1. Divisibility in the Integers

The first part of the class was devoted to introducing the goals of the course and describing the content and logistics. While discussing the intrigue of the integers, the following quotation by Plato was pointed out. (It is believed that Plato displayed this message above the entrance to his Academy.)

Quote: [Plato] "Let no one ignorant of Mathematics enter here."

We then went on to build a framework for our discussions. The symbol $\mathbb{Z}$ is used to denote the set of integers. This sounded a bit strange to some when Susan said it out loud (since she has a Canadian accent), leading to a discussion of why we use the last letter of the alphabet. This notation comes from the German word *Zahl* which means number. Using set notation we have

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

We listed other number systems: $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of natural numbers; $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ is the set of natural numbers and zero; the rational numbers, denoted by $\mathbb{Q}$, is the set of all fractions of integers; the real numbers ($\mathbb{R}$) involve both rational and irrational numbers; and the complex numbers ($\mathbb{C}$) involve real and imaginary numbers.

After comparing various number systems we listed a few notational items that may be convenient. For example, the symbol $\in$ is used to mean "is a member of". So we would write $a \in \mathbb{Z}$ to indicate that the number a is an integer. We may sometimes write $\forall$ to mean "for all". Finally, the symbol $\exists$ stands for "there exists". Using this notation we re-wrote our definition of the rational numbers as:

$$\mathbb{Q} = \left\{ x \mid \ \exists\, m, n \in \mathbb{Z} \ \text{ such that } \ x = \frac{m}{n} \right\}.$$

In addition to discussing notation and number systems, we spent a few minutes recalling some arithmetic laws for the integers.

Properties of the Integers: Let x, y, z be integers. Then we have the following rules for arithmetic.

(1) (Commutative Laws) $x + y = y + x$ and $xy = yx$
(2) (Associative Laws) $x + (y + z) = (x + y) + z$ and $x(yz) = (xy)z$
(3) (Distributive Laws) $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$

The remainder of the class was spent on the question of what it means for one integer to divide another ("evenly"). This led to small discussions within the table groups. We had to play with some examples and try to explain the patterns we were seeing in words. After some group discussions, Zach's table wrote the following on the board.

Observation: [Zach's Table] Let z and x be two integers. Then x divides z means that z must be a multiple of x.

Zach's table then gave the example: let $z = 56$ and $x = 8$ and notice that $(8)(7) = 56$. Susan wanted to probe this a bit and asked Zach's table what it meant for an integer to be a multiple of another. As a reply, Zach's table offered the following.

Observation: [Zach's Table] Let x and z be integers. Then z is a multiple of x if there exists an integer y such that xy equals z.

Putting these ideas together, we obtain the following definition.

Definition 1.1. Let a and b be integers. We say that a *divides* b, if there is some integer c such that $b = ac$.

Here is some related terminology and notation: Let a and b be integers. All of the following statements mean the same thing:

(1) a *divides* b.
(2) a is a *factor* of b.
(3) a is a *divisor* of b.
(4) b is a *multiple* of a.
(5) $a|b$.

Example: 2 is a divisor of 4 since $4 = 2(2)$. We write $2|4$.

Example: 5 is a divisor of 15 since $15 = 5(3)$. We write $5|15$.

Example: 6 is not a divisor of 15 since there is no integer c with $15 = 6(c)$.

Example: 117 is not a divisor of 5375 since there is no integer c with $5375 = 117(c)$.

Example: $1|6$ since $6 = (1)(6)$.

The class together noticed that there is nothing overly special about the number 6 in our last example. This led to our first proof!

Theorem 1.2 (Class)**.** *Let n be any integer. Then $1|n$ and $-1|n$.*

Proof: This is clear from the definition, since for any integer n we have $n = (1)(n)$ and $n = (-1)(-n)$. □

Susan thought that a second quote by Plato was appropriate for today.

Quote: [Plato] "He who can properly define and divide is to be considered a god."

Homework:

(1) Let a, b and c be integers.
  (a) If $a|b$, does $a|(bc)$?
  (b) If $a|(bc)$, must $a|b$ or $a|c$?
(2) Write down a formal definition of what it means for an integer to be even. Repeat this for an odd integer.
(3) What can you say about the product and sum of:
  (a) two odd integers?
  (b) two even integers?
  (c) an odd integer and an even integer?

2. More on Divisibility

We began class with a quote.

Quote: [L. Kronecker] "God made the integers, all else is the work of man."

In order to recall our work on division, we considered 3 examples.

Example: -4 divides 32 since $32 = (-4)(-8)$.

Example: 2 doesn't divide 7 since there is no integer k such that $7 = 2k$.

Example: -3 doesn't divide -5 since there is no integer k such that $-5 = (-3)k$.

We then listed a few additional axioms of the integers which the class agreed we needed.

The Closure Properties of the Integers: Let x and y be integers. Then we have:

- $x + y$ is an integer (i.e., $\mathbb{Z}$ is closed under addition)
- $x - y$ is an integer (i.e., $\mathbb{Z}$ is closed under subtraction)
- xy is an integer (i.e., $\mathbb{Z}$ is closed under multiplication)

It was noted that the integers are not closed under division. For example, $3 \div 8$ is not an integer even though 3 and 8 are.

We briefly returned to an observation from last class regarding division and the number 0. Zero is never allowed to be a divisor!! This led to a lively discussion about $0|0$. After some convincing, we all agreed that even $0|0$ was not permitted. So it will be implicit when we write $a|b$ that a is non-zero. However, note that the expression $a|0$ is allowed, and in fact holds true for all non-zero integers a (since $0 = a(0)$).

We then turned our attention to the homework from the previous class. The first problem asked us to assume $a|b$ and to determine if we must have $a|(bc)$. Dan answered "yes, $a|(bc)$" and shared the example where $a = 7, b = 21$ and $c = 3$. This led to a discussion of what it means to prove a mathematical claim. We decided that a specific example does not constitute a proof since it doesn't verify the statement in full generality. Matt then put the following proof on the board.

Theorem 2.1 (Matt)**.** *Let a, b and c be integers. If $a|b$, then $a|(bc)$.*

Proof: Since $a|b$ there exists an integer d such that $b = ad$. Multiplying by c, we obtain $bc = a(dc)$. Since dc is an integer, this equation shows that a divides bc. □

We did note that we know dc is an integer in the above proof because of the closure axiom of the integers under multiplication.

The next question we looked at was: If a, b, c are integers such that $a|(bc)$ then must $a|b$ or $a|d$? Many people said this was true after doing a number of examples. However, Zach answered in the negative by giving two *counter-examples*: $a = 4, b = c = 2$ or $a = 8, b = 4, c = 10$. In both examples, $a|(bc)$ but a does not divide either b or c.

The second part of the homework dealt with even and odd integers. Patrick gave us his definitions of these types of integers and then the class as a whole extended them.

Definition 2.2. The integer a is *even* if any of the following equivalent conditions hold.

(1) a is divisible by 2.
(2) The remainder upon dividing a by 2 is 0.
(3) There is some integer k such that $a = 2k$.

Definition 2.3. The integer a is *odd* if any of the following equivalent conditions hold.

(1) a is not divisible by 2.
(2) The remainder upon dividing a by 2 is 1.
(3) There is some integer k such that $a = 2k + 1$.

We finished our homework discussion by looking at what we can say about the product and sum of even and odd integers. I'll include here more than what was discussed in class (we proved parts (3) and (6)).

Theorem 2.4 (Class)**.**

(1) *The product of two odd integers is odd.*
(2) *The product of two even integers is even.*
(3) *The product of an odd integer and an even integer is even.*
(4) *The sum of two odd integers is even.*
(5) *The sum of two even integers is even.*
(6) *The sum of an even integer and an odd integer is odd.*

Proof. Let a and b be integers.

(1) If a and b are odd, then there are integers c and d such that $a = 2c+1$ and $b = 2d+1$. Then
$$ab = (2c + 1)(2d + 1) = 4cd + 2c + 2d + 1 = 2(2cd + c + d) + 1.$$
Since $k := 2cd + c + d$ is an integer, this shows that ab is odd since it is of the form $2k + 1$.
(2) If a and b are even, then there are integers c and d such that $a = 2c$ and $b = 2d$. Then
$$ab = (2c)(2d) = 4cd = 2(2cd).$$
Since $k := 2cd$ is an integer, this shows that ab is even since it is of the form $2k$.
(3) If a is even and b is odd, then there are integers c and d such that $a = 2c$ and $b = 2d + 1$. Then
$$ab = (2c)(2d + 1) = 4cd + 2c = 2(2cd + c).$$
Since $k := 2cd + c$ is an integer, this shows that ab is even since it is of the form $2k$.
(4) If a and b are odd, then there are integers c and d such that $a = 2c+1$ and $b = 2d+1$. Then
$$a + b = (2c + 1) + (2d + 1) = 2c + 2d + 2 = 2(c + d + 1).$$
Since $k := c + d + 1$ is an integer, this shows that $a + b$ is even since it is of the form $2k$.
(5) If a and b are even, then there are integers c and d such that $a = 2c$ and $b = 2d$. Then
$$a + b = 2c + 2d = 2(c + d).$$
Since $k := c + d$ is an integer, this shows that $a + b$ is even since it is of the form $2k$.
(6) If a is even and b is odd, then there are integers c and d such that $a = 2c$ and $b = 2d + 1$. Then
$$a + b = (2c) + (2d + 1) = 2(c + d) + 1.$$
Since $k := c + d$ is an integer, this shows that ab is odd since it is of the form $2k + 1$.

□

We then looked at seven questions. The first two were proved in class, leaving the remaining five as homework. The first two questions were:

Question: If d divides a and d divides b, then must it be true that d divides $a + b$?

Question: If d divides a and d divides b, then must it be true that d divides $a - b$?

The general consensus was that the answers to these two questions are both "yes". We worked on the proofs in class and came up with the following.

Theorem 2.5 (Trevor)**.** *Let a, b and d be integers. If d divides a and d divides b, then d divides $a + b$.*

Proof. By definition of division, we can write $a = dm$ and $b = dn$ for some integers m and n. Then

$$a + b = dm + dn = d(m + n).$$

Since $m + n$ is an integer, this equation says that d divides $a + b$. □

Theorem 2.6 (Blake)**.** *Let a, b and d be integers. If d divides a and d divides b, then d divides $a - b$.*

Proof. By definition of division, we can write $a = dn$ and $b = dk$ for some integers n and k. Since $n - k$ is an integer and 1 divides any integer (by Theorem 1.2 from last class), we know that $1|(n - k)$. Multiplying by d gives $d|d(n - k)$, or $d|(dn - dk)$. □

The class wondered if Blake's different approach was acceptable. To add some peace of mind, note that we could have used the following argument: Write $a = dn$ and $b = dk$. Then

$$a - b = dn - dk = d(n - k).$$

Since $n - k$ is an integer, we can conclude that d indeed divides $a - b$.

Homework: Let a, b and d be integers.

(1) If $d|a$ and $d|b$, does $d|(ax + by)$ for all integers x and y?
(2) If $d|a$ and $d|b$, does $d|(ab)$?
(3) If $d|(a + b)$, does $d|a$ and $d|b$?
(4) If $d|(a + b)$ and $d|a$, does $d|b$?
(5) If $d|(a + b)$ or $d|a$, does $d|b$?

3. Divisibility Revisited

We began class with a discussion about how it can be challenging to prove statements about the integers which we have believed to be true for years without question. This led to the following quote.

Quote: [C. F. Gauss] "I have had my results for a long time: but I do not yet know how to arrive at them."

Courtney then shared with us what *Q.E.D.* stands for. In Latin this says "quod erat demonstrandum" which means "that which was to be demonstrated". Some mathematicians will mark the end of a proof by writing *Q.E.D.*

We then went on to discuss the homework problems from last class.

Theorem 3.1 (Garrett)**.** *Let a, b and d be integers. If d divides a and d divides b, then d divides $ax + by$ for all integers x and y.*

Proof. Let x and y be any integers. Since $d|a$ and $d|b$, there exist integers f and g such that $a = df$ and $b = dg$. So

$$ax + by = dfx + dgy.$$

This shows that $d|(ax + by)$ since $ax + by = d(fx + gy)$ and $fx + gy$ is an integer. □

Theorem 3.2 (Courtney)**.** *Let a, b and d be integers. If d divides a and d divides b, then d divides ab.*

Proof. Since $d|a$ and $d|b$, there exist integers m and n such that $a = dm$ and $b = dn$. We know that 1 divides any integer, and so $1|dmn$. Multiplying this relationship by d, we see that $d|d^2mn$ and so $d|(dmdn)$. But, $(dm)(dn) = ab$. Therefore $d|ab$. □

Courtney's proof at the board used different symbols for the integers m and n which brought many smiles: m was a cloud and n was a sun. An alternative proof is: $ab = (dm)(dn) = d(dmn)$ and since dmn is an integer, we see that d divides ab. We noted that this proof also shows more than what is claimed. In particular, $ab = d^2(mn)$ and so we see that d^2 divides ab.

The next homework question asked the following: If a, b and d are integers such that $d|(a + b)$, does $d|a$ and $d|b$? This is the *converse* of Trevor's Theorem from the end of last class (which said that if $d|a$ and $d|b$, then $d|(a + b)$). Bryce concluded that this statement is not always true. For example, let $a = 3, b = 6$ and $d = 3$. Then $3|(6 + 3)$ and $3|3$ and $3|6$. However, if $a = 2, b = 7$ and $d = 3$. Then $3|(2 + 7)$ yet 3 does not divide either 2 or 7. This counter-example shows the statement is false in general.

Theorem 3.3 (Ethan)**.** *Let a, b and d be integers. If d divides $(a + b)$ and d divides a, then d divides b.*

Proof. Since $d|(a+b)$ and $d|a$, there exist integers m and n such that $a+b = dm$ and $a = dn$. Now

$$a + b = dm = dn + b$$

showing that $b = dm - dn = d(m - n)$. Since $m - n$ is an integer, $d|b$. □

4. Greatest Common Divisors

We next turned our attention to the greatest common divisor of two integers.

Definition 4.1. Let a and b be integers (not both zero). A *common divisor* of a and b is an integer d that divides both a and b.

Definition 4.2. Let a and b be integers (not both zero). The *greatest common divisor* of a and b is the largest positive integer d which divides both a and b. We write $d = \gcd(a, b)$.

Example: To make sure we all understood divisors we did a specific example. The divisors of 14 are: $\pm 1, \pm 2, \pm 7, \pm 14$. Similarly, the divisors of 21 are: $\pm 1, \pm 3, \pm 7, \pm 21$. Thus, $\gcd(14, 21) = 7$.

Example: We did several more examples.

$\gcd(8, 10) = 2$	$\gcd(-5, 0) = 5$
$\gcd(10, 40) = 10$	$\gcd(96, 64) = 32$
$\gcd(7, 5) = 1$	$\gcd(42, 78) = 6$
$\gcd(45, 23) = 1$	$\gcd(140, 364) = 28$
$\gcd(-2, -8) = 2$	$\gcd(7696, 4144) = 592$

After doing the examples, we made a few observations:

- If a is an integer, $a \neq 0$, then $\gcd(a, 0) = |a|$.
- If a is an integer, then $\gcd(a, 1) = 1$.

The method people used to do the above examples was essentially trial and error: find the factors of one of the numbers and test if they divide the other. This won't work so well with larger numbers, however. It would be impossible to do it in any reasonable amount of time with numbers which are of the size needed for cryptography, and even "smallish" numbers pose a problem – no one was very anxious to compute $\gcd(7696, 4144)$ by hand.

Instead, we hoped for a theoretical tool which would give us a new, simpler method for computing gcds. That tool is based on the next theorem.

Theorem 4.3 (Euclid's Division Lemma)**.** *Let a and b be integers with $b > 0$. Then there are unique integers q and r with $0 \leq r < b$ and $a = bq + r$.*

Example: If $a = 1150$ and $b = 12$, then $a = bq + r$ with $q = 95$ and $r = 10$: $1150 = 12(95) + 10$.

Before talking about the proof of this theorem, we had a discussion of what it means. We noticed that the theorem has two parts: First, q and r *exist*, i.e., we can always find q and r which work. Secondly, they're *unique*. The word "unique" needed a bit of clarification. It doesn't mean that q and r cannot be equal, as the next example shows:

Example: If we take $a = 14$ and $b = 6$, then $q = r = 2$ since $14 = 6(2) + 2$.

The word *unique* means that there are no other integers that work, i.e., if $a = bq + r$ with $0 \leq r < b$ and $a = bp + s$ with $0 \leq s < b$, then it must be true that $q = p$ and $r = s$.

