MATH 4573 Elementary Number Theory

In Person Notes, Spring 2020

July 21, 2021

Contents

1 Monday: Introduction and Divisibility

1.1 Introduction

Roll

What is number theory?

Elementary number theory is the study of integers, especially the positive integers. A lot of the course focuses on prime numbers, which are the multiplicative building blocks of the integers. Another big topic in number theory is integer solutions to equations such as the Pythagorean triples $x^2+y^2=z^2$ or the generalization $x^n+y^n=z^n$. Proving that there are no integer solutions when $n>2$ was an open problem for close to 400 years.

Go over syllabus

Think-Pair-Share. What makes for productive group work?

1.2 Divisibilty

The goal of this chapter is to build us up towards the fundamental theorem of arithmetic, namely unique prime factorization of natural numbers.

Ask: what is a definition for "a divides b"?

Definition. Let $a, b \in \mathbb{Z}$. If there is an integer x such that $b = ax$, and we write $a \mid b$. int he case b is not divisible by a, we write $a \nmid b$.

If $a \mid b$ we say that a is a divisor of b.

Note that 0 is not a divisor of any integer other than itself. Also all integers are divisors of 0, as odd as that sounds at first.

Some basic facts about divisibility:

Theorem 1. *(i) $a \mid b$ implies $a \mid bc$ for any integer c*

(ii) $a \mid b$ and $b \mid c$ imply $a \mid c$

(iii) $a \mid b$ and $a \mid c$ imply $a \mid bx + cy$ for any integers x, y

(iv) $a \mid b$ *and* $b \mid a$ *impy* $a = \pm b$

(v) $a \mid b$, $a > 0$, $b > 0$, *imply* $a \leq b$

(vi) if $m \neq 0$, $a \mid b$ *implies and is implied by* $ma \mid mb$.

Proof. We will only prove part 3 directly, as it is by far the most useful fact about divisibility. We'll use it a bunch. For the most part, these follow fairly directly from applying the definition of divisibilty and slight manipulation. Let's reemphasize that: apply the definition and slightly manipulate it.

Let's see this in part 3.

Since $a \mid b$ and $a \mid c$, we can write $b = ja$ and $c = ka$ for some integers x and y. Then for any integers x, y, we have that

$$bx + cy = (ja)x + (ka)y = a(jx + ky).$$

Since $jx + ky$ is the sum and product of integers, it is also an integer and so, by the definition of divisibility, $a \mid bx + cy$.

□

Think-Pair-Share. Prove: $a \mid b$ and $b \mid c$ imply $a \mid c$, (that is, division is *transitive*).

Proof. Since $a \mid b$ and $b \mid c$, there exist $e, f \in \mathbb{Z}$ such that $b = ae$ and $c = bf$. Then $c = (ae)f = a(ef)$, so $a \mid c$. □

2 Wednesday: Division algorithm, greatest common divisors, Euclidean algorithm

Preclass assignment. Problem 1 Section 3.1:

$[\frac{3}{2}] = 1, [-\frac{3}{2}] = -2, [\pi] = 3, [-7] = -7$, and $[x] = 0$ for $0 \leq x \leq 1$.

Problem 3e Section 4.1:

For what real numbers x is it true that $[9x] = 9$?

Solution. Let $[9x] = k$. Then $k \leq 9x < k + 1$ by the definition of the greatest integer (or floor) function. Thus, the equation is true when $\frac{k}{9} \leq x < \frac{k+1}{9}$. □

Definition. For real x, the symbol $[x]$ denotes the greatest integer less than or equal to x. This is also called the *floor function* and written $\lfloor x \rfloor$.

2.1 Division algorithm

Think-Pair-Share. Prove: If $x \in \mathbb{R}$, then $x - 1 < [x] \leq x$.

Solution. By definition, there exists an integer k such that $[x] = k$ and $k \leq x < k + 1$. Then we can replace k with $[x]$. This gives $[x] \leq x < [x] + 1$. Immediately, we have $[x] \leq x$. Subtraction 1 from both parts of the second inequality, we get $x - 1 < [x]$. □

Theorem 2 (The Division Algorithm, Textbook theorem 1.2)**.** *Let* $a, b \in \mathbb{Z}$ *with* $b > 0$. *Then there exists a unique* $q, r \in \mathbb{Z}$ *such that*

$$a = bq + r, \quad 0 \leq r < b.$$

Proof. Let $q = \left[\frac{a}{b}\right]$ and $r = a - b\left[\frac{a}{b}\right]$. Then $a = bq + r$ by rearranging the equation. Now we need to show $0 \leq r < b$.

Since $x - 1 < [x] \leq x$, we have

$$\frac{a}{b} - 1 < \left[\frac{a}{b}\right] \leq \frac{a}{b}.$$

Multiplying all terms by $-b$, we get

$$-a + b > -b\left[\frac{a}{b}\right] \geq -a.$$

Adding a to every term gives

$$b > a - b\left[\frac{a}{b}\right] \geq 0.$$

By the definition of r, we have shown $0 \leq r < b$.

Finally, we need to show that q and r are unique. Assume

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

$$a = bq_2 + r_2, \quad 0 \leq r_2 < b.$$

We need to show $q_1 = q_2$ and $r_1 = r_2$. We can subtract the two equations from each other.

$$\begin{aligned} a &= bq_1 + r_1, \\ \underline{-(a &= bq_2 + r_2)}, \\ 0 &= bq_1 + r_1 - bq_2 - r_2 = b(q_1 - q_2) + (r_1 - r_2). \end{aligned}$$

Rearranging, we get $b(q_1 - q_2) = r_1 - r_2$. Thus, $b \mid r_1 - r_2$. From rearranging the inequalities:

$$\begin{aligned} 0 \leq r_1 &< b \\ \underline{-b < -r_2 &\leq 0} \\ -b < r_1 - r_2 &< b. \end{aligned}$$

Thus, the only way $b \mid r_1 - r_2$ is that $r_1 - r_2 = 0$ and thus $r_1 = r_2$. Now, $0 = b(q_1 - q_2) + (r_1 - r_2)$ becomes $0 = b(q_1 - q_2)$. Since we assumed $b > 0$, we have that $q_1 - q_2 = 0$. □

Think-Pair-Share. Use the division algorithm on $a = 47, b = 6$ and $a = 281, b = 13$.

Solution. For $a = 47, b = 6$, we have that $a = (7)6 + 5, q = 7, r = 5$.

For $a = 281, b = 13$, we have that $a = (21)13 + 8, q = 21, r = 8$. □

2.2 Greatest common divisor

Definition. If $a \mid b$ and $a \mid c$ then a is a *common divisor* of b and c.

If at least one of b and c is not 0, the greatest (positive) number among their common divisors is called the *greatest common divisor of a and b* and is denoted $gcd(a, b)$ or just (a, b).

If $gcd(a, b) = 1$, we say that a and b are *relatively prime*.

If we want the greatest common divisor of several integers at once we denote that by $(b_1, b_2, b_3, \ldots, b_n)$.

For example, $(4, 8)$ is 4 but $(4, 6, 8)$ is 2.

The GCD always exists. How to show this: 1 is always a divisor, and no divisor can be larger than the maximum of $a + b$. So there is a finite number of divisors, thus there is a maximum.

Definition (Well ordering principle)**.** Every nonempty set of positive integers contains a least element.

Proposition 3. *[Textbook Theorem 1.4] Let $a, b \in \mathbb{Z}$ with a, b not both zero. Then $(a, b) = \min\{ma + bn : m, n \in \mathbb{Z}, ma + nb < 0\}$.*

Proof. Since, without loss of generality, $a \neq 0$, either $1a + 0b > 0$ or $-1a + 0b > 0$. So $\min\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$ exists by the well ordering principle. Then $\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\} \neq \emptyset$. □

Think-Pair-Share. Prove: For any positive integer k, $(ka, kb) = k(a, b)$.

Solution. By the previous theorem,

$$\begin{aligned}(ka, kb) &= \min\{mka + bkn : m, n \in \mathbb{Z}, mka + nkb < 0\} \\ &= \min\{k(ma + bn) : m, n \in \mathbb{Z}, ma + bn < 0\} \\ &= k * \min\{ma + bn : m, n \in \mathbb{Z}, ma + bn < 0\} \\ &= k(a, b)\end{aligned}$$

□

There are many more facts about greatest common divisors in the textbook and homework. The last one we will prove right now is:

Lemma 4. *If $a, b \in \mathbb{Z}, a \geq b > 0$, and $a = bq + r$ with $q, r \in \mathbb{Z}$, then $(a, b) = (b, r)$.*

Proof. Let c be a common divisor of a and b. Then $c \mid a$ and $c \mid b$ implies $c \mid a - bq$ by Theorem 1 part (iii). By definition, $a - bq = r$. That is, $c \mid r$.

Since c is any common divisor of a and b, we find that the greatest common divisor (a, b) is also a common divisor of b and r. If we can show any common divisor of b and r is a common divisor of a and b, we are done.

Let d be a common divisor of b and r. Then we have that $d \mid bq + r$, so $d \mid a$.

Thus, every common divisor of a and b is a common divisor of b and r and vice versa. Since the common divisors are the same, the greatest common divisors are also the same. □

Theorem 5 (Euclidean algorithm,Textbook Theorem 1.11)**.** *Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the division algorithm, there exist $q_1, r_1 \in \mathbb{Z}$ such that*

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

If $r_1 > 0$, (by the division algorithm) there exist $q_2, r_2 \in \mathbb{Z}$ such that

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 > 0$, (by the division algorithm) there exist $q_3, r_3 \in \mathbb{Z}$ such that

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

Continuing this process, $r_n = 0$ for some n. If $n > 1$, then $(a, b) = r_{n-1}$. If $n = 1$, then $(a, b) = b$.

Proof. Note that $r_1 > r_2 > r_3 > \cdots \geq 0$ by construction. If the sequence did not stop, then we would have an infinite, decreasing sequence of positive integers, which is not possible. Thus, $r_n = 0$ for some n.

When $n = 1$, $a = bq + 0$ and $(a, b) = b$.

If $n > 1$, then by repeated application of the previous lemma, we have

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1})$$

Then $r_{n-2} = r_{n-1} q_n + 0$. Thus $(r_{n-2}, r_{n-1}) = r_{n-1}$. □

The Euclidean algorithm allows us to write the gcd (a, b) as a linear combination of a and b. That is $(a, b) = ma + by$ for some $m, n \in \mathbb{Z}$.

Think-Pair-Share. Use the Euclidean algorithm to find $(803, 154)$. Then find $(803, 154)$ as a linear combination of 803 and 154.

Possible: LCM

2.3 Primes

Definition. Let $p \in \mathbb{Z}$ with $p > 1$. Then p is *prime* if and only if the only positive divisors of p are 1 and p. If $n \in \mathbb{Z}$, $n > 1$ and not prime, then n is *composite*.

Lemma 6 (Textbook Theorem 1.14)**.** *Every integer greater than 1 has a prime divisor.*

Proof. Assume by contradiction that there exists $n \in \mathbb{Z}$ greater than 1 with no prime divisor. By the well ordering principle, we may assume n is the least such integer. By definition, $n \mid n$, so n is not prime. Thus, n is composite and there exists $a, b \in \mathbb{Z}$ such that $n = ab$ and $1 < a < n$, $1 < b < n$. Since $a < n$, then it has a prime divisor p. But since $p \mid a$ and $p \mid n$, by Theorem 1(ii), $p \mid n$. This contradicts our assumption, so no such integer exists. □

Think-Pair-Share (Euclid, textbook Theorem 1.17)**.** Prove that there are infinitely many prime numbers.

Conjecture (Twin Prime Conjecture)**.** There are infinitely many prime numbers p for which $p + 2$ is also a prime number.

Contents

3 Monday: Greatest common divisor and Primes

Preclass assignment. Let $a = \prod_p p^{\alpha(p)}$ and $b = \prod_p p^{\beta(p)}$. What conditions must the exponents satisfy if $(a, b) = 1$?

Solution. At least one of $\alpha(p)$ and $\beta(p)$ is 0, otherwise p divides both a and b. Another way to say this is $\min\{\alpha(p), \beta(p)\} = 0$ for all primes p. □

Preclass assignment. How would the fundamental theorem of arithmetic (Theorem 1.16) change if we said 1 is a prime number?

Solution. There are several ways to answer this. The main difference some from the actual fundamental theorem of arithmetic is that $1 = 1 * 1 = 1 * 1 * 1 = \cdots$. □

3.1 Greatest common divisor problems

Think-Pair-Share (Textbook Theorem 1.4 parts 2)**.** The greatest common divisor of b and c is the positive common divisor of b and c that is divisible by every common divisor.

Proof. Let $g = (b, c) = \min\{ma + bn : m, n \in \mathbb{Z}, ma + nb > 0\}$. Then any common divisor d divides $g = xb + yc$ by Theorem 1.1. □

Think-Pair-Share (Textbook Theorem 1.10)**.** If $c \mid ab$ and $(b, c) = 1$, then $c \mid a$.

Proof. By Theorem 1.6, $(ab, ac) = a(b, c) = a$. By the hypothesis, $c \mid ab$ and by definition $c \mid ac$, so $c \mid a$ by Theorem 1.4 part 2. □

3.2 Primes

Why is 1 not prime?

It has to do with units and invertibility. The number 1 holds a special place. It is the multiplicative identity, i.e., anything multiplied by 1 is just that thing again. Something is said to be invertible in a "group" (more on that later) if there exist something, which, when multiplied to it, gives you 1. How many invertible elements are there among the integers? Just two. 1 and -1. And that's the key. If we want to extend our results from positive integers to non-zero integers, we often just need to take into account ± 1. That sounds obvious, but it turns out to be suprisingly critical and yet non-intuitive when we start moving from real integers to complex ones.

Theorem 7 (The Fundamental Theorem of Arithmetic, Textbook Theorem 1.14 and 1.16)**.** *Every integer $n \geq 2$ can be factored into a product of primes $n = p_1 p_2 p_3 \dots p_n$ in a unique way (up to rearrangement).*

Proof. We work by induction. We can check that $2 = 2$, $3 = 3$ and $4 = 2^2$ all have prime factorizations. So assume now that all numbers n in the range $2 \leq n < N$ can be factored in the specified way, and we will show that N can be factored this way as well. If N is prime, then N is its own prime factorization. Otherwise N is composite and has some factor $2 \leq n_1 < N$. Thus we can write $N = n_1 n_2$. But n_2 must also be in the range $2 \leq n_2 < N$. Therefore n_1 and n_2 must be factorable into primes, say $n_1 = p_1 p_2 \dots p_r$ and $n_2 = q_1 q_2 \dots q_s$. Then $N = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$. By induction, all integers $n \geq 2$ can be factored into a product of primes.

Now we must show this product is unique up to rearrangement. Suppose that n has two factorizations $p_1 p_2 \dots p_r$ and $q_1 q_2 \dots q_s$, and let us assume that $r \leq s$. By our previous theorem, since p_1 divides $q_1 q_2 \dots q_s$, it must divide one of the q_i's, and, by rearranging, we can assume that $p_1 \mid q_1$. But q_1 is prime and only has 1 and q_1 as prime factors, so therefore, $p_1 = q_1$. Therefore we have $p_2 p_3 \dots p_r = q_2 q_3 \dots q_s$.

