Math 202 notes

Jason Riedy

6 October, 2008

Contents

Notes also available as PDF.

What we covered last week:

- divisibility and prime numbers,
- factorization into primes,
- modular arithmetic,
- finding divisibility rules,

This week's topics:

- review modular arithmetic and finding divisibility rules,
- greatest common divisors and least common factors,
- Euclid's algorithm for greatest common divisors, and
- solving linear Diophantine equations.

These all are useful when you deal with integral numbers of things

1 Modular arithmetic

Remember the divisibility form for b with respect to dividing by $a \neq 0$,

$$b = q \cdot a + r, \text{ with } 0 \leq r < |a|.$$

This form is *unique* for a given a and b.

Consider $a = 5$. There are only five possible values of r, zero through four. Because the form is unique, we can place every b into one of r **congruence classes**. Each congruence class is a set. For $a = 5$, we have the following classes:

$$\begin{array}{llllllll}
\{\ldots, & \text{-10}, & \text{-5}, & \mathbf{0}, & 5, & 10, & \ldots\} & = \{5k + 0 \,|\, k \in \mathbb{J}\} \\
\{\ldots, & \text{-9}, & \text{-4}, & \mathbf{1}, & 6, & 11, & \ldots\} & = \{5k + 1 \,|\, k \in \mathbb{J}\} \\
\{\ldots, & \text{-8}, & \text{-3}, & \mathbf{2}, & 7, & 12, & \ldots\} & = \{5k + 2 \,|\, k \in \mathbb{J}\} \\
\{\ldots, & \text{-7}, & \text{-2}, & \mathbf{3}, & 8, & 13, & \ldots\} & = \{5k + 3 \,|\, k \in \mathbb{J}\} \\
\{\ldots, & \text{-6}, & \text{-1}, & \mathbf{4}, & 9, & 14, & \ldots\} & = \{5k + 4 \,|\, k \in \mathbb{J}\}
\end{array}$$

We say that two numbers are in the same congruence class for a given a by

$$b \equiv c \pmod{a}.$$

Or b is equivalent to c **modulo** a. A collection of one entry from each set is called a **complete residue system**. We typically select the least positive numbers, those in bold above.

We define arithmetic on congruence classes by arithmetic on the remainders. The remainders wrap around every multiple of the modulus. For example, addition modulo 4 and modulo 5 are defined as follows:

+ (mod 4)	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+ (mod 5)	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

This works as you expect. Addition is **commutative** and **associative**. There is an **additive identity**, because $b + 0 \equiv 0 \pmod{a}$. Unlike the positive integers, there also is an **additive inverse** for every residue because $b + (a - b) \equiv 0 \pmod{a}$.

Multiplication likewise is **commutative** and **associative**, and there is a **multiplicative identity**, 1. The unusual aspect appears with the **multiplicative inverse**. Some residues have inverses, and some don't:

× (mod 4)	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

× (mod 5)	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The difference here is that 5 is prime while 4 is composite. Any factor of the modulus will not have a multiplicative inverse.

2 Divisibility rules

One common application of modular arithmetic (besides telling time) is in testing whether one integer divides another. We use modular arithmetic and positional notation. Both help us break the larger problem, testing divisibility of a potentially large number, into the smaller problems of breaking apart the number and evaluating expressions in modular arithmetic.

If $a \mid b$ (a divides b), then $b \equiv 0 \pmod{a}$. So we can test for divisibility by expanding b in positional notation and evaluating the operations modulo a.

When the divisor is small, a straight-forward evaluation is simplest. Because $10 \equiv 1 \pmod{3}$, we can test for divisibility by 3 by adding the number's digits modulo 3. For example,

$$\begin{aligned} 1234 &\equiv 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4 \pmod{3} \\ &\equiv 1^3 + 2 \cdot 1^2 + 3 \cdot 1 + 4 \pmod{3} \\ &\equiv 1 + 2 + 3 + 4 \equiv 1 + 2 + 0 + 1 \equiv 1 \pmod{3}. \end{aligned}$$

Hence $3 \nmid 1234$. The same "trick" applies to 9 because $10 \equiv 1 \pmod{9}$.

