Math 202 notes

Jason Riedy

29 September, 2008

Contents

Notes also available as PDF.

This week, we will cover the following topics from Chapter 4 and Chapter 5:

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

I'm pulling modular arithmetic (clock arithmetic) from Chapter 5 because it explains divisibility rules. We'll return to the clock form in the future.

Once upon a time, number theory was both decried and revered as being "pure mathematics" with no practical applications. That is no longer remotely true. There are oblique applications in error correction (*e.g.* how CDs still play when scratched), but one overwhelming, direct application is in **encryption**.

So I also will discuss at some point

- Euler's totient function ($\phi(n)$) and the RSA encryption algorithm.

The RSA algorithm is at the core of the ***s**ecure **s**ocket **l**ayer* (SSL) protocol used to secure web access (the `https` prefix, colored locks, *etc.*).

1 Divisibility

When defining operations on integers, we skipped division. As with subtraction, the integers are not closed over division; $1/2$ is not an integer. So we define division implicitly.

For any integers a and b, we can write

$$b = q \cdot a + r,$$

where q is an integer called the **quotient**, and $r < |a|$ is a *non-negative* integer called is the **remainder**, **residue**, or **residual**. We will see that requiring $0 \leq r < |a|$ is very important and makes division well-defined.

Then a **divides** b, or $a \mid b$, when $r = 0$. Alternately, b is a **multiple** of a and a is a **divisor** of b. If we cannot write $b = q \cdot a + r$ with $r = 0$, then a does not divide b, or $a \nmid b$. When $a \mid b$, then we define division as $b/a = q$.

For example,

$$\begin{aligned} 14 &= 2 \cdot 7 + 0, \text{ so } 7 \mid 14 \text{ and } 14/7 = 2, \text{ and} \\ 20 &= 2 \cdot 7 + 6, \text{ so } 7 \nmid 20 \text{ and } 20/7 \text{ is not an integer.} \end{aligned}$$

In the latter case, though, $20/7 = 2 + 6/7$, which rounds down to 2.

Some other examples showing extreme and negative cases,

$$\begin{aligned} -6 &= -3 \cdot 2 + 0, \text{ so } 2 \mid -6 \text{ and } -6/2 = -3, \\ -6 &= 3 \cdot -2 + 0, \text{ so } -2 \mid -6 \text{ and } -6/-2 = 3, \\ 6 &= -3 \cdot -2 + 0, \text{ so } -2 \mid 6 \text{ and } 6/-2 = -3, \\ -7 &= -4 \cdot 2 + 1, \text{ so } 2 \nmid -7, \\ -7 &= 4 \cdot -2 + 1, \text{ so } -2 \nmid -7, \\ 7 &= -3 \cdot -2 + 1, \text{ so } -2 \nmid 7 \text{ (}\textbf{note}\text{: not } -4 \cdot -2 - 1), \\ 5 &= 0 \cdot 10 + 5, \text{ so } 10 \nmid 5, \text{ and} \\ 0 &= 0 \cdot 13 + 0, \text{ so } 13 \mid 0 \text{ and } 0/13 = 0. \end{aligned}$$

What about when $a = 0$? Then $b = q \cdot 0 + b$ is true for any quotient q. Without further restrictions on q, division by zero is not be well-defined. In calculus and some applications, there are times when you fill in the hole left by a division by zero by some obvious completion.

But is the form $b = qa + r$ well-defined when $a \neq 0$?

Theorem: The expansion $b = qa + r$ with $0 \leq r < |a|$ is unique for $a \neq 0$, so division is well-defined.

Proof. We begin by assuming there are two ways of expanding $b = qa + r$. Then we show that the forms must be identical.

Let there be two distinct ways of writing $b = qa + r$ with $a \neq 0$,

$$b = q_1 a + r_1, \text{ and}$$
$$b = q_2 a + r_2,$$

with $0 \leq r_1 < |a|$ and $0 \leq r_2 < |a|$.

If $r_1 = r_2$, then $b - r_1 = b - r_2$. From the equations above $b - r_1 = q_1 a$ and $b - r_2 = q_2 a$, so $q_1 a = q_2 a$ or $(q_1 - q_2)a = 0$. Because $a \neq 0$, $q_1 = q_2$ and the forms are identicall.

For $r_1 \neq r_2$, we know one of them is larger. *Without loss of generality*, assume $r_1 < r_2$. Then there is some positive integer k such that increases r_1 to match r_2, or $r_2 = r_1 + k$. Note that $k \leq r_2$.

