTRUCT a rule one-seventh of a foot-long. Lay out three meters and you'll discover you've covered $3(3 + 2/7) = 9 + 6/7$ feet. Now lay out ten foot-long rulers to 10 feet.



The 10 foot distance is (about) one-seventh of a foot longer than 3 meters. That is,

$$\begin{aligned} 3\,\text{meters} &= 3(3 + \frac{2}{7}\ \text{feet} \\ &= 3\frac{23}{7}\ \text{feet} \\ &= \frac{69}{7}\ \text{feet} \\ &= 10 - \frac{1}{7}\ \text{feet} \end{aligned}$$

Look at the equation

$$3 \cdot (23/7) = 10 - 1/7)$$

Clear its denominator 7

$$3 \cdot 23 = 10 \cdot 7 - 1)$$

and rearranging terms to find that

$$1 = 10 \cdot 7 - 3 \cdot 23$$

which states

> If you lay out 10 feet, measured by 7 one-seventh of a foot-long rulers, and compare it to 3 meters, measured by 23 of the one-seventh of a foot-long rulers, then 1 unit of measure (one-seventh of a foot) will be leftover.

This is the extended Euclidean algorithm which when given 7 and 23 computes 1, 10 and -3. 1 is the greatest common divisor of 7 and 23. Ten and -3 are parameters that express the $1 = \gcd(7, 23)$ as a linear combination of 7 and 23.

Modular Numbers

For every natural number n there is a set $\mathbb{Z}_n$ of modular numbers where

$$\mathbb{Z}_n = \{0, 1, \ldots, (n-1)\}$$

Initial instances of these sets are given below.

The set $\mathbb{Z}_n$ is often read as "the integers mod n".

- $\mathbb{Z}_0 = \emptyset$
- $\mathbb{Z}_1 = \{0\}$
- $\mathbb{Z}_2 = \{0, 1\}$
- $\mathbb{Z}_3 = \{0, 1, 2\}$
- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$
- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

Any integer a can be mapped to one of the integers mod n by computing the non-negative remainder when a is divided by n.

For instance, mod 2 maps all even integers map to 0 and all odd integers map to 1.

Let a be an integer. Divide a by n to compute a quotient q and non-negative remainder r, that is,

$$a = qn + r,\ 0 \le r < n$$

The mod n function maps the integer a to the remainder r. This is written

$$a \bmod n = r$$

For instance

$$\begin{aligned} 38 \bmod 7 &= 3 & 53 \bmod 12 &= 5 \\ 27 \bmod 7 &= 6 & 78 \bmod 12 &= 6 \\ -38 \bmod 7 &= 4 & -53 \bmod 12 &= 7 \\ -27 \bmod 7 &= 1 & -78 \bmod 12 &= 6 \end{aligned}$$

Do you see the easy way to compute $-38 \bmod 7$ given the value of $38 \bmod 7$ is 3? Since -38 and 38 sum to 0, $-38 \bmod 7$ and 3 must sum to 0. That is, $-38 \bmod 7$ must equal 4. Alternatively compute a quotient $q = -6$ and remainder $r = 4$ such that $-38 = -6 \cdot 7 + 4$.

When arithmetic operations are performed on modular numbers it can occur that the result lies outside the set $\mathbb{Z}_n$. The integers mod n is a CYCLIC number system. For instance, in mod 5 arithmetic, counting starts at 0, goes to 4, and continues by CYCLING back to 0. While in mod 7 arithmetic counting cycles every seven steps.

On $\mathbb{Z}_7$

$$\begin{aligned} 3+4 &= 7 = 0+7 = 0 \\ 3\cdot 4 &= 12 = 5+7 = 5 \\ 2-5 &= -3 = 4-7 = 4 \end{aligned}$$

When the context is clear, the syntatic sugar can be dropped and you can write $r = [r]_n$.