When the divisor is closer to a power of 10, using a negative element of the congruence class may be useful. For 11, remember that 10 and -1 are in the same congruence class because $10 = 0 \cdot 11 + 10$ and $-1 = -1 \cdot 11 + 10$. So $10 \equiv -1 \pmod{11}$ and we can expand the powers of ten,

$$\begin{aligned} 1234 &\equiv 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4 \pmod{11} \\ &\equiv (-1)^3 + 2 \cdot (-1)^2 + 3 \cdot (-1) + 4 \pmod{11} \\ &\equiv -1 + 2 + -3 + 4 \pmod{11} \equiv 2 \pmod{11}. \end{aligned}$$

Hence $11 \nmid 1234$. Here, the "trick" form is that you start from the units digit and then alternate subtracting and adding digits.

For more complicated examples, we can factor the divisor. To test if a number is divisible by 72, factor $72 = 2^3 \cdot 3^2 = 8 \cdot 9$. Then test if the number is divisible by 8 and by 9.

If $a \mid b$ and $c \mid b$, then it **may** be true that $ac \mid b$. This is certainly true of a and b are powers of different primes. The key point is that a and b share no common divisors. Note that $72 = 6 \cdot 12$, $6 \mid 24$, and $12 \mid 24$, but obviously $72 \nmid 24$ because $24 < 72$.

3 Greatest common divisor

So finding common divisors is useful for testing divisibility. The greatest common divisor of numerator and denominator reduces a fraction into its simplest form. In general, common divisors help break problems apart.

> Written (a, b) or $\gcd(a, b)$, the greatest common divisor of a and b is the largest integer $d \geq 1$ that divides both a and b.

We'll discuss a total of two methods for finding the greatest common divisor. The first uses the prime factorization, and the second uses the divisibility form in the Euclidean algorithm. Later we'll extend the Euclidean algorithm to provide integer solutions x and y to equations $ax + by = c$.

The prime factorization method factors both a and b. Consider $a = 1400 = 2^3 \cdot 5^2 \cdot 7$ and $b = 1350 = 2 \cdot 3^3 \cdot 5^2$.

Lining up the factorizations and remembering that $x^0 = 1$, we have

$$a = 1400 = 2^3 \cdot 3^{\mathbf{0}} \cdot 5^{\mathbf{2}} \cdot 7^1, \text{ and}$$
$$b = 1350 = 2^{\mathbf{1}} \cdot 3^3 \cdot 5^{\mathbf{2}} \cdot 7^{\mathbf{0}}.$$

Now chose the least exponent for each factor. Then

$$d = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^0 = 50$$

is the greatest common divisor. For more than two integers, factor all the integers and find the least exponents across the corresponding factors in all of the factorizations.

For an example use, reduce a fraction $a/b = 1350/1400$ to its simplest form. To do so, divide the top and bottom by $d = 50$. Then $a/b = 1350/1400 = 27/28$.

Now we can state the requirement about divisibility given some factors:

> If two relatively prime integers a and b both divide c, then ab divides c.

Some other properties of the gcd:

- Because the gcd is positive, $(a, b) = (|a|, |b|)$.
- $(a, b) = (b, a)$
- If the gcd of two numbers is 1, or $(a, b) = 1$, then a and b are called **relatively prime**.

4 Least common multiple

Before the other method for finding the gcd, we consider one related quantity.

> The least common multiple, often written $\operatorname{lcm}(a, b)$, is the least number $L \geq a$ and $L \geq b$ such that $a \mid L$ and $b \mid L$.

There are clear, every day uses. Think of increasing a recipe when you can only buy whole bags of some ingredient. You need to find the least common multiple of the recipe's requirement and the bag's quantity. Or when you need to find the next day two different schedules intersect.

Again, you can work from the prime factorizations

$$\begin{aligned} a &= 1400 = 2^{\mathbf{3}} \cdot 3^0 \cdot 5^{\mathbf{2}} \cdot 7^{\mathbf{1}}, \text{ and} \\ b &= 1350 = 2^1 \cdot 3^{\mathbf{3}} \cdot 5^{\mathbf{2}} \cdot 7^0. \end{aligned}$$

Now the least common multiple is the product of the *larger* exponents,

$$\operatorname{lcm}(a, b) = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^1 = 37\,800.$$

And for more than two integers, take the maximum across all the exponents of corresponding factors.