We can repeat this process (and repeatedly rearrange the q_i's as necessary) to show that $p_2 = q_2$, and then $p_3 = q_3$, and so on until we show that $1 = q_{r+1} q_{r+2} \dots q_s$. If $s > r$, then the number on the right-hand side here is greater than 1, which is impossible, so we have that $r = s$ and $p_i = q_i$ for $1 \leq i \leq r$. This proves that the factorization is unique up to rearrangement. □

So let's suppose we want to factor an integer n. Let's start with $d = 2$.

We check to see if $d \mid n$. If it does, then we factor d out of n to get $n' = n/d$. We record the divisor d and henceforth work with n' in place of n, restarting at this step. Otherwise, we increment d by one and repeat this step.

Once $n = 1$, we have all the factors.

Now there are various ways we could try to speed this up. You might think we could only work with those trial divisors d that are prime, but it would take more time to check if d is a prime than it would to just see if it divides n. If it's composite, it won't, because we'll have already taken all its factors out of n beforehand.

One thing we can do is only check d up to $\sqrt{n}$. This is because n cannot have two prime factors that are each $> \sqrt{n}$. So if we reach this point, whatever n remains must be prime. So that takes us down from a worst case scenario of $d = n$ to a worst case scenario of $d = \sqrt{n}$. That's a big improvement. It's still very slow.

We can write out a prime factorization (of a positive integer) by

$$a = \prod_p p^{\alpha(p)}$$

where $\alpha(p)$ is the number of times p divides a evenly. Note that $\prod$ denote a product in the same way that $\sum$ denotes a sum, and that the subscript p means that the product ranges over all primes.

This is what we are doing when we write $12 = 2^2 \cdot 3$.

Definition. The integers $a_1, a_2, a_3, \ldots, a_n$, all nonzero, have a *common multiple* b if every $a_i \mid b$. The smallest number is the *least common multiple* written $[a_1, a_2, a_3, \ldots, a_n]$.

Common multiples always exist. For example, we can write $a_1 a_2 \cdots a_n$.

We can use this to give a quick version of the gcd and lcm. If a corresponds to $\alpha(p)$ and b to $\beta(p)$, then

$$(a,b) = \prod_p p^{\min\{\alpha(p),\beta(p)\}} \qquad [a,b] = \prod_p p^{\max\{\alpha(p),\beta(p)\}}$$

This is a very useful fact for proofs.

Lemma 8. *Let $a, b \in \mathbb{Z}$ be positive integers. Then $(a,b)[a,b] = ab$.*

Proof. Note that $\min\{x,y\}+\max\{x,y\} = x+y$. Now $(a,b)[a,b] = \prod_p p^{\min\{\alpha(p),\beta(p)\}} p^{\max\{\alpha(p),\beta(p)\}} = \prod_p p^{\min\{\alpha(p),\beta(p)\}+\max\{\alpha(p),\beta(p)}$

$\prod_p p^{\alpha(p)+\beta(p)} = \prod_p p^{\alpha(p)} p^{\beta(p)}$. □

4 Wednesday: Counting primes and congruences

Preclass assignment. Prove Textbook Theorem 2.1 Let a, b, c, d denote integers, then:

(5) $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$ implies $a \equiv b \pmod{d}$

(6) $a \equiv b \pmod{m}$ implies $ac \equiv bc \pmod{mc}$ for $c > 0$.

Solution. (5) Since $a \equiv b \pmod{m}$, that means $m \mid a - b$. Since $d \mid m$, we have that $d \mid a - b$. Thus $a \equiv b \pmod{d}$

(6) Since $a \equiv b \pmod{m}$, that means $m \mid a - b$. Thus, $mc \mid ac - bc$, and $ac \equiv bc \pmod{mc}$. **Note:** We require $c > 0$ since the definition of modulus requires positive.

□

4.1 Counting primes

Theorem 9 (Textbook Theorem 1.18)**.** *There are arbitrarily large gaps in the primes. In other words, for any positive integer k, there exist k consecutive composite integers.*

Proof. Consider the integers

$$(k+1)!+2, (k+1)!+3, \ldots, (k+1)!+k, (k+1)!+k+1$$

Every one of these is composite because j divides $(k+1)!+j$ if $2 \le j \le k+1$. □

Now, what about how many primes there are? We let $\pi(x)$ denote the number of primes up to x. So $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$ and so on.

Theorem 10 (Prime Number Theorem)**.**

$$\lim_{n\to\infty} \frac{\pi(x)}{x/\log x} = 1$$

Section 8.1 of the textbook is dedicated to proving the weaker result that there exists $a, b \in \mathbb{R}$ such that $a\frac{x}{\log x} < \pi(x) < b\frac{x}{\log x}$ for all large x. That section also has a proof that if $\lim_{n\to\infty} \frac{\pi(x)}{x/\log x}$ exists, it is 1.

4.2 Congruences

Congruences generalize the concept of evenness and oddness. We typically think of even and odd as "divisible by 2" and "not divisible by 2", but a more useful interpretation is even means "there is no remainder when divided by 2" and "there is a remainder of 1 when divided by 2". This interpretation gives us more flexibility when replacing 2 by 3 or larger numbers. Instead of "divisible" or "not divisible" we have several gradations.

Definition. We say that a is congruent to b modulo m and write $a \equiv b \pmod{m}$ if m divides $a - b$. (Sometimes we say "equivalent" in place of "congruent".) We generally apply this for $a, b \in \mathbb{Z}$ and an integer $m \geq 2$.

While this is a useful starting point for understanding congruences, it's only a starting point. Here's are two alternate definitions:

Lemma 11. *1. a and b are equivalent modulo m if and only if a and b have the same remainder when divided by m.*

2. a and b are equivalent modulo m if and only if they differ by a multiple of m.

Proof. 1. If a and b have the same remainder when divided by m, that means that there exists $x, y, r \in \mathbb{Z}$ such that $a = xm + r, b = ym + r$ such that $0 \leq r < m$. Then, $a - b = (x - y)m + (r - r) = (x - y)m$. By the definition, $m \mid a - b$ so $a \equiv b \pmod{m}$.

In the other direction, if $a \equiv b \pmod{m}$, $m \mid a - b$. By the Euclidean algorithm, there exists $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that $a = q_1 m + r_1, b = q_2 m + r_2, 0 \leq m < r_1$, and $0 \leq m < r_2$. Then, $a - b = q_1 m + r_1 - (q_2 m + r_2) = (q_1 - q_2)m + (r_1 - r_2)$. Since $m \mid a - b, r_1 - r_2 = 0$, thus $r_1 = r_2$.

2. We have that a and b differ by a multiple of m if and only if there exists $k \in \mathbb{Z}$ such that $a = mk + b$. This is equivalent to $mk = a - b$ and $m \mid a - b$, and thus $a \equiv b \pmod{m}$. □

This is why it is helpful to know that every integer m divides 0.

Going back to our "generalization of even/odd" idea, we can see several congruences immediately:

$$5 \equiv 2 \pmod{3} \qquad 10 \equiv 2 \pmod{4} \qquad 100 \equiv 1 \pmod{9}.$$

Be careful with this idea and negative values. Make sure you understand why $-2 \equiv 1 \pmod{3}$ or $-10 \equiv 4 \pmod{7}$.

Sometimes it will be helpful to think of congruences one way, sometimes the other. The latter is helpful for understanding why -2, 1, 4, and 7 are all equivalent modulo 3.

Theorem 12 (Textbook Theorem 2.1)**.** *Let a, b, c, d denote integers, then:*

1. *$a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$ and $a - b \equiv 0 \pmod{m}$ are equivalent.*
2. *$a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ implies $a \equiv c \pmod{m}$*
3. *$a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $a + c \equiv b + d \pmod{m}$*
4. *$a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $ac \equiv bd \pmod{m}$.*
5. *$a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$ implies $a \equiv b \pmod{d}$*
6. *$a \equiv b \pmod{m}$ implies $ac \equiv bc \pmod{mc}$ for $c > 0$.*

Proof. 1. By definition, $a - b \equiv 0 \pmod{m}$ is equivalent to $a \equiv b \pmod{m}$. Now, we write $m \mid (-1)(a - b) = (b - a)$ to see $b \equiv a \pmod{m}$.

4. By definition, $m \mid a-b$ and $m \mid c-d$. The $m \mid c(a-b)$ and $m \mid b(c-d)$. Combining these, we have $m \mid ca-cb+bc-bd = ca-bd$. Thus, $ca \equiv bd \pmod{m}$.

□

Let's look at the various parts of Theorem 2.1 and see what they tell us about how congruences and moduli work.

The first two parts tell us that congruences behave a lot like equality. (Specifically, congruences are a form of equivalence relation.)

The last two parts tell us how we can manipulate the modulus m. We can replace the modulus with a divisor of it at any time. We can replace the modulus with a multiple of it, provided we multiply a and b by the same multiple.

The remaining two parts are perhaps the most useful: they let us do arithmetic with congruences. In particular, they imply that whenever I'm adding or multiplying numbers, I can replace the numbers I have with any equivalent number that is more convenient to use. So for example, $37 * 210 \equiv 1 * 0 \pmod{2}$ or $651262 * 697016 \equiv 2 * 6 \pmod{10}$.

Note that this doesn't work for powers. It is not the case that $2^{20} \equiv 2^0 \pmod{2}$. Also, unlike for regular equality, we cannot cancel a common factor of both sides unless it is relatively prime to m. That is to say $ac \equiv bc \pmod{m}$ implies $a \equiv b \pmod{m}$ if $gcd(c, m) = 1$. (If $gcd(c, m) > 1$ we'll talk more on this later.)

This allows us to quickly prove an old fact from grade school:

Proposition 13. *A natural number is divisible by* 3 *if and only if the sum of its (base* 10*) digits is divisble by* 3*.*

Proof. Let a number $n \in \mathbb{N}$ have base 10 expansion $a_k a_{k-1} a_{k-2} \dots a_1 a_0$ so that $n = \sum_{i \le k} a_i 10^i$. By the definition of congruences, we have that $3 \mid n$ if and only if $n \equiv 0 \pmod{3}$. Using the fact that $10 \equiv 1 \pmod{3}$, we know by Theorem 2.1 that any time we multiply by 10 (modulo 3) we could instead just multiply by 1 (modulo 3). So,

$$n \equiv \sum_{i \le k} a_i 10^i \equiv \sum_{i \le k} a_i 1^i \equiv \sum_{i \le k} a_i \pmod{3}.$$

Therefore $n \equiv 0 \pmod{3}$ if and only if the sum of the digits of n is $0 \pmod{3}$. □

So this brings up an interesting point: Why study congruence relations? Why not stick to good old integers all the time?

There's two major reasons. As we've already seen, calculations get simplified for modular arithmetic. We'll see later that taking MASSIVE powers of MASSIVE numbers is a fairly doable feat in modular arithmetic. The second reason is that by reducing a question from all integers to modular arithmetic, we often have an easier time seeing what is not allowed.

Here's an example of this second phenomenon. Consider $a^2 + b^2 = c^2$, the Pythagorean relation. Suppose we have a solution to this. Since equality holds, then the weaker fact of congruence modulo 3 must also hold. So $a^2 + b^2 \equiv c^2 \pmod{3}$. Because of what we said before about multiplication, we can reduce all the values here to either 0, 1, or 2. But $0^2 \equiv 0 \pmod{3}$, $1^2 \equiv 1 \pmod{3}$, and $2^2 \equiv 4 \equiv 1 \pmod{3}$. Since it is impossible to have $c^2 \equiv 2 \pmod{3}$, we cannot have that $a^2 + b^2 \equiv 2 \pmod{3}$. Thus at least one of a or b must be $0 \pmod{3}$. We have learned something about what the possible solutions to $a^2 + b^2 = c^2$ look like by studying a congruence.

5 Friday: More congruences

Preclass assignment. List all integers in the range 1 to 100 that are congruent to 7 mod 17.

Solution. The easiest way to go about this is using Lemma 11 part 2. $7 \equiv 24 \equiv 41 \equiv 58 \equiv 75 \equiv 92 \pmod{17}$ □

We will continue to look at basic congruences. Section 2.2 is called "Solutions of Congruences." However, it is only 3 pages long, so a lot of the theorems that help with solving systems of congruences are actually in Sections 2.1 and 2.3. We are going to spend a bit more time in 2.1 because of this. Section 2.2 does not need two weeks.

Here's a brief look at some of the things we will be studying with congruences in the future.

First we are going to study when we can solve the linear relation $ax \equiv c \pmod{m}$. A little later, we're going to see when can we solve $x^2 \equiv c \pmod{m}$ (for fixed c and m). The answer here will be a little surprising: it will depend on when we can solve $x^2 \equiv m \pmod{c}$. Solving higher powers, cubes, quartics and the like, is still a really hard problem and we won't cover it too much. But in one simple case, we can give reasonable answers for when $x^n \equiv 1 \pmod{m}$ is solvable.

Another thing we'll find to be generally true is that working modulo primes is much better than working modulo composite numbers. We will make use of certain results to go from look at primes to prime powers, and then to composites.

Now a big point of the previous theorem (Theorem 2.1) is that congruences act a lot like equality when it comes to addition and multiplication. The point of the next theorem is to say that DIVISION is different and we must be careful with it. Here's the special rule.

Theorem 14 (Textbook Theorem 2.3)**.** *1. $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \pmod{m/(a,m)}$.*

2. If $ax \equiv ay \pmod{m}$ and $(a,m) = 1$ then $x \equiv y \pmod{m}$.

3. $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$ if and only if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

(This second part gives an idea of why prime values of m are so helpful!)

Proof. 1. If $ax \equiv ay \pmod{m}$ then $ay - ax = mz$ for some integer z, thus

$$\frac{a}{(a,m)}(y-x) = \frac{m}{(a,m)}z,$$

and so $\frac{m}{(a,m)}$ divides $\left(\frac{a}{(a,m)}\right)(y-x)$. We can rewrite Theorem 1.6 to say that $(a,m)\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = (a,m)$, and thus $\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$. Therefore, the only way $\frac{m}{(a,m)}$ divides $\left(\frac{a}{(a,m)}\right)(y-x)$ is if it divides $y - x$. Then by definition $x \equiv y \pmod{\frac{a}{(a,m)}}$.

On the other hand, suppose $x \equiv y \pmod{\frac{m}{(a,m)}}$. Then $\frac{m}{(a,m)} \mid x - y$. Multiplying through by (a,m) gives $m \mid (a,m)x - (a,m)y$. Since $\frac{a}{(a,m)} \in \mathbb{Z}$, we have $m \mid \frac{a}{(a,m)}\big((a,m)x - (a,m)y\big)$. Thus, $ax \equiv by \pmod{m}$.

2. The second part comes from applying the first part when $(a,m) = 1$.

3. If $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$, then $m_i \mid (y - x)$ for $i = 1, 2, \ldots, r$. That is, $y - x$ is a common multiple of $m_1, m_2, \ldots, m_r$. Therefore, by Theorem 1.12, $[m_1, m_2, \ldots, m_r] \mid y - x$. This implies $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$

In the other direction, if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$, then $x \equiv y \pmod{m_i}$ by Theorem 2.1 part 5, since $m_i \mid [m_1, m_2, \ldots, m_r]$. □

Think-Pair-Share. Find all positive integers m for which the following statements are true:

1. $13 \equiv 5 \pmod{m}$
2. $10 \equiv 9 \pmod{m}$

3. $-7 \equiv 6 \pmod{m}$.