Another observation about the statement of the theorem, is that there is no requirement that $a > b$ or that $a > 0$. Here are two examples:

Example: If $a = 36$ and $b = 67$, then $a = bq + r$ with $q = 0$ and $r = 36$: $36 = 67(0) + 36$.

Example: If $a = -28$ and $b = 6$, then $a = bq+r$ with $q = -5$ and $r = 2$: $-28 = 6(-5)+2$.

We did the proof of the existence part in class, and left the uniqueness part for later. The proof uses the following notation.

Notation: Let a and b be integers where $b \neq 0$. Then $\lfloor \frac{a}{b} \rfloor$ is the greatest integer which is at most equal to $\frac{a}{b}$. This is called the *floor* of $\frac{a}{b}$.

Example: $\lfloor \frac{2}{3} \rfloor = 0, \lfloor \frac{6}{3} \rfloor = 2, \lfloor \frac{5}{2} \rfloor = 2, \lfloor \frac{10}{3} \rfloor = 3$

The idea behind the proof of Euclid's Division Lemma is to take q so that $bq \leq a$ but $b(q+1) > a$, and then take $r = a - bq$. More formally, we have:

Proof of "existence" portion of Euclid's Division Lemma. Set $q = \lfloor \frac{a}{b} \rfloor$. Then set $r = a - bq$. Certainly, by definition of r, we have $a = bq + r$. So we just need to show that $0 \leq r < b$. By definition of q, we have

$$\frac{a}{b} - 1 < q \leq \frac{a}{b}.$$

Multiplying each term by -1 reverses the inequalities:

$$-\frac{a}{b} \leq -q < -\left(\frac{a}{b} - 1\right)$$

Adding $\frac{a}{b}$ to each of these terms gives the inequalities:

$$\frac{a}{b} - \frac{a}{b} \leq \frac{a}{b} - q < \frac{a}{b} - \left(\frac{a}{b} - 1\right)$$

Rewriting this gives

$$0 \leq \frac{a}{b} - q < 1.$$

Multiplying through by b gives

$$0 \leq a - bq < b,$$

and since $r = a - bq$, we have our result. □

To tie this back to greatest common divisors, we performed an experiment and wrote out the following table:

a	b	$\gcd(a, b)$	r such that $a = bq + r$	$\gcd(b, r)$
45	23	1	22	1
96	64	32	32	32
78	42	6	36	6
364	140	28	84	28

From this table, we made the guess that, if $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$. In order to prove a statement like this, however, it is helpful to slightly revise our definition:

Definition 4.4. Let a and b be integers (not both zero). The *greatest common divisor* of a and b is the positive integer d such that

(1) d divides a
(2) d divides b
(3) if e is a positive integer which divides both a and b, then it must be true that $e \leq d$.

We then did a formal statement and proof of our guess from above. Notice that, if we use Euclid's Division Lemma to find q and r with $a = bq + r$, then $r < b$. So one interpretation of the statement is that it reduces the size of the numbers we're trying to take the gcd of. The statement is therefore called the GCD Reduction Theorem, and the class as a group filled in the harder details of the proof.

Theorem 4.5 (GCD Reduction Theorem)**.** *If a, b, q and r are integers such that $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Set $d = \gcd(a, b)$ and $e = \gcd(b, r)$. We want to show $d = e$, which we'll do by showing that $e \leq d$ and $d \leq e$. We'll do this using the definition of gcd.

First, since $d = \gcd(a, b)$, we know that d divides a and d divides b. So there are integers x and y such that $a = dx$ and $b = dy$. Since $a = bq + r$, we have

$$r = a - bq = dx - dyq = d(x - yq),$$

and so d divides r. We already know that d divides b, and so, since $e = \gcd(b, r)$, we must have $d \leq e$.

On the other hand, since $e = \gcd(b, r)$, there are integers m and n such that $b = me$ and $r = ne$. We have

$$a = bq + r = meq + ne = e(mq + n),$$

and so e divides a. We already know that e divides b, and so, since $d = \gcd(a, b)$, we must have $e \leq d$.

Putting everything together, we have $d = e$, as desired. □

Homework:

(1) Let a and b be integers such that $a \neq 0$. Show that $\gcd(a, b) = \gcd(a, a + b)$. (Hint: Use a past homework problem and show both $\gcd(a, b) \leq \gcd(a, a + b)$ and $\gcd(a, a + b) \leq \gcd(a, b)$).

(2) Suppose $7 = ax + by$ for some integers a, b, x and y. What are the possible values of $\gcd(a, b)$?

(3) Alice is thirsty. Bob sells a variety of drinks at prices \$1, \$2, \$3, ... Suppose that there are only \$6 and \$11 coins in society. What is the cheapest drink Alice can buy from Bob without losing any money?

5. More on GCDs

The class started with a discussion of how there was confusion with the homework. People seemed to find the questions open-ended and didn't understand the point nor what type of answers were expected. I reminded everyone that these problems are tricky; it takes time to get used to looking at concrete examples, notice patterns, and prove conjectures. As usual this led to a quote.

Quote: [A. Weil] "Rigour is to the mathematician what morality is to men."

We then tackled the first two homework exercises from class.

Theorem 5.1 (Kimberley)**.** *Let a and b be integers such that $a \neq 0$. Then* $\gcd(a, b) = \gcd(a, a + b)$.

Proof. Let $\gcd(a, b) = c$ and $\gcd(a, a + b) = d$. We need to show both $c \leq d$ and $d \leq c$. By definition of the greatest common divisor, we know that $c|a$ and $c|b$. So, by Theorem 2.5 on August 27, $c|(a + b)$. Therefore, c is a common divisor of a and $a + b$, showing that $c \leq d = \gcd(a, a + b)$.

Similarly, we know that $d|a$ and $d|(a + b)$. So, by a homework question on August 27, we have $d|b$. This shows that d is a common divisor of a and b. Therefore, $d \leq c = \gcd(a, b)$.

We conclude that $c = d$ as claimed. □

The second homework problem was solved with joint effort as described below.

Question: Suppose $7 = ax + by$ for some integers a, b, x and y. What are the possible values of $\gcd(a, b)$?

Answer: (Dan, Sam, and Class) Dan gave an example that shows $\gcd(a, b) = 1$ is possible: namely, $a = 4, b = 3, x = y = 1$. Then $(4)(1) + (3)(1) = 7$ and $\gcd(4, 3) = 1$. Sam then showed that 7 is also a possible gcd: let $a = 35, b = -7, x = 2, y = 9$. Then $(35)(2) + (-7)(9) = 7$ and $\gcd(35, -7) = 7$. The class together then cam up with a proof that 1 and 7 are the only possibilities for $\gcd(a, b)$. Here is the proof: Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$. So, by a homework problem from August 27, we know that $d|(ax + by)$ for any integers x and y. Since $ax + by = 7$, by assumption, this shows that $d|7$. We conclude that $d = 1$ or $d = 7$.

Our next goal was to compute $\gcd(7696, 4144)$ using Euclid's Division Lemma and the GCD Reduction Theorem. After a few minutes, everyone understood why we looked at the Division Lemma last class. We start by writing

$$7696 = 4144(1) + 3552,$$

which tells us that $\gcd(7696, 4144) = \gcd(4144, 3552)$ (by the GCD Reduction Theorem). Since these numbers are still big, we repeat the process. We have

$$4144 = 3552(1) + 592,$$

which tells us that $\gcd(4144, 3552) = \gcd(3552, 592)$. Again, these numbers are too big to deal with in our heads, so we write

$$3552 = 592(6) + 0,$$

which tells us that $\gcd(3552, 592) = \gcd(592, 0)$. Since $\gcd(592, 0) = 592$, we can trace the equalities backwards to get that $\gcd(7696, 4144) = 592$.

This procedure for finding the gcd is known by the fancy name of the Euclidean Algorithm and may be summed up as follows.

Theorem 5.2 (The Euclidean Algorithm)**.** *Let a and b be integers with $b > 0$. Use the Division Lemma to write*

$$a = bq_1 + r_1$$

for some integers q_1 and $0 \leq r_1 < b$. If $r_1 \neq 0$, apply the Division Lemma again to write

$$b = r_1 q_2 + r_2$$

for some integers q_2 and $0 \leq r_2 < r_1$. If $r_2 \neq 0$, apply the Division Lemma again to write

$$r_1 = r_2 q_3 + r_3$$

for some integers q_3 and $0 \leq r_3 < r_2$. Continue to repeat this process. Then

(1) *For some $t \geq 0$, we will have $r_t \neq 0$ and $r_{t+1} = 0$. (If $t = 0$, we define $r_0 := b$.)*
(2) *With t as above, $\gcd(a, b) = r_t$.*

Proof. We have $b = r_0 > r_1 > \cdots \geq 0$, so the r_i's form a strictly decreasing sequence of non-negative integers. Such a sequence cannot go on forever, so we've proven (1). For (2), we have

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{t-1}, r_t) = \gcd(r_t, 0) = r_t$$

by the GCD Reduction Theorem and the fact that $\gcd(s, 0) = s$ for any positive integer s. □

We did one more example:

Example: (Michelle) Use the Euclidean algorithm to compute $\gcd(3017, 101)$.

$$\begin{aligned} 3017 &= 101(29) + 88 \\ 101 &= 88(1) + 13 \\ 88 &= 13(6) + 10 \\ 13 &= 10(1) + 3 \\ 10 &= 3(3) + 1 \\ 3 &= 1(3) + 0 \end{aligned}$$

Since the last nonzero remainder is 1, we have $\gcd(3017, 101) = 1$.

6. The Money Problem

Then we turned to a discussion of the last homework problem involving the characters Alice and Bob. The original question from the homework was: Alice is thirsty. Bob sells a variety of drinks at prices \$1, \$2, \$3, ... Suppose that there are only \$6 and \$11 coins in society. What is the cheapest drink Alice can buy from Bob without losing any money? Everyone figured out that Alice could buy a \$1 drink by giving Bob two \$6 coins. In return Bob would give Alice the \$1 drink plus one \$11 coin. Moreover, everyone decided that this meant Alice could buy any priced drink by just doing this repeatedly. For example, to purchase a \$2 drink, Alice would give Bob four \$6 coins and receive the drink and two \$11 coins in return.

Next, we discussed the same question, but using \$6 and \$10 coins. This time, we easily saw that Alice could buy a \$2 drink by giving Bob two \$6 coins. In return Bob would give

Alice one \$10 coin (and the \$2 drink!). And then the same argument as before says that Alice can buy an \$$n$ drink for any even positive integer n. But everyone quickly claimed that Alice couldn't buy any drink whose price is an odd integer since 6 and 10 are both even. We are indeed correct, and we'll make this precise later.

Finally, we discussed the same question, but using \$6 and \$9 coins. There was more controversy this time (Courtney tried really hard to find a way for Alice to purchase a \$1 drink), but eventually we all came to believe that Alice could buy an \$$n$ drink if and only n is a multiple of 3. More generally, we made the following guess:

Conjecture 6.1 (Class)**.** *Let a and b be positive integers. Let $d = \gcd(a, b)$. Then Alice can purchase an \$$n$ drink using \$$a$ and \$$b$ coins if and only if n is a multiple of d.*

Notice that our conjecture has two parts. It says:

- If d divides n, then Alice can buy an \$$n$ drink using \$$a$ and \$$b$ coins.
- If Alice can buy an \$$n$ drink using \$$a$ and \$$b$ coins, then it must be true that d divides n.

We left the proof of this conjecture as homework.

7. Loose Ends: Euclid's Division Lemma

I had promised you a proof of the "uniqueness" portion of Euclid's Division Lemma, but we didn't get to it today (instead we discussed policies for the first first take-home test). So here it is, just so you'll have it.

Proof of the "uniqueness" portion of Euclid's Division Lemma. Suppose that $a = bq+r$ and $a = bs + t$, where q, r, s, and t are integers with $0 \leq r < b$ and $0 \leq t < b$. We need to show that $q = r$ and $s = t$. We can start by saying that $a = bq + r = bs + t$, so that $bq - bs = t - r$. This means that b divides $t - r$. By the restriction of the sizes of r and t, we know that $-(b - 1) \leq t - r \leq b - 1$. The only integer in this range which is divisible by b is 0, so we must have $t - r = 0$. In other words, we have $t = r$. But then we have $a = bq + r = bs + t = bs + r$, so $bq = bs$, which means that $q = s$, finishing the proof of the uniqueness part of the theorem. □

Homework:

(1) From the Money Problem, can Alice buy a \$1 drink using only \$243 and \$41 coins?
(2) Use the Euclidean Algorithm to find $d := \gcd(141, 120)$. Also, find integers u and v so that $141u + 120v = d$.
(3) Try to prove the Money Problem Conjecture.

8. The Extended Euclidean Algorithm

Today's quote was:

Quote: [J. J. Sylvester] "Mathematics is the music of reason."

We began with a discussion of the first homework problem from last time. In the Money Problem, we were to determine if Alice could buy a \$1 drink using only \$243 and \$41 coins. Sam spoke up and said that Alice could. When asked to justify this, Sam suggested two reasons: (1) Alice could give Bob eighty-three \$41 coins and then Bob would return fourteen \$243 coins and a \$1 drink; (2) By the Money Problem Conjecture from last class, Alice can buy a \$1 drink since $\gcd(243, 41) = 1$ and 1 is a multiple of 1. The class then decided that Sam's first reason was preferred since we haven't yet proven the Money Problem Conjecture. Prompted by Sam's second reason, we used the Euclidean Algorithm to find $\gcd(243, 41)$.

Example: (Blake)

$$\begin{aligned} 243 &= 41(5) + 38 \\ 41 &= 38(1) + 3 \\ 38 &= 3(12) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

Since the last nonzero remainder is 1, we have $\gcd(243, 41) = 1$.

Question: We know that $\gcd(243, 41) = 1$, and so the Money Problem Conjecture says that Alice should be able to buy a \$1 drink using only \$243 and \$41 coins? But *how* can Alice do this?

The first step was to put the question in a more mathematical context. Patrick nicely summarized his thoughts for us:

Question: How can we find integers u and v so that $243u + 41v = 1$?

Dan then helped us see that to find u and v we could simply work backwards from the Euclidean Algorithm.

Example: We can obtain the integers u and v by using "back-substitution" with the above equations. First, we rewrite Blake's equations from above:

$$\begin{aligned} 243 = 41(5) + 38 &\implies 38 = 243 - 41(5) \\ 41 = 38(1) + 3 &\implies 3 = 41 - 38(1) \\ 38 = 3(12) + 2 &\implies 2 = 38 - 3(12) \\ 3 = 2(1) + 1 &\implies 1 = 3 - 2(1) \end{aligned}$$

Now we start with the bottom equation and back-substitute our way up, simplifying (but not too much!) at each stage. We have:

$$\begin{aligned}
1 &= 3 - 2(1) \\
&= 3 - (38 - 3(12))(1) = 3 - 38(1) + 3(12) = 3(13) - 38(1) \\
&= (41 - 38(1))(13) - 38(1) = 41(13) - 38(13) - 38(1) = 41(13) - 38(14) \\
&= 41(13) - (243 - 41(5))(14) = 41(13) - 243(14) + 41(70) = 41(83) - 243(14) \\
&= 41(83) + 243(-14).
\end{aligned}$$

In terms of the Money Problem, this means that if Alice wants to buy a \$1 drink from Bob, then Alice can give Bob 83 of the \$41 coins, and then Bob can give Alice 14 of the \$243 coins.

Ethan shared his solution to the second homework problem from last class.

Example: (Ethan) Our goal is to find $d := \gcd(141, 120)$ and then to find integers u and v so that $141u + 120v = d$. We start by using the Euclidean algorithm to find d and then rearrange the equations to be in the form we need for the back-substitution step.

$$\begin{aligned}
141 = 120(1) + 21 &\implies 21 = 141 - 120(1) \\
120 = 21(5) + 15 &\implies 15 = 120 - 21(5) \\
21 = 15(1) + 6 &\implies 6 = 21 - 15(1) \\
15 = 6(2) + 3 &\implies 3 = 15 - 6(2) \\
6 = 3(2) + 0
\end{aligned}$$

This shows that $\gcd(141, 120) = 3$. To find u and v, we start with the bottom equation and back-substitute:

$$\begin{aligned}
3 &= 15 - 6(2) \\
&= 15 - (21 - 15(1))(2) \\
&= 15 - 21(2) + 15(2) \\
&= 15(3) - 21(2) \\
&= (120 - 21(5))(3) - 21(2) \\
&= 120(3) - 21(15) - 21(2) \\
&= 120(3) - 21(17) \\
&= 120(3) - (141 - 120(1))(17) \\
&= 120(3) - 141(17) + 120(17) \\
&= 120(20) - 141(17).
\end{aligned}$$

We can write this as

$$3 = 141(-17) + 120(20),$$

which shows that $u = -17$ and $v = 20$.