Another relation for two integers a and b is that

$$\operatorname{lcm}(a, b) = \frac{ab}{d}.$$

So given $a = 1350$, $b = 1400$, and $d = 50$,

$$\operatorname{lcm}(1350, 1400) = \frac{1350 \cdot 1400}{50} = \frac{1\,890\,000}{50} = 37\,800.$$

This does not hold directly for more than two integers.

5 Euclidean GCD algorithm

Another method for computing the gcd of two integers a and b is due to Euclid. This often is called the first algorithm expressed as an abstract sequence of steps.

We start with the division form of b in terms of $a \neq 0$,

$$b = qa + r \text{ with } 0 \leq r < a.$$

Because $(a, b) = (|a|, |b|)$, we can assume both a and b are non-negative. And because $(a, b) = (b, a)$, we can assume $b \geq a$.

Let $d = (a, b)$. Last week we showed that if $d|a$ and $d|b$, then $d|ra + sb$ for any integers r and s. Then because $d|a$ and $d|b$, we have $d|b - qa$ or $d|r$. So we have that $d = (b, a)$ also divides r. Note that any number that divides a and r also divides b, so $d = (a, r)$.

Continuing, we can express a in terms of r as

$$a = q'r + r' \text{ with } 0 \leq r' < r.$$

Now $d|r'$ and $d = (r, r')$. Note that $r' < r < a$, so the problem keeps getting smaller! Eventually, some remainder will be zero. Then the *previous* remainder is the greatest common divisor.

1. Find q_0 and r_0 in $b = q_0 a + r_0$ with $0 \leq r_0 < a$.
2. If $r_0 = 0$, then $(a, b) = a$.
3. Let $r_{-1} = a$ to make the loop easier to express.
4. Then for $i = 1, \ldots$
   (a) Find q_i and r_i in $r_{i-2} = q_i r_{i-1} + r_i$ with $0 \leq r_i < r_{i-1}$.
   (b) If $r_i = 0$, then $(a, b) = r_{i-1}$ and quit.
   (c) Otherwise continue to the next i.

Consider calculating $(53, 77)$. Following the steps, we have

$$\begin{aligned} 77 &= 1 \cdot 53 + 24, \\ 53 &= 2 \cdot 24 + 5, \\ 24 &= 4 \cdot 5 + 4, \\ 5 &= 1 \cdot 4 + 1, \text{ and} \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

And thus $(53, 77) = 1$.

For another example, take $(128, 308)$. Then

$$\begin{aligned} 308 &= 2 \cdot 128 + 52, \\ 128 &= 2 \cdot 52 + 24, \\ 52 &= 2 \cdot 24 + 4, \text{ and} \\ 24 &= 6 \cdot 4 + 0. \end{aligned}$$

So $(128, 308) = 4$.

6 Linear Diophantine equations

Later in the semester, we will examine linear equations $ax + by = c$ over real numbers. But many every-day applications require integer solutions. We can use the Euclidean algorithm to find one integer solution to $ax + by = c$ or prove there are none. Then we can use the computed gcd to walk along the line to all integer solutions.

Say we need to solve $ax + by = c$ for integers a, b, and c to find **integer** solutions x and y.

Let $d = (a, b)$. Then, as before, $d \mid ax + by$ for all integers x and y. So $d \mid c$ for any solutions to exist. If $d \nmid c$, then there are **no integer solutions**. If a and b are relatively prime, then $(a, b) = 1$ and solutions exist for any integer c.

Consider solving $ax + by = d$. Because $d \mid c$, we can multiply solutions to $ax + by = d$ by c/d to obtain solutions of $ax + by = c$. To solve $ax + by = d$ we work backwards after using the Euclidean algorithm to compute $d = (a, b)$.

Say the algorithm required k steps, so $d = r_{k-1}$. Working backward one step,

$$\begin{aligned} d = r_{k-1} &= r_{k-3} - q_{k-1}r_{k-2} \\ &= r_3 - q_{k-1}(r_{k-4} - q_{k-2}r_{k-3}) \\ &= (1 + q_{k-1}q_{k-2})r_3 - q_{k-1}r_{k-4}. \end{aligned}$$

So $d = r_{k-1} = i \cdot r_{k-3} + j \cdot r_{k-4}$ where i and j are integers. Continuing, the gcd d can be expressed as an integer combination of each pair of remainders.