Think-Pair-Share. Let a be an even integer. Prove that $a^2 \equiv 0 \pmod 4$. Let b be an odd integer. What is $b^2 \pmod 4$

Now some more definitions.

Definition. If $x \equiv y \pmod m$ then y is called a residue of $x \pmod m$. A set $x_1, x_2, \ldots, x_m$ is called a *complete residue system modulo* m if every integer y there exists exactly one x_j such that $y \equiv x_j \pmod m$. The set of all numbers x satisfying $x \equiv a \pmod m$ is the *arithmetic progression* $\ldots, a-m, a, a+m, a+2m, \ldots$ and this is called a *residue class or congruence class modulo* m.

Definition. A *reduced residue system modulo* m is a set of integers r_i such that $(r_i, m) = 1$, and for every x coprime to m is congruent modulo m to exactly one member r_i of the set.

Now we need to know if this is well defined. How do we know if $(r, m) = 1$ is something that is preserved over a given residue class? By the following result:

Theorem 15 (Textbook Theorem 2.4)**.** *If* $b \equiv c \pmod m$ *then* $(b, m) = (c, m)$.

Proof. By assumption $c = b + mx$ for some integer x. Now, by Theorem 1.1, any common divisor of b and m divides the linear combination $b + mx$. We need to show that any common divisor of $b + mx$ and m also divides b. To do this, we consider the linear combination $b + mx + m(-x)$. Thus, $(b, m) = (b + mx, m) = (c, m)$.

□

Contents

Preclass assignment. Fill in the table with the values of $a^m \pmod m$. The values of a are in the first column, the values of m are in the first row. Use a value between 0 and $m - 1$ (inclusive).

$a \backslash m$	1	2	3	4	5	6
2						
3						
4						
5						
6						

Solution.

$a \backslash m$	1	2	3	4	5	6
2	$2^1 \equiv 0 \pmod 1$	$2^2 \equiv 0 \pmod 2$	$2^3 \equiv 2 \pmod 3$	$2^4 \equiv 0 \pmod 4$	$2^5 \equiv 2 \pmod 5$	$2^6 \equiv 4 \pmod 6$
3	$3^1 \equiv 0 \pmod 1$	$3^2 \equiv 1 \pmod 3$	$3^3 \equiv 0 \pmod 3$	$3^4 \equiv 1 \pmod 4$	$3^5 \equiv 3 \pmod 5$	$3^6 \equiv 3 \pmod 6$
4	$4^1 \equiv 0 \pmod 1$	$4^2 \equiv 0 \pmod 2$	$4^3 \equiv 1 \pmod 3$	$4^4 \equiv 0 \pmod 4$	$4^5 \equiv 4 \pmod 5$	$4^6 \equiv 4 \pmod 6$
5	$5^1 \equiv 0 \pmod 1$	$5^2 \equiv 1 \pmod 2$	$5^3 \equiv 2 \pmod 3$	$5^4 \equiv 1 \pmod 4$	$5^5 \equiv 0 \pmod 5$	$5^6 \equiv 1 \pmod 6$
6	$6^1 \equiv 0 \pmod 1$	$6^2 \equiv 0 \pmod 2$	$6^3 \equiv 0 \pmod 3$	$6^4 \equiv 0 \pmod 4$	$6^5 \equiv 1 \pmod 5$	$6^6 \equiv 0 \pmod 6$

□

Think-Pair-Share. Find a complete residue system mod 17 where every number is a multiple of 3.

Solution. We need a list of $3k$ where $3k \equiv 1, 2, 3, \ldots 16$. Some of these are easy: $3, 6, 9, 12, 15$ are already divisible by 3. Next, we have $18 \equiv 1 \pmod{17}, 21 \equiv 4 \pmod{17}, 24 \equiv 7 \pmod{17}, 27 \equiv 10 \pmod{17}, 30 \equiv 13 \pmod{17}, 33 \equiv 16 \pmod{17}, 36 \equiv 2 \pmod{1}7, 39 \equiv 5 \pmod{17}, 42 \equiv 8 \pmod{17}$ □

Based on this excercise, some groups started trying to figure out whether it is important that 17 is prime, 3 is prime, or just that $(17, 3) = 1$. We proved that this works when the mod is prime.

Theorem 16 (Textbook Theorem 2.6)**.** *Let p be a prime number and a be an integer not divisible by p. Then the numbers $a, 2a, 3a, \ldots, (p-1)a \pmod{p}$ are congruent to $1, 2, 3, \ldots, (p-1) \pmod{p}$, but may be in a different order. In other words, multiplying a complete residue system by a non-zero constant gives another complete residue system. (Note: you can do the same with reduced residue systems.)*

Proof. The list $a, 2a, \ldots, (p-1)a$ contains $p-1$ numbers. Each takes the form ka for some $1 \leq k \leq p-1$, and thus, since neither k nor a is divisible by p, we have that nothing in this list is divisible by p either. Now we want to show the elements of this list are distinct. Let $1 \leq j < k \leq p-1$ and suppose $ja \equiv ka \pmod{p}$. Then $p \mid (k-j)a$, or, since $p \nmid a$, we have $p \mid (k-j)$. So $k - j = px$ for some integer x. But we divide by p and see that $(k-j)/p$ is an integer between 0 and 1 again, thus a contradiction.

So $a, 2a, 3a, \ldots, (p-1)a$ is a list of $p-1$ distinct elements from the set $1, 2, 3, \ldots, (p-1)$, thus it must be the list $1, 2, 3, \ldots, (p-1)$, just possibly rearranged. □

We can then generalize this idea to get a theorem:

Theorem 17 (Theorem 2.7 (Fermat's Little Theorem))**.** *Let p be a prime and let a be any number with $a \not\equiv 0 \pmod{p}$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

In other words, $x^{p-1} \equiv 1 \pmod{p}$ has LOTS of solutions, it has as many as it possibly could. This is also a somewhat peculiar result. This says, for instance that if you take ANY number that is not a multiple of 5, raise it to the fourth power and subtract one, you get a multiple of 5, every single time.

Proof. Fermat's Little Theorem Since a is not divisible by p by assumption, we have that the lists

$$a, 2a, \ldots, (p-1)a \pmod{p} \text{ and } 1, 2, \ldots, (p-1) \pmod{p}$$

are the same, and thus

$$a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

or, after rearranging both sides

$$a^{p-1}((p-1)!) \equiv (p-1)! \pmod{p}$$

Now p does not divide $(p-1)!$, so it can be canceled from both sides, leaving the modulus alone. Thus we have the desired relation $a^{p-1} \equiv 1 \pmod{p}$. □

Fermat's little theorem can be greatly extended to cases where things aren't prime moduli.

Definition. Given $m \geq 1$, let $\phi(m)$ denote the number of positive integers less than or equal to m that are relatively prime to m.

Theorem 18 (Textbook Theorem 2.8)**.** *Euler's generalized of Fermat's Theorem. If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

The proof of this follows almost identically to the proof of Fermat's little theorem, just that one has to care about only counting things that are reduced residue classes.

Now here is one fact about the phi-function: The question is about what values can $\phi(m)$ take? Well let V be the set of all values $\phi(m)$ can take for some m. Note that $2 \in V$ because $\phi(3) = 2$, but you cannot find an m so that $\phi(m) = 3$, so $3 \notin V$.

This gives us some powerful tools to do computations in modular arithmetic. Whenever we are adding or multiplying numbers, we can always reduce them modulo m, and we can reduce any exponents modulo $\phi(m)$ because $a^0 \equiv a^{\phi(m)} \pmod{m}$. (Note, this does require that $(a, m) = 1$). For example $500^{100} \pmod 3$ is just $2^0 \equiv 1 \pmod 3$.

Example 1. Reduce $6^{4162} \pmod{41}$

Solution. $6^{4162} \equiv 6^{4000+160+2} \equiv 6^{4000}6^{160}6^2 \equiv (6^{40})^{10}(6^{40})^4 6^2 \equiv 1^{10}1^4 36 \equiv 36 \pmod{41}$. □

8 Friday: Where the Fundamental Theorem of Arithmetic is not true

Consider the $\pmod 8$ multiplication chart:

x_8	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	0	2	4	6	0
3	3	6	1	4	7	2	5	0
4	4	0	4	0	4	0	4	0
5	5	2	7	4	1	6	3	0
6	6	4	2	0	6	4	2	0
7	7	6	5	4	3	2	1	0
8	0	0	0	0	0	0	0	0

Preclass assignment. Write every combination a, b in the chart where $ab \equiv 0 \pmod 8$ and neither a or b is $8 \equiv 0 \pmod 8$. Write every combination $ab \equiv 1 \pmod 8$.

Solution. $2(4) \equiv 4(2) \equiv 4(4) \equiv 4(6) \equiv 6(4) \equiv 0 \pmod 8$. $1(1) \equiv 3(3) \equiv 5(5) \equiv 7(7) \equiv 1 \pmod 8$. □

Right away, we can see things are weird. We have that $ab \equiv 0 \pmod 8$ does not imply either a or b is 0. This means that our proof of the division algorithm (theorem 1.2) falls apart at the step where $0 = b(q_1 - q_2), b > 0$ implies $q_1 = q_2$ if we try to use the division algorithm mod m. That means that every proof that relies on the division algorithm, including the gcd results and the fundamental theorem of arithmetic, either fall apart or require new proofs. However, it is ok to use these as proven, we just can't say

Another thing that is unusual is that $ab \equiv 1 \mod 8$ does not imply that $a = b = \pm 1$. This is a little less unusual, since this is true for rational numbers, just not integers.

Definition. A number $a \in \mathbb{Z}$ is *invertible* $\pmod m$ if there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod m$.

This definition works in a more general setting. If we have some operation $*$ on a set S and some $e \in S$ where $e * a = a * e = a$ for all $a \in S$, then $a \in S$ is *invertible with respect to* $*$ if there exists $b \in S$ such that $a * b = e$. We call e the *identity*. For our normal and modular arithmetic, 0 is the additive identity and 1 is the multiplicative identity. For matrices, the matrix with all 0 entries is the additive identity and the identity matrix is the multiplicative identity. Every integer is invertible with respect to addition, but only ± 1 are invertible with respect to multiplication. However, when we look at rational numbers, every ration is invertible with respect to addition and multiplication.

So that we do not have to deal with the infinitely many integers $a + km \equiv a \pmod{m}$, we tend to talk about *equivalences classes.*

Definition. An *equivalence class* is the set $\{a + km : k \in \mathbb{Z}\}$. A *representative of an equivalence class* is a number $a + km$. There are infinitely many representatives of each equivalence class, but there are m equivalence classes $\pmod{m}$.

When we talk about the solutions to an equivalence $\pmod{m}$, we are talking about which equivalence classes are solutions. Since $a \equiv a+m \equiv a+2m \equiv a+3m \equiv \cdots \pmod{m}$, it is not necessary to consider each a separate solution. Since there are $p-1$ equivalence classes where to $a^{p-1} \equiv 1 \pmod{p}$, there are $p-1$ solutions to $x^{p-1} \equiv 1 \pmod{m}$.

Returning to our $\pmod 8$ chart, we have that $1, 3, 5$ and 7 are invertible $\pmod 8$.

Theorem 19 (Textbook Theorem 2.9 rephrased)**.** *If $(a, m) = 1$, then a is invertible $\pmod{m}$. That is, there exists x such that $ax \equiv 1 \pmod{m}$. Any two such x are equivalent $\pmod{m}$. If $(a, m) > 1$, then no such x exists.*

Proof. If $(a, m) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Thus, $ax \equiv 1 \pmod{m}$. If $ax \equiv 1 \pmod{m}$, then there exists y such that $ax + ym = 1$. Thus, $(a, m) = 1$. □

Let's summarize what we know: if $(a, m) = 1$ then:

- $a^{\phi(m)} \equiv 1 \pmod{m}$. In other words, there are solutions to the equivalence $x^{\phi(m)} \equiv 1 \pmod{m}$, and the solutions are precisely the integers the $\phi(m)$ integers $0 \leq a \leq m-1$ where $(a, m) = 1$.
- There is exactly one solution to $ax \equiv 1 \pmod{m}$.

We will return to solving equivalences, but first we are going to work towards a setting we do not have a version of the fundamental theorem of arithmetic (but we do have a way to define primes).

Definition. The *Gaussian integers* $\mathbb{Z}[i]$ are the set of complex numbers $\{a+bi : a, b \in \mathbb{Z}, i^2 = -1\}$. We define addition and subtraction as normal:

$$a + bi + c + di = (a + c) + (b + d)i, \quad (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Now, $ab = 0$ implies $a = 0$ or $b = 0$ like we are used to; $ab = 1$ has four solutions: $a = b = \pm 1$ and $a = -b = \pm i$. In this new setting, it is not clear what it means for $1 < a + bi$. Is $1 < -1 + 2i$? So, we can't just copy/paste our definition of prime from the regular integers. From the homework, we know that Theorem 1.15 is equivalent to our definition of prime, and it still works here.

Definition. A number $p \in \mathbb{Z}[i]$ is *prime* if $p \mid ab$ implies $p \mid a$ or $p \mid b$ for all $a, b \in \mathbb{Z}[i]$.

Now, a quick note about the regular integers: $2 = (1 + i)(1 - i)$, so is not prime in $\mathbb{Z}[i]$. Our goal is to show which integers are prime in $\mathbb{Z}[i]$.

Theorem 20. *The primes in $\mathbb{Z}[i]$ have the form:*

- *$p \in \mathbb{Z}$ where p is a prime and $p \equiv 3 \pmod 4$*
- *$a + bi$ where $a^2 + b^2$ is prime.*

We will not prove this fully now, but we can prove that $a^2 + b^2 \not\equiv 3 \pmod 4$ and that $q \equiv 1 \pmod 4$ is not prime in $\mathbb{Z}[i]$.

Lemma 21 (Contrapositive of Textbook Lemma 2.14)**.** $a^2 + b^2 \not\equiv 3 \pmod 4$.

Proof. We quickly check that $0^0 \equiv 0 \mod 4, 1^2 \equiv 1 \pmod 4, 2^2 \equiv 0 \pmod 4, 3^2 \equiv 1 \pmod 4$, so $a^2, b^2 = 0, 1, 2$. Thus, the only options for $a^2 + b^2 \pmod 4$ are $0, 1, 2$. □

Lemma 22 (Textbook Lemma 2.13)**.** *If p is prime and $p \equiv 1 \pmod 4$, then there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = p$.*

We will save this proof for after quadratic residues. However, we can use this to see that $p = (a + bi)(a - bi)$. So our only candidates for primes $a + 0i$ are those congruent to 3 mod 4.[1]

Now we consider the example from the middle of page 21 of your textbook: The even integers (sometimes written $2\mathbb{Z}$) are still "well behaved" since adding/subtracting two even numbers gives an even number and multiplying two even numbers gives an even number. However, factoring is going to work differently if we require that every factor is even. Now, $10 = 2 * 5$, but 5 is not even so does not count as a prime factor. We say 10 is **irreducible over the even numbers**. In fact, there are a lot of composite integers that are irreducible over the even numbers: $6, 10, 14, 22, 26, \ldots, 2p$ for all primes $p > 2$. We also see that $60 = 2 * 30 = 6 * 10$, where 30 and 10 are both irreducible. Thus, we no longer have unique factorization.