Substituting for r_2, we see that $b = q_2 a + r_1 + k$, or equivalently $b - k = q_2 a + r_1$. Now we can subtract this equation from $b = q_1 a + r_1$ to obtain

$$k = (q_1 - q_2)a = z \cdot a + 0$$

for some quotient z.

So $a \mid k$, but $k \leq r_2 < |a|$. The only way we can satisfy this is if $q_1 - q_2 = 0$ and $q_1 = q_2$. Thus also $k = 0$ and $r_1 = r_2$. So we cannot have to different ways to write $b = q \cdot a + r$, and our form of division is well-defined. □

Some useful properties of divisibility:

- If $d \mid a$ and $d \mid b$, then $d \mid ra + sb$ for all integers r and s. A quick proof: $a = q_a d$ and $b = q_b d$, so $ra + sb = rq_a d + sq_b d = (rq_a + sq_b)d$, then $d | ra + sb$.
- If $a \mid b$ and $b \mid c$, then $a \mid c$. Quick proof: $b = q_a a$, $c = q_b b$, so $c = q_b(q_a a) = (q_b q_a)a$.
- If $a \mid bc$ and $a \nmid b$, then $a \mid c$.

2 Primes

Divisibility gives a numbers a multiplicative structure that's different than the digit-wise structure we previously examined.

To build the structure, we start from numbers which cannot be decomposed. An integer $p > 1$ is called a **prime** number if its only divisors are 1 and p itself. We will explain why 1 is not considered prime when we discuss factorization. All other numbers are **composite** and must have some prime divisor.

Consider possible *divisors* of 11,

$$\begin{aligned} 11 &= 11 \cdot 1 + 0 \text{ so } 1 \mid 11, \\ 11 &= 5 \cdot 2 + 1 \text{ so } 2 \nmid 11, \text{ and} \\ 11 &= 3 \cdot 3 + 2 \text{ so } 3 \nmid 11. \end{aligned}$$

We can stop at 3. Because multiplication is commutative, any divisors come in pairs. The smaller of the pair must be $\leq \sqrt{11} \approx 3.3$; that's the point where any pairs $a \cdot b$ are repeated as $b \cdot a$.

So the only divisor less than $\sqrt{11}$ is 1, and 11 is prime.

How many primes are there?
Theorem: There are infinitely many primes.

Proof. Assume there are only k primes $p_1, p_2, \ldots, p_k$ and all other numbers are composite. Then let $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$, one larger than the product of all primes.

Consider dividing n by some prime, say p_k. Then we can write $n = (p_1 \cdot p_2 \cdot \cdots \cdot p_{k-1})p_i + 1$. Given the form is unique and $r = 1$, p_k does not divide n. We could have chosen any of the primes, so $p_i \nmid n$ for all $i = 1, \ldots, k$. Thus no prime divides n.

For a number n to be composite, it must have some factor or divisor other than 1 and n. If that factor is not prime, then the factor has another factor, and so forth until you reach some prime. Because of transitivity of division ($a \mid b$ and $b \mid c$ imply $a \mid c$), the prime must divide n. Here, though, no primes divide n, so n cannot be composite and must be prime itself.

So assuming there are k primes leads to a contradiction because we can construct one more. Thus there are either no primes or infinitely many. We demonstrated that 11 is prime, so there must be infinitely many primes. □

There are mountains of unanswered questions about prime numbers. Consider the pairs of primes $(3, 5)$, $(5, 7)$, $(11, 13)$, and $(17, 19)$. Each are separated by two. Are there infinitely many such pairs? No one knows. Similarly, there are **Mersenne primes** of the form $2^n - 1$. No one knows how many Mersenne primes exist.

3 Factorization

A **factorization** of a number is a decomposition into factors. So $24 = 8 \cdot 3$ is a factorization of 24, as is $24 = 4 \cdot 2 \cdot 3$. A **prime factorization** is a factorization

into primes. Here $24 = 2 \cdot 2 \cdot 2 \cdot 3$ is a prime factorization of 24. We use exponents to make this easier to write, and $24 = 2^3 \cdot 3$.

You can be systematic about prime factorization and discover the primes through the **sieve of Eratosthenes**. Consider finding a prime factorization of 110.

We start just by writing possible factors. Technically we need integers only $\leq \sqrt{1100} \approx 33.6$, but we only fill enough here to demonstrate the point.