We then did one more for good measure.

Example: (Class) The goal is to find $d := \gcd(5336, 1541)$ and then find integers u and v so that $5336u + 1541v = d$. The first step is, as usual, to use the Euclidean algorithm to

find d. We also rearrange the equations to be in a useful form for back-substitution.

$$\begin{aligned} 5336 = 1541(3) + 713 &\implies 713 = 5336 - 1541(3) \\ 1541 = 713(2) + 115 &\implies 115 = 1541 - 713(2) \\ 713 = 115(6) + 23 &\implies 23 = 713 - 115(6) \\ 115 = 23(5) + 0 & \end{aligned}$$

This shows that $\gcd(5336, 1541) = 23$. To find u and v, we start with the bottom equation and back-substitute:

$$\begin{aligned} 23 &= 713 - 115(6) \\ &= 713 - (1541 - 713(2))(6) \\ &= 713 - 1541(6) + 713(12) \\ &= 713(13) - 1541(6) \\ &= (5336 - 1541(3))(13) - 1541(6) \\ &= 5336(13) - 1541(39) - 1541(6) \\ &= 5336(13) - 1541(45) \\ &= 5336(13) + 1541(-45). \end{aligned}$$

Zach asked after the first back-substitution if we might "back-substitute" for two numbers at the same time. We had a brief discussion about Zach's suggestion for doing the problem. Although there was a feeling that his method had fewer steps, it doesn't really according to how it's written out above. It's very nice, though, and it requires a bit of cleverness beyond just following an algorithm. The upshot is that it doesn't much matter how you do these, as long as you're careful. It might be easier to avoid mistakes (or confusion) if you follow the algorithm, but it doesn't much matter.

By the way, the "back-substitution" process we've been following is called the *Extended Euclidean Algorithm*.

9. More on the Money Problem

The other homework problem from last time was to try to prove the Money Problem Conjecture.

Conjecture 9.1 (Class)**.** *Let a, b and n be integers and set $d = \gcd(a, b)$. Then we can purchase an \$n drink using only \$a and \$b coins (without losing money) if and only if n is a multiple of d.*

Patrick put the conjecture into more mathematical language for us:

Conjecture 9.2 (The Money Problem Conjecture, Revised by Patrick)**.** *Let a, b and n be integers and set $d = \gcd(a, b)$. Then there are integers x and y with $ax + by = n$ if and only if n is a multiple of d.*

We noticed that we actually already have a proof for half of this conjecture!

Proposition 9.3 (Class)**.** *Let , b and n be integers and set $d = \gcd(a, b)$. If there are integers x and y such that $ax + by = n$, then n must be a multiple of d.*

Proof. We know that $d|a$ and $d|b$. So, by a homework problem on Thursday, August 27, we know that $d|(au + bv)$ for any integers u and v. Since $n = ax + by$, this shows that n must be a multiple of d. □

We still have the other half of the Money Problem Conjecture to prove, and we left that as homework after looking at an example which will, I hope, add some insight.

Example: Suppose we wish to find integers x and y so that $69 = 5336x + 1541y$. We know that $69 = 23 \times 3$ and we know that $23 = 5336(13) + 1541(-45)$. Multiplying both sides of this last equation by 3 gives

$$69 = (23)(3) = (5336(13) + 1541(-45))\,(3) = 5336(39) + 1541(-135)$$

and so $x = 39 = 3(13)$, $y = -135 = 3(-45)$ works.

10. The equation $ax + by = n$

After seeing the equation $ax + by$ pop up numerous times today, we decided to end class with some language and discussion.

Definition 10.1. Let a and b be integers. An expression of the form $ax + by$ is called a *linear combination* of a and b.

We then asked the following questions.

Question: Let a, b and n be integers. If $ax + by = n$, then do x and y have to be unique?

Answer: No! Let $a = 3, b = 2$ and $n = 5$. Then

$$3(1) + 2(1) = 5 = 3(-1) + 2(4)$$

So, we could have $x = y = 1$ or $x = -1$ and $y = 4$.

Question: Let a, b and n be integers. Can we always find integers x and y such that $ax + by = n$?

Answer: No! Let $a = b = 2$ and $n = 1$. Then the equation $2x + 2y = 1$ will never be satisfied for any integers x and y.

Question: Let a, b and n be integers. If there are integers x and y with $ax + by = n$, then how many such pairs (x, y) are there?

Almost everyone immediately conjectured that there are infinitely many such pairs, but didn't know why. Even accepting that answer, it brings up new questions:

Question: Let a, b and n be integers. If there are integers x and y with $ax + by = n$, then can we describe an infinite set of such pairs (x, y)?

Question: Let a, b and n be integers. If there are integers x and y with $ax + by = n$, then can we describe all such pairs (x, y)?

This was obviously too much to think about in the last two minutes of class, so we left it for next time, with a homework problem to help get us started.

Homework:

(1) For each of the following equations, decide whether there is a solution, i.e., a pair of integers (x, y) which satisfies the equation. If there is a solution, find at least six solutions. If there is no solution, say why not.

$$3x + 5y = 22$$
$$8x + 12y = 26$$
$$6x + 8y = 20$$
$$3x + 2y = 17$$
$$12x + 15y = 39$$
$$12x + 18y = 9$$

(2) Prove the other half of the Money Problem Conjecture. In other words, prove that if n is a multiple of $\gcd(a, b)$, then there are integers x and y with $ax + by = n$.

11. Solutions To The Equation $ax + by = n$

Today marked the due date for the first take-home test. We celebrated with a quote that many could relate to.

Quote: [A. S. Eddington] "Proof is an idol before whom the pure mathematician tortures himself."

We then recalled the following fact from last class: Let a, b and n be integers and set $d = \gcd(a, b)$. If there exist integers x and y such that $ax + by = n$, then n is a multiple of d. The second homework question from last class was to prove the converse of this statement. That is, our goal was to prove that if n is a multiple of d then there exist integers x and y such that $ax + by = n$. After a few minutes we realized that we weren't quite ready to prove this last statement. So, to get started, we brainstormed a list of facts that we know in hopes that we could pick out the useful items for our task at hand. Our list is below.

Brainstorming Exercise: Let a, b and n be integers and set $d = \gcd(a, b)$. Assume that n is a multiple of d. Then we know the following:

- $d|a$ and $d|b$
- $d|n$ and so there exists an integer q such that $n = dq$
- $d|(a + b)$
- $d|(am + bj)$ for any integers m and j
- The Extended Euclidean Algorithm can be applied to find integers u and v such that $d = au + bv$

Dan made the key observation that the second and fifth items are key to our desired proof!

We then put everything together and obtained a formal proof. Since we now have a proof of the entire Money Problem Conjecture, I'm going to restate the whole thing here as a theorem.

Theorem 11.1 (Class)**.** *Let a, b and n be integers and set $d = \gcd(a, b)$. Then there are integers x and y with $ax + by = n$ if and only if n is a multiple of d.*

Proof. Suppose first that there are integers x and y with $ax + by = n$. Then, by a homework problem from Thursday, August 27, we know that $d|(au + bv)$ for any integers u and v. Since $n = ax + by$, this shows that n must be a multiple of d.

Now suppose that n is a multiple of d. Then we can write $n = dq$ for some integer q. We can use the Extended Euclidean Algorithm to find integers u and v so that $au + bv = d$. Multiplying both sides of this equation by q gives $(au + bv)q = dq$, i.e., $a(uq) + b(vq) = n$, i.e., $ax + by = n$, where $x = uq$ and $y = vq$. □

Then we moved on to the first homework problem. We decided that $8x + 12y = 26$ has no solution since $\gcd(8, 12) = 4$ and 4 doesn't divide 26. We also decided that $12x + 18y = 9$ has no solution since $\gcd(12, 18) = 6$ and 6 doesn't divide 9. But the rest of the equations $ax + by = n$ have solutions since $\gcd(a, b)$ divides n. We put up a table listing the solutions

we found:

Equation	$3x+5y=22$	$6x+8y=20$	$3x+2y=17$	$12x+15y=39$
Some solutions (x,y):	(4,2) (-1,5) (44,-22) (-26,20) (-6,8) (-11,11) (-16,14) (-21,17)	(2,1) (-10,10) (-2,4) (-6,7) (6,-2) (-14,13)	(5,1) (1,7) (3,4) (7,-2) (17,-17) (9,-5) (-1,10)	(2,1) (-13,13) (-8,9) (7,-3) (12,-7) (-18,17)

We spent the rest of the day working in groups to try to find the pattern of these solutions. We were looking for statements of the form "Suppose $(x = x_0, y = y_0)$ is one solution to the equation $ax + by = n$. Then (all?) (some?) other solutions are ...." Here's what we came up with:

Conjecture 11.2. *[Zach, Matt, Patrick, Ethan]*

(1) *Suppose $ax + by = n$, let $d = \gcd(a, b)$ and let m be any integer. Then*

$$a\left(x + \frac{b}{d}m\right) + b\left(y - \frac{a}{d}m\right) = n$$

and

$$a\left(x - \frac{b}{d}m\right) + b\left(y + \frac{a}{d}m\right) = n.$$

(2) *If (x_n, y_n) is a solution to the equation $ax + by = n$, then so is (x_{n+1}, y_{n+1}) where*

$$x_{n+1} = x_n - b$$

and

$$y_{n+1} = y_n + a.$$

Conjecture 11.3. *[T.J., Kai, Blake, Evan, Dan] Let $z = \frac{b}{\gcd(a,b)}$ and $k = \frac{a}{\gcd(a,b)}$. If (x_0, y_0) is a solution to the equation $ax + by = n$, then $(x_0 - zq, y_0 + kq)$ is also a solution to $ax + by = n$ for any integer q.*

Conjecture 11.4. *[Courtney, Kimberley, Bryce, Randy] Suppose (x_0, y_0) is a solution to the equation $ax + by = n$ and let $\gcd(a, b) = d$. Then*

$$\left(x_0 - \frac{b}{d}, y_0 + \frac{a}{d}\right)$$

and

$$\left(x_0 + \frac{b}{d}, y_0 - \frac{a}{d}\right)$$

are also solutions to $ax + by = n$.

Conjecture 11.5. *[Michelle, Sam, Trevor, Garrett] Suppose (x_0, y_0) is a solution of the equation $ax + by = n$. Thus we know $ax_0 + by_0 = n$. Then we can solve for y_0 so that*

$$y_0 = \frac{n - ax_0}{b}$$

which is a linear equation. All points on this line are solutions to the equation $ax + by = n$. *The line has slope* $m = \frac{-ax}{b} = \frac{\Delta y}{\Delta x}$, *where* $-ax$ *equals how much the* y *value changes and* b *equals how much the* x *value changes.*

Homework: Examine each of these four conjectures.

(1) Does each conjecture work? In other words, are the values of x and y generated by each conjecture actually solutions to the equations?
(2) Which one will yield the most solutions? Does that one yield all solutions? Prove that conjecture. Feel free to rework the statement too if you want.

In addition, everyone was asked to prepare for an activity next week by writing a list of integers from 1 to 100, with 10 numbers on each line. The first line should be

1 2 3 4 5 6 7 8 9 10

12. More On The Solutions To The Equation $ax + by = n$

Garrett started our class by sharing the following quote:

Quote: [B. Russel] "Mathematics may be defined as the subject in which we never know what we are talking about, nor whether what we are saying is true."

In preparation for the discussion about the conjectures from last class, we began with two corollaries. Let a, b and n be integers and set $d = \gcd(a, b)$. Recall that the equation $ax + by = n$ has a solution (x, y) where x and y are integers if and only if n is a multiple of d.

Corollary 12.1 (Class)**.** *Let a and b be integers such that $\gcd(a, b) = 1$ and $a|(bc)$ for some integer c. Then $a|c$.*

Proof. Since $\gcd(a, b) = 1$, the Extended Euclidean Algorithm can be used to obtain integers u and v such that $au + bv = 1$. Also, since $a|(bc)$, there exists an integer p such that $bc = ap$. Thus

$$c = (1)(c) = (au + bv)(c) = auc + bvc = auc + apv = a(uc + pv).$$

Since $uc + pv$ is an integer, we have that $a|c$. □

Notice that in the above corollary we indeed need $\gcd(a, b) = 1$. For example, Zach noted that if we let $a = 4, b = 8$ and $c = 9$ then $a|(bc)$ but a does not divide c. We can obtain another example by letting $a = 8, b = 4$ and $c = 2$.

Matt gave us the key step in proving the second corollary.

Corollary 12.2 (Class)**.** *Let a and b be integers such that $\gcd(a, b) = d$. Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proof. Since $\gcd(a, b) = d$, the numbers $\frac{a}{d}$ and $\frac{b}{d}$ are both integers. Also, the Extended Euclidean Algorithm can be used to obtain integers u and v such that $au + bv = d$. Thus,

$$\frac{a}{d}u + \frac{b}{d} = 1.$$

That is (u, v) is a solution to the equation

$$\frac{a}{d}x + \frac{b}{d}y = 1.$$

So, by Theorem 11.1, $\gcd(\frac{a}{d}, \frac{b}{d})$ divides 1. Since greatest common divisors are positive, we can conclude that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. □

We then spent some time discussing Conjectures 11.2 - 11.5 from last class. We all agreed that these seemed to be saying essentially the same thing. So, we reworded the conjectures and proved them. The results are the next two propositions.

Proposition 12.3 (Class)**.** *Let a, b and n be integers. Suppose x_0 and y_0 are integers which give a solution (x_0, y_0) to the equation $ax + by = n$. Then (x, y) where*

$$x = x_0 + bl, \qquad y = y_0 - al$$

is also a solution to $ax + by = n$ for every integer l.

Proof. We have

$$\begin{aligned} a\,(x_0 + bl) + b\,(y_0 - al) &= ax_0 + abl + by_0 - abl \\ &= ax_0 + by_0 \\ &= n, \end{aligned}$$

since we know that (x_0, y_0) is a solution to $ax + by = n$. □

Randy put the proof of the first part of the next proposition on the board. The class together battled the second part.

Proposition 12.4 (Class)**.** *Let a, b and n be integers and set $d = \gcd(a, b)$. Suppose x_0 and y_0 are integers which give a solution (x_0, y_0) to the equation $ax + by = n$. Then*

(1) *For every integer k, $x = x_0 + \frac{b}{d}k$, $y = y_0 - \frac{a}{d}k$ gives a solution (x, y) to the equation $ax + by = n$.*
(2) *Every solution (x, y), where x and y are integers, to the equation $ax + by = n$ is of the form $x = x_0 + \frac{b}{d}k$, $y = y_0 - \frac{a}{d}k$ for some integer k.*

Proof. To prove part (1) note that we have

$$\begin{aligned} a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}k\right) &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k \\ &= ax_0 + by_0 \\ &= n, \end{aligned}$$

since we know that (x_0, y_0) is a solution to $ax + by = n$.

We now concentrate on part (2). To make the proof a little neater, let's treat the cases where $a = 0$ or $b = 0$ separately before we look at the case where they're both nonzero.

If $a = 0$, then our original equation is $by = n$. There is a unique value of y that works here (call it y_0), and then x can be anything. So the general form of the solution is $x = k$, $y = y_0$, where k is any integer. This fits with our claim if we take $x = x_0 = 0$, $y = y_0$ as our initial solution.

Similarly, if $b = 0$, then our original equation is $ax = n$. There is a unique value of x that works here (call it x_0), and then y can be anything. So the general form of the solution is $x = x_0$, $y = k$, where k is any integer. This fits with our claim if we take $x = x_0$, $y = y_0 = 0$ as our initial solution.