We can use the same definition of *primes* that we had for $\mathbb{Z}[i]$. Here the definition from the integers does not work since 1 is not an even number. One the homework, you proved that the primes over $2\mathbb{Z}$ are 2 and $2q$ where q is prime in $\mathbb{Z}$.

Contents

9 Monday: Where the Fundamental Theorem of Arithmetic is not true, some solutions to quadratic congruences

Preclass assignment. Prove there are not integers a, b where $(a + b\sqrt{-6})(2 + \sqrt{-6}) = 2$ or 5.

Solution. We know that $(a + b\sqrt{-6})(2 + \sqrt{-6}) = 2a - 6b + (a + 2b)\sqrt{-6} = 2$ if

$$\begin{aligned} 2a - 6b = 2 \quad \text{if} \quad a + 2b = 0, \\ 2(-2b) - 6b = -10b = 2, \end{aligned}$$

which has no integer solutions. Similarly, $(a + b\sqrt{-6})(2 + \sqrt{-6}) = 2a - 6b + (a + 2b)\sqrt{-6} = 5$ if

$$\begin{aligned} 2a - 6b = 5 \quad \text{if} \quad a + 2b = 0, \\ 2(-2b) - 6b = -10b = 5, \end{aligned}$$

which has no integer solutions. □

Let $\mathbb{Z}[\sqrt{-6}] := \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$. We use the standard multiplication and addition:

$$\begin{aligned} a + b\sqrt{-6} + c + d\sqrt{-6} &= (a + c) + (b + d)\sqrt{-6} \\ (a + b\sqrt{-6})(c + d\sqrt{-6}) &= (ac - 6bd) + (ad + bc)\sqrt{-6}. \end{aligned}$$

Like with our previous examples, factoring in $\mathbb{Z}[\sqrt{-6}]$ means that all factors are in $\mathbb{Z}[\sqrt{-6}]$. Notice that $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-6}]$ where $b = 0$. Now $10 = 2 * 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$. There are not integers a, b where $(a + b\sqrt{-6})(2 + \sqrt{-6}) = 2$ or 5, so prime factorization is not unique. However, we can check

$$(a + b\sqrt{-6})(c + d\sqrt{-6}) = (ac - 6bd) + (ad + bc)\sqrt{-6} = 0$$

if and only if $ac - 6bd = 0, ad + bc = 0$. That is, $ac = 6bd, ad = -bc$.

We want to check if there are 0 divisors: ie, there are nonzero integers a, b, c, d where $ac = 6bd, ad = -bc$.

[1] We also have not dealt with why we want $a^2 + b^2$ to be prime.

We can manipulate these equations to see $abc = 6b^2d, -a^2d = abc$. So we need to find $6b^2 = -a^2$. We know there are no nonzero real solutions to this equation (thus no nonzero integer solutions). Thus, $\mathbb{Z}[\sqrt{-6}]$ does not have zero divisors, but also does not have unique factorization. We should not take the fundamental theorem of arithmetic for granted!

We can study things like $\mathbb{Z}[i], \mathbb{Z}[x], \mathbb{Z}[\sqrt{-d}]$ and even $\mathbb{Z}_n[x] = \{a_k x^k + a_{k-1}x^{k-1} + \cdots a_1 c + a_0 \pmod{n}\}$. Some questions we can ask are whether factorization is unique or zero divisors exist. This is part of *algebraic number theory*.

Equations with integer solutions are called *Diophantine equations*. We are going to study them in depth after midterm 2, but they will pop up periodically before then.

Some congruences

We continue our quest to classify when we can find solutions to congruence relations (which will also help in solving Diophantine equations).

So far, we have: if $(a, m) = 1$ then:

- $a^{\phi(m)} \equiv 1 \pmod{m}$. In other words, there are solutions to the equivalence $x^{\phi(m)} \equiv 1 \pmod{m}$, and the solutions are precisely the integers the $\phi(m)$ integers $0 \leq a \leq m-1$ where $(a, m) = 1$.
- There is exactly one solution to $ax \equiv 1 \pmod{m}$.

and $a^2 + b^2 \not\equiv 3 \pmod{4}$.

Oddly enough, the next easiest to prove fact is:

Think-Pair-Share (Textbook Theorem 2.10)**.** Let p be a prime number. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

Before we leave the prime modulus world for a bit, we have one more theorem:

Theorem 23 (Wilson's Theorem. Textbook Theorem 2.11)**.** *If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. If $p = 2$, we are done since $1! \equiv -1 \pmod{2}$. Similarly $2! \equiv -1 \pmod{3}$.

Let $p > 5$ be a prime and consider the list $2, 3, \ldots, p-2$. By the previous theorem, none of the elements of the list are their own inverse. Thus, each element on the list has a unique inverse that is also on the list by Theorem 2.9. Since there are an even number of elements on the list, we can cancel each with its inverse. Thus,

$$1(2)(3)\cdots(p-2)(p-1) \equiv 1(p-1) \equiv -1 \pmod{p}.$$

□

Note: The factorial is missing in the statement of the theorem in the textbook!

However, it would be somewhat satisfying to be able to solve $ax \equiv b \pmod{m}$.

Think-Pair-Share. Either find all solutions or show that no solutions exist:

1. $2x \equiv 3 \pmod{4}$
2. $2x \equiv 3 \pmod{5}$
3. $2x \equiv 3 \pmod{6}$ and $2x \equiv 4 \pmod{6}$

Theorem 24 (Textbook Theorem 2.17)**.** *Let $a, b, m \in \mathbb{Z}$ and $g = (a, m)$. There exists a solution to $ax \equiv b \pmod{m}$ if and only if $g \mid b$. If $g \mid b$, there are exactly d incongruent solutions $\bmod m$ given by*

$$x + \frac{mn}{d} \quad n = 0, 1, \ldots, d-1$$

where x_0 is a particular solution to the congruence.

Proof. We can rephrase this to ask whether there exists $x, y \in \mathbb{Z}$ where $ax + my = b$. We see that $g \mid ax + my$ if and only if $g \mid b$, thus such x, y exist if and only if $g \mid b$.

Suppose a solution x_0 exists. Let $a = gj, b = gk$, and $m = gl$. Then by the first part of theorem 2.3, we have that $ax_0 \equiv b \pmod{m}$ if and only if $jx_0 \equiv k \pmod{l}$. We know that $(j, l) = 1$, since dividing by the greatest common divisor leaves no positive common divisors other than 1. Thus by Theorem 2.9, there is a unique $\overline{j} \pmod{l}$ such that $j\overline{j} \equiv 1 \pmod{l}$. Multiplying through by $\overline{j}$, we get that $x_0 \equiv j\overline{j}x_0 \equiv \overline{j}k \pmod{l}$. That is, we get that the solutions all satisfy $x_0 \equiv \overline{j}k \pmod{l}$ and all solutions have the form $\overline{j}k + nl$ for some $n \in \mathbb{Z}$. Plugging in our definitions, we can let $\overline{j}k = x_0$ and replace l with $\frac{m}{g}$. Thus all solutions have the form $x_0 + n\frac{m}{g}$.

To see that there are d incongruent solutions, we consider the set

$$\{x_0, x_0 + \frac{m}{g}, x_0 + \frac{m}{g}2, \ldots, x_0 + \frac{m}{g}(g-1)\}.$$

From the note right before Theorem 2.4, we have that this is a complete residue system mod l. That is, this set is precisely the incongruent solutions modulo l. By applying the contrapositive of Theorem 2.1 part 5, we find that if $x_0 \not\equiv x_0 + \frac{m}{g}n \pmod{l}$ iether $ax_0 \not\equiv ax_0 + a\frac{m}{g}n \pmod{m}$ or $l \nmid m$. But $l \mid m$ by definition, so we have that the set of solutions are also incongruent mod m. □

The notes titled Linear Congruence in One Variable gives a more detailed proof using slightly different methods.

10 Wednesday: Chinese remainder theorem

Preclass assignment. Find the least nonnegative solution to:

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 1 \pmod{8} \end{aligned}$$

Solution. The proof of the Chinese remainder theorem helps us solve this system of congruences. We know that there is a unique solutions mod 280. We now solve the system

$$\begin{aligned} 56x_1 &\equiv 1 \pmod{5}, \quad \text{so} \quad 1x_1 \equiv 1 \pmod{5} \\ 40x_2 &\equiv 1 \pmod{7}, \quad \text{so} \quad 5x_2 \equiv 1 \pmod{7} \\ 35x_3 &\equiv 1 \pmod{8}, \quad \text{so} \quad 3x_3 \equiv 1 \pmod{8} \end{aligned}$$

Then $x_1 = 1, x_2 = 3, x_3 = 3$. We compute the solution

$$\begin{aligned} x &= 2(56)(1) + 3(40)(3) + 1(35)(3) \\ &= 557 \\ x &\equiv 17 \pmod{280} \end{aligned}$$

Thus the least nonnegative solution is 280. □

Clarify proof of Theorem 2.17

Chinese Remainder Theorem

We are going to go through the proof of the Chinese remainder theorem.

Theorem 25 (Chinese remainder theorem, Theorem 2.18)**.** *Let $m_1, m_2, \dots m_r$ be pairwise relatively prime positive integers (that is, any pair $(m_i, m_j) = 1$ when $i \neq j$). Let $a_1, a_2, \dots, a_r$ be integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots_r$. This solution has the form

$$x_0 = \sum_{i=1}^{r} \frac{M}{m_i} b_i a_i,$$

where $b_i a_i \equiv 1 \pmod{m_i}$.

Proof. We start by constructing a solution mod $M = m_1 m_2 \cdots_r$. By construction, $\frac{M}{m_i}$ is an integer. Since each the m_i are pairwise relatively prime, $(\frac{M}{m_i}, m_i) = 1$. Thus, by Theorem 2.9, for each i there is an integer b_i where $\frac{M}{m_i} b_i \equiv 1 \pmod{m_i}$. We also have that $(\frac{M}{m_i}, m_j) = m_j$ when $i \neq j$, so $\frac{M}{m_i} b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Let

$$x_0 = \sum_{i=1}^{r} \frac{M}{m_i} b_i a_i.$$

Then $x_0 \equiv \frac{M}{m_i} b_i a_i \equiv a_i \pmod{m_i}$ for each $i = 1, 2, \dots, r$. We have found a solution to the system of equivalences.

If we have some other solution x_1, we have that $x_0 \equiv x_1 \pmod{m_i}$ for all $i = 1, 2, \dots, r$. Then $m_i \mid x_0 - x_1$ for all $i = 1, 2, \dots, r$ and $M \mid x_0 - x_1$. Thus, $x_0 \equiv x - 1 \pmod{M}$. □

However, we don't have to work with relatively prime moduli.

Example 2. Solve the system of equivalences

$$\begin{aligned} x &\equiv 2 \pmod{6} \\ x &\equiv 8 \pmod{9} \end{aligned}$$

and find a (possible) modulus m where solutions are congruent $\pmod{m}$.

Solution. One thing we can do is list possible solutions.

$$\begin{aligned} x &\equiv 2 \pmod{6}, \quad x = 2, 8, 14, 20, 26, \dots, 2 + 6j, \dots \\ x &\equiv 8 \pmod{9}, \quad x = 8, 17, 26, \dots, \dots 8 + 9k, \dots \end{aligned}$$

We see that 8 and 26 are solutions. We have $26 - 8 = 18$, so $m = 18$. □

We have another Diophantine equation! Solutions to the equivalences have the form $2 + 6j = 8 + 9k$. We have that $8 = 2 + 6(1) = 8 + 9(0)$. We can play with this equation to see $3(2j - 3k) = 6$ or $2j - 3k = 2$ or $2(j - 2) = 3k$. Thus k is even and $j \equiv 2 \pmod{3}$. Knowing that the solution has the form $8 + 18l = 2 + 6 + 18l$, we have that $j = 1 + 3l$ and $k = 3l$.

Theorem 26 (Generalized Chinese Remainder Theorem)**.** *Let $m_1, m_2, \dots m_r$ be positive integers, and let $a_1, a_2, \dots, a_r$ be integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a solution if and only if $(m_i, m_j) \mid a_i - a_j$ for all $i \neq j$. In this case, the solution is unique modulo $[m_1, m_2, \dots, m_r]$.

Proof. This is on homework 4 due February 14. □

11 Friday: Start of polynomials $\pmod m$

Preclass assignment. Read the notes on math writing and resubmit a solution to the last homework.

Non-calculator solution to Homework 3 problem 6(iii):

Solution. There exists x such that $9x \equiv 1 \pmod{23}$. That is, there exist $x, y \in \mathbb{Z}$ such that $9x + 23y = 1$. We can use the Euclidean algorithm,

$$\begin{aligned} 23 &= 2 * 9 + 5 \\ 9 &= 5 + 4 \\ 5 &= 4 + 1. \end{aligned}$$

Rewriting, we get that

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (9 - 5) = 5 * 2 - 9 \\ &= (23 - 2 * 9) * 2 - 9 = 2 * 23 - 5 * 9 \end{aligned}$$

Thus, $1 \equiv (-5)9 \equiv 18{*}9 \pmod{23}$. We use this to see $9x \equiv 21 \equiv -2 \pmod{2}3$ has solution $x \equiv (-5)8x \equiv (-5)(-2) \equiv 10 \pmod{23}$. □

Polynomials

Now that we've seen some linear and very limited higher power equivalences, we are going to look at polynomials. It is even harder to say anything about higher power polynomials. This will also give us a chance to review the congruence material in a slightly different context.

Think-Pair-Share (Theorem 2.2)**.** Let f denote a polynomial with integer coefficients. If $a \equiv b \pmod m$ then $f(a) = f(b) \pmod m$.

Solution. We can write $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$ for some integers c_i. Then by Theorem 2.1 part 4, we have that $a \equiv b \pmod m$ implies $a^2 \equiv b^2 \pmod m, a^3 \equiv b^3 \pmod m, \dots, a^n \equiv b^n \pmod m$. Also by Theorem 2.1 part 4, we have $c_i a^i \equiv c_i b^i \pmod m$. Finally, putting everything together with Theorem 2.1 part 3, we have that $c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0 \equiv c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0 \pmod m$. □

Definition. Let $r_1, r_2, \ldots, r_m$ denote a complete residue system modulo m. The *number of solutions of* $f(x) = 0 \pmod m$ is the number of r_i such that $f(r_i) = 0 \pmod m$. That is, each solution r_1 is the representative of a congruence class of solutions, and we only count the number of congruence classes. This agrees with asking for the number of incongruent solutions (why?).

Theorem 27 (Corollary to the Chinese Remainder Theorem)**.** *Let $m = \prod p_i^{\alpha_i}$ be the prime factorization of m. For each element y of the complete residue system $\{0, 1, \ldots, m-1\}$, there exists a system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{p_1^{\alpha_1}} \\ x &\equiv a_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ x &\equiv a_r \pmod{p_r^{\alpha_r}} \end{aligned}$$

where y is a solution modulo m. The same is true for any pairwise relatively prime m_i where $m = \prod m_i$.