Integers Mod 5

$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
⋮	⋮	⋮	⋮	⋮
−10	−9	−8	−7	−6
−5	−4	−3	−2	−1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
⋮	⋮	⋮	⋮	⋮

Integers Mod 7

$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
−14	−13	−12	−11	−10	−9	−8
−7	−6	−5	−4	−3	−2	−1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
⋮	⋮	⋮	⋮	⋮	⋮	⋮

A key idea is: The integers mod n partition the integers into n EQUIVALENCE CLASSES. The names of these classes are $[0]_n$ through $[n-1]_n$. Each class represents a subset of the integers. In particular,

$$[r]_n = \{nk + r : k \in \mathbb{Z}\}$$

The syntatic sugar of brackets and subscripts can be dropped when the context is clear.

For instance, an integer mod 5 is a name for one of five subsets of integers.

Subsets that partition a set are called EQUIVALENCE CLASSES.

$$
\begin{aligned}
0 &= [0]_5 = \{5k : k \in \mathbb{Z}\} \\
1 &= [1]_5 = \{5k+1 : k \in \mathbb{Z}\} \\
2 &= [2]_5 = \{5k+2 : k \in \mathbb{Z}\} \\
3 &= [3]_5 = \{5k+3 : k \in \mathbb{Z}\} \\
4 &= [4]_5 = \{5k+4 : k \in \mathbb{Z}\}
\end{aligned}
$$

For the mod 5 instance, convince yourself of the following statements about the equivalence classes $[0]_5$, $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$.

1. Every integer is in one and only one equivalence classes.
2. When two integers a and b are in the same equivalence class $[r]_5$, then
   (a) $a - b$ is a multiple of 5
   (b) a and b have the same remainder r when divided by 5

The union of equivalence classes is the set of all integers. Th equivalence classes are pairwise disjoint.

When $a, b \in [r]_n$ write

$$a \equiv b \bmod n$$

For instance,

$$5 \equiv 0 \bmod 5 \qquad 16 \equiv 1 \bmod 5 \qquad 17 \equiv -3 \bmod 5$$

Addition and multiplication operations behave as with integers,

$$(a+b) \bmod n = (a \bmod n) + (b \bmod n)$$

$$(a \cdot b) \bmod n = (a \bmod n) \cdot (b \bmod n)$$

except answers are REDUCED mod n. For instance, the following calculations hold in mod 9 arithmetic.

If $a = sn + r$ and $b = tn + p$ where $0 \le r, p < (n-1)$ so that $a \bmod n = r$ and $b \bmod n = p$ then

$$
\begin{aligned}
a + b \bmod n &= ((s+t)n + r + p) \bmod n \\
&= (r + p) \bmod n \\
&= (r \bmod n) + (p \bmod n) \\
&= (a \bmod n) + (b \bmod n)
\end{aligned}
$$

Also,

$$
\begin{aligned}
a \cdot b \bmod n &= (stn^2 + (sp + rt)n + rp) \bmod n \\
&= rp \bmod n \\
&= (r \bmod n) \cdot (p \bmod n) \\
&= (a \bmod n) \cdot (b \bmod n)
\end{aligned}
$$

$$
\begin{array}{lclclcl}
2 \cdot 8 & = & 16 & = & 7 + 9 & = & 7 \\
3 \cdot 3 & = & 9 & = & 0 + 9 & = & 0 \\
4 \cdot 7 & = & 28 & = & 1 + 3 \cdot 9 & = & 1 \\
5 \cdot 42 & = & 5 \cdot 6 & = & 3 + 3 \cdot 9 & = & 3 \\
314 \cdot 23 & = & 8 \cdot 5 & = & 4 + 4 \cdot 9 & = & 4
\end{array}
$$

The mod 9 multiplication table below contains interesting informa-

tion.

$\times$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

The integers 1, 2, 4, 5, 7 and 8 have multiplicative inverses mod 9.

Division mod n

Recall from college algebra that the RECIPROCAL $a^{-1} = \frac{1}{a}$, the MULTIPLICATIVE INVERSE, of a non-zero real number $a \neq 0$ satisfies the equation

$$a \cdot a^{-1} = a \cdot \frac{1}{a} = 1$$

The multiplicative inverse is also called the reciprocal.