So now we can assume that a and b are both nonzero. We're given a solution (x_0, y_0). If (x_1, y_1) is some other solution, then we need to show that $x_1 = x_0 + \frac{b}{d}k$, $y_1 = y_0 - \frac{a}{d}k$ for some integer k. Start with what we know:

$$\begin{aligned} ax_0 + by_0 &= n \\ ax_1 + by_1 &= n \end{aligned}$$

Either by setting the two left-hand sides equal to each other and then rearranging, or by subtracting the top equation from the bottom one and then rearranging, we get

$$a(x_1 - x_0) = b(y_0 - y_1).$$

Now, since $d = \gcd(a, b)$, we know that d divides both a and b. So there are integers s and t so that $a = ds$, $b = dt$. Substituting, we get

$$ds(x_1 - x_0) = dt(y_0 - y_1).$$

Since d is a gcd, we know $d \neq 0$, and so we can divide both sides by d to get

$$s(x_1 - x_0) = t(y_0 - y_1).$$

In particular, we have that s divides $t(y_0 - y_1)$. From Corollary 12.2, we know that $\gcd(s, t) = 1$. From Corollary 12.1, this means that s must divide $y_0 - y_1$. Hence there is some integer k so that $sk = y_0 - y_1$. Rearranging and then substituting $s = \frac{a}{d}$, we get

$$y_1 = y_0 - \frac{a}{d}k.$$

On the other hand, we have that t divides $s(x_1 - x_0)$. Again using Corollaries 12.1 and 12.2, we get that there is some integer l so that $tl = x_1 - x_0$. Rearranging and then substituting $t = \frac{b}{d}$, we get

$$x_1 = x_0 + \frac{b}{d}l.$$

All that remains is to show that $k = l$. Since we know that (x_1, y_1) is a solution to $ax + by = n$, let's substitute:

$$\begin{aligned} n &= ax_1 + by_1 \\ &= a\left(x_0 + \frac{b}{d}l\right) + b\left(y_0 - \frac{a}{d}k\right) \\ &= ax_0 + \frac{ab}{d}l + by_0 - \frac{ab}{d}k \\ &= n + \frac{ab}{d}(l - k), \end{aligned}$$

where we've also used that (x_0, y_0) is a solution. Subtracting n from both sides and multiplying through by d, we get

$$ab(l - k) = 0.$$

Since we've assumed $a \neq 0$ and $b \neq 0$, we must have $l - k = 0$, i.e., $l = k$. □

Example: We summarized our work with an example. We want to find a general form for infinitely many solutions to $141x + 120y = 12$.

Solution: We know from September 8 that $\gcd(141, 120) = 3$ and that

$$141(-17) + 120(20) = 3.$$

Multiplying both sides by 4, we get

$$141(-68) + 120(80) = 12.$$

So our "initial solution" is (x_0, y_0) where $x_0 = -68$ and $y_0 = 80$.

Proposition 12.3 gives solutions (x, y):

$$x = -68 + 120l, \qquad y = 80 - 141l$$

for any integer l.

Proposition 12.4 gives solutions (x, y):

$$x = -68 + \frac{120}{3}k = -68 + 40k, \qquad y = 80 - \frac{141}{3}k = 80 - 47k.$$

for any integer k.

Both of these solutions are valid, and both give infinitely many solutions. But, in a certain sense, we noticed that Proposition 12.4 gives *more* solutions. In fact, Proposition 12.4 gives three times as many solutions as Proposition 12.3 does. For example, if we take $l = 1$ in the first solution set, this is the same as taking $k = 3$ in the second. If we take $l = -7$ in the first, this is the same as taking $k = -21$ in the second. But there is no value of l which will give us the same thing in the first solution set as we get from the second solution set with $k = 1$.

Homework:

(1) Find all integer solutions (x, y) to the equation $27x + 33y = 18$.
(2) Define what it means for a positive integer to be prime.
(3) If p is prime, what is $\gcd(a, p)$ for any integer a?
(4) If p is prime and a and b are integers such that $p|(ab)$, then must $p|a$ or $p|b$?

13. A Last Example For The Equation $ax + by = n$

Sam started class with two quotes.

Quote: [G. Polya] "Mathematics consists of proving the most obvious thing in the least obvious way."

Quote: [P. J. Hilton] "Mathematics should be fun."

We then went over the homework. Bryce represented his table and offered the first solution.

Example: The general form of the solution to the equation $27x + 33y = 18$ is given by (x, y) where $x = -3 + 11k$, $y = 3 - 9k$ for any integer k. To see this, first note that $27(-3) + 33(3) = 18$, and so $x_0 = -3$ and $y_0 = 3$ is one solution. Since $\gcd(27, 33) = 3$, we use our last proposition from last time to get that the general form for all solutions is

$$x = -3 + \frac{33}{3}k = -3 + 11k$$
$$y = 3 - \frac{27}{3}k = 3 - 9k.$$

Other people had found different solutions. With Courtney's help we obtained:

$$x = 30 + 33l, \qquad y = -24 - 27l$$

Courtney explained that she used the Euclidean Algorithm to find $\gcd(27, 33) = 3$. Then she applied the Extended Euclidean Algorithm to write $27(5) + 33(-4) = 3$. Multiplying both sides of the equation by 6 we see that $27(30) + 33(-24) = 18$. So, one solution is given by $x_0 = 30$ and $y_0 = -24$. Then, by Proposition 12.3, we obtain the solution above for any integer l.

We then discussed that the first solution set gives *all* solutions to the equation $27x+33y = 18$ yet the second solution set does not. Indeed, if we let $k = 4$ in the first solution then $(x, y) = (41, -33)$ but no value of l in the second solution will give $x = 41$. (If we tried to find such an l we would solve the equation $30 + 33l = 41 \implies 11 = 33l$ and this can not happen for any integer l.)

Finally, we talked about whether it was okay to have two different descriptions of the general form of the solutions to the equation $27x + 33y = 18$. Note that our work from last class shows we can start start with *any* initial solution (x_0, y_0) and so, since there are infinitely many solutions, there are infinitely many ways to describe the general solution.

14. A First Look At Primes

We then turned our attention to prime numbers. Representing his table, and with some revisions from the class, Trevor gave the important definition.

Definition 14.1. A positive integer is *prime* if it has exactly two positive divisors: one and itself.

Note that 1 is not a prime since it has 1 positive divisor, not two. This fact alarmed some but we'll continue with the popular convention.

An integer $x > 1$ which is not prime is called a *composite*.

The homework from last class involved some facts involving prime numbers. Evan's table offered the following to settle one of the questions.

Observation: Let p be a prime number and a be any integer. Then $\gcd(a, p) = 1$ or p. Further, $\gcd(a, p) = p$ if and only if p divides a. The class agreed that this was clear using the definitions of prime numbers and greatest common divisors.

Blake's table then conjectured that if p is a prime number and a and b are integers such that $p|(ab)$ then p must divide either a or b. We saw two proofs of this theorem. As one argument, Matt wrote the following up on the board: $p|ab$ means that there is some integer c such that $pc = ab$. Thus, $c = \frac{ab}{p}$. Since c is an integer, we must have that either $p|a$ or $p|b$. I offered an alternate proof.

Theorem 14.2. *Let p be a prime number and a and b be integers. If $p|(ab)$ then $p|a$ or $p|b$.*

Proof. If $p|a$ then we are done. So assume p does not divide a. We must show that p divides b. By the above observation, $\gcd(a, p) = 1$. So, by Corollary 12.1 last class, we can conclude that $p|b$ as claimed. □

Even though the definition of a prime number is straightforward to state, there are many unresolved questions about prime numbers. Two such famous unsolved conjectures are:

The Twin Prime Conjecture: There are infinitely many pairs of integers $(p, p + 2)$ such that both p and $p + 2$ are prime.

We noted that it is easy to think of pairs of integers $(p, p + 2)$ where both p and $p + 2$ are prime. For example, $(3, 5), (5, 7)$ and $(11, 13)$ are all twin primes. However, the Twin Primes Conjecture says that that there are *infinitely* many such examples.

Goldbach's Conjecture: Every even integer greater than 2 is the sum of two prime numbers.

As examples, we noted that $4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, 16 = 13 + 3, 10 = 7 + 3 = 5 + 5$. The last example shows that the prime numbers involved do not have to be unique.

We wanted to find a list of all the primes less than or equal to 100, so we started with a list of all the integers up to 100. We then crossed off 1 because it's not prime. We know 2 is prime, but certainly any multiple of 2 can't be, so we crossed off all the even numbers (other than 2). Then, since 3 was the smallest number not already crossed off, we knew 3 was prime, and we crossed off all multiples of 3 (greater than 3). We did this for 5 and 7 as well. The next smallest number that wasn't crossed off was 11, so we decided it was prime. We noticed that there were no multiples of 11 left to be crossed off (22, 44, 66 and 88 are even, 33 and 99 are multiples of 3, 55 is a multiple of 5, and 77 is a multiple of 7), and so we moved on to 13. Again, we saw that there were no multiples of 13 left to be crossed off.

Just so you have it, here's the list of primes less than or equal to 100 that we came up with. Numbers in bold and underlined are prime; consider everything else to be crossed off.

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

At this point, we made a conjecture.

Conjecture 14.3 (Kimberley)**.** *Everything left is a prime. In other words, any positive integer greater than 1 and at most 100 which is not a multiple of* 2*,* 3*,* 5*, or* 7 *is prime.*

This conjecture is indeed true, and we can prove it by just checking everything that's left.

We wanted to devise an algorithm to test if a positive integer is prime or not. Matt and T.J. offered the following.

Conjecture 14.4 (Matt and T.J.)**.** *To see if the positive integer n is prime, you only need to check for divisibility by primes which are less than or equal to $\lfloor\sqrt{n}\rfloor$.*

Example: To see if 7679 is prime, we check for prime divisors which are at most $\lfloor\sqrt{7679}\rfloor = 87$. We have a list of all the primes less than 100, and so we start checking. Although 2, 3 and 5 don't divide 7679, we do find that

$$7679 = (7)(1097).$$

This shows that 7679 is not prime, and so we're done. But we might also ask if 1097 is prime, or if it can be factored further. Applying our conjecture again, we need to check for prime divisors which are at most $\lfloor\sqrt{1097}\rfloor = 33$. None of 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 or 31 divide 1097, and so we can conclude (based on the conjecture) that 1097 is prime.

Example: To see if 9301 is prime, we check for prime divisors which are at most $\lfloor\sqrt{9301}\rfloor = 96$. We have a list of all the primes less than 100, and so we start checking. We find that

$$9301 = (71)(131)$$

and so 9301 is not prime. We know that 71 is prime, and might also ask if 131 is prime, or if it can be factored further. Applying our conjecture again, we need to check for prime divisors which are at most $\lfloor\sqrt{131}\rfloor = 11$. None of 2, 3, 5, 7 or 11 divide 131, and so we can conclude (based on the conjecture) that 131 is prime.

This brings up an important observation. Namely, Conjecture 14.4 asserts two statements:

- It's sufficient to check for prime factors.
- It's sufficient to check for factors which are at most $\lfloor\sqrt{n}\rfloor$.

For the second assertion, we ended up with a lemma.

Lemma: [Class] If n, a and b are positive integers with $n = ab$, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof. Suppose this statement is false. Then we have $n = ab$ with $a > \sqrt{n}$ and $b > \sqrt{n}$. This means that

$$n = ab > \sqrt{n}\sqrt{n} = n,$$

i.e., $n > n$ which is never true. So it must be the case that the statement is true. □

Finally, we can prove Conjecture 14.4.

Theorem 14.5 (Simple Primality Test)**.** *An integer $n > 1$ is prime if and only if it has no prime factors which are less than or equal to $\lfloor\sqrt{n}\rfloor$.*

Proof. Let $n > 1$. Then, by definition, n is prime if and only if it has exactly two positive divisors: 1 and itself. We need to show two things. First, *if* n is prime, *then* n has no prime factors less than or equal to $\lfloor\sqrt{n}\rfloor$. And second, *if* n has no prime factors less than or equal to $\lfloor\sqrt{n}\rfloor$, *then* n is prime.

The first statement is easy. If n is prime, then n has exactly two positive divisors: 1 and itself. Since 1 isn't prime and $\lfloor\sqrt{n}\rfloor < n$, n doesn't have any positive factors other than 1, let alone *prime* factors, which are less than $\lfloor\sqrt{n}\rfloor$.

For the second statement, suppose n has no prime factors less than or equal to $\lfloor\sqrt{n}\rfloor$. Assume that n is not prime. Then $n = ab$ for some positive integers a and b. By the above lemma, we know that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. By relabeling if necessary, assume $a \leq \sqrt{n}$. We know a cannot be prime since we assumed that n has no prime factors which are less than or equal to $\lfloor\sqrt{n}\rfloor$ (which is at most $\sqrt{n}$). This means that either $a = 1$, or a is an integer greater than 1 which is not prime. In the latter case, we see (by the Fundamental Theorem of Arithmetic; see below) that a is divisible by some prime p. But then we have $p < a \leq \sqrt{n}$ and p divides n (since p divides a and a divides n). This is impossible, since n has no prime factors which are at most $\sqrt{n}$. Hence we must have $a = 1$ and $b = n$. In other words, the only way of factoring n is as $n = (1)(n)$, and so n is prime. □

There is one assertion of the above proof which needs more detail. Namely, if $a > 1$ is a composite integer then there is a prime integer p which divides a.

Theorem 14.6 (Fundamental Theorem of Arithmetic)**.** *Every positive integer greater than 1 can be factored into a product of primes. Further, up to the order of the prime factors, this factorization is unique.*

We'll prove the Fundamental Theorem of Arithmetic later. For now, let's assume it's true. We finished class with some examples illustrating the fact.

Example: $9301 = (71)(131)$

Example: $35 = (5)(7)$

Example: $36 = (2)(2)(3)(3) = (2^2)(3^2)$

Example: $45 = (3^2)(5)$

Example: $19 = 19$

Notice that the third example shows us that the primes appearing in the factorization need not be distinct, and the last example shows us how to write a prime as a product of primes — the product has only one term (which some of us didn't approve of!).

Homework:

(1) Determine whether 8777 is prime or composite. If it's prime, prove it. If it's composite, give its complete prime factorization.

(2) Set $a_1 = 1$, $a_2 = 1+2 = 3$, $a_3 = 1+2+3 = 6$, and so on, so that $a_k = 1+2+\cdots+k$ is the sum of the first k positive integers. Complete the following table, and then conjecture a formula for a_k. (Your formula should be a function of k. For example, you should be able to use your formula to compute what a_{3000} ought to be without actually adding 3000 numbers together.) You do not need to prove that your formula works.

k	1	2	3	4	5	6	7	8
a_k	1	3	6					

(3) Set $b_1 = 1^2 = 1$, $b_2 = 1^2 + 2^2 = 5$, $a_3 = 1^2 + 2^2 + 3^2 = 14$, and so on, so that $b_k = 1^2 + 2^2 + \cdots + k^2$ is the sum of the squares of the first k positive integers. Complete the following table, and then conjecture a formula for b_k. (Your formula should be a function of k. For example, you should be able to use your formula to compute what b_{3000} ought to be without actually squaring 3000 numbers and adding them together.) You do not need to prove that your formula works.

k	1	2	3	4	5	6	7	8
b_k	1	5	14					

15. Prime Integers, Revisited

Bryce started our week with the following quote.

Quote: [Sir A. Eddington] "We used to think that if we knew one, we knew two, because one and one is two. We are finding that we must learn a great deal more about 'and'."

We then discussed the first homework problem from last class, which was to determine whether 8777 is prime or composite. Dan explained that 8777 is composite. To see this he used the Simple Primality Test by checking that none of the prime integers less than or equal to $\lfloor\sqrt{8777}\rfloor = 93$ divides 8777. Moreover, the prime factorization of 8777 is $8777 = (67)(131)$. We noted that 67 is prime since it's on our list of primes less than 100. We also know that 131 is prime because $\lfloor\sqrt{131}\rfloor = 11$ and none of the primes 2, 3, 5, 7, 11 divide 131.

Zach then asked if we would prove that there are infinitely many prime integers. We agreed that it was time for such a theorem.

Theorem 15.1 (Euclid)**.** *There are infinitely many prime integers.*

Proof. Suppose there are finitely many primes. In fact, let $\{p_1, p_2, \ldots p_k\}$ be the complete list of all the primes. Following Ethan and Dan's suggestion, set

$$N = p_1 \cdot p_2 \cdots p_k + 1.$$

We claim that no p_i divides N for any i with $1 \leq i \leq k$. To see this, assume p_j divides N. Then, $p_j | N$ and $p_j | (p_1 \cdot p_2 \cdots p_k)$. So, by Theorem 2.6 from Thursday, August 27, we must have that $p_j | (N - p_1 \cdot p_2 \cdots p_k)$. That is, $p_j | 1$ which implies that $p_j = 1$, a contradiction. We conclude that indeed no p_i divides N for an i with $1 \leq i \leq k$. But the Fundamental Theorem of Arithmetic says that we can write any integer as a product of primes! Since $\{p_1, \ldots, p_k\}$ is a complete list of all the primes and none of them divide N, this is a contradiction. Therefore, there must be infinitely many primes. □

Notice that this proof shows that it's impossible to have a finite list containing all the primes. It *does not* show that the number N constructed is always prime. This is the subject of one of the problems on your second test.

Zach observed that we are using the Fundamental Theorem of Arithmetic which we have yet to prove! Indeed, we have been assuming this theorem is true without proof. In order to prove the Fundamental Theorem of Arithmetic we need a tool which is useful to prove a statement is true for all integers greater than or equal to some integer a. We turned our attention to this technique.

16. The Principle of Mathematical Induction

The second homework problem from last class was to consider the sequence of integers given by $a_k = 1 + 2 + \cdots + k$ for an integer $k \geq 1$, i.e., a_k is the sum of the first k positive integers. The first step was to fill in a table of values of a_k for $1 \leq k \leq 8$. We get:

k	1	2	3	4	5	6	7	8
a_k	1	3	6	10	15	21	28	36

The next step was to conjecture a formula for a_k. Many in the class came up with the following guess.