Solution. There are $p_1^{\alpha_1}$ choices for a_1, $p_2^{\alpha_2}$ choices for a_2, etc, thus there are $\prod p_i^{\alpha_i}$ such systems of congruences. From the Chinese remainder theorem, there exists a unique solution modulo m. Since the solution to two distinct systems of congruences are incongruent for some mod $p_i^{\alpha_i}$, they are distinct mod m by the contrapositive of Theorem 2.1 part 5. The same proof holds for any pairwise relatively prime m_i where $m = \prod m_i$. □

Definition. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. The *degree of the polynomial* $\pmod m$ is the largest integer j such that $a_j \not\equiv 0 \pmod m$. If all of the $a_i \equiv 0 \pmod m$, then the degree is 0.

This is similar to Definitions 2.5 in the book, but using more modern algebraic language. Note: in class we did this before the definition of a solution modulo m or the Corollary to the Chinese Remainder Theorem.

The degree of the polynomial $\pmod m$ is not the same as the degree of the polynomial over $\mathbb{Z}$. For example, $f(x) = 6x^3 + 3x^2 + 1$ has degree 3 over the integers and $\pmod 5$, but degree 2 $\pmod 6$ and $\pmod 2$.

It'd be nice to be able to use similar techniques to those we use in for integers. Remember, we can't factor and set equal to 0 because of zero divisors. One thing that would be nice is to know exactly when we have zero divisors.

Theorem 28. *If p is prime, then $ax \equiv 0 \pmod p$ implies either $a \equiv 0 \pmod p$ or $x \equiv 0 \pmod p$. If m is a positive composite integer, then there is a solution to $ax \equiv 0 \pmod m$ where both $a \not\equiv 0 \pmod m$ and $x \not\equiv 0 \pmod m$.*

Proof. From Theorem 2.9, there exists $\overline{a}$ where $\overline{a}a \equiv 1 \pmod p$ if and only if $(a, p) = 1$. Since $\{0, 1, \ldots, p-1\}$ is a complete residue class mod p, we can assume $0 \le a \le p-1$. Since p is prime, a has a multiplicative inverse $\overline{a}$ mod p for all $1 \le a \le p-1$. Returning to our congruence $ax \equiv 0 \pmod p$, either $a \equiv 0 \pmod p$ or $\overline{a}ax \equiv x \equiv 0 \pmod p$.

For the case where m is composite, then there exist integers $1 < a, x < m$ where $m = ax$. Then $ax \equiv 0 \pmod m$ but $\not\equiv 0 \pmod m$ and $x \not\equiv 0 \pmod m$. □

Example 3. Let's look at two examples:

$$\begin{aligned} x^3 + 2x - 3 &\equiv 0 \pmod 5 \\ x^3 + 2x - 3 &\equiv 0 \pmod 4 \end{aligned}$$

One has 0 divisors and the other does not. Both of these are small enough to guess-and-check, but let's try a technique that is going to generalize a bit better. Although cubics are hard to factor, we can quickly guess-and-check that $x = 1$ is solution over the integers, so $x^3 + 2x - 3 = (x-1)(x^2 + x + 3)$.

(mod 5) Let's start modulo 5. Then $(x-1)(x^2+x+3) \equiv 0 \pmod 5$ when either $x-1 \equiv 0 \pmod 5$ or $x^2+x+3 \equiv 0 \pmod 5$, since 5 is prime. Then one solution is $x \equiv 1 \pmod 5$, which is good since $x = 1 \equiv 1 \pmod m$ for any integer m.
We are going to do something a bit funny for the other equivalence. We rewrite $x^2 + x + 3 \equiv 0 \pmod 5$ as $x(x+1) \equiv 2 \pmod 5$. Then we have a slightly faster time checking $1(1+1), 2(2+1), 3(3+1), 4(4+1)$. The only solutions are $x \equiv 1 \pmod 5$ (which we already found) and $x \equiv 3 \pmod 5$.

(mod 4) We will do this on Monday, February 3.

12 Monday: Polynomials, groups, rings, and fields

Preclass assignment. Look at the definition and congruence modulo m and Theorem 2.1. Which part tells us that congruence modulo m is reflexive? Symmetric? Transitive?

Preclass assignment. Look at the definition and congruence modulo m and Theorem 2.1. Which part tells us that addition modulo m is closed? What is the identity element of addition modulo m? How can we write $-a \pmod m$ so that $0 \leq a \leq m-1$?

12.1 Polynomials

We will continue our example from Friday. In the next few weeks, we will learn better techniques for solving these congruences.

Example 4. Let's look at two examples:

$$x^3 + 2x - 3 \equiv 0 \pmod 5$$
$$x^3 + 2x - 3 \equiv 0 \pmod 4$$

One has 0 divisors and the other does not. Both of these are small enough to guess-and-check, but let's try a technique that is going to generalize a bit better. Although cubics are hard to factor, we can quickly guess-and-check that $x = 1$ is solution over the integers, so $x^3 + 2x - 3 = (x-1)(x^2+x+3)$.

(mod 5) From last time, the solutions are $x \equiv 1 \pmod 5$ and $x \equiv 3 \pmod 5$.

(mod 4) Now we do modulo 4. Then $(x-1)(x^2+x+3) \equiv 0 \pmod 4$ when $x - 1 \equiv 0 \pmod 4, x^2 + x + 3 \equiv 0 \pmod 4$ or $x - 1 \equiv x^2 + x + 3 \equiv 2 \pmod 4$.
We start with $x - 1 \equiv 0 \pmod{}$, so $x \equiv 1 \pmod 4$ as expected.
We rewrite $x^2+x+3 \equiv 0 \pmod 4$ as $x(x+1) \equiv 1 \pmod 4$. This means that both x and $x+1$ are odd, so there are no solutions $\pmod 4$.
Finally, we check $x-1 \equiv x^2+x+3 \equiv 2 \pmod 4$. The only possible solution is $x \equiv 3 \pmod 4$, but $3^2+3+3 \equiv 3 \pmod 4$, so it is not a solution.

Think-Pair-Share (Theorem 2.16)**.** If $d \mid m, d > 0$, and u is a solution to $f(x) \equiv 0 \pmod m$, then u is a solution to $f(x) \equiv 0 \pmod d$.

Solution. From the definition of a solution $f(x) \equiv 0 \pmod m$, $f(u) \equiv 0 \pmod m$. Then from Theorem 2.1, we have that $f(u) \equiv 0 \pmod d$, meaning u is a solution to $f(x) \equiv 0 \pmod d$. □

One way to try to find solutions to congruences is to reduce the modulus. However, we do have a powerful tool from the contrapositive. If $d \mid m, d > 0$ and u is not a solution to $f(x) \equiv 0 \pmod d$, then u is not a solution to $f(x) \equiv 0 \pmod m$. This means that we can make a list of possible solutions to $f(x) \equiv 0 \pmod m$.

Example 5. Solve $x^3 + 2x - 3 \equiv 0 \pmod{20}$. It would be tempting to try to factor this, although cubics are hard to factor, but

$$\begin{aligned} 5*4 \equiv 5*8 \equiv 5*10 \equiv 5*16 \equiv 10*2 \equiv 10*4 \equiv 10*6 \equiv 10*8 \\ \equiv 10*10 \equiv 10*12 \equiv 10*14 \equiv 10*16 \equiv 10*18 \equiv 0 \pmod{20}. \end{aligned}$$

($5*4k \equiv 10*2 \equiv 0 \pmod{25}, k = 1, 2, 3, 4, j = 1, 2, 3, \ldots, 9$ for 13 total options). Checking each option is going to be really time consuming. Let's reduce the modulus to reduce this list.

We already found that the possible solutions are $x \equiv 1 \pmod 5, x \equiv 3 \pmod 5$, and $x \equiv 1 \pmod 4$. In fact, we need a solution that works both modulo 5 and modulo 4. Then we are looking for a solution to the system of congruences $x \equiv 1 \pmod 5$ and $x \equiv 1 \pmod 4$ and a solution to the congruence $x \equiv 3 \pmod 5$, and $x \equiv 1 \pmod 4$.

Case $x \equiv 1 \pmod 5$**:** By the Chinese remainder theorem, there is a unique solution modulo 20. We have that $a_1 = 1, M_1 = 4$, and $x_1 * 4 \equiv 1 \pmod 5$, so $x_1 \equiv 4 \pmod 5$. Notice that we can find this using the Euclidean algorithm:

$$5 = 4 + 1, \quad 5 - 4 = 1,$$

so -1 is the multiplicative inverse of 4 mod 5. It is easier to do arithmetic with -1 that 4, so we will use that representative of the congruence class.

We also have that $a_2 = 1, M_2 = 5$, and $x_2 * 5 \equiv x_2 \equiv 1 \pmod 4$, so $x_2 \equiv 1 \pmod 4$.

This solution is $1 * 4 * (-1) + 1 * 5 * 1 \equiv 1 \pmod{20}$.

Case $x \equiv 3 \pmod 5$**:** By the Chinese remainder theorem, there is a unique solution modulo 20. $a_1 = 3, M_1 = 4$, and $x_1 * 4 \equiv 1 \pmod 5$, so $x_1 \equiv -1 \pmod 5$, and $a_2 = 1, M_2 = 5, x_2 = 1$ as before. This solution is $3 * 4 * (-1) + 1 * 5 * 1 \equiv 13 \pmod{20}$.

Now we check: $1^2 + 2*1 - 3 \equiv 0 \pmod{20}$ (again, we expect this since $x = 1$ is a solution to the equation $x^2 + 2x - 3 = 0$), and $13^2 + 2 * 13 - 3 \equiv 0 \pmod{20}$.

Theorem 29 (Textbook Theorem 2.20)**.** *Let $f(x)$ be a polynomial with integer coefficients, and for any integer m let $N(m) = \#\{\text{solutions to } f(x) \equiv 0 \pmod m\}$. If $m = \prod p_i^{\alpha_i}$ where the p_i are prime, then $N(m) = \prod N(p^\alpha)$.*

Solution. We will start with $m = p^\alpha q^\beta$ for primes p, q, then apply the same technique to generalize. Let $a_1, a_2, \ldots, a_{N(p^\alpha)}$ be the solutions to $f(x) \equiv 0 \pmod{p^\alpha}$, and $b_1, b_2, \ldots, b_{N(q^\beta)}$ be the solutions to $f(x) \equiv 0 \pmod{b^\beta}$. From Theorem 2.16, we know that a solution to $f(x) \equiv 0 \pmod m$ is also a solution to $f(x) \equiv 0 \pmod{p^\alpha}$ and $f(x) \equiv 0 \pmod{q^\beta}$. So we are looking for solutions that work modulo p^α and q^β. Then for each pair $x \equiv a_i \pmod{N(p^\alpha)}, x \equiv b_j \pmod{N(q^\beta)}$, the Chinese remainder theorem tells us that there exists a unique solution modulo m. There are $N(p^\alpha)N(q^\beta)$ such pairs, so there are at most $N(p^\alpha)N(q^\beta)$ solutions to $f(x) \equiv 0 \pmod m$.

We can also say that for each a_i, b_j, there is a $0 \le x_{ij} \le m$ where $f(x_{ij}) \equiv 0 \pmod{p^\alpha}$ and $f(x_{ij}) \equiv 0 \pmod{q^\beta}$. The Theorem 2.3 part 3 gives us $f(x_{ij}) \equiv 0 \pmod m$. Thus, all possible $N(p^\alpha)N(q^\beta)$ solutions to $f(x) \equiv 0 \pmod m$ are solutions.

Since the Chinese remainder theorem and Theorem 2.3 part 3 apply to arbitrarily many factors, this proof holds with more prime power factors. □

12.2 Groups

Definition. An *equivalence relation* on a set A is denoted $a \sim b$ where:

1. $a \sim a$ is defined for all $a \in A$. Then we say that $\sim$ is *reflexive*.
2. $a \sim b$ implies $b \sim a$ for all $a, b \in A$. Then we say that $\sim$ is *symmetric*.
3. If $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in A$. Then we say that $\sim$ is *transitive*.

Since congruence is an equivalence relation, we can talk about the congruence classes $\{a + mn : a, n \in \mathbb{Z}\}$ modulo m as one element mod m. We will formalize this statement in a bit.

Definition. A *group* is a set A along with a binary operation $*$ where:

1. $a * b \in A$ for all $a, b \in A$. We say A is *closed* under the operation.
2. there exists an element $e \in A$ such that $e * a = a * e = a$ for all $a \in A$. We call e the *identity element*.
3. for each $a \in A$, there exists $\overline{a} \in A$ where $a\overline{a} = \overline{a}a = e$. We call $\overline{a}$ the *inverse*. Another way to phrase this requirement is to say that every element $a \in A$ is *invertible under the binary operation*.
4. $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$ (we say the binary operation is *associative*)

If $a * b = b * a$, we say a *and* b *commute*. If $a * b = b * a$ for all $a, b \in A$, then we say the group is *commutative*.

On the preclass assignment, we saw that addition on the integers modulo m is a group. Since an integer a has a multiplicative inverse modulo m if and only if $(a, m) = 1$ by Theorem 2.9, multiplication on the integers modulo m is a group precisely when m is prime. Multiplication is also commutative.

Definition. A *ring* is a nonempty set, R, together with a two binary operations on R(which we will denote by the symbols, $+$ and $*$), where:

- If $a, b \in R$, then $a + b \in R$ and $a * b \in R$ (we say R is *closed under addition and multiplication*).
- If $a, b, c \in R$, then $(a + b) + c = a + (b + c)$ and $a * (b * c) = (a * b) * c$ (we say addition and multiplication are *associative*).
- There is some $e \in R$ where $a + e = e + a = a$ for all $a \in R$ (we say e is the *additive identity*).
- For every $a \in R$, there is some $b \in R$ where $a + b = e$ (we say b is the *additive inverse of* a).
- For every $a, b \in R$, $a + b = b + a$ (we say addition is *commutative*).
- For ever $a, b, c \in R$, $a * (b + c) = a * b + a * c$ (we say *multiplication distributes*).
- *There is a multiplicative identity. Some sources leave off this requirement and say a ring with a multiplicative identity is a *ring with unity*. We are going to include it.

13 Wednesday: Groups, rings, and fields

Preclass assignment. Write a potential exam question. Solve this question.

Definition. A *group* is a set A along with a binary operation $*$ where:

1. $a * b \in A$ for all $a, b \in A$. We say A is *closed* under the operation.
2. there exists an element $e \in A$ such that $e * a = a * e = a$ for all $a \in A$. We call e the *identity element*.
3. for each $a \in A$, there exists $\overline{a} \in A$ where $a\overline{a} = \overline{a}a = e$. We call $\overline{a}$ the *inverse*. Another way to phrase this requirement is to say that every element $a \in A$ is *invertible under the binary operation*.
4. $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$ (we say the binary operation is *associative*)

If $a * b = b * a$, we say a *and* b *commute*. If $a * b = b * a$ for all $a, b \in A$, then we say the group is *commutative*.

On the preclass assignment for Monday, we saw that addition on the integers modulo m is closed, has an identity, and has additive inverses for every element a which can be written as $m - a$.

We need to check associativity.

Solution. Since $a+(b+c)=(a+b)+c$ in the integers, $[a+(b+c)]-[(a+b)+c]=0$, thus $a+(b+c)\equiv(a+b)+c \pmod m$ for any positive integer m. □

We also saw on the preclass assignment that addition on the integers modulo m is also commutative, so we have a commutative group.