This is how division is defined: The integer b divided by a is b times a^{-1}.

$$\frac{b}{a} = b \cdot a^{-1}$$

The multiplication table above shows the mod 9 integers: 1, 2, 4, 5, 7, and 8 have reciprocals. They are

$$\begin{aligned}
1^{-1} &= 1, && \text{because} \quad 1 \cdot 1 = 1 \mod 9 \\
2^{-1} &= 5, && \text{because} \quad 2 \cdot 5 = 1 \mod 9 \\
4^{-1} &= 7, && \text{because} \quad 4 \cdot 7 = 1 \mod 9 \\
5^{-1} &= 2, && \text{because} \quad 5 \cdot 2 = 1 \mod 9 \\
7^{-1} &= 4, && \text{because} \quad 7 \cdot 4 = 1 \mod 9 \\
8^{-1} &= 8, && \text{because} \quad 8 \cdot 8 = 1 \mod 9
\end{aligned}$$

In mod 9 arithmetic, "divide by 2" means "multiply by 5". If you divide 51 by 2 mod 9 the answer is 3.

$$51 \div 2 = (45+6) \div 2 = 6 \div 2 = 3 \mod 9$$

If you multiply 51 by 5 mod 9 the answer is 3.

$$51 \cdot 5 = 255 = 252 + 3 = 9 \cdot 28 + 3 = 3 \mod 9$$

If you divide 50 by 2 mod 9 the answer is 7.

$$50 \div 2 = 25 = 18 + 7 = 7$$

If you multiply 50 by 5 mod 9 the answer is 7.

$$50 \cdot 5 = 250 = 243 + 7 = 9 \cdot 27 + 7$$

Linear Congruence Equations

An equation of the form

$$ax = b \bmod n$$

is called a linear congruence equation. The basic problem is to compute the value of x given parameters a, b and n. Furthermore, x must be an integer mod n. That is, x is an integer between 0 and $(n-1)$.

Each of the following are LINEAR CONGRUENCE EQUATIONS mod 9.

$$2x = b \bmod 9$$
$$4x = b \bmod 9$$
$$5x = b \bmod 9$$
$$7x = b \bmod 9$$
$$8x = b \bmod 9$$

Using the reciprocals $2^{-1} = 5$, $4^{-1} = 7$, $5^{-1} = 2$ $7^{-1} = 4$, and $8^{-1} = 8$, a solution $x \in \mathbb{Z}_9$ can be computed for each of the above equations.

$$x = 5b \bmod 9$$
$$x = 7b \bmod 9$$
$$x = 2b \bmod 9$$
$$x = 4b \bmod 9$$
$$x = 8b \bmod 9$$

On the other hand, 3 and 6 do not have reciprocals mod 9. Recall row 3 and 6 from the multiplication table.

$\times$	0	1	2	3	4	5	6	7	8
3	0	3	6	0	3	6	0	3	6
6	0	6	3	0	6	3	0	6	3

$3x$ is never equal to 1, so 3 has no multiplicative inverse, and likewise neither does 6. The linear congruence equations

$$3x \equiv b \bmod 9$$
$$6x \equiv b \bmod 9$$

have solutions $x \in \mathbb{Z}_9$ only when $b = 3$ or $b = 6$, and in these cases there are multiple solutions.

$3x \equiv 3 \bmod 9$	has solutions	$x = 1, 4, 7$
$3x \equiv 6 \bmod 9$	has solutions	$x = 2, 5, 8$
$6x \equiv 3 \bmod 9$	has solutions	$x = 2, 5, 8$
$6x \equiv 6 \bmod 9$	has solutions	$x = 1, 4, 7$

Euclidean Algorithm for the Greatest Common Divisor

THE EUCLIDEAN ALGORITHM COMPUTES THE GREATEST COMMON DIVISOR OF TWO NATURAL NUMBERS.

Definition 1 (Greatest Common Divisor)**.** The GREATEST COMMON DIVISOR of a and n, call it $\gcd(a, n)$ or g for short, is a natural number that divides both a and n.

$$g \mid a \quad \text{and} \quad g \mid n$$

Furthermore, if d is any divisor of both a and n, then d divides g.

Some people call IT the greatest common FACTOR. For instance, 10 is the greatest common divisor of 30 and 50. And 7 is the greatest common divisor of 1512 and 1925. The mathematical notation for these instances is

$$10 = \gcd(30, 50)$$

and

$$7 = \gcd(1512, 1925)$$

Table 1 lists the greatest common divisor of a pair of numbers (a, n).