Conjecture 16.1 (Class)**.** *For an integer $k \geq 1$, let a_k be the sum of the first k positive integers, i.e.,*

$$a_k = 1 + 2 + \cdots + k.$$

Then

$$a_k = \frac{k(k+1)}{2}.$$

Courtney and Kimberley also made the following conjecture:

Conjecture 16.2 (Courtney and Kimberley)**.** *For an integer $k \geq 1$, let a_k be the sum of the first k positive integers, i.e.,*

$$a_k = 1 + 2 + \cdots + k.$$

Then

$$a_k = a_{k-1} + k.$$

I also made noted the pattern that for an integer $k \geq 1$,

$$1 + 2 + \cdots + k = k^2 - a_{k-1}.$$

Everyone agreed with Conjectures 16.1 and 16.2. Moreover, we all noticed that Conjecture 16.2 followed immediately from the definition of a_k. We decided to check that Conjecture 16.1 implies Conjecture 16.2.

Proposition 16.3. *Conjecture 16.1 implies Conjecture 16.2.*

Proof. Assume Conjecture 16.1 is true. Then

$$a_k = \frac{k(k+1)}{2}$$

and

$$a_{k-1} = \frac{(k-1)((k-1)+1)}{2} = \frac{k(k-1)}{2}.$$

This means that

$$\begin{aligned} a_{k-1} + k &= \frac{k(k-1)}{2} + k \\ &= \frac{k^2 - k + 2k}{2} \\ &= \frac{k^2 + k}{2} \\ &= \frac{k(k+1)}{2} \\ &= a_k, \end{aligned}$$

which shows that Conjecture 16.2 is true also

.

□

To show that Conjecture 16.2 implies Conjecture 16.1 we need to use the technique of induction as described below.

We then talked for a bit about which conjecture we liked better. The formula from Conjecture 16.2 is what's called a *recursive* formula: it tells us the value of a_k based on the values of a_l for $l < k$ (in this case, we only care about a_{k-1}). The formula from Conjecture 16.1 is what's called an *explicit* formula: it tells us the value of a_k based only on k itself. Each has its advantages and disadvantages, but we decided that, for example, the explicit formula would be better if we wanted to know the value of a_{500}. This is because we can just compute it directly:

$$a_{500} = \frac{500(501)}{2} = 125250.$$

To compute the value of a_{500} using Conjecture 16.2, we'd first need to compute a_{499}. To compute a_{499}, we'd need a_{498}, and so on.

I then pointed out that we can show that Conjecture 16.1 is true for $k = 9$. We already know that $a_8 = 36$; this is in our table. Therefore

$$\begin{aligned} a_9 &= a_8 + 9 = (1 + 2 + 3 + 4 + 5 + 6 + 7 + 8) + 9 \\ &= 36 + 9 \\ &= 45. \end{aligned}$$

But also

$$\frac{9(9+1)}{2} = \frac{90}{2} = 45$$

and so Conjecture 16.1 is also true for $k = 9$. In groups, we showed that if we assume Conjecture 16.1 is true for $k = 100$, then it must also be true for $k = 101$. Patrick did this on the board for us.

Example: (Patrick) Assume Conjecture 16.1 is true for $k = 100$. Then we know

$$a_{100} = \frac{(100)(101)}{2} = 5050.$$

But then

$$\begin{aligned} a_{101} &= (1 + 2 + \cdots + 100) + 101 \\ &= a_{100} + 101 \\ &= 5050 + 101 \\ &= 5151. \end{aligned}$$

Note that we also have

$$\frac{101(101+1)}{2} = \frac{10302}{2} = 5151,$$

and so Conjecture 16.1 is true for $k = 101$ (under the assumption that it's true for $k = 100$).

The idea in Patrick's example is a special case of a general mathematical principle:

The Principle of Mathematical Induction (PMI): Let P be some property of integers, and suppose two things are true:

(1) P is true for some integer b (called the *base case*).
(2) If $k > b$ and P is true for all integers q with $b \leq q < k$, then P must also be true for k.

Then P is true for all integers $s \geq b$.

We can think of the Principle of Mathematical Induction as a game of dominoes with infinitely many dominoes. The first step is to knock the first domino over; the second step is to be certain (i.e., show) that if the nth domino is knocked down then the $(n+1)$st domino will fall over in addition.

We can use PM to prove Conjecture 16.1.

Theorem 16.4 (Class)**.** *For all integers $k \geq 1$, we have:*

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

Proof. **Base Case:** We already know the statement is true when $k = 1$, and so we can use $b = 1$ as our "base case". Indeed,

$$1 = \frac{(1)(1+1)}{2}.$$

Inductive Hypothesis: Let $k > 1$ be an integer and assume we know the conjecture is true for all integers q with $1 \leq q < k$. That is, assume

$$1 + 2 + \cdots + q = \frac{(q)(q+1)}{2}$$

for all integers q such that $1 \leq q < k$.

Inductive Step: We want to show the conjecture is true for the integer k. In particular, by the Inductive Hypothesis, we know it's true for $k-1$ and so we have

$$\begin{aligned} 1 + 2 + \cdots + k &= (1 + 2 + \cdots + (k-1)) + k \\ &= \frac{(k-1)((k-1)+1)}{2} + k \\ &= \frac{(k-1)k}{2} + k \\ &= \frac{k^2 - k + 2k}{2} \\ &= \frac{k^2 + k}{2} \\ &= \frac{k(k+1)}{2}, \end{aligned}$$

which shows that the statement is true for k as well. Therefore, we know that the statement is true for all $s \geq 1$ by the Principle of Mathematical Induction.

□

The third homework problem was to consider the sequence b_k, where b_k is the sum of the squares of the first k positive integers. Our table looks like:

k	1	2	3	4	5	6	7	8
b_k	1	5	14	30	55	91	140	204

Conjecture 16.5. *For an integer $k \geq 1$, let b_k be the sum of the squares of the first k positive integers, i.e.,*

$$b_k = 1^2 + 2^2 + \cdots + k^2.$$

Then

$$b_k = \frac{k(k+1)(2k+1)}{6}.$$

The proof is again by induction, and we left it as homework.

Homework:

(1) Use PMI to prove that $1 + 3 + 5 + \cdots + (2n-1) = n^2$ for all integers $n \geq 1$.

(2) Define the function f as follows:

$$f(0) = 1$$
$$f(1) = 2$$
$$f(n) = f(n-1) + 2f(n-2), \text{ for integers } n \geq 2.$$

Find $f(0), f(1), f(2), f(3)$, and $f(4)$. Use PMI to prove that $f(n) = 2^n$ for all integers $n \geq 0$.

(3) Prove Conjecture 16.5.

17. More On Induction

Matt gave us today's quote.

Quote: [A. Einstein] "Pure mathematics is, in its way, the poetry of logical ideas."

We spent much of the day working in groups on the homework problems from last class. After verifying the claim from Conjecture 16.5 for a number of integers, Courtney shared her solution on the board.

Theorem 17.1 (Courtney)**.** *For all integers $k \geq 1$, we have the formula*

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Proof. **Base case:** When $k = 1$, the left-hand side of the equation is $1^2 = 1$, and the right-hand side gives

$$\frac{1(1+1)(2(1)+1)}{6} = \frac{(1)(2)(3)}{6} = 1.$$

So the formula holds when $k = 1$.

Inductive hypothesis: Let $k > 1$ be an integer and assume the formula holds for all integers q with $1 \leq q < k$. That is, assume

$$1^2 + 2^2 + \cdots + q^2 = \frac{q(q+1)(2q+1)}{6}$$

for all integers q where $1 \leq q < k$.

Inductive step: We wish to show that the formula holds for k, i.e., that

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

We start with the left-hand side. We have:

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 &= \left(1^2 + 2^2 + \cdots + (k-1)^2\right) + k^2 \\ &= \frac{(k-1)((k-1)+1)(2(k-1)+1)}{6} + k^2 \end{aligned}$$

by the inductive hypothesis. Continuing to simplify, we have

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 &= \frac{(k-1)k(2k-1)}{6} + k^2 \\ &= \frac{2k^3 - 3k^2 + k}{6} + \frac{6k^2}{6} \\ &= \frac{2k^3 + 3k^2 + k}{6} \\ &= \frac{k(k+1)(2k+1)}{6}, \end{aligned}$$

which shows that the formula holds for k. So, by the Principle of Mathematical Induction, the formula holds for all integers $k \geq 1$.

□

Our next goal was to find and prove a formula for the sum of the first n odd numbers. Sam started us by looking at examples:

n	n^{th} odd number	sum of the first n odd numbers
1	$1 = 2(1) - 1$	$1 = 1^2$
2	$3 = 2(2) - 1$	$4 = 2^2$
3	$5 = 2(3) - 1$	$9 = 3^2$
4	$7 = 2(4) - 1$	$16 = 4^2$
5	$9 = 2(5) - 1$	$25 = 5^2$

At this point, the pattern seemed pretty clear and we made our conjecture. Matt carried out the details of the proof on the board.

Theorem 17.2 (Matt)**.** *For each integer $n \geq 1$, the sum of the first n odd numbers is n^2. Since the n^{th} odd number is given by the formula $2n - 1$, we have*

$$1 + 3 + \cdots + (2n - 1) = n^2.$$

Proof. **Base case:** When $n = 1$, the left-hand side of the equation is $2(1) - 1 = 1$, and the right-hand side gives $1^2 = 1$. So the formula holds when $n = 1$.

Inductive hypothesis: Let $n > 1$ be an integer and assume the formula holds for all integers l with $1 \leq l < n$. That is, assume

$$1 + 3 + \cdots + (2l - 1) = l^2.$$

Inductive step: We wish to show that the formula holds for n, i.e., that

$$1 + 3 + \cdots + (2n - 1) = n^2.$$

We start with the left-hand side. We have:

$$\begin{aligned} 1 + 3 + \cdots + (2n - 1) &= (1 + 3 + \cdots + (2(n - 1) - 1)) + (2n - 1) \\ &= (n - 1)^2 + (2n - 1) \end{aligned}$$

by the inductive hypothesis. Continuing to simplify, we have

$$\begin{aligned} 1 + 3 + \cdots + (2n - 1) &= n^2 - 2n + 1 + 2n - 1 \\ &= n^2, \end{aligned}$$

which shows that the formula holds for n. By the Principle of Mathematical Induction, the formula holds for all integers $n \geq 1$.

□

We then worked together as a class for the remaining homework exercise from last class. We present it here as an example.

Example: Define the function f as follows:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 2 \\ f(n) &= f(n - 1) + 2f(n - 2), \text{ for integers } n \geq 2. \end{aligned}$$

We calculated $f(n)$ for a few integers n to get a feel for the function. We said:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 2 \\ f(2) &= f(1) + 2f(0) = 2 + 2(1) = 4 \\ f(3) &= f(2) + 2f(1) = 4 + 2(2) = 8 \\ f(4) &= f(3) + 2f(2) = 8 + 2(4) = 16. \end{aligned}$$

At this point we saw a pattern and guessed that $f(n) = 2^n$ for all integers $n \geq 0$. We proved the claim using PMI.

Proof. **Base case:** When $n = 0$, $f(0) = 1 = 2^0$. So the formula holds when $n = 0$.

Inductive hypothesis: Let $n > 0$ be an integer and assume the formula holds for all integers q with $1 \leq q < n$. That is, assume

$$f(q) = 2^q.$$

Inductive step: We wish to show that the formula holds for n, i.e., that

$$f(n) = 2^n.$$

Note that the inductive hypothesis says the formula works for *both* $n - 1$ and $n - 2$. We start with the definition of $f(n)$. We have:

$$\begin{aligned} f(n) &= f(n-1) + 2f(n-2) \\ &= 2^{n-1} + 2 \cdot 2^{n-2} \end{aligned}$$

by the inductive hypothesis. Continuing to simplify, we have

$$\begin{aligned} f(n) &= 2^{n-1} + 2^{n-1} \\ &= 2 \cdot 2^{n-1} \\ &= 2^n, \end{aligned}$$

which shows that the formula holds for n. Thus, by the Principle of Mathematical Induction, the formula holds for all integers $n \geq 0$.

□

We ended class with a theorem that will later help us prove the Fundamental Theorem of Arithmetic.

Theorem 17.3. *Let $n > 1$ be an integer. Then n can be factored as a product of primes. More precisely, there are primes $p_1, \ldots, p_s$ such $n = p_1 \cdots p_s$.*

The power of PMI allows us to prove this result.

Proof. Note that the smallest possible value for n is $n = 2$, so we use that as our base case.

Base case: When $n = 2$, we can write "$2 = 2$" as a factorization of 2 into primes, since 2 is prime. So the statement holds for $n = 2$.

Inductive hypothesis: Let $n > 1$ be an integer and assume the statement holds for all l with $2 \leq l < n$. In other words, for every integer l with $2 \leq l < n$, assume that l can be factored into a product of primes.

Inductive step: We wish to show that the statement holds for n, i.e., that n can be factored into a product of primes. If n is itself prime, then we can write "$n = n$" as a factorization of n into primes, and we're done. So assume n is not prime. Then $n = ab$ for some integers a and b with $2 \leq a < n$ and $2 \leq b < n$. But then both a and b are integers to which the inductive hypothesis applies, and so there are primes $p_1, \ldots, p_s$ and $q_1, \ldots, q_t$ such that $a = p_1 \cdots p_s$ and $b = q_1 \cdots q_t$. Therefore, we have

$$n = ab = p_1 \cdots p_s q_1 \cdots q_t,$$

i.e., we have a factorization of n into primes. This shows that the statement holds for n. By the Principle of Mathematical Induction, the statement holds for all integers $n \geq 2$.

□

Homework: Suppose p is a prime integer and $a_1, \ldots, a_n$ are any integers such that $p|(a_1 \cdots a_n)$. Show that $p|a_i$ for some i such that $1 \leq i \leq n$. [*Hint*: Try to use PMI and the fact that if $p|(cd)$ for any integers c and d then either $p|c$ or $p|d$ (why?).]

18. The Fundamental Theorem of Arithmetic

Today's quote was:

Quote: [P. Halmos] "The only way to learn mathematics is to do mathematics."

In order to prove the Fundamental Theorem of Arithmetic we need to look at the homework problem from last class. We began by clarifying notation and then completed the problem together as a class. Zach provided us with the key Inductive Step.

Proposition 18.1. *Suppose p is a prime integer and $a_1, \ldots, a_n$ are any integers such that p divides the product $(a_1)(a_2)\cdots(a_n)$. Then p divides a_i for some i such that $1 \leq i \leq n$.*

Proof. We prove this by induction on n.

Base case: When $n = 1$, we just have p divides a_1. Then of course p divides one of the factors. In the case $n = 2$ we have that p divides $(a_1)(a_2)$. Thus, by Theorem 14.2, p divides a_1 or p divides a_2.

Inductive hypothesis: Let $n > 2$ be an integer and assume the statement holds for all integers q with $1 \leq q < n$. In other words, for every integer q with $1 \leq q < n$, if p divides $(a_1)(a_2)\cdots(a_q)$ then p divides a_i for some $1 \leq i \leq q$.

Inductive step: Suppose p divides $(a_1)\cdots(a_n)$. Group the first $n-1$ factors together and let $c = (a_1)\cdots(a_{n-1})$. Then $p|ca_n$. By Theorem 14.2, p divides c or p divides a_n. If p divides a_n, we are done. Otherwise, if p divides $c = (a_1)\cdots(a_{n-1})$, we apply the inductive hypothesis to see that p divides a_i for some integer i where $1 \leq i \leq n-1$. So, by the Principle of Mathematical Induction, the claim is true for all integers $n \geq 1$.

□

We were then (finally) ready to prove the Fundamental Theorem of Arithmetic. First, we stated the theorem carefully.

Theorem 18.2 (Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ has a unique factorization into prime integers. By the word "unique" we mean the following: If $n = p_1 \cdot p_2 \cdots p_k$ and $n = q_1 \cdot q_2 \cdots q_l$ are two prime factorizations of n then $k = l$ and, after reordering, $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$.*

Proof. By Theorem 17.3, every integer $n \geq 2$ has a prime factorization. We just need to prove the uniqueness claim. To do this, we proceed by induction on the number k of factors in the first factorization.

Base case: Let $k = 1$. In this case $n = p_1$, so n is prime. Since p_1 has no factors other than 1 and itself, it is clear that $q_1 = p_1$ and $l = k = 1$.

Inductive hypothesis: Let $k \geq 1$ be an integer and assume the uniqueness claim is true for whenever n has q prime factors where $1 \leq q < k$.