Since an integer a has a multiplicative inverse modulo m if and only if $(a,m)=1$ by Theorem 2.9, multiplication on the nonzero integers modulo m is a group precisely when m is prime. Associativity also comes from the integers and the multiplicative identity is 1. Multiplication is also commutative.

Let's return to Theorem 2.1:

Theorem 30 (Textbook Theorem 2.1)**.** *Let a,b,c,d denote integers, then:*

1. $a\equiv b \pmod m$, $b\equiv a \pmod m$ *and* $a-b\equiv 0 \pmod m$ *are equivalent.*
2. $a\equiv b \pmod m$ *and* $b\equiv c \pmod m$ *implies* $a\equiv c \pmod m$
3. $a\equiv b \pmod m$ *and* $c\equiv d \pmod m$ *implies* $a+c\equiv b+d \pmod m$
4. $a\equiv b \pmod m$ *and* $c\equiv d \pmod m$ *implies* $ac\equiv bd \pmod m$.
5. $a\equiv b \pmod m$ *and* $d\mid m$, $d>0$ *implies* $a\equiv b \pmod d$
6. $a\equiv b \pmod m$ *implies* $ac\equiv bc \pmod{mc}$ *for* $c>0$.

Example 6.
1. The first two equivalences say that congruence mod m is reflexive.
2. This says that equivalence mod m are transitive
3. This says that addition of elements mod m is well defined.
4. This says that multiplication of elements mod m is well defined.

Definition. Two groups $(G,+)$ and $(H,*)$ are *isomorphic* if there exists a bijective map $F: G\to H$ such that $f(a+b)=f(a)*f(b)$ for all $a,b\in G$.

Proposition 31. *Any two complete residue systems mod m are isomorphic as additive groups.*

Proof. Let $\{a_1,a_2,\ldots,a_m\}$ and $\{b_1,b_2,\ldots,b_m\}$ be complete residue systems mod m. Then for each a_i, there exists a unique b_j where $a_i\equiv b_j \pmod m$. Define f to be that map $f(a_i)=b_j$ where $a_i\equiv b_j$. By the definition of complete residue system, this map is injective and surjective. By Theorem 2.1 part 3, $f(a_i+a_k)=f(a_i)+f(a_k)$ since $a_i\equiv f(a_i) \pmod m$ and $a_k\equiv f(a_k) \pmod m$. □

Definition. We use the standard convention that a multiplied by itself n times is a^n and a added to itself n times is na. A group is cyclic is a group where every element can be written as a^n (for multiplication) for some integer n. (For addition, it makes sense to write na instead of a^n). The element a is called the *generator*

Think-Pair-Share. Show that addition mod m is a cyclic group.

Think-Pair-Share. Is multiplication of nonzero integers mod 5 cyclic?

Definition. A *ring* is a nonempty set, R, together with a two binary operations on R(which we will denote by the symbols, $+$ and $*$), where:

- R is a commutative group under $+$.
- If $a,b\in R$, then $a*b\in R$ (we say R is *closed under multiplication*).
- If $a,b,c\in R$, then $a*(b*c)=(a*b)*c$ (we say multiplication are *associative*).

- There is some $e \in R$ where $a * e = e * a = a$ for all $a \in R$ (we say e is the *multiplicative identity*). *Some sources leave off this requirement and say a ring with a multiplicative identity is a *ring with unity*. We are going to include it.
- For ever $a, b, c \in R$, $a * (b + c) = a * b + a * c$ (we say *multiplication distributes*).

Definition. Proving that addition and multiplication on the integers modulo m is a ring is part of Homework 4. We call this ring $\mathbb{Z}_m$ and use the complete congruence class $\{0, 1, 2, \ldots, m-1\}$. Two elements $a, b \in \mathbb{Z}_m$ where $a \equiv b \pmod{m}$ are said to be *representatives of the same congruence class* $\pmod{m}$.

Any two complete residue systems mod m are also isomorphic as rings.

Definition. A *field* is a nonempty set, F, together with two binary operations $+$ and $*$ where:

1. F is a ring.
2. $a * b = b * a$ for all $a, b, \in F$.
3. For all $a \in F, a \neq 0$, there exists $a^{-1} \in F$ where $a * a^{-1} = a^{-1}a = 1$. Here 0 is the additive identity and 1 is the multiplicative identity.

Proving that $\mathbb{Z}_p$ is a field if and only if p is prime is on Homework 4.

14 Friday: Midterm 1

15 Monday: Order of elements $\mathbb{Z}_p$

Preclass assignment. None

Pass back exams. Briefly discuss score distributions and corrections due next Monday: 3 70-79, 4 80-89, 11 90-100. The most missed question was the third True/False, followed by 3c and missing details in 4a and 5.

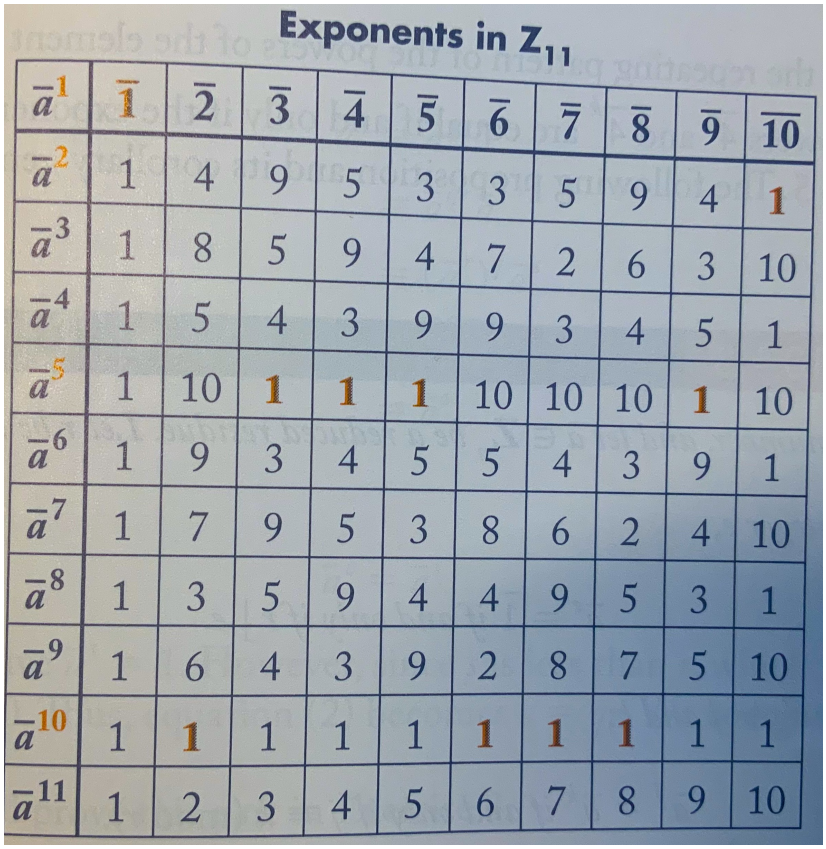
Discuss staying in groups so that we can go back and forth between lecture and working on problems. Today we will have a handout so that they don't have to construct the chart themselves.

We are going to be working through Sections 2.6,2.7, and 2.8. Like with Sections 2.1-2.3, we are not always going to go in order. Today we are going to start with the beginning of Section 2.8, then we will talk about quadratic polynomials. Finally, we will circle back to general polynomials modulo a prime followed by Section 2.6, then the rest of Section 2.8.

Reminder: We shorten the sentence "Let $a, n \in \mathbb{Z}, n > 0, a \pmod{n}$ where $0 \leq a \leq n-1$" to "Let $a \in \mathbb{Z}_n$".

Think-Pair-Share. Look at the chart of $a^n \pmod{11}$. The first column is 1^n, the second column is 2^n, etc. That is, the top of the column is the base, the left gives the exponent, all are reduced mod 11.

1. For each $a \in \mathbb{Z}_{11}$, what is the smallest n such that $a^n = 1$ (ie, what is the smallest n such that $a^n \equiv 1 \pmod{11}$?
2. What patterns do you notice?



Exponents in Z_{11}

$\bar{a}^1$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$
$\bar{a}^2$	1	4	9	5	3	3	5	9	4	1
$\bar{a}^3$	1	8	5	9	4	7	2	6	3	10
$\bar{a}^4$	1	5	4	3	9	9	3	4	5	1
$\bar{a}^5$	1	10	1	1	1	10	10	10	1	10
$\bar{a}^6$	1	9	3	4	5	5	4	3	9	1
$\bar{a}^7$	1	7	9	5	3	8	6	2	4	10
$\bar{a}^8$	1	3	5	9	4	4	9	5	3	1
$\bar{a}^9$	1	6	4	3	9	2	8	7	5	10
$\bar{a}^{10}$	1	1	1	1	1	1	1	1	1	1
$\bar{a}^{11}$	1	2	3	4	5	6	7	8	9	10

Solution. 1. $1^1 \equiv 2^{10} \equiv 3^5 \equiv 4^5 \equiv 5^5 \equiv 6^{10} \equiv 7^{10} \equiv 8^{10} \equiv 9^5 \equiv 10^2 \equiv 1 \pmod{11}$

2. Some patterns people found were: for every number, the smallest n where $a^n \equiv 1 \pmod{11}$ is 1,2,5, or 10. The even power rows are symmetric.[2] □

Think-Pair-Share. For each $a \in \mathbb{Z}_{11}$, what are all of the values of n where $a^n \equiv 1 \pmod{11}$?

Solution. 1,2,5 or 10. □

Think-Pair-Share. Make a similar chart for $\mathbb{Z}_3$ and $\mathbb{Z}_4$. What patterns do you notice?

Solution.

a^1	1	2
a^2	1	2
a^3	1	2

a^1	1	2	3
a^2	1	0	1
a^3	1	0	3
a^4	1	0	1

□

Definition. Let $a \in \mathbb{Z}_n$ be a reduced residue (ie, $(a, n) = 1$). The *order of a in $\mathbb{Z}_n$* is the smallest positive integer r such that $a^r \equiv 1 \pmod{n}$. Our textbook just gives the order a name (often h) when it is notationally useful, but the standard notation is $\text{ord}_n(a)$.

From the previous exercise, what can you guess about $\text{ord}_n(a)$?

[2] We will prove this Wednesday, I was not expecting this pattern

Think-Pair-Share (Textbook Lemma 2.31)**.** Let $n \in \mathbb{Z}, n > 0, a \in \mathbb{Z}_n$ where $(a, n) = 1$, and $r = \text{ord}_n(a)$. For an integer e, $a^e \equiv 1 \pmod{n}$ (or $a^e = 1$ in $\mathbb{Z}_n$) if and only if $r \mid e$.

Solution. □

Proof. ($\Leftarrow$) Assume $r \mid e$. Then there exists an integer k where $e = rk$. By exponent rules,

$$a^e \equiv a^{rk} \equiv (a^r)^k \equiv 1^k \equiv 1 \pmod{n}.$$

($\Rightarrow$) (*Proof by contradiction*) Assume $a^e \equiv 1 \pmod{n}$. To get a contradiction, assume that $r \nmid e$. By the division algorithm, there exist q, b where $e = rq + b$ and $0 < b < r$. By assumption, we have $1 \equiv a^e \equiv a^{rq+b} \equiv a^{rq}a^b \equiv a^b \pmod{n}$. By assumption, r is the smallest positive integer where $a^r \equiv 1 \pmod{n}$, we have a contradiction. Thus, $r \mid e$.

(*Direct proof*) Assume $a^e \equiv 1 \pmod{n}$. Then by the division algorithm, there exist q, b where $e = rq+b$ and $0 \leq b < r$. By assumption, we have $1 \equiv a^e \equiv a^{rq+b} \equiv a^{rq}a^b \equiv a^b \pmod{n}$. By assumption, r is the smallest positive integer where $a^r \equiv 1 \pmod{n}$, we have that $b = 0$. Thus, $r \mid e$. □

Theorem 32 (Textbook Theorem 2.36)**.** *Let p be prime and $a \in \mathbb{Z}_p, a \neq 0$. Then* $\text{ord}_p(a) \mid p - 1$.

Proof. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Then from the previous theorem, $\text{ord}_p(a) \mid p - 1$. □

16 Wednesday: Order of elements $\mathbb{Z}_p$, quadratic polynomials mod n, polynomials mod p.

Preclass assignment. How many incongruent solutions are there to $x^2 \equiv 1 \pmod{8}$? Why does this not violate Theorem 10.2.1 in the reading? What part of the proof of Theorem 10.2.1 no longer holds?

Solution. The incongruent solutions are 1,3,5, and 7. 8 is not prime. At equation 6, the proof uses the fact that $\mathbb{Z}_p$ does not have 0 divisors when p is prime. □

First, let's return to the pattern in the exponent table: that the even exponent rows are symmetric mod 11. It turns out that this is true for all mods, not just prime. We need to translate this into a math statement that we can prove:

Theorem 33. *For positive integers m and k and any integer a, $a^{2k} \equiv (m - a)^{2k} \pmod{m}$.*

Proof. First we note that $-a \equiv m - a \pmod{m}$ for any integer a and positive integer n. By repeated applications of modular multiplication (or induction), we have seen that $(-a)^n \equiv (m - a)^n \pmod{m}$ for any nonnegative integer n. Then $(m - a)^{2k} \equiv (-a)^{2k} \equiv (-1)^{2k}a^{2k} \equiv a^{2k} \pmod{m}$. □

We will finish the discussion of order of an element (for now).

Theorem 34 (Lemma 2.33)**.** *Let $a, m \in \mathbb{Z}, m > 0$, and $(a, m) = 1$. Then for any positive integer k,* $\text{ord}_m(a^k) = \dfrac{\text{ord}_m(a)}{(k, \text{ord}_m(a))}$.

Proof. From Lemma 2.31, $(a^k)^{\text{ord}_m(a^k)} \equiv 1 \pmod{m}$ if and only if $\text{ord}_m(a) \mid k \,\text{ord}_m(a^k)$. We also have that this is true if and only if $\frac{\text{ord}(a)}{(k,\text{ord}(a))} \mid \frac{k}{(k,\text{ord}(a))} \text{ord}(a^k)$. Now we have that $\left(\frac{\text{ord}(a)}{(k,\text{ord}(a))}, \frac{k}{(k,\text{ord}(a))}\right) = 1$, so $\frac{\text{ord}(a)}{(k,\text{ord}(a))} \mid \text{ord}(a^k)$. Thus, the smallest integer where this is true is $\frac{\text{ord}(a)}{(k,\text{ord}(a))}$. □

Alternate proof with names for $\text{ord}_m(a)$ and $\text{ord}_m(a^k)$:

Proof. Let $\text{ord}_m(a) = h$ and $\text{ord}_m(a^k) = j$. From Lemma 2.31, $(a^k)^j \equiv 1 \pmod{m}$ if and only if $h \mid kj$. We also have that this is true if and only if $\frac{h}{(k,h)} \mid \frac{k}{(k,h)}j$. Now we have that $\left(\frac{h}{(k,h)}, \frac{k}{(k,h)}\right) = 1$, so $\frac{h}{(k,h)} \mid j$). Thus, the smallest integer j where $(a^k)^j \equiv 1 \pmod{m}$ is $\frac{h}{(k,h)}$. □

Quadratic polynomials mod n

Let's take a minute go back to the integers. For integers a, b and c, we have a formula for when $ax^2 + bx + c = 0$. We are going to start with this familiar case.