Table 1: Greatest common divisors on digit pairs.

Greatest Common Divisor $\gcd(a, n)$

	$n = 0$	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	2	1	2	1	2	1	2	1	2	1	2
3	3	1	1	3	1	1	3	1	1	3	1
$a =$ 4	4	1	2	1	4	1	2	1	4	1	2
5	5	1	1	1	1	5	1	1	1	1	5
6	6	1	2	3	2	1	6	1	2	3	2
7	7	1	1	1	1	1	1	7	1	1	1
8	8	1	2	8	4	1	2	1	8	1	2
9	9	1	1	3	1	1	3	1	1	9	1
10	10	1	2	1	2	5	2	1	2	1	10

The Euclidean algorithm is based on the quotient remainder theorem which states: For any integer $a \in \mathbb{Z}$ and natural number n there exists a unique integer q and a unique natural number $0 \leq r < n$ such that $a = q \cdot n + r$ The Euclidean algorithm can be summarized by the recursive function described in the code below. The interpretation of the code is this: Given natural numbers a and n, compute their greatest common divisor $\gcd(a, n)$ by doing the following.

1. If $n = 0$, then a is the greatest common divisor of a and n.
2. Otherwise, when $n \neq 0$, $\gcd(a, n)$ is the gcd of n and the remainder r when a is by n. That is, compute $\gcd(n, r)$ to find the answer.

$$(\forall a \in \mathbb{Z})(\forall n \in \mathbb{N})$$
$$(\exists! q \in \mathbb{Z})(\exists! r \in \mathbb{Z}_n)(a = q \cdot n + r)$$

Although it is not a practical algorithm, you can find the greatest common divisor $\gcd(a, n)$ from the prime factorization of a and n. For instance

$$a = 30 = 2 \cdot 3 \cdot 5 \quad \text{and} \quad n = 50 = 2 \cdot 5^2$$

implies that $2 \cdot 5 = \gcd(30, 50)$.

$$a = 1512 = 2^3 \cdot 3^3 \cdot 7 \quad \text{and} \quad n = 1925 = 5^2 \cdot 7 \cdot 11$$

implies $7 = \gcd(1512, 1925)$.
What happens when $a = 0$ and $n \neq 0$?

Here's the Haskell code for the Euclidean algorithm when a is a natural number. A more robust $\gcd(a, n)$ function is defined in Haskell's Prelude.

```
 euclid :: Natural Natural -> Natural

{- if n = 0, then gcd(a, 0) = a -}
euclid a 0 = a

{- else gcd(a, n) = gcd(n, a `mod` n) -}
euclid a n = euclid n (a `mod` n)
```

The table below shows three steps of Euclidean algorithm applied to the pair $(14, 5)$. The numbers are color-coded to illustrate divisors values moving up to the dividend row and remainders moving up to the divisor row.

Euclidean Algorithm Compute $\gcd(14, 5)$				
Dividend	a	14	5	4
Divisor	n	5	4	1
Remainder	r	4	1	0
Quotient	q	2	1	4

Each column represents an instance of the quotient remainder theorem

$$\begin{aligned} 14 &= 5 \cdot 2 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

The OUTPUT of the Euclidean algorithm is the last non-zero divisor, 1 in this instance. The OUTPUT is the GREATEST COMMON DIVISOR of the INPUT.

$$\gcd(14, 5) = 1$$

Let us compute the $\gcd(189, 80)$ to provide another example of the Euclidean algorithm.

Scratch work:

$$\begin{aligned} 189 \div 80 &= 2 & 189 \mod 80 &= 29 \\ 80 \div 29 &= 2 & 80 \mod 29 &= 22 \\ 29 \div 22 &= 1 & 29 \mod 22 &= 7 \\ 22 \div 7 &= 3 & 22 \mod 7 &= 1 \\ 7 \div 1 &= 7 & 7 \mod 1 &= 0 \end{aligned}$$

Euclidean Algorithm Compute $\gcd(189, 80)$						
Dividend	a	189	80	29	22	7
Divisor	n	80	29	22	7	1
Remainder	r	29	22	7	1	0
Quotient	q	2	2	1	3	7