Inductive step: Suppose $n = p_1 \cdot p_2 \cdots p_k$ and $n = q_1 \cdot q_2 \cdots q_l$ are two prime factorizations of n. We know that p_k divides n. Thus, p_k divides $q_1 \cdot q_2 \cdots q_l$. Since p_k is prime, we know by Proposition 18.1 that p_k divides q_j for some j with $1 \leq j \leq l$. After reordering the q's, we can assume p_k divides q_l. Now we cancel $p_k = q_l$ from the equation

$$p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_l$$

which gives us

$$p_1 \cdot p_2 \cdots p_{k-1} = q_1 \cdot q_2 \cdots q_{l-1}.$$

By our inductive hypothesis, we know the unique factorization claim holds for the integer $p_1 \cdot p_2 \cdots p_{k-1}$. Therefore, $k-1 = l-1$ and $p_1 = q_1, \ldots, p_{k-1} = q_{q-1}$. We conclude that $k = l$ and $p_1 = q_1, p_2 = q_2, \ldots, p_{k-1} = q_{k-1}, p_k = q_k$. So, by the Principle of Mathematical Induction, the claim is true for all integers $n \geq 1$.

□

19. Congruence modulo n

We next moved on to a new topic: congruences!

Definition 19.1. Let a, b, and n be integers with $n > 0$. Then we say a *is congruent to* b *modulo* n if n divides $a - b$. We write $a \equiv b \pmod{n}$.

Example: $7 \equiv 4 \pmod{3}$ since $3|(7-4)$.

Example: $12 \equiv 7 \pmod{5}$ since $5|(12-7)$.

Example: $7 \equiv -3 \pmod{5}$ since $5|(7-(-3))$.

We then worked in our table groups on the following two tasks. Randy, Ethan, Michelle, and Kai wrote up their solutions to Task 1 on the board.

Task 1: For each integer a among 0, 1, 2, 3, 4, 5, 6, and 7, find 4 positive integers and 4 negative integers b such that a is congruent to b modulo 6.

a	some positive b's congruent to a modulo 6	some negative b's congruent to a modulo 6
0	$6, 12, 18, 24$	$-6, -12, -18, -24$
1	$7, 13, 19, 25$	$-5, -11, -17, -23$
2	$8, 14, 20, 26$	$-4, -10, -16, -22$
3	$9, 15, 21, 27$	$-3, -9, -15, -21$
4	$10, 16, 22, 28$	$-2, -8, -14, -20$
5	$11, 17, 23, 29$	$-1, -7, -13, -19$
6	$6, 12, 18, 24$	$-6, -12, -18, -24$
7	$7, 13, 19, 25$	$-5, -11, -17, -23$

Task 2: Let a and n be integers with $n \geq 1$. Complete the blanks in the following sentences:

(1) (Blake) a is even if and only if $a \equiv \underline{0 \pmod{2}}$.
(2) (Blake) a is odd if and only if $a \equiv \underline{1 \pmod{2}}$.
(3) (Garrett) a is a 6-zero if and only if $a \equiv \underline{0 \pmod{6}}$.
(4) (Garrett) a is a 6-two if and only if $a \equiv \underline{2 \pmod{6}}$.
(5) (Patrick) a is a 6-four if and only if $a \equiv \underline{4 \pmod{6}}$.
(6) (Patrick) $a \equiv 0 \pmod{n}$ if and only if $\underline{n|a}$.
(7) (Bryce) $a \equiv \underline{a} \pmod{n}$.
(8) (Bryce) For any integer b, we have $a \equiv b \underline{\pmod{1}}$.

We then decided to prove some easy facts about congruences. The first fact says that congruence modulo n is *symmetric*.

Theorem 19.2. *Let a, b, n be integers where $n > 0$. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.*

Proof. By definition, we have that $n|(a-b)$. We all agreed that this implies n divides $(-1)(a-b)$. Thus, $n|(b-a)$ which shows that $b \equiv a \pmod{n}$. □

The second fact says that congruence modulo n is *transitive*.

Theorem 19.3. *Let a, b, c, n be integers where $n > 0$. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

Proof. We know that $n|(a-b)$ and $n|(b-c)$. Thus, n divides $(a-b)+(b-c)$. Simplifying we see that $n|(a-c)$ as desired. □

What happens if we multiply both sides of a congruence equation by an integer?

Theorem 19.4. *Let a, b, n be integers with $n > 0$. If $a \equiv b \pmod{n}$ then $ac \equiv bc \pmod{n}$ for any integer c.*

Proof. Since $n|(a-b)$ there exists an integer x such that $a - b = nx$. Multiplying both sides of this equation by c gives $c(a-b) = ac - bc = n(xc)$. This implies that n divides $ac - bc$ and so $ac \equiv bc \pmod{n}$. □

To continue our investigation of congruence modulo arithmetic we looked at an example.

Example:

- 86 is congruent to 22 modulo 4
- 21 is congruent to 5 modulo 4

To check these facts, just notice that $86 - 22 = 64 = 4(16)$ and $21 - 5 = 16 = 4(4)$.

We then noticed that $86 + 21 = 107$ and $22 + 5 = 27$, and that 107 and 27 are congruent modulo 4. Further, we also noticed that $(86)(21) = 1806$ and $(22)(5) = 110$, and that 1806 and 110 are congruent modulo 4. This led us to the following conjecture.

Conjecture 19.5. *Let a, b, c, d and n be integers with $n > 0$. Assume that*

- *a is congruent to b modulo n*
- *c is congruent to d modulo n*

Then

1. *ac is congruent to bd modulo n*
2. *$a + c$ is congruent to $b + d$ modulo n*
3. *$a - c$ is congruent to $b - d$ modulo n*

Homework:

1. Prove Conjecture 19.5.
2. Come up with as many ways as possible to say that a is congruent to b modulo n. For example, "a and b have the same lists modulo n" is one way to say it.

20. Modular Arithmetic

Zach gave us the following quote (borrowed from Matt!):

Quote: [Johann von Neumann] "In mathematics, you don't understand things. You just get used to them."

We started class with a discussion of Conjecture 19.5 which was homework from last class.

Theorem 20.1. *Let a, b, c, d and n be integers with $n > 0$. Assume that*

- *a is congruent to b modulo n*
- *c is congruent to d modulo n*

Then

(1) *ac is congruent to bd modulo n*
(2) *$a + c$ is congruent to $b + d$ modulo n*
(3) *$a - c$ is congruent to $b - d$ modulo n*

Proof. Since $a \equiv b \pmod{n}$, we know that $n|(a - b)$. Thus, there is an integer x such that $nx = a - b$. Thus, $a = nx + b$. Similarly, there is an integer s such that $c = ns + d$.

(1) (Evan) We have:

$$\begin{aligned} ac - bd &= (nx + b)(ns + d) - bd \\ &= n^2xs + nxd + nsb + bd - bd \\ &= n^2xs + nxd + nsb \\ &= n(nxs + xd + sb). \end{aligned}$$

Thus n divides $ac - bd$ and so $ac \equiv bd \pmod{n}$.

(2) (Matt) We know that $n|(a - b)$ and $n|(c - d)$. So, by Theorem 2.5, we know that n divides $(a-b)+(c-d)$. Rearranging this sum, we see that n divides $(a+c)-(b+d)$. Thus, $a + c \equiv b + d \pmod{n}$.

(3) (Dan) We have:

$$\begin{aligned} (a - c) - (b - d) &= ((nx + b) - (ns + d)) - (b - d) \\ &= nx + b - ns - d - b + d \\ &= nx - ns \\ &= n(x - s). \end{aligned}$$

Thus n divides $(a - c) - (b - d)$ and so $a - c \equiv b - d \pmod{n}$.

□

We then turned our attention to finding different ways we could say "a is congruent to b modulo n." We came up with the following list.

Proposition 20.2 (Class)**.** *The following are equivalent:*

- *$a \equiv b \pmod{n}$.*
- *$\frac{a-b}{n}$ is an integer.*
- *$\frac{b-a}{n}$ is an integer.*
- *$b \equiv a \pmod{n}$.*
- *$a = nk + b$ for some integer k.*

- $\frac{ca-cb}{n}$ *is an integer for every integer* c.
- $n|(a-b)$.
- $n|(b-a)$.
- *There exists an integer* m *such that* $mn = a - b$.
- $\frac{a}{n} - \frac{a}{n}$ *is an integer.*

Taking powers in a congruence equation was our next topic of discovery. To see what happens we first looked at some examples.

Example: Let $a = 3, b = -9, n = 6$. Since $6|(3-(-9))$ we know that $3 \equiv -9 \pmod 6$. We observed that $3^2 \equiv (-9)^2 \pmod 6, 3^4 \equiv (-9)^4 \pmod 6, 3^5 \equiv (-9)^5 \pmod 6$ and $3^9 \equiv (-9)^9 \pmod 6$.

Almost everyone made the conjecture that if $a \equiv b \pmod n$, then $a^m \equiv b^m \pmod n$ for any positive integer m. However, Zach wasn't quite convinced yet. His concern was that we were working with $a = 3, b = -9$ and $n = 6$ and that there was something special going on since $3|(-9)$ and $3|6$. So, he asked us to look at $a = 7, b = 11$ and $n = 4$.

Example: Note that $7 \equiv 11 \pmod 4$. Also, $7^4 \equiv 11^4 \pmod 4$ and $7^{73} \equiv 11^{73} \pmod 4$.

We were then ready to prove our conjecture.

Theorem 20.3. *Let* a, b, n *be integers with* $n \geq 1$. *If* $a \equiv b \pmod n$, *then* $a^m \equiv b^m \pmod n$ *for all integers* $m \geq 1$.

Proof. We proceed by induction on the power m.

Base case: Let $m = 1$. By assumption, we have $a^1 \equiv b^1 \pmod n$.

Inductive hypothesis: Let $m > 1$ and assume $a^k \equiv b^k \pmod n$ for all integers k such that $1 \leq k < m$.

Inductive step: By the inductive hypothesis, we have $a^{m-1} \equiv b^{m-1} \pmod n$. Also, by assumption, $a \equiv b \pmod n$. So, by Theorem 20.1, we know that

$$a^{m-1}a \equiv b^{m-1}b \pmod n.$$

Thus, $a^m \equiv b^m \pmod n$. Therefore, by the Principle of Mathematical Induction, $a^m \equiv b^m \pmod n$ for all integers $m \geq 1$.

□

21. Non-negative Residue of a Modulo

After verifying that modular arithmetic makes sense, we moved on to a new question.

Question: Let b and n be integers with $n \geq 1$. How can we find all integers a such that $a \equiv b \pmod n$?

In order to get a feel for this question, we took a few minutes to discuss some examples in our table groups. Our task was to look at the table of congruences in Task 1 from last class and describe how we found the values b. After a few minutes we came up with an algorithm. Courtney gave us the key observation.

Observation: Let b and n be integers with $n \geq 1$. We know that an integer $a \in \mathbb{Z}$ satisfies $a \equiv b \pmod n$ if and only if:

$$n|(a-b) \iff a - b = nk \iff a = nk + b$$

for some integer k.

For example, if we want to write down a bunch of integers which are congruent to 10 modulo 4, we start with 10 and add or subtract multiples of 4. So 10, 14, 18, 22 as well as $6, 2, -2, -6$ are all congruent to 10 modulo 4. We noted that 2 was the smallest non-negative integer which is congruent to 10 modulo 4. This last observation brought us to the next question.

Question: Let a and n be integers such that $n \geq 1$. What is the *smallest* non-negative integer b such that $a \equiv b \pmod{n}$? We call this integer r and write $a\,\%n$. We say that r is the *least non-negative residue (lnr) of a modulo n.*

We worked out a few examples to get a hold of this concept.

Example: $10\,\%4 = 2$; $12\,\%7 = 5$; $25\,\%6 = 1$.

After these examples, Patrick conjectured that the $a\,\%n$ is the remainder upon dividing a by n. We finished class with a proof of Patrick's conjecture.

Theorem 21.1 (Patrick)**.** *Let a and n be integers with $n \geq 1$. The smallest non-negative integer which is congruent to a modulo n is the remainder r upon dividing a by n.*

Proof. By Euclid's Division Lemma, there exist integers q and r such that $a = nq + r$ where $0 \leq r < n$. By definition, r is the remainder upon dividing a by n. Also, since $a - r = nq$, we see that n divides $a - r$. Thus, $a \equiv r \pmod{n}$. Now let s be the smallest non-negative integer such that $a \equiv s \pmod{n}$. Suppose $s \neq r$. Then $0 \leq s < r < n$, and so $0 < r - s < n$. Since $a \equiv r \pmod{n}$ and $a \equiv s \pmod{n}$, subtracting and applying Theorem 20.1 gives that $0 \equiv r - s \pmod{n}$. Hence, $n|(r - s)$. But n cannot divide any integer which is positive and less than n. Thus we have a contradiction. We conclude that $s = r$. □

Homework:

(1) Find $29\,\%6$, $-61\,\%8$ and $80\,\%20$.
(2) Prove the following statement: Let a and n be integers with $n \geq 1$. Suppose $r = a\%n$ and $r > 0$. Then $n - r = -a\%n$.
(3) State a divisibility test for 3.

22. Fast Exponentiation

Zach put the following quote up on the board:

Quote: [Unknown] "Black holes result from God dividing the universe by zero."

We started the class with a discussion of the first two homework problems from Thursday.

Example: (Sam) $29\,\%6 = 5$ since 5 is the remainder obtained upon dividing 29 by 6 (i.e., $29 = 6(4) + 5$). That is, $29 \equiv 5 \pmod 6$ and 5 is the least non-negative integer b such that $29 \equiv b \pmod 6$.

Using similar arguments we completed the following examples.

Example: (Bryce) $80\,\%20 = 0$ since 0 is the remainder obtained upon dividing 80 by 20 (i.e., $80 = 20(4) + 0$).

Example: (Zach) $-61\,\%8 = 3$ since 3 is the remainder obtained upon dividing -61 by 8 (i.e., $-61 = 8(-8) + 3$).

Zach noted that it is tricky to find $-a\,\%n$, where a is a positive integer, because we need to remember that the result should be a non-negative integer. For example, we could have noted $-61 = 8(-7) - 5$, but -5 is not the remainder upon dividing -61 by 8 since it is not non-negative. This brought us to the second homework exercise which can be a useful trick!

Theorem 22.1. *Let a and n be integers with $n \geq 1$. Suppose $r = a\%n$ and $r > 0$. Then $n - r = -a\%n$.*

Proof. Since $r = a\%n$, we know that there exists an integer q such that $a = nq + r$ where $0 \leq r < n$. By assumption $r \geq 1$, and so we have $1 \leq r \leq n - 1$. After multiplying by -1, we have

$$\begin{aligned} -a &= n(-q) - r \\ &= n(-q) - n + n - r \\ &= n(-q - 1) + (n - r). \end{aligned}$$

Now, since $1 \leq r \leq n-1$, we must have $-1 \geq -r \geq -(n-1)$. Thus, $n-(n-1) \leq n-r \leq n-1$. That is, $1 \leq n - r \leq n - 1$.

Therefore, we have $-a = n(-q - 1) + (n - r)$ and $1 \leq n - r < n$. By Euclid's Division Lemma, this means that $n - r$ is the remainder we obtain upon dividing $-a$ by n. So, by definition, we conclude that $n - r = -a\%n$. □

We verified that this theorem works for the homework question Zach did. We have $61\,\%8 = 5$ and $8 - 5 = 3$. We also have that $-61\,\%8 = 3$ as claimed above.

Now that we know that modular arithmetic makes sense, it's time to have some fun!

Example: Suppose we want to compute $5^{47}\,\%21$. Let's start squaring:

$$\begin{aligned}
5 &\equiv 5 \pmod{21}\\
5^2 = 25 &\equiv 4 \pmod{21}\\
5^4 = (5^2)^2 &\equiv 4^2 \pmod{21}\\
&\equiv 16 \pmod{21}\\
&\equiv -5 \pmod{21}\\
5^8 = (5^4)^2 &\equiv (-5)^2 \pmod{21}\\
&\equiv 25 \pmod{21}\\
&\equiv 4 \pmod{21}\\
5^{16} = (5^8)^2 &\equiv 4^2 \pmod{21}\\
&\equiv -5 \pmod{21}\\
5^{32} = (5^{16})^2 &\equiv (-5)^2 \pmod{21}\\
&\equiv 4 \pmod{21}
\end{aligned}$$

Now, since

$$5^{47} = 5^{32+8+4+2+1} = 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5^2 \cdot 5^1,$$

we have

$$\begin{aligned}
5^{47} &\equiv 4 \cdot 4 \cdot (-5) \cdot 4 \cdot 5 \pmod{21}\\
&\equiv 4 \cdot (-20) \cdot 20 \pmod{21}\\
&\equiv 4 \cdot 1 \cdot (-1) \pmod{21}\\
&\equiv -4 \pmod{21}\\
&\equiv 17 \pmod{21}.
\end{aligned}$$

Note that even though we don't know the value of 5^{47}, we do know that $5^{47} \equiv 17 \pmod{21}$. Also notice how we used positive and negative numbers throughout the computation to keep things small and manageable. Finally, since $0 \leq 17 < 21$, we know that $5^{47}\,\%21 = 17$.