	2	**3**	*4*	**5**	*6*	**7**	*8*	*9*	*10*
11	*12*	**13**	*14*	*15*	*16*	**17**	*18*	**19**	*20*

The first possible factor is 2, and $2 \mid 1100$. We divide by two until the result is not divisible by 2. This gives $1100 = 2^2 \cdot 275$. Then we cross out all multiples of 2; these cannot divide 275. Because $275 = 91 \cdot 3 + 2$, $3 \nmid 275$. But we also know no multiples of 3 divide 275, so we cross out all remaining multiples of 3.

The next not crossed out is 5, which divides 275. Now $1100 = 2^2 \cdot 5^2 \cdot 11$. We showed 11 is prime before, but let's continue this method. Cross out all multiples of five. The next number to try is 7, which does not divide 11. But we can cross out all multiples of 7. The next free number is 11, which we have again shown to be prime.

In our (short) list, it happens that only primes remain. We have sieved out all the non-primes. Actually, once we removed all multiples of primes $\leq \sqrt{20}$, only primes remained.

Moving from one prime to the next is a systematic method both for finding prime numbers and for finding a prime factorization.

Factorizations provide a useful mechanism for working

We will not prove the following, but is often called the **fundamental theorem of arithmetic**:
Theorem: Every integer greater than one has a unique prime factorization.

4 Modular Arithmetic

Factorization itself will prove useful later. Now we will explore modular arithmetic and find some quick rules for determining when $d \mid a$ for some d.

Modular arithmetic is arithmetic on remainders.

Consider expressions of 7 and 4 in terms of multiples of 3 plus remainders: $7 = 2 \cdot 3 + 1$ and $4 = 1 \cdot 3 + 1$. Now $11 = 7 + 4 = (2 \cdot 3 + 1) + (1 \cdot 3) + 1 = 3 \cdot 3 + 2$. Note that the sum of the remainders was < 3 and was the new remainder itself.

If the remainder is ≥ 3, we can just pull a three out of it: $11 + 8 = (3 \cdot 3 + 2) + (2 \cdot 3 + 2) = 5 \cdot 3 + 4$. To convert this into the correct form, note that

$4 = 1 \cdot 3 + 1$, and $19 = 5 \cdot 3 + (1 \cdot 3 + 1) = 6 \cdot 3 + 1$. We need consider only the sum of remainders to compute the result's remainder.

The remainder of the sum just wraps around. Think about time. If you add a few hours and cross 12, the result just wraps around. So 1:00 is the same as 13:00 or 25:00.

We don't identify 1:00 as just one time but a member of a set of all times that are one hour after a multiple of 12. Similarly, we can identify numbers as elements of sets where all members have the same remainder relative to a given divisor.

The **congruence class** of r **modulo** a is $\{x \mid \exists q : x = qa + r\}$. If a number b is in the congruence class of r modulo a, we write $b \equiv r \pmod{a}$.

The canonical member of a congruence class is its least positive member. Just as we don't naturally consider 25:00 as 1:00, we tend to identify congruence classes by the least r. So while $13 \equiv 87 \pmod{2}$ is correct (both 13 and 87 are odd), we prefer $13 \equiv 1 \pmod{2}$.

We define addition and multiplication on entire congruence classes. For the operation to be defined, the **modulus** of each class must be the same. Then we're adding numbers of the form $b_1 = q_1 a + r_1$ for $b_1 \equiv r_1 \pmod{a}$ and $b_2 = q_2 a + r_2$ for $b_2 \equiv r_2 \pmod{a}$. As in our example above, the remainders add. Here $b_1 + b_2 = q_1 a + r_1 + q_2 a + r_2 = (q_1 + q_2)a + (r_1 + r_2) \equiv r_1 + r_2 \pmod{a}$.

Identifying congruence classes by their least positive element, we can write a table showing all additions modulo 4:

$+ \pmod 4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Addition of congruence classes maintains the **additive identity** that we expect, $b + 0 \equiv b \pmod{a}$.

Note that every class has an **additive inverse**, a class where $b + (-b) \equiv 0 \pmod{a}$. Remember that we forced the residual to be positive when we defined division. Then we can see that the inverse of 1 modulo 4 is $-1 = -1 \cdot 4 + 3 \equiv 3 \pmod{4}$.

Another way to see this is that the canonical representation of $-b$ is the least number which increases b to be equal to the modulus a. So the inverse of 1 is 3 because $1 + 3 = 4 \equiv 0 \pmod{4}$.