Theorem 35. *Let $a, b, c \in \mathbb{Z}$ where $a \neq 0$. Consider the polynomial equation*

$$ax^2 + bx + c = 0. \tag{★}$$

Let $d = b^2 - 4ac$.

1. *If there exists $s \in \mathbb{Z}$ such that $s^2 = d$, then the rational solutions to ★ are*

$$x = (-b + s)(2a)^{-1} \quad \text{and} \quad x = (-b - s)(2a)^{-1}.$$

2. *If no such s exists, there is no rational solution. If $d < 0$, no real solution exists.*

Proof. We are going to derive the quadratic formula. Since we have an idea of where we are going, we start with multiplying through by $4a$.

$$4a^2x^2 + 4abc + 4ac = 0 \tag{1}$$
$$4a^2x^x + 4abx = -4ac \tag{2}$$
$$4a^2x + 4abx + b^2 = b^2 - 4ac \tag{3}$$
$$(2ax + b)^2 = d \tag{4}$$
$$2ax + b = \pm\sqrt{d} \tag{5}$$
$$x = \frac{-b \pm \sqrt{d}}{2a}. \tag{6}$$

Thus, if there exists an integer s where $s^2 = d$, x is rational. Otherwise, there are no rational solutions, and if $d < 0$ there are no real solutions. □

Think-Pair-Share. Without talking, write on an index card: which steps might not work for modular arithmetic. Think to yourself, this is a quick gut-check, write it down by the time everyone has a card. Hold it up where I can see it (you can hold it close to yourself), then we will do the pair-share steps.

Solution. Step 5 does not always exist in the integers (or real numbers), and this is also true mod p. Step 6 also might not work. □

For modular arithmetic, we do not have square roots and may not have multiplicative inverses. We may also have zero divisors. We can avoid some of these problems by working modulo a prime.

Theorem 36. *Let $p > 2$ be prime, and $a, b, c \in \mathbb{Z}_p$ where $a \not\equiv 0$. Consider the polynomial congruence*

$$ax^2 + bx + c \equiv 0 \pmod{p}. \qquad (\bigstar\bigstar)$$

Let $d \in \mathbb{Z}_p$ where $d \equiv b^2 - 4ac \pmod{p}$.

1. *If there exists $s \in \mathbb{Z}_p$ such that $s^2 = d$ (ie, $s^2 \equiv d \pmod{p}$), then the rational solutions to $\bigstar\bigstar$ are*

$$x \equiv (-b + s)(2a)^{-1} \pmod{p} \quad \text{and} \quad x \equiv (-b - s)(2a)^{-1} \pmod{p},$$

   where $(2a)^{-1}$ denotes the multiplicative inverse of $2a \pmod{p}$.

2. *If no such s exists, there is no solution in $\mathbb{Z}_p$.*

Proof. Since we have an idea of where we are going, we start with multiplying through by $4a$.

$$\begin{aligned} 4a^2x^2 + 4abc + 4ac &\equiv 0 \pmod{p} \\ 4a^2x^x + 4abx &\equiv -4ac \pmod{p} \\ 4a^2x + 4abx + b^2 &\equiv b^2 - 4ac \pmod{p} \\ (2ax + b)^2 &\equiv d \pmod{p} \end{aligned}$$

Thus, if there exists an $s \in \mathbb{Z}_p$ where $s^2 \equiv d \pmod{p}$,

$$\begin{aligned} 2ax + b &\equiv \pm s \pmod{p} \\ x &\equiv (-b \pm s)(2a)^{-1} \pmod{p}. \end{aligned}$$

If no such s exists, then there is no integer $2ax + b \equiv d \pmod{p}$, and thus no such x exists. □

Think-Pair-Share. Why do we need $p > 2$? How many different quadratic polynomials are there mod 2? What are their roots?

Solution. $2a \equiv 0 \pmod{2}$ for every integer a. There are four polynomials: $x^2 + x + 1$ with no roots, $x^2 + x$ with roots $0, 1$, $x^2 + 1$ with root 1, and x^2 with root 0. □

What happens for composite modulus?

Think-Pair-Share. Without talking, write on an index card: which steps might not work for composite modulus. Think to yourself, this is a quick gut-check, write it quickly on the other side of your card. Hold it up where I can see it (you can hold it close to yourself), then we will do the pair-share steps.

Solution. Multiplicative inverses may not exist. □

There may not be a multiplicative inverse. On the preassignment, we saw that $x^2 \equiv 1 \pmod{8}$ has four incongruent solutions. From the very end of Section 2.3, we have that we can break composite cases into prime power moduli (like mod 8).

17 Friday: Polynomials mod p.

Preclass assignment. None.

Remember that it is possible to have extra assumptions in a theorem. If you never use an assumption in the proof, it is not necessary. For example, if we say "If cows are purple, a and m are integers, and $(a, m) = 1$, then $ax \equiv 1 \pmod{m}$ has a unique solution," this is still true if we find a brown cow, because the proof did not involve cows. We did, however, use the fact that a and m are relatively prime, so we can't get rid of that assumption. Throughout this section, be on the look out for when we use the fact that p is prime.

Think-Pair-Share. True/False (cards): $a_n x^n + a^{n-1}x^{n-1} + \cdots + a_1 x + a_0$ has more than n roots mod p and p is prime if and only if p divides every coefficient.

Think quietly, hold up card, then discuss with neighbor.

Theorem 37 (Textbook Theorem 2.26, Lagrange)**.** *Let p be a prime number and let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be a polynomial of degree $n \geq 0$ with integral coefficients where $p \nmid a_n$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n incongruent solutions mod p (in other words, at most n solutions in $\mathbb{Z}_p$).

Proof. We are going to use induction on the degree n. If $n = 0$, then $f(x) \equiv a_0 \equiv 0 \pmod{p}$ has no (ie, 0) solutions since we assumed $p \nmid a_0$. For $n = 1$, we have that $f(x) = a_1 x + a_0$ where $p \nmid a_1$. Since p is prime, this guarantees $(a_1, p) = 1$ and $a_1 x \equiv -a_0 \pmod{p}$ has exactly one incongruent solution by Theorem 2.9, so the theorem holds for $n = 1$.

Next, we induct. Assume that the theorem is true for all $n = k \geq 1$. Then we need to show that the theorem is true for $n = k+1$. Let $f(x) = a_{k+1}x^{k+1} + a_k x^k + \cdots a_1 x + a_0$ where $p \nmid a_{k+1}$. If there are no solutions to $f(x) \equiv 0 \pmod{n}$, then the theorem is true and we are done.

If $f(x) \equiv 0 \pmod{p}$ has at least one solution a_1, then we can factor out $x - a_1$. However, proving this is difficult, and we need to show that modulo a prime is enough to say we have reduced the degree. We are going to use a different method.

Let's relate this to the proof we have already seen: assume there are $k + 2$ distinct roots mod p, and call them $d_1, d_2, \ldots, d_{k+2}$. Then we define $h(x) = f(x) - a^{k+1}(x - d_1)(x - d_2)\cdots(x - d_{k+1})$. Then $h(x)$ has at least $k+1$ distinct roots mod p.

Case1: If every coefficient of $h(x)$ is $0 \pmod{p}$, then $h(x) \equiv 0 \pmod{p}$ for all integers x. Then $f(d_{k+2}) \equiv 0 \pmod{p}$ and $h(d_{k+2}) \equiv 0 \pmod{p}$ implies d_{k+2} is a root of $a^{k+1}(x-d_1)(x-d_2)\cdots(x-d_{k+1}) \bmod p$. But this is a contradiction, since none of the factors are 0 and p is prime.

Case 2: $h(x)$ is not identically 0. Then $h(x)$ has degree less $n = k + 1 \bmod p$. By induction hypothesis, $h(x)$ has at more k roots, so $f(x)$ has at more k roots. □

Contents

18 Monday: Polynomials mod p

Preclass assignment. Let $f(x) = ax + b, g(x) = cx + d$. Find integers of a, b, c, d, and m, $a, c, m > 0$, where $f(x)g(x)$ is constant mod m.

Solution. One easy solution is to find $ac = m$. The smallest composite number is $m = 4$, so one solutions is $f(x) = 2x + 1, g(x) = 2x + 3$, and $f(x)g(x) = 4x^2 + 8x + 3 \equiv 3 \pmod 2$. □

We are going to come back to when we can factor out a root–it turns out that this is a fairly complicated proof even for the rationals, and even more complicated for integers. In short–we only sorta can factor out linear factors from polynomials with integer coefficients to still have integer coefficients. For something like the Euclidean algorithm, we want to be able to divide any a by any b, and find a unique q and r where $a = bq + r$ and $0 \leq r < b$. For polynomials with integer coefficients, we can divide one polynomial by another polynomial (ie, factor) when the degree of the factor is smaller, but we also need to be careful about getting rational coefficients instead of integer coefficients. The textbook is a bit sloppy about using the division algorithm for rational polynomials to apply to polynomials mod p. The reason this works is that both the rationals and $\mathbb{Z}_p$ are fields. The integers and $\mathbb{Z}_m$ are not (where m is composite).

Theorem 38 (Textbook Theorem 2.25)**.** *Let p be prime. If the degree of $f(x) \equiv 0 \pmod p$ is greater than p, then either $f(x) \equiv 0 \pmod p$ for every integer x or there exists a polynomial $g(x)$ with degree less than p where $f(x) \equiv g(x) \pmod p$ for every integer x. In the second case, we can find a polynomial $h(x)$ with leading coefficient 1 which has the same roots mod p as $f(x)$.*

Proof. If every integer x is a solution to $f(x) \equiv 0 \pmod p$, we are done. We need to worry about the case where this is not true.

Since p is prime, Fermat's little theorem tells us that $a^{p-1} \equiv 1 \pmod p$ for all $a \not\equiv 0 \pmod p$. Thus, $a^p \equiv a \pmod p$ for all integers, since $0^p \equiv 0 \pmod p$. Thus, for $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_p x^p + \cdots + a_1 x + a_0$, there exist $q_n, q_{n-1}, \ldots q_p$ and $) \leq r_n, r_{n-1}, \ldots, r_p < p$ such that $n = q_n * p + r_n, n-1 = q_{n-1} * p + r_{n-1} \ldots n - n - p - 1 = p + 1 = q_{p+1} * p + r_{p+1}$. Since $x^p \equiv x \pmod p$ for all x, we can replace each $x^i = (x^p)^{q_i} x^{r_i}$ with x^{r_i+1} for $i = p+1, \ldots, n$ and x^p with x. If $q_i + r_i > p - 1$, repeat this process until we to get a polynomial of degree less than p that agrees with $f(x) \bmod p$ for every integer x. This is our $g(x)$.

Now assume $g(x) = b_{p-1}x^{p-1} + b_{p-2}x^{p-2} \ldots b_1 x + b_0 \pmod p$ with degree $i < p \bmod p$. Then by definition of degree, $b_i \not\equiv 0 \pmod p$. If $b_i \equiv 1 \pmod p$, then we are done. Otherwise, there exists a multiplicative inverse mod p, $\overline{b_i}$. Then $\overline{b_i} g(x)$ has leading coefficient 1, degree less than p, and $\overline{b_i} g(x) \equiv 0 \pmod p$ if and only if $g(x) \equiv 0 \pmod p$. □

Think-Pair-Share. Find $g(x)$ such that $f(x) \equiv g(x) \pmod p$ for all x, and $h(x)$ such that $f(x)$ and $h(x)$ have the same roots mod p and the leading coefficient of $h(x)$ is 1:

$$f(x) = x^{20} + x^{13} + x^7 + x \pmod 3$$
$$f(x) = x^{20} + x^{13} + x^7 + x \pmod 5$$
$$f(x) = x^{20} + x^{13} + x^7 + x \pmod 7$$

Solution. For the first congruence, $20 = 3*6+2, 13 = 3*4+1, 7 = 3*2+1$, so the congruence becomes

$$\begin{aligned} g(x) &\equiv x^{20} + x^{13} + x^7 + x \pmod 3 \\ &\equiv (x^3)^6 x^2 + (x^3)^4 x^1 + (x^3)^2 x^1 + x \pmod 3 \\ &\equiv x^6 x^2 + x^4 x^1 + x^2 x^1 + x \pmod 3 \\ &\equiv (x^3)^2 x^2 + x^3 x^2 + x^3 + x \pmod 3 \\ &\equiv x^2 x^2 + x x^2 + x + x \pmod 3 \\ &\equiv x^3 x^1 + x^3 + 2x \pmod 3 \\ &\equiv x x^1 + x + 2x \pmod 3 \\ &\equiv x^2 + 3x \pmod 3 \\ &\equiv x^2 \pmod 3. \end{aligned}$$

Since $g(x)$ has leading coefficient 1, it is also our $h(x)$.

For the second congruence, $20 = 4*5, 13 = 2*5+3, 7 = 5+2$, so the congruence becomes

$$\begin{aligned} g(x) &\equiv x^{20} + x^{13} + x^7 + x \pmod 5 \\ &\equiv (x^5)^4 + (x^5)^2 x^3 + x^5 x^2 + x \pmod 5 \\ &\equiv x^4 + x^2 x^3 + x x^2 + x \pmod 5 \\ &\equiv x^4 + x^5 + x^3 + x \pmod 5 \\ &\equiv x^4 + x + x^3 + x \pmod 5 \\ &\equiv x^4 + x^3 + 2x \pmod 5. \end{aligned}$$

Since $g(x)$ has leading coefficient 1, it is also our $h(x)$.

For the third congruence, $20 = 7*2+6, 13 = 7+6$, so the congruence becomes

$$\begin{aligned} g(x) &\equiv x^{20} + x^{13} + x^7 + x \pmod 7 \\ &\equiv (x^7)^2 x^6 + x^7 x^6 + x^7 + x \pmod 7 \\ &\equiv x^2 x^6 + x x^6 + x + x \pmod 7 \\ &\equiv x^7 x + x^7 + 2x \pmod 7 \\ &\equiv x x + x + 2x \pmod 5 \\ &\equiv x^2 + 3x \pmod 5. \end{aligned}$$

Since $g(x)$ has leading coefficient 1, it is also our $h(x)$. □

19 Wednesday: Revisiting the Chinese remainder theorem, primitive roots

We are getting into really theoretical material. Not all of the sections on the syllabus is a required part of the course, and some is better handled in an abstract algebra course or numerical methods course. It's going to be better to spend more time understanding this material, and skipping 2.4. I have some other material on primality testing that we can use instead. It actually ties in with today's material on primitive roots, so I put it on Carmen for Friday.

19.1 Revisiting the Chinese remainder theorem

Let's go back to the homework for a second. I think there was a decent amount of confusion on the Chinese Remainder Theorem problem, so let's start there:

Theorem 39. *The system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a solution if and only if $(m_i, m_j) \mid a_j - a_i$ *for all* $i, j = 1, \ldots, n$.