Let us discover how the Euclidean algorithm iterates through its steps. To compute the greatest common divisor $\gcd(a, n)$ start by

renaming them

$$r_0 = a$$
$$r_1 = n$$

Also rename the quotient and remainder from the quotient remainder theorem

$$q_1 = q$$
$$r_2 = r$$

Then the quotient-remainder equation $a = n \cdot q + r$ can be rewritten as

$$r_0 = r_1 \cdot q_1 + r_2$$

Generalize this equation by replacing 0 with an index variable k, and likewise replace 1 are 2 with $k+1$ and $k+2$, respectively.

$$r_k = r_{k+1} \cdot q_{k+1} + r_{k+2}$$

Given r_k and r_{k+1}, the Euclidean algorithm iteratively computes quotients q_{k+1}

$$q_{k+1} = r_k \operatorname{div} r_{k+1}$$

and remainders r_{k+2}

$$r_{k+2} = r_k \mod r_{k+1}$$

The algorithm terminates when a remainder r_{k+2} is 0. The value returned by the algorithm is r_{k+1}.

It is also useful to write the recurrence for the remainders using the equation

$$r_{k+2} = r_k - q_{k+1} \cdot r_{k+1}$$

Recall from the discussion on unit conversion, we would like to be able to compute the greatest common divisor of a and n as a linear combination of a and n, that is,

$$\gcd(a, n) = as + tn$$

for some integers s and t. But before learning this extension to the Euclid's algorithm, the concept of RELATIVELY PRIME natural numbers will be introduced.

Relatively Prime Numbers

TWO NATURAL NUMBERS THAT HAVE NO COMMON FACTOR ARE PRIME RELATIVE TO EACH OTHER.

Definition 2 (Relative Prime)**.** Two natural numbers a and n are RELATIVELY PRIME when their GREATEST COMMON DIVISOR is 1.

$\gcd(a, n) = 1 \implies a$ and n are relatively prime.

As instances, the following pairs are relatively prime.

$$\begin{aligned} (3, 8) \qquad & 1 = \gcd(3, 8) = 8 \cdot 2 + 3 \cdot (-5) \\ (12, 35) \qquad & 1 = \gcd(12, 35) = 35 \cdot (-1) + 12 \cdot 3 \end{aligned}$$

One interesting fact about a relatively prime pair is that every integer can be written as a linear combination of them. That is, if a and n are relatively prime, then there exists integers s and t such that $1 = as + tn$. Therefore for every $z \in \mathbb{Z}$, $z = a(zs) + n(zt)$.

When a and n are relatively prime the linear congruence equation

$$ax = b \bmod n$$

always has a solution: ba^{-1} where a^{-1} is an integer mod n. On the other hand, when a and n are not relatively prime the linear congruence equation

$$ax = b \bmod n$$

may or may not have a solution. In this case, a solution exists if and only if b is a multiple of the greatest common divisor of a and n.

Extended Euclidean Algorithm

THE EUCLIDEAN ALGORITHM CAN BE EXTENDED TO COMPUTE INTEGERS s AND t SUCH THAT

$$gcd(a, n) = as + tn$$

This is a simple example of Bézout's Theorem.
Linear combinations are fundamentally useful! Relating an input value x to an output value y by the equation

$$ax + ny = c$$

Determines a line in (x, y)-space that is characterized by the coefficients a, n, and c.

Consider the problem of computing s and t such that

$$121s + 21t = \gcd(121, 21)$$

Start by writing trivial equations for 120 and 21.

$$\begin{aligned} 121 \cdot 1 + 21 \cdot 0 &= 121 \\ 121 \cdot 0 + 21 \cdot 1 &= 21 \end{aligned}$$

We can organize the computation by starting a "magic table" that contains the coefficients from the above equations.

121	21
1	0
0	1
	+

Table 2: A magic table for the extended Euclidean algorithm.