Returning to the example of $(77, 53)$,

$$\begin{aligned} 1 &= 5 - 1 \cdot 4, \\ &= 5 - 1 \cdot (24 - 5 \cdot 5) = 5 \cdot 5 - 1 \cdot 24 \\ &= 5 \cdot (53 - 2 \cdot 24) - 1 \cdot 24 = 5 \cdot 53 - 11 \cdot 24 \\ &= 5 \cdot 53 - 11 \cdot (77 - 1 \cdot 53) = 16 \cdot 53 - 11 \cdot 77. \end{aligned}$$

To solve $53x + 77y = 22$, we start with $53 \cdot 16 + 77 \cdot (-1) = 1$. Multiplying by 22,

$$53 \cdot (16 \cdot 22) + 77 \cdot (-1 \cdot 22) = 22,$$

and $x = 352$, $y = -22$ is one solution.

But if there is one solution, there are infinitely many! Remember that $d = (a, b)$, so a/d and b/d are integers. Given one solution $x = x_0$ and $y = y_0$, try substituting $x = x_0 + t \cdot (b/d)$ and $y = y_0 - t \cdot (a/d)$ for any integer t. Then

$$\begin{aligned} a(x_0 + t \cdot (b/d)) + b(x_0 - t \cdot (a/d)) &= ax_0 + bx_0 + t \cdot (ab/d)) + -t \cdot (ba/d)) \\ &= ax_0 + bx_0 = c. \end{aligned}$$

Actually, *all* integer solutions to $ax + by = c$ are of the form

$$x = x_0 + t \cdot (b/d), \quad \text{and} \quad y = y_0 - t \cdot (a/d),$$

where t is any integer, $d = (a, b)$, and x_0 and y_0 are a solution pair.

Another example, consider solving $12x + 25y = 331$. First we apply the Euclidian algorithm to compute $(12, 25) = 1$:

$$\begin{aligned} 25 &= 2 \cdot 12 + 1, \text{ and} \\ 12 &= 12 \cdot 1 + 0. \end{aligned}$$

Substituting back,

$$12 \cdot (-2) + 25 \cdot 1 = 1, \text{ and} 12 \cdot (-662) + 25 \cdot 331 \qquad = 331.$$

So we can generate any solution to $12x + 25y = 331$ with the equations

$$x = -662 + 25t \quad \text{and} \quad y = 331 - 12t.$$

Using these, we can find a "smaller" solution. Try making x non-negative with

$$\begin{aligned} -662 + 25t &\geq 0, \\ 25t &\geq 662, \text{ thus} \\ t &> 26. \end{aligned}$$

Substituting $t = 27$,

$$x = 13, \quad \text{and} \quad y = 7.$$

Interestingly enough, this must be the *only* non-negative solution. A larger t will force y negative, and a smaller t forces x negative. But the solution for $t = 26$ is still "small",

$$x = -12, \quad \text{and} \quad y = 19.$$

7 Homework

Practice is absolutely critical in this class.

Groups are fine, turn in your own work. Homework is due in or before class on Mondays.

- Problem set 4.3, p264:
  - 6, 7, 13 (using any method, not the specified one), 15, 18, 25
- Compute the following using **both** the prime factorization method and the Euclidean algorithm:
  - $(720, 241)$
  - $(64, 336)$
  - $(-15, 75)$
- Compute the least common multiples:
  - $\text{lcm}(64, 336)$
  - $\text{lcm}(11, 17)$
  - $\text{lcm}(121, 187)$
  - $\text{lcm}(2025, 648)$

- Find **two** integer solutions to each of the following, or state why no solutions exist:
  - $64x + 336y = 32$
  - $33x - 27y = 11$
  - $31x - 27y = 11$

Note that you *may* email homework. However, I don't use Microsoft™ products (*e.g.* Word), and software packages are notoriously finicky about translating mathematics.

If you're typing it (which I advise just for practice in whatever tools you use), you likely want to turn in a printout. If you do want to email your submission, please produce a PDF or PostScript document.