We worked in groups on a second example, which Ethan put on the board for us.

Example: (Ethan) We wish to compute $7^{23}\,\%17$. As before, we start squaring:

$$\begin{aligned} 7 &\equiv 7 \pmod{17} \\ 7^2 = 49 &\equiv 15 \pmod{17} \\ &\equiv -2 \pmod{17} \\ 7^4 = (7^2)^2 &\equiv (-2)^2 \pmod{17} \\ &\equiv 4 \pmod{17} \\ 7^8 = (7^4)^2 &\equiv 4^2 \pmod{17} \\ &\equiv 16 \pmod{17} \\ &\equiv -1 \pmod{17} \\ 7^{16} = (7^8)^2 &\equiv (-1)^2 \pmod{17} \\ &\equiv 1 \pmod{17}. \end{aligned}$$

Now, since

$$7^{23} = 7^{16+4+2+1} = 7^{16} \cdot 7^4 \cdot 7^2 \cdot 7^1,$$

we have

$$\begin{aligned} 7^{23} &\equiv 1 \cdot 4 \cdot (-2) \cdot 7 \pmod{17} \\ &\equiv 4 \cdot (-14) \pmod{17} \\ &\equiv 4 \cdot 3 \pmod{17} \\ &\equiv 12 \pmod{17}. \end{aligned}$$

Therefore, since $0 \leq 12 < 17$,

$$7^{23}\,\%17 = 12.$$

We noted that we shouldn't just carelessly start squaring in these types of problems.

Example: (Dan) Suppose we wish to find $18^{23}\,\%17$. Observe that $18 \equiv 1 \pmod{17}$. So, $18^{23} \equiv 1^{23} \pmod{17} \equiv 1 \pmod{17}$. Thus, $18^{23}\,\%17 = 1$.

Example: Suppose we wish to find $16^{23}\,\%17$. We have $16 \equiv -1 \pmod{17}$. Thus, $16^{23} \equiv (-1)^{23} \pmod{17} \equiv -1 \pmod{17} \equiv 16 \pmod{17}$. Thus, $16^{23}\,\%17 = 16$.

23. Divisibility Tests

Patrick announced that a number is divisible by 2 if and only if its last digit is divisible by 2. Everyone agreed with the claim. As a gentle introduction to divisibility tests, we decided to prove this. However, before moving forward I probed the idea of what we meant by "digit".

Definition 23.1. Let n be a positive integer. We say that a string of integers $d_0, d_1, \ldots, d_k$ are the *base 10 digits* for n if $0 \leq d_j \leq 9$ for each j and

$$n = 10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10^1 d_1 + d_0.$$

Example: The base 10 digits of 5742 are 5, 7, 4, and 2 since

$$\begin{aligned} 5742 &= 5000 + 700 + 40 + 2 \\ &= 5(1000) + 7(100) + 4(10) + 2(1) \\ &= 5(10^3) + 7(10^2) + 4(10^1) + 2(10^0). \end{aligned}$$

We see that 5 is "d_3", 7 is "d_2", 4 is "d_1" and 2 is "d_0".

We were then ready to prove Patrick's claim!

Theorem 23.2 (Divisibility by 2)**.** *A positive integer n is divisible by 2 if and only if its last digit is divisible by 2. In other words, let n be a positive integer and write $n = 10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10^1 d_1 + d_0$ with $0 \leq d_i \leq 9$ for each i. Then n is divisible by 2 if and only if d_0 is, i.e., $n \equiv 0 \pmod 2$ if and only if $d_0 \equiv 0 \pmod 2$.*

Proof. We have

$$\begin{aligned} n &= 10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10^1 d_1 + d_0 \\ &= 10(10^{k-1} d_k + \cdots + 10 d_2 + d_1) + d_0 \\ &= 2(5)(10^{k-1} d_k + \cdots + 10 d_2 + d_1) + d_0 \\ &\equiv d_0 \pmod 2. \end{aligned}$$

We've now shown that n and d_0 are always congruent modulo 2, and so certainly one of them is divisible by 2 (i.e., congruent to 0 modulo 2) if and only if the other is. □

Many of us remembered being taught that a number is divisible by 3 if and only if the sum of its digits was divisible by 3. We made this more precise using base 10 representation.

Conjecture 23.3 (Divisibility by 3)**.** *Let n be a positive integer with base 10 representation*

$$n = 10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10 d_1 + d_0.$$

Then

$$n \text{ is divisible by } 3 \qquad \text{if and only if} \qquad d_k + d_{k-1} + \cdots + d_1 + d_0 \text{ is divisible by } 3.$$

Example: Consider the number $n = 4,584,789,675$. If we add up the digits, we get $4+5+8+4+7+8+9+6+7+5 = 63$. At this point we might know that $63 = 3(21)$, or we could go ahead and say $6 + 3 = 9$ and hopefully then we all do know that $9 = 3(3)$. So since the sum of the digits is divisible by 3, our conjecture says that the original number is also.

At this point, we ran out of time and decided to prove the "Divisibility by 3 Conjecture" next class.

Homework:

(1) Compute $911^{853} \,\%4$.
(2) Find the last two digits of 23^{23}.
(3) Come up with divisibility tests for 4, 9 and 11.

24. More Fast Exponentiation

I started class with the following quote. Zach agreed to bring another quote on Tuesday.

Quote: [G. Leibniz] "Music is the pleasure the human mind experiences from counting without being aware that it is counting."

Since we just handed in Test 3, we decided to work a few minutes in groups on the homework from Tuesday. Afterwards volunteers put their solutions on the board.

Example: (Sam) We want to compute $911^{853}\,\%4$. We have

$$\begin{aligned}
911 &\equiv 3 \pmod 4\\
911^2 &\equiv 3^2 \pmod 4\\
&\equiv 1 \pmod 4\\
911^4 = (911^2)^2 &\equiv 1^2 \pmod 4\\
&\equiv 1 \pmod 4\\
911^8 = (911^4)^2 &\equiv 1^2 \pmod 4\\
&\equiv 1 \pmod 4\\
911^{16} = (911^8)^2 &\equiv 1^2 \pmod 4\\
&\equiv 1 \pmod 4\\
911^{32} = (911^{16})^2 &\equiv 1^2 \pmod 4\\
&\equiv 1 \pmod 4\\
911^{64} = (911^{32})^2 &\equiv 1^2 \pmod 4\\
&\equiv 1 \pmod 4\\
911^{128} = (911^{64})^2 &\equiv 1^2 \pmod 4\\
&\equiv 1 \pmod 4\\
911^{256} = (911^{128})^2 &\equiv 1^2 \pmod 4\\
&\equiv 1 \pmod 4\\
911^{512} = (911^{256})^2 &\equiv 1^2 \pmod 4\\
&\equiv 1 \pmod 4.
\end{aligned}$$

Now, since

$$911^{853} = 911^{512+256+64+16+4+1} = 911^{512}\cdot 911^{256}\cdot 911^{64}\cdot 911^{16}\cdot 911^{4}\cdot 911^{1},$$

we have

$$\begin{aligned}
911^{853} &\equiv 1\cdot 1\cdot 1\cdot 1\cdot 1\cdot 3 \pmod 4\\
&\equiv 3 \pmod 4.
\end{aligned}$$

Therefore,

$$911^{853}\,\%4 = 3.$$

Randy's table noticed that there was a much easier way to approach the above example:

Example: (Randy) We want to compute $911^{853}\,\%4$. We have

$$911 \equiv -1 \pmod 4$$

and so

$$911^{853} \equiv (-1)^{853} \pmod 4.$$

Since 853 is odd, $(-1)^{853} = -1$ and so

$$911^{853} \equiv -1 \pmod 4.$$

Therefore, $911^{853}\,\%4 = 3$.

Patrick did the second problem for us:

Example: (Patrick) We wish to find the last two digits of 23^{23}. This is the same as finding $23^{23}\,\%100$. We have:

$$\begin{aligned}
23 &\equiv 23 \pmod{100} \\
23^2 &= 529 \\
&\equiv 29 \pmod{100} \\
23^4 &= (23^2)^2 \\
&\equiv 29^2 \pmod{100} \\
&\equiv 841 \pmod{100} \\
&\equiv 41 \pmod{100} \\
23^8 &= (23^4)^2 \\
&\equiv 41^2 \pmod{100} \\
&\equiv 1681 \pmod{100} \\
&\equiv -19 \pmod{100} \\
23^{16} &= (23^8)^2 \\
&\equiv (-19)^2 \pmod{100} \\
&\equiv 361 \pmod{100} \\
&\equiv -39 \pmod{100}.
\end{aligned}$$

Now, since

$$23^{23} = 23^{16+4+2+1} = 23^{16} \cdot 23^4 \cdot 23^2 \cdot 23^1,$$

we have

$$\begin{aligned}
23^{23} &\equiv (-39) \cdot 41 \cdot 29 \cdot 23 \pmod{100} \\
&\equiv -1066533 \pmod{100} \\
&\equiv -33 \pmod{100} \\
&\equiv 67 \pmod{100}.
\end{aligned}$$

Therefore,

$$23^{23}\,\%100 = 67$$

and so the last two digits of 23^{23} are 6 and 7.

25. More Divisibility Tests

We then decided to prove the "Divisibility by 3 Conjecture" from last class.

Theorem 25.1 (Divisibility by 3)**.** *Let n be a positive integer with base 10 representation*

$$n = d_0 + 10d_1 + \cdots + 10^{k-1}d_{k-1} + 10^k d_k.$$

Then n is divisible by 3 if and only if the sum of the digits of n is divisible by 3. In other words,

$$n \text{ is divisible by } 3 \qquad \text{if and only if} \qquad d_0 + d_1 + \cdots + d_k \text{ is divisible by } 3.$$

Proof. Note that $10 \equiv 1 \pmod 3$. Thus, $10^j \equiv 1^j \pmod 3 \equiv 1 \pmod 3$ for all positive integers j. Thus,

$$\begin{aligned} n &= d_0 + 10d_1 + \cdots + 10^{k-1}d_{k-1} + 10^k d_k \\ &\equiv d_0 + 1 \cdot d_1 + \cdots + 1 \cdot d_{k-1} + 1 \cdot d_k \pmod 3 \\ &\equiv d_0 + d_1 + \cdots + d_{k-1} + d_k \pmod 3. \end{aligned}$$

So, n is divisible by 3 if and only if $n \equiv 0 \pmod 3$, if and only if $d_0 + \cdots + d_k \equiv 0 \pmod 3$, if and only if $d_0 + d_1 + \cdots + d_k$ is divisible by 3. □

Everyone then made the crucial observation that $10 \equiv 1 \pmod 9$ and so the above proof can be modified to obtain a divisibility test for 9! We didn't write this on the board, but it is included below.

Theorem 25.2 (Divisibility by 9)**.** *Let n be a positive integer with base 10 representation*

$$n = d_0 + 10d_1 + \cdots + 10^{k-1}d_{k-1} + 10^k d_k.$$

Then n is divisible by 9 if and only if the sum of the digits of n is divisible by 9. In other words,

$$n \text{ is divisible by } 9 \qquad \text{if and only if} \qquad d_0 + d_1 + \cdots + d_k \text{ is divisible by } 9.$$

Proof. Note that $10 \equiv 1 \pmod 9$. Thus, $10^j \equiv 1^j \pmod 9 \equiv 1 \pmod 9$ for all positive integers j. Thus,

$$\begin{aligned} n &= d_0 + 10d_1 + \cdots + 10^{k-1}d_{k-1} + 10^k d_k \\ &\equiv d_0 + 1 \cdot d_1 + \cdots + 1 \cdot d_{k-1} + 1 \cdot d_k \pmod 9 \\ &\equiv d_0 + d_1 + \cdots + d_{k-1} + d_k \pmod 9. \end{aligned}$$

So, n is divisible by 9 if and only if $n \equiv 0 \pmod 9$, if and only if $d_0 + \cdots + d_k \equiv 0 \pmod 9$, if and only if $d_0 + d_1 + \cdots + d_k$ is divisible by 9. □

Using the same technique from the last two proofs we came up with a divisibility test for 4. At first there was some confusion on how to say it correctly, but we eventually came up with the next theorem.

Theorem 25.3 (Divisibility by 4)**.** *Let n be a positive integer with base 10 representation*

$$n = d_0 + 10d_1 + \cdots + 10^{k-1}d_{k-1} + 10^k d_k.$$

Then n is divisible by 4 if and only if the number formed by the last two digits of n is divisible by 4. In other words,

$$n \text{ is divisible by } 4 \qquad \text{if and only if} \qquad 10d_1 + d_0 \text{ is divisible by } 4.$$

Proof. Note that $10^2 = 100 \equiv 0 \pmod 4$. Thus, $10^j \equiv 0^j \pmod 4 \equiv 0 \pmod 4$ for all positive integers $j \geq 2$. Thus,

$$\begin{aligned} n &= d_0 + 10d_1 + \cdots + 10^{k-1}d_{k-1} + 10^k d_k \\ &\equiv d_0 + 10 \cdot d_1 + 0 \cdot d_2 + \cdots + 0 \cdot d_{k-1} + 0 \cdot d_k \pmod 4 \\ &\equiv d_0 + 10 \cdot d_1 \pmod 4. \end{aligned}$$

So, n is divisible by 4 if and only if $n \equiv 0 \pmod 4$, if and only if $d_0 + 10d_1 \equiv 0 \pmod 4$, if and only if $d_0 + 10d_1$ is divisible by 4. □

We then worked in groups to find a divisibility test for 11. Zach's table noticed an interesting pattern which we did not prove, but which is worth noting.

Example: (Zach) Consider the integer 30795237. Group the last two digits together and the remaining first 6 digits together. Add the number formed by the last two digits to the number formed by the first 6 digits: $307952 + 37 = 307989$. Repeat the process on this new integer: $3079 + 89 = 3168$. And repeat again: $31 + 68 = 99$. Observe that 99 is divisible by 11!

Try this on the integer 209: $2 + 09 = 11$ which is divisible by 11.

How about the integer 1089? We have $10 + 89 = 99$ which is also divisible by 11.

Everyone was very impressed with Zach's table's pattern!

Michelle's table noticed a different pattern which turned into the divisibility test we proved.

Theorem 25.4 (Divisibility by 11)**.** *Let n be a positive integer with base 10 representation*

$$n = d_0 + 10d_1 + \cdots + 10^{k-1}d_{k-1} + 10^k d_k.$$

Then n is divisible by 11 if and only if the alternating sum of the digits of n is divisible by 11. In other words,

$$11|n \qquad \text{if and only if} \qquad 11|(d_0 - d_1 + d_2 + \cdots + (-1)^{k-1}d_{k-1} + (-1)^k d_k).$$

Proof. Note that $10 \equiv -1 \pmod{11}$. Thus, $10^j \equiv (-1)^j \pmod{11}$ for all positive integers j. Thus,

$$\begin{aligned} n &= d_0 + 10d_1 + \cdots + 10^{k-1}d_{k-1} + 10^k d_k \\ &\equiv d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^{k-1} \cdot d_k + (-1)^k \cdot d_k \pmod{11}. \end{aligned}$$

So, $11|n$ if and only if $n \equiv 0 \pmod{11}$, if and only if $d_0 - d_1 + \cdots + (-1)^k d_k \equiv 0 \pmod{11}$, if and only if $d_0 - d_1 + \cdots + (-1)^{k-1}d_{k-1} + (-1)^k d_k$ is divisible by 11. □

We spent the remainder of class working in groups to find a divisibility test for 37. In addition, we discussed the *group project* guidelines.

Homework: Find and prove divisibility tests for 37 and 2^t. *Hint*: A positive integer n is divisible by 2^t if and only if the number formed by the last t digits of n are divisible by 2^t.

26. Two More Divisibility Tests

Zach shared his second promised quote:

Quote: [Carl Friedrich Gauss] "Mathematics is the Queen of the sciences, and number theory the Queen of mathematics."

As usual, class started with a discussion of homework problems from last class. Our first goal was to come up with a test to decide when a positive integer is divisible by 37. We worked in groups to get started.