Note that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is a matrix with determinate

$$\det \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

Next apply a step of the quotient remainder theorem to write

$$121 = 21 \cdot 5 + 16$$

and extend the magic table 2 to the right by appending a new column labeled by the quotient 5. Foll in the third column by comput-

121	21	5
1	0	1
0	1	−5
	+	−

ing the values

$$\text{first column} - 5 \times \text{second column} = \text{third column}$$
$$1 - 5 \cdot 0 = 1$$
$$0 - 5 \cdot 1 = -5$$

These values come from the quotient-remainder equation with some rearrangement of terms.

$$121 = 21 \cdot 5 + 16$$
$$121 \cdot 1 + 21 \cdot 0 = (121 \cdot 0 + 21 \cdot 1) \cdot 5 + 16$$
$$121(1 - 5 \cdot 0) + 21(0 - 5 \cdot 1) = 16$$

The next step of the Euclidean algorithm divides 21 by the remainder 16 to yield a new quotient $q = 1$ and new remainder $r = 5$.

$$21 = 16 \cdot 1 + 5$$

Extends the "magic table" by appending a fourth column labeled 1 with values computed by the formula

$$\text{second column} - 1 \times \text{third column} = \text{fourth column}$$
$$0 - 1 \cdot 1 = -1$$
$$1 - 1 \cdot (-5) = 6$$

These values come from the quotient-remainder equation with some rearrangement of terms.

$$21 = 16 \cdot 1 + 5$$
$$21 = (121 \cdot 1 + 21 \cdot (-5)) \cdot 1 + 5$$
$$121 \cdot (-1) + 21 \cdot 6 = 5$$

121	21	5	1
1	0	1	−1
0	1	−5	6
	+	−	+

Continuing the Euclidean algorithm, compute quotients

$$121 = 21 \cdot 5 + 16$$
$$21 = 16 \cdot 1 + 5$$
$$16 = 5 \cdot 3 + 1$$
$$5 = 1 \cdot 5 + 0$$

See how the values in each row are computed by the recursion

$$s_{k-2} + s_{k-1} q_k = s_k$$
$$t_{k-2} + t_{k-1} q_k = t_k$$

with initial conditions

$$s_0 = 0 \quad s_1 = 1$$
$$t_0 = 1 \quad t_1 = 0$$

and fill in the "magic table"

121	21	5	1	3	5
1	0	1	−1	4	−21
0	1	−5	6	−23	121
	+	−	+	−	+

The next to last column represent the equation

$$121 \cdot 4 + 21 \cdot (-23) = 1$$

This equation expresses the greatest common divisor of 21 and 121 as a linear combination of 121 and 21.

$$1 = \gcd(121, 21) = 121 \cdot 4 + 21 \cdot (-23) = 121s + 21t$$

where $s = 4$ and $t = -23$.

Here is another example of the extended Euclidean algorithm. To find parameters s and t such that

$$1 = \gcd(13, 5) = 13s + 5t$$

Start a magic table

13	5
1	0
0	1
	+

$13 = 13 \cdot 1 + 5 \cdot 0$
$5 = 13 \cdot 0 + 5 \cdot 1$

Compute a quotient and remainder when 13 is divided by 5

$$13 = 5 \cdot 2 + 3$$

Append a column to the magic table: Label the column by the quotient 2 and compute values in the third column by the formula

$$\text{third column} = \text{first column} - \text{quotient} \times \text{second column}$$

$13 \cdot 1 + 5 \cdot (-2) = 3$

13	5	2
1	0	1
0	1	−2
	+	−

Compute a quotient and remainder when 5 is divided by 3

$$5 = 3 \cdot 1 + 2$$

Append a column to the magic table: Label the column by the quotient 1 and compute values by the formula

$$\text{fourth column} = \text{second column} - \text{quotient} \times \text{third column}$$

$13 \cdot (-1) + 5 \cdot 3 = 2$

13	5	2	1
1	0	1	−1
0	1	−2	3
	+	−	+

Compute a quotient and remainder when 3 is divided by 2

$$3 = 2 \cdot 1 + 1$$

Append a column to the magic table: Label the column by the quotient 1 and compute values by the formula

$$\text{fifth column} = \text{third column} - \text{quotient} \times \text{fourth column}$$

13	5	2	1	1
1	0	1	−1	2
0	1	−2	3	−5
	+	−	+	−

Notice that this last computation expresses 1, the greatest common divisor of 13 and 5 as a linear combination of 13 and 5.

$$1 = 13 \cdot 2 + 5 \cdot (-5)$$

It is wise to continue one more step to verify your calculations. Compute a quotient and remainder when 2 is divided by 1

$$2 = 1 \cdot 2 + 0$$

Append a column to the magic table: Label the column by the quotient 2 and compute values by the formula

$$\text{sixth column} = \text{fourth column} - \text{quotient} \times \text{fifth column}$$

13	5	2	1	1	2
1	0	1	−1	2	−5
0	1	−2	3	−5	13
	+	−	+	−	+

The last column contains the (plus or minus) the original values, and this serves as a check that the computations are correct.