We also define multiplication on congruence classes.

If $b_1 = q_1 a + r_1$ and $b_2 = q_2 a + r_2$, then

$$\begin{aligned} b_1 \cdot b_2 &= (q_1 a + r_1) \cdot (q_2 a + r_2) \\ &= q_1 q_2 a^2 + q_1 r_2 a + q_2 r_1 a + r_1 r_2 \\ &= (q_1 q_2 a + q_1 r_2 + q_2 r_1) a + r_1 r_2 \\ &\equiv r_1 r_2 \pmod{a}. \end{aligned}$$

So we need only multiply remainders.

Identifying congruence classes by their least positive element, we can write a table showing all multiplications modulo 4:

$\times \pmod 4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Again, there is a **multiplicative identity**, $b \cdot 1 \equiv b \pmod{a}$.

Unlike plain integer division, some congruence classes have an inverse. The only integer that has an integer inverse is 1. But modulo 4, both 1 and 3 have **multiplicative inverses**. Here $3 \cdot 3 = 9 \equiv 1 \pmod 3$.

5 Divisibility Rules

Using modular arithmetic and positional notation, we can derive some quick divisibility tests.

First, consider divisibility by powers of 2 and 5. The factorization of $10 = 2 \cdot 5$, and so $10^k = 2^k \cdot 5^k$. So $2^k \mid 10^k$ and $5^k \mid 10^k$, or $10^k \equiv 0 \pmod 2^k$ and $10^k \equiv 0 \pmod 5^k$.

Now remember how to expand positional notation. We know that $1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4$. So $1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \equiv 0 + 0 + 0 + 4 \pmod 2 \equiv 0 \pmod 2$. Divisibility by 2 depends only on the final digit. Similarly, $1234 \equiv 0 + 0 + 0 + 4 \pmod 5$, and divisibility by 5 depends only on the final digit.

For $2^2 = 4$ and $5^2 = 25$, all but the last two digits are equivalent to zero. And for $2^3 = 8$ and $5^3 = 125$, all but the last three digits are equivalent to zero. So one divisibility rule:

> When testing for divisibility by 2^k or 5^k, we need only consider the last k digits.

Now consider divisibility by 3 or 9. We know that $10 \equiv 1 \pmod 3$ and $10 \equiv 1 \pmod 9$. Using modular arithmetic, $123 = 1 \cdot 10^2 + 2 \cdot 10 + 3 \equiv 1 + 2 + 3$

$(\text{mod } 3) \equiv 6 \pmod 3 \equiv 0 \pmod 3$. Hence $3 \mid 123$ because the sum of its digits is divisible by 3.

Similarly, $10 \equiv 1 \pmod 3$. So $123 \equiv 1+2+3 \pmod 9 \equiv 6 \pmod 9$, and $9 \nmid 123$. If the sum of the digits is greater than 9, simply add those digits.

> Test for divisibility by 3 or 9 by adding the number's digits and checking that sum. If that sum is greater than 9, add the digits again. Repeat until the result is obvious.

Other primes are not so straight-forward. Divisibility by 7 is a pain; there is an example method in the text's problems for Section 5.1.

The rule for 11 is worth exploring. Because $10 < 11$, the canonical member of its congruence class is just 10. But there is another member of interest, $10 \equiv -1 \pmod 1 1$. So you can alternate signs on alternate digits from the right. So $123456 \equiv -1+2-3+4-5+6 \equiv 3 \pmod 1 1$, and $11 \nmid 123456$.

For divisibility by 6, 12, 18, or other composite numbers, factor the divisor and test for divisibility by each factor. To test for divisibility by $72 = 2^3 \cdot 3^2 = 8 \cdot 9$, test for divisibility by 8 and by 9.

6 Homework

- Problem Set 4.1 (p242):
  - Problem 2, but don't repeat the drawings.
  - 4, 7, 9, 10, 13, 14, 23, 24
- Also draw diagrams showing that $8 \nmid 18$ and $3 \nmid 11$.
- Problem Set 4.2 (p252):
  - 1, 2, 8, 14, 15
- Take a familiar incomplete integer, _679_. Using the expression of _679_ as $N = 10^4 \cdot x_4 + x_0 + 6790$, use $8 \mid N$ to find x_0? Given that, use $9 \mid N$ to find x_4. Now if 72 turkeys cost $_679_, what is the total?