Solution. Let's start with the case where $n = 2$ and see how this generalizes. Start with definitions: $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$ if and only if there exist integers k_1, k_2 such that $m_1k_1 = a_1 - x, m_2k_2 = a_2 - x$. Subtracting one equation from the other, we see that this is true if and only if $m_1k_1 - m_2k_2 = a_1 - x - a_2 + x = a_1 - a_2$. Since $(m_1, m_2) \mid m_1k_1 - m_2k_2$, we see that the congruence has a solution if and only if $(m_1, m_2) \mid a_1 - a_2$. (In office hours we took a slightly different approach to show that the solution is unique mod$[m_1, m_2]$). For a given solution y, $x \equiv y \pmod{m_1}, x \equiv y \pmod{m_2}$ if and only if $x \equiv y \pmod{[m_1, m_2]}$ by Theorem 2.3.

Now to generalize: ($\Rightarrow$) for a system of n congruences, if any pair does not have a solution, then the entire system does not have a solution. That is, if there exists i, j where $(m_i, m_j) \nmid a_i - a_j$, then no solution exists. Thus, if a solution exists, $(m_i, m_j) \mid a_j - a_i$ for all $i, j = 1, \ldots, n$.

($\Leftarrow$) Assume that $(m_i, m_j) \mid a_j - a_i$ for all $i, j = 1, \ldots, n$, and proceed by induction. That is, assume that a system of $k < n$ such congruences has a solution y. Here it is useful to use Theorem 2.3 again. A y where

$$\begin{aligned} x &\equiv y \pmod{m_1} \\ x &\equiv y \pmod{m_2} \\ &\vdots \\ x &\equiv y \pmod{m_{n-1}} \end{aligned}$$

exists if and only if $x \equiv y \pmod{[m_1, m_2, \ldots, m_{n-1}]}$. Now we have a system of two congruences: $x \equiv y \pmod{[m_1, m_2, \ldots, m_{n-1}]}$ and $x \equiv a_n \pmod{m)_n}$. Then, by our inductive hypothesis, a solution to this congruence exists. □

19.2 Primitive roots

Definition. Let p be a prime, and let $a \in \mathbb{Z}_p$ with $a \neq 0$ (ie, $0 < a \leq p - 1 \pmod{p}$). Then a is a *primitive root* in $\mathbb{Z}_p$ if $\text{ord}_p(a) = p - 1$. We can also say that a *is a primitive root mod* p.

We looked at powers modulo 11 last week. As a review, we have

$$\begin{aligned} &\text{ord}_{11}(1) = 1, \\ &\text{ord}_{11}(10) = 2, \\ &\text{ord}_{11}(3) = \text{ord}_{11}(4) = \text{ord}_{11}(5) = \text{ord}_{11}(9) = 5, \\ &\text{ord}_{11}(2) = \text{ord}_{11}(6) = \text{ord}_{11}(7) = \text{ord}_{11}(8) = 10. \end{aligned}$$

Thus, the primitive roots modulo 11 are 2,6,7, and 8.

Contents

20 Monday: Primality testing

We have seen a lot of places where it is useful to have prime numbers. We need to be able to determine if a number is prime or composite. Factoring is slow, so we would like a better algorithm.

For the preclass assignment, we looked at $a^{n-1} \pmod n$. If $a^{n-1} \not\equiv 1 \pmod n$, we know that n is composite. In this case, we say that a is a *Fermat witness to the compositeness of n.*

Think-Pair-Share. 1. Is there a Fermat witness to the compositeness of 4?

2. Using this test, $2^{340} \equiv 1 \pmod{341}$. What can we conclude?

Solution. 1. $2^3 \equiv 0 \pmod 4$ is a witness. $3^3 \equiv 3 \pmod 4$.

2. That 2 is not a Fermat witness for 341. In fact, $3^{340} \equiv 56 \pmod{341}$. □

Think-Pair-Share. A *nontrivial* factor of a number n is a factor that is not equal to ± 1 or $\pm n$. It is nontrivial because all numbers n have ± 1 and $\pm n$ as factors. Are all *nontrivial* factors of positive composite integers n Fermat witnesses to the compositeness of n? Prove or provide counterexample.

Solution. Let a be a factor of n. If $a^{n-1} \equiv 1 \pmod n$, then $n \mid a^{n-1} - 1$. Since division is transitive, $a \mid a^{n-1} - 1$. Since $a \mid a^{n-1}$, we must have that $a \mid 1$. Thus, the only factor of n that is not a Fermat witness is ± 1. □

Definition. A *Carmichael number* is a composite integer where for every integer a where $(a, n) = 1$ implies $a^{n-1} \equiv 1 \pmod n$.

The smallest Carmichael number is $561 = 3 * 11 * 17$. There are only 43 Carmichael numbers less than 1 million, but Alford, Granville, and Pomerance proved that there are infinitely many in 1994.

Theorem 40. *Let n be a positive composite integer. Then n is a Carmichael number if and only if*

1. *For every prime p such that $p \mid n$, we have $p - 1 \mid n - 1$.*
2. *n is the product of distinct primes (ie, n is* square free *meaning no prime is raised to a power higher than 1).*

Proof. ($\Leftarrow$) Let n be composite and assume (1) and (2) are true. Then $n = p_1 p_2 \dots p_s$ where the p_j are distinct and $p_j - 1 \mid n - 1$.

In order to show that n is a Carmichael number, we need to show that $a^{n-1} \equiv 1 \pmod n$ for every integer a where $(a, n) = 1$. If $(a, n) = 1$, then $a^{p_j - 1} \equiv 1 \pmod{p_j}$ by Fermat's Little Theorem. Since $p_j - 1 \mid n - 1$, there exists a positive integer k_j such that $(p_j - 1)k_j = n - 1$. Thus, $a^{n-1} \equiv a^{(p_j-1)k_j} \equiv 1 \equiv 1^{k_j} \equiv 1 \equiv \pmod{p_j}$. Thus, we have a system of congruences

$$\begin{aligned} x = a^{n-1} &\equiv 1 \pmod{p_1} \\ x = a^{n-1} &\equiv 1 \pmod{p_2} \\ &\vdots \\ x = a^{n-1} &\equiv 1 \pmod{p_s}. \end{aligned}$$

By the Chinese remainder theorem, there exists a unique solution to this system of congruences modulo n, we want to show that the solution is $1 \pmod n$. There is a one-to-one correspondence between systems of congruences modulo $p_1, p_2, \dots, p_s$ and possible solutions modulo n. By the corollary to the Chinese remainder theorem, there is a unique system of congruences modulo $p_1, p_2, \dots, p_s$ with solution $x \equiv 1 \pmod n$. By Theorem 2.1 part 4, since each $p_j \mid n$, if $x \equiv 1 \pmod n$, then $x \equiv 1 \pmod{p_j}$. Thus, $x = a^{n-1} \equiv 1 \pmod n$.

($\Rightarrow$) This is much harder. More primality testing and proving this theorem is a possible optional topic. $\square$

We have a related test:

Theorem 41. *Let n be a positive integer. If an integer a exists such that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all prime divisors q of $n-1$, then n is prime.*

Proof. Since $a^{n-1} \equiv 1 \pmod{n}$, we have that $\text{ord}_n(a) \mid n-1$, so there exists positive integer k such that $n-1 = k\,\text{ord}_n(1)$. We want to show that $k = 1$. In order to get a contradiction, assume that $\text{ord}_n(1) \neq n-1$, so $k > 1$. Let q be a prime divisor of k, and thus $n-1$. Thus,

$$a^{(n-1)/q} = a^{k(\text{ord}_n(a))/q} = (a^{\text{ord}_n(a)})^{k/q} \equiv 1 \pmod{n}.$$

This is a contradiction. Now, $\text{ord}_n(a) \leq \phi(n) \leq n-1$. Since $\text{ord}_n(a) = n-1$, we have that $\phi(n) = n-1$ and thus n is prime. $\square$

21 Wednesday: Primality testing, Diffie-Hellman Key Exchange

Think-Pair-Share. Why can we conclude n is prime when $\phi(n) = n-1$?

Solution. For all integers n, there are $n-1$ positive integers less than n. Thus, $\phi(n) \leq n-1$. If the exists some other factor of n, then it is not relatively prime to n, and thus $\phi(n) \leq n-2$. $\square$

(This next exercise is based on the Chocolate Key Cryptography file on Carmen and an exercise from the Summer Illinois Math Camp). On homework 3, we saw some basics of encrypting secret messages: translate the alphabet into the integers 1-26, pick an encryption scheme and an encryption key. With the Caesar shift, we add 3. We can actually avoid the modular arithmetic by using this decoder wheel.

The word DOG becomes GRJ, and we can undo this by applying -3. There are many problems with this encryption scheme, including that it's not hard for a computer to check all 25 additive schemes, or really even all 26! possible schemes that send one letter of the English alphabet to another. However, for any encryption scheme, there is an issue of communicating sharing both the encryption rules and the key. If you know how to encrypt a message, then in theory you know how to decrypt it. We need to come up with a way to share keys and rules that does not give away how to decrypt the message.

We are going to do a thought experiment.

Think-Pair-Share. Alice wants to buy something from Bob. She has to put her credit card into his website, so she wants to make sure it is encrypted. They have some sort of magical encryption device where they can use the content of these envelopes to encrypt and decrypt her credit card number, but only if the content of both envelopes is identical. The eavesdroppers (Eve) cannot see the content of the envelopes when they are closed, or when Alice or Bob are putting pieces in, but she can see inside if either Alice or Bob looks. Also, anyone holding the envelope can magically duplicate the contents and use it for encryption and decryption...

The tricky part is for Alice and Bob to obtain identical envelopes to begin with, without anyone else obtaining copies of those envelopes or guessing their contents (knowledge of the contents would allow someone else to create an identical envelope thus defeating the purpose of encrypting the message.)

I am going to pass out some envelopes with wooden triangles, black circles, and white circles. You will work in groups of 3 (or 4). First, empty both envelopes. Then figure out a method of making sure both envelopes have exactly the same number of wooden triangles, black circles, and white circles. You cannot communicate any sort of algorithm for deciding this, since this algorithm could be intercepted by the third person! You may also not remove anything from the envelope (other than emptying the envelope to start). If we did this with two tins with a coin slot, instead of

envelopes, the rule would be that you can put triangles and circles into the tin, but no one, including Alice and Bob can remove the lid.

Ideally, you should come up with something that works with one person in the hallway and one in the room.

We will also demonstrate with Skittle and containers more like the ones that are supposed to be used in the activity. Give students about 5 minutes then give the hint that they don't have to know the content of the envelope and they can switch envelopes. Give about 5 more minutes, then ask if any are confident, but they have to explain the plan with Skittles, the new containers, and one person on either end of the classroom. If no one thinks theirs will work, give it a bit longer.

Solution. Alice and Bob both put pieces in their envelope, remember what they did, then switch envelopes and put the same pieces in. □

How does this relate to real world encryption algorithms? Diffie-Hellman key exchange works by exchanging encryption keys modulo a prime p. One difficult step of this is finding a primitive root modulo p.

22 Friday: Practice with additive ciphers, Diffie-Hellman, and RSA

a	b	c	d	e	f	g	h	i	j	k	l	m
01	02	03	04	05	06	07	08	09	10	11	12	13
n	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	26
space	.	,										
27	28	00										

In order to send encrypted messages, we must convert to numbers. To get a feel for how these encryption rules work, we are going to work with small numbers.

To convert the word CAT to numbers, we use this chart: 03 01 20. First, we are going to work modulo 29. Using additive key 3, the encrypted message is 06 04 24.

If we know that the message 08 18 10 was encrypted with additive key 3 modulo 29, we can decrypt by subtracting 3 to get 05 15 07, then convert to letters to get DOG.

We are going to start with Diffie-Hellman key exchange to get an additive key modulo 29. $29 = 2 * 14 + 1$ and 14 is not prime, so it is not quite as easy to find a primitive root as the examples in the preclass assignment. The possible orders of elements modulo 29 are: 1, 2, 4, 7, 14, 28. Checking the possibilities, 2 and 3 are both primitive roots. (Remember, exponentiation is much faster than logarithms).

Think-Pair-Share.

- Public knowledge: working modulo $p = 29$ with primitive root $a = 2$.
- Private knowledge: Alice randomly generates $m = 3$ and Bob randomly generates $n = 8$.

1. Calculate the publicly published $a^m \pmod p$ and $a^n \pmod p$.
2. Calculate the privately known $(a^m)^n \equiv (a^n)^m \pmod p$.
3. Use the table and additive key a^{mn} to encrypt the message "CAT AND DOG".

Solution.

1. $2^3 \equiv 8 \pmod 2)9$ and $2^8 \equiv 24 \pmod 2)9$
2. $24^3 \equiv (-5)^3 \equiv -25 * 5 \equiv 4 * 5 \equiv 20 \pmod 2)9$.
3. Translate to numbers: 03 01 20 27 01 14 04 27 04 15 07. Add 20 modulo 29: 23 21 11 18 21 05 11 06 27 □

We can also look at messages for RSA. The person decrypting the message:

- Calculates $n = pq$ for distinct primes p, q. The smallest such n greater than 26 is $n = 7 * 5 = 35$.
- Calculates $\phi(n)$.
- Choses e such that $(e, \phi(n)) = 1$.
- Use the Euclidean algorithm (or some other method) to find d such that $ed \equiv 1 \pmod{\phi(n)}$.
- Publishes n and e so that anyone can encrypt a message m modulo e.

The person decrypting the message:

- Converts the message to numbers.
- Calculates $m^e \pmod{n}$.
- Publishes/sends the message.

The person decrypting now calculates $(m^e)^d \equiv m^{k\phi(n)+1} \equiv m \pmod{n}$.

Lemma 42 (Textbook Lemma 2.22)**.** *Let n be a positive integer. If $(e, \phi(n)) = 1$ for some integer e, then there exists an integer d such that $ed \equiv 1 \pmod{\phi(n)}$ by Theorem 2.9. For any positive integer m, $m^{ed} \equiv m \pmod{n}$.*

Proof. If $m \equiv 0 \pmod{n}$, we are done, since $0^a \equiv 0 \pmod{n}$ for any nonzero integer a. Otherwise, we use the fact that $ed \equiv 1 \pmod{\phi(n)}$ means there exists an integer k such that $k\phi(n) = ed - 1$. Thus, $m^{ed} \equiv m^{k\phi(n)+1} \equiv m \pmod{n}$. □

Theorem 43 (Part of Textbook Theorem 2.19)**.** *If $n = pq$ for distinct primes p and q, $\phi(n) = (p-1)(q-1)$.*

Proof. There are $n - 1 = pq - 1$ positive integers less that n. Now, we need to determine how many are relatively prime to n. We do this by subtracting off those that are not relatively prime. Here, we have $p, 2p, \ldots, (q-1)p$ are $q-1$ distinct positive integers less that n that are not relatively prime to n. Now we can say $\phi(n) \leq n-1-(q-1) = pq-q$. We repeat this process for q: $q, 2q, \ldots, (p-1)q$. This list is disjoint from the other since p and q are relatively prime. Thus $\phi(n) \leq pq - q - p + 1$. Since p and q are the only prime factors of n, these two lists give all possible numbers less that n that are not relatively prime to n. Thus, $\phi(n) = pq - q - p + 1 = (p-1)(q-1)$. □

If we use $n = 12$, this theorem breaks down for factors $2, 6$, since they are not relatively prime. We would get the lists $2, 2(2), 3(2), 4(2), 5(2)$ and 6. Notice that 6 is on both lists, but 3 and 9 are not on either list. We will prove that $\phi(12) = \phi(3)\phi(4)$, although this counting method does not work (2 and 10 will not be on either list).