Solving Linear Congruence Equations

Once you've discovered the equality

$$13 \cdot 3 + 5 \cdot (-5) = 1$$

you've also discovered that

$13 \cdot 3$ is equivalent to 0 mod 13.

$$5 \cdot (-5) = 1 \bmod 13$$

That is, 5 and −5 are multiplicative inverses of one another mod 13. Or, the reciprocal of 5 is −5 mod 13. Or, 5^{-1} is −5 mod 13. Of course

$-5 = 8 \bmod 13$, so that 5 and 8 are reciprocals of one another mod 13. That is,

$$\begin{aligned} 5 \cdot 8 = 40 = (39+1) &= 1 \bmod 13 \\ 5^{-1} &= 8 \bmod 13 \\ 8^{-1} &= 5 \bmod 13 \end{aligned}$$

Therefore, the value of x that solves the linear congruence equation

$$5x = 6 \bmod 13$$

is

$$x = 8 \cdot 6 = 48 = 9 \bmod 13$$

Multiply both sides of $5x = 6 \bmod 13$ by 8. Use $8 \cdot 5 = 1 \bmod 13$ and $48 = 13 \cdot 3 + 9 = 9 \bmod 13$.

To solve the general linear congruence equation

$$ax = b \bmod n$$

execute the extended Euclidean algorithm to find the greatest common divisor g of a and n and parameters s and t such that

$$g = \gcd(a, n) = as + nt$$

In $1 = as + nt$, the term nt is equal to $0 \bmod n$.

1. If $g = 1$, then $as = 1 \bmod n$ and a and s are reciprocals mod n. In this case, the value of x that solves the linear congruence equation

$$ax = b \bmod n$$

is

$$x = bs \bmod n$$

Multiply both sides of $ax = b \bmod n$ by s and use $as = 1 \bmod n$.

2. If $g \neq 1$, then $ax = b \bmod n$ has a solution only when b is a multiple of g.

   If b is a multiple of g, that is, if $b = gk$ for some integer k, then one value of x that solves the linear congruence equation

$$ax = b \bmod n$$

is

$$x = ks \bmod n$$

Replace b in $ax = b \bmod n$ by gk, multiply both sides of $ax = gk \bmod n$ by s and use $as = g \bmod n$, to get $gx = gks \bmod n$ or, canceling the common g, $x = ks \bmod n$.

Consider two examples: One where a and n are relatively prime, and a second where a and n are not relatively prime.

1. Consider the case where a and n are relatively prime. Let $a = 14$ and $n = 115$ and pick $b = 2$. To solve the linear congruence equation

$$14x = 2 \bmod 115$$

execute the extended Euclidean algorithm to compute $g = \gcd(115, 14)$ and parameters s and t such that $g = 115s + 14t$.

115	14	8	4	1	2
1	0	1	−4	5	−14
0	1	−8	33	−41	115
	+	−	+	−	+

$$115 = 14 \cdot 8 + 3$$
$$14 = 3 \cdot 4 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

Therefore the greatest common divisor of 14 and 115 is 1 and

$$115 \cdot 5 + 14 \cdot (-41) = 1$$

Moreover, $-41 = 74 \bmod 115$ is the reciprocal of 14 mod 115, and value of x that solves the linear congruence equation

$$14x = 2 \bmod 115$$

is

$$x = 2 \cdot 74 = 148 = 33 \bmod 115$$

2. Now consider the case where a and n are not relatively prime. To solve the linear congruence equation

$$14x = 2 \bmod 105$$

execute the extended Euclidean algorithm to compute $g = \gcd(105, 14)$ and parameters s and t such that $g = 105s + 14t$.

105	14	7	2
1	0	1	−2
0	1	−7	15
	+	−	+

$$105 = 14 \cdot 7 + 7$$
$$14 = 7 \cdot 2 + 0$$

Therefore the greatest common divisor of 14 and 105 is 7. Compute the determinant

$$\det \begin{vmatrix} 1 & -2 \\ -7 & 15 \end{vmatrix} = 15 \cdot 1 + 2 \cdot (-7) = 1$$

This looks like an error has been made, but it demonstrates what occurs when $a = 14$ and $n = 105$ are not relatively prime. The equation

$$15 \cdot 1 + 2 \cdot (-7) = 1$$

can be "fixed" by multiplying through by 7 to obtain

$$105 \cdot 1 + 14 \cdot (-7) = 7$$

In mod 105 arithmetic $105 \cdot 1$ is 0 and -7 is 98.

$$105 \cdot 1 + 14 \cdot 98 = 14 \cdot 98 = 7 \bmod 105$$

Consider the start of the multiplication table for 14 mod 105

$\times$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	$\cdots$
14	0	14	28	42	56	70	84	98	7	21	35	49	63	77	91	0	14	28	$\cdots$

The value 7 is smallest non-zero value and every and only multiple of 7 up to 98 are mapped onto in cycles of length 15.

In particular, there is no mod 105 integer x such that

$$14x = 2 \bmod 105$$

On the other hand,

$$14x = 21 \bmod 105$$

has seven solutions: $x = 9, 25, 39, 54, 69, 84, 99$. The first value $x = 9$ can be computed by multiplying the equation $14x = 2$ mod 105 through by 98 and using $14 \cdot 98 = 7$ mod 105 to obtain

$$14 \cdot 98x = 7x = 21 \cdot 98 = 63 = 7 \cdot 9 \bmod 105$$

so that, on canceling the common 7 you'll find

$$x = 9 \bmod 105$$

The next six values can be computing by incrementing by 14.

Problems on Modular Numbers

1. Describe an algorithm that could be used to convert 1 pound into kilograms.
2. Describe the residue (equivalence) classes for
   (a) Congruence mod 4.
   (b) Congruence mod 5.
3. How many residue classes are there mod n?
4. For the given values of a and n below, compute the quotient q and non-negative remainder r that satisfy the quotient-remainder equation

$$a = qn + r, \quad r \geq 0$$

(a) $a = 26$, $n = 13$.
(b) $a = 27$, $n = 13$.
(c) $a = -27$, $n = 13$.
(d) $a = -45$, $n = 13$.

5. Construct an addition table for the integers mod 6.
6. Construct a multiplication table for the integers mod 4.
7. Construct a multiplication table for the integers mod 7.
8. Solve the following linear congruence equations.
   (a) $3x \equiv 5 \pmod 7$
   (b) $5x \equiv 4 \pmod 7$
   (c) $2x \equiv 1 \pmod 7$
   (d) $6x \equiv 3 \pmod 7$
9. Let $p = 2^5 3^4 11^7 13^{10} 19^6$ and $q = 3^6 11^5 13^{12} 17^4$.
   (a) What is the greatest common divisor of p and q?
   (b) What is the least common multiple of p and q?
   (c) Verify the $\gcd(p, q) \cdot \operatorname{lcm}(p, q) = pq$.
10. Use Euclid's algorithm to compute the greatest common divisors listed below.
    (a) $\gcd(19, 8)$.
    (b) $\gcd(25, 40)$.
    (c) $\gcd(70, 27)$.
    (d) $\gcd(66, 99)$.
    (e) $\gcd(189, 80)$.
    (f) $\gcd(511, 255)$.
11. Using your work from question 10, find integers a and b such that
    (a) $1 = 19a + 8b$.
    (b) $5 = 40a + 25b$.
    (c) $1 = 70a + 27b$.
    (d) $1 = 66a + 99b$.
12. Using your work from question 11, solve the following linear congruence equations.
    (a) $8x = 5 \bmod 19$.
    (b) $25x = 38 \bmod 40$.
    (c) $27x = 4 \bmod 70$.
    (d) $66x = 22 \mod 99$.