Theorem 26.1 (Ethan, Trevor; Divisibility by 37)**.** *Let n be a positive integer with base 10 representation*

$$n = 10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10d_1 + d_0.$$

Then n is divisible by 37 if and only if

$$d_0 + 10d_1 - 11d_2 + d_3 + 10d_4 - 11d_5 + \cdots$$

is divisible by 37.

Proof. We have

$$\begin{aligned} 10^0 = 1 &\equiv 1 \pmod{37} \\ 10^1 = 10 &\equiv 10 \pmod{37} \\ 10^2 = 100 &\equiv -11 \pmod{37} \\ 10^3 = 1000 &\equiv 1 \pmod{37}, \end{aligned}$$

and, since $10^4 = 10^3 \cdot 10$, the pattern repeats from there. More precisely, since

$$10^{3q+r} = (10^3)^q (10)^r \equiv 10^r \pmod{37},$$

we can now find a formula:

$$10^i \equiv \begin{cases} 1 & \text{if } i \equiv 0 \pmod 3, \\ 10 & \text{if } i \equiv 1 \pmod 3, \\ -11 & \text{if } i \equiv 2 \pmod 3. \end{cases}$$

This means that if $n = d_0 + 10d_1 + \cdots + 10^{k-1} d_{k-1} + 10^k d_k$, then

$$n \equiv d_0 + 10d_1 - 11d_2 + d_3 + 10d_4 - 11d_5 + d_6 + \cdots \pmod{37}.$$

Now, n is divisible by 37 if and only if $n \equiv 0 \pmod{37}$. Since

$$n \equiv d_0 + 10d_1 - 11d_2 + d_3 + 10d_4 - 11d_5 + d_6 + \cdots \pmod{37},$$

we get that n is divisible by 37 if and only if $d_0 + 10d_1 - 11d_2 + d_3 + 10d_4 - 11d_5 + d_6 + \cdots$ is divisible by 37. □

Example: Suppose we want to know if 9876543 is divisible by 37, and we don't want to divide to find out. We compute

$$\begin{aligned} 9876543 &\equiv 3 + 10(4) - 11(5) + 6 + 10(7) - 11(8) + 9 \pmod{37} \\ &\equiv 3 + 40 - 55 + 6 + 70 - 88 + 9 \pmod{37} \\ &\equiv -15 \pmod{37} \\ &\equiv 22 \pmod{37} \end{aligned}$$

Not only does this tell us that 9876543 is not divisible by 37, it also tells us that the remainder when you divide 9876543 by 37 is 22. Sure enough, $9876543 = (266933)(37) + 22$.

Matt helped us with the key step in our next divisibility test.

Theorem 26.2 (Divisibility by 2^t)**.** *Let n be a positive integer. Then n is divisible by 2^t if and only if the number formed by the last t digits of n is divisible by 2^t.*

Proof. We can use Euclid's Division Lemma to write $n = 10^t k + r$ for some integers k and r with $0 \leq r < 10^t$. Then r is the number formed by the last t digits of n. We have

$$\begin{aligned} n &= 10^t k + r \\ &= (2^t)(5^t)k + r \\ &\equiv r \pmod{2^t}. \end{aligned}$$

So, n is divisible by 2^t if and only if $n \equiv 0 \pmod{2^t}$, if and only if $r \equiv 0 \pmod{2^t}$, if and only if r is divisible by 2^t. □

27. UPC's

We decided it was time for a new topic and moved on to a discussion of UPC numbers. Most identification numbers in use today have at least one digit which is used as a check digit. We shall consider a scheme which is used on things that all college students are familiar with: the *Universal Product Code (UPC).*

The Universal Product Code (UPC) number, which appears today on almost everything one buys, is encoded in bars of varying width (to be read by a scanner), with the numbers represented by the bars often printed below (for typing in by the clerk when the scanner balks). The UPC is a 12 digit number. Usually, the first and last digit are listed separately, on either side of the bar code, and the middle 10 digits are broken into two chunks of 5. Thus, we will write UPC numbers as

$$a_1 - a_2a_3a_4a_5a_6 - a_7a_8a_9a_{10}a_{11} - a_{12},$$

where a_1 through a_{12} are individual digits between 0 and 9 (inclusive). The first example we looked at was the desktop copy holder I bought from Staples. The UPC on the box is

$$7 - 18103 - 02335 - 1.$$

The first six digits (a_1 through a_6) are assigned to the manufacturer by some overseeing agency, and the next five (a_7 through a_{11}) are assigned to the product by the manufacturer. The last digit (a_{12}) is a check digit. This check digit is chosen to satisfy the condition

$$3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + (a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) \equiv 0 \pmod{10}.$$

Example: Note that the UPC number on my copy holder satisfies this formula since

$$\begin{aligned} 3(7+8+0+0+3+5)+(1+1+3+2+3+1) &= 3(23)+11 \\ &= 69+11 \\ &= 80 \\ &\equiv 0 \pmod{10}. \end{aligned}$$

The next example we looked at was the bag of snack-sized Kit-Kat bars I brought to class.

Example: The first 11 digits of the UPC number from the bag of Kit-Kat bars are

$$0-34000-08752.$$

What is the last digit a_{12}? We need

$$3(0+4+0+0+7+2)+(3+0+0+8+5+a_{12}) \equiv 0 \pmod{10},$$

i.e.,

$$3(13)+16+a_{12} \equiv 0 \pmod{10},$$

i.e.,

$$39+16+a_{12} \equiv 0 \pmod{10},$$

i.e.,

$$55+a_{12} \equiv 0 \pmod{10}.$$

This means that a_{12} must be 5. (And indeed, checking the bag, it is.)

We then spent most of the remainder of class of a couple tasks in our table groups.

Task 1: I wrote down the following UPC number, but I made a mistake when I wrote it: I changed the value of one digit. (So 11 of the 12 are correct, but one is incorrect.)

$$6-18135-00002-7.$$

(1) Verify that this is not a valid UPC number.
(2) Find all possible ways to "fix" what I wrote to get a valid UPC number.

Kim wrote up her solution to the first part of the task. We see that this UPC is invalid because

$$3(6+8+3+0+0+2)+(1+1+5+0+0+7) = 71 \not\equiv 0 \pmod{10}.$$

Matt noted that the easiest way to change this UPC to be valid is to subtract one from the sum, which we can do by decreasing any of the non-zero entries in the even-numbered positions by 1. This gives the following valid UPC's:

$$\begin{gathered} 6-08135-00002-7 \\ 6-18035-00002-7 \\ 6-18134-00002-7 \\ 6-18135-00002-6 \end{gathered}$$

Each of these gives a weighted sum of 70, which is certainly 0 modulo 10.

Matt also pointed out that we could also change either of the 0's in even-numbered positions to 9, giving the following valid UPC's:

$$\begin{gathered} 6-18135-09002-7 \\ 6-18135-00092-7 \end{gathered}$$

Each of these gives a weighted sum of 80, again certainly 0 modulo 10.

Finally, Garrett observed that we could also add 3 (modulo 10) to any of the entries in odd-numbered positions. This gives the following valid UPC's:

$$9-18135-00002-7$$
$$6-11135-00002-7$$
$$6-18165-00002-7$$
$$6-18135-30002-7$$
$$6-18135-00302-7$$
$$6-18135-00005-7$$

The weighted sums here are each 80 (we've added 3(3)), except the second one which is 50 (we subtracted 3(7)).

Task 2: I again gave a UPC number, but this time I transposed two (adjacent) digits when I wrote it down on the board:

$$0-71662-04042-6.$$

(1) Show that this is not a valid UPC number.
(2) List all the possible ways you could obtain a valid UPC number from this number, given that a transposition error occurred.

Bryce showed that the number $0-71662-04042-6$ is not a valid UPC number because

$$3(0+1+6+0+0+2)+(7+6+2+4+4+6)=3(9)+29=56\equiv 6 \pmod{10}$$

and if it were valid, this sum would be congruent to 0 modulo 10. If we assume that the error made was a transposition error, then we can check all the possibilities. In general, there are 11 things to check: we switch a_i and a_{i+1} for $1\le i\le 11$. In this case, however, since $a_4=a_5=4$, switching a_4 and a_5 isn't really an error and so there are only 10 things to check. Three of them work and were quickly found by Matt, Kai, and Evan:

$$\mathbf{7}-\mathbf{0}1662-04042-6$$
$$0-7166\mathbf{0}-\mathbf{2}4042-6$$
$$0-71662-040\mathbf{24}-6$$

are all valid UPC numbers and hence are possibilities for the original UPC number. Since we don't know which of these transposition errors actually occurred, we see that the transposition error cannot be corrected.

The purpose of the check digit is so that common errors can be detected or possibly even corrected. The most common errors that could occur are *single digit errors*, *transposition errors*, and *erasures*. A single digit error occurs when one digit is read incorrectly. This could be a result of a scratch in the bar code, or some dust either on the bar code or on the scanner. A transposition error occurs when two digits are switched. This is most likely to happen in a situation where the scanner has failed and a person is typing in the number. An erasure occurs when one part of the bar code is so badly mangled that the scanner doesn't know what one of the digits was supposed to be. We say an error is *detected* if a computer can see that the resulting UPC number is not valid, i.e., if the weighted sum

$$3(a_1+a_3+a_5+a_7+a_9+a_{11})+(a_2+a_4+a_6+a_8+a_{10}+a_{12})$$

fails to be congruent to 0 modulo 10. An error is *corrected* if there is a unique way to fix the invalid UPC (under the assumption that a certain type of error occurred) to obtain a valid one.

We already know, from Tasks 1 and 2, that single digit errors and transposition errors cannot always be corrected. But it's unclear whether they can be detected. We decided to treat transposition errors first, and left single digit errors as homework.

Example: Transposition errors cannot always be detected. For example,

$$0 - 55000 - 00000 - 0$$

is a valid UPC number, but switching the first and second digits yields

$$5 - 05000 - 00000 - 0,$$

which is also valid.

We then discussed erasure errors. It was noted that these can always be detected.

Theorem 27.1. *The UPC scheme can correct all erasures.*

Proof. If an erasure occurs, then we know that an error has occurred because we are given a UPC with a blank or a "?" in it. We even know where the erasure occurred. So it only makes sense to ask whether such an error can always be corrected. The answer is yes.

Let "?" represent the erased digit. Suppose first that the error occurs in an even-numbered position. Let A be the sum of the digits in the odd-numbered positions, and let B be the sum of the digits (except the one which was erased) in the even-numbered positions. Then, to have a valid UPC number, we must have

$$3A + B + ? \equiv 0 \pmod{10},$$

which means that

$$? \equiv -3A - B \pmod{10}.$$

Since we know the value of "?" is an integer between 0 and 9 inclusive, its value is uniquely determined by its value modulo 10. So we're done with the even case.

Now suppose the erasure occurred in an odd-numbered position. Let A be the sum of the digits (except the one that was erased) in the odd-numbered positions, and let B be the sum of the digits in the even-numbered positions. Then to have a valid UPC number, we must have

$$3(A + ?) + B \equiv 0 \pmod{10},$$

which simplifies to

$$3? \equiv -3A - B \pmod{10}.$$

If we multiply both sides by 7 and note that $21 \equiv 1 \pmod{10}$, we get

$$? \equiv -A - 7B \pmod{10}.$$

In summary, we've given a formula for the missing digit must be in the case of any erasure. This means that any erasure can be corrected. □

Homework: Can single-digit errors always be detected? In other words, suppose $a_1 - a_2a_3a_4a_5a_6 - a_7a_8a_9a_{10}a_{11} - a_{12}$ is a valid UPC number. If a single digit error occurs, i.e., if the value of some a_j is changed to some new value a'_j, is it always the case that the resulting string of 12 digits is *not* a valid UPC number?

28. UPC's Revisited

Ethan gave us the following great quote:

Quote: [Ted Mosby from *How I Met Your Mother* and Descartes] "In order to determine whether there is anything we know with certainty, we first have to doubt everything we know."

We took the first 5 or so minutes of class to fill out mid-semester feedback forms. Thank you for the feedback!

We then recalled what we learned about UPC numbers last class. In particular, we noted that transposition errors cannot always be detected and even when they are detected they cannot always be corrected. Further, erasures can always be both detected and corrected. We recalled that Task 1 from last class showed that single digit errors cannot always be corrected. This left us to deal with the homework question last class which asked if single digit errors could always be detected. The answer is "yes" and we proved half of this claim. I have included the entire proof here in the notes.

Theorem 28.1. *The UPC scheme always detects single digit errors. More precisely, let*

$$a_1 - a_2a_3a_4a_5a_6 - a_7a_8a_9a_{10}a_{11} - a_{12}$$

be a valid UPC number. For some j, where $1 \leq j \leq 12$, change a_j to a'_j. Then the resulting new 12-digit number is never a valid UPC number.

Proof. Recall that, since

$$a_1 - a_2a_3a_4a_5a_6 - a_7a_8a_9a_{10}a_{11} - a_{12}$$

is a valid UPC number, we must have

$$3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + (a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) \equiv 0 \pmod{10}.$$

We consider two cases, depending on whether j is odd or even. Suppose first that j is odd. Let

$$k = 3(\text{sum of the } a_i\text{'s with } i \text{ odd and } i \neq j) + (a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}).$$

Then, since the original UPC is valid, we have

$$3a_j + k \equiv 0 \pmod{10}.$$

If the new UPC is valid, then we also have

$$3a'_j + k \equiv 0 \pmod{10}.$$

Subtracting the bottom equation from the top one, we get

$$3(a_j - a'_j) \equiv 0 \pmod{10}.$$

Since $0 \leq a_j \leq 9$ and $0 \leq a'_j \leq 9$, we see that the only way this equation can hold is if $a_j = a'_j$. This is a contradiction, and so we must have that the new UPC is not valid.

Now suppose j is even. Let

$$l = 3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + (\text{sum of the } a_i\text{'s with } i \text{ even and } i \neq j).$$

Then, since the original UPC is valid, we have

$$a_j + l \equiv 0 \pmod{10}.$$

If the new UPC is valid, then we also have

$$a'_j + l \equiv 0 \pmod{10}.$$

Subtracting the bottom equation from the top one, we get

$$a_j - a'_j \equiv 0 \pmod{10}.$$

Adding a'_j to both sides yields $a_j \equiv a'_j \pmod{10}$. Since $0 \leq a_j \leq 9$ and $0 \leq a'_j \leq 9$, we see that the only way this equation can hold is if $a_j = a'_j$. This is a contradiction, and so we must have that the new UPC is not valid. □

Craving a change of pace with Fall Break right around the corner, we decided to watch the *Nova* documentary on Andrew Wiles' work to prove *Fermat's Last Theorem*.

Before heading off to Fall Break, we decided on our groups for the group projects. The 6 groups (with some very creative names) are:

- *Group* $\frac{2}{0}$: Evan, Dan, TJ
- *Group Unknown*: Kai, Bryce
- *Group Gerbils*: Courtney, Kim
- *Group Mathamagic*: Patrick, Blake, Michelle
- *Group Epsilon*: Zach, Ethan, Matt
- *Team Wiles*: Garrett, Sam, Trevor

To prepare for our next class, we agreed to think about the following:

29. Card Shuffling

Suppose we have a deck of 52 cards and we cut it into two equal piles, the top half and the bottom half. If we then interlace the cards, with the bottom card of the top half going on the bottom of the shuffled pile, the bottom card of the bottom half going on top of this card, etc., we call this process a *perfect in-shuffle* ("perfect" because we've divided and interlaced the cards perfectly, "in-shuffle" because the original top and bottom cards of the deck are inside the deck after the shuffle).

Homework:

(1) If a card starts out x spots from the bottom of the original deck, where does it end up after one perfect in-shuffle? For example, the bottom card starts at $x = 1$ and ends up 2 positions from the bottom.
(2) If a card starts out x spots from the bottom of the original deck, where does it end up after *two* perfect in-shuffles? three? $\ldots k$?
(3) What happens if we start with a deck of 50 cards? 54 cards? m cards?
(4) Is there a positive value of k such that performing k perfect in-shuffles on a standard 52-card deck will return the deck to its original position? If so, what is the smallest such k? What if we have 50 cards? 54 cards? m cards?

Happy Fall Break!!

30. More On Card Shuffling

We started class with a quote brought by Blake:

Quote: [C. Darwin] "A mathematician is a blind man in a dark room looking for a black cat which isn't there."

The first 10 minutes or so of class was dedicated to a discussion of the comments from the mid-semester feedback forms. We then spent much of our time time discussing the homework exercises on Card Shuffling distributed before Fall Break. In groups, we first examined the following question:

Question: Using 52 cards, if a card starts out x spots from the bottom of the original deck, where does it end up after one perfect in-shuffle? For example, the bottom card starts at $x = 1$ and ends up 2 positions from the bottom.

Kim, Courtney and Bryce shared their findings. All groups agreed with the solution. We let $f(x)$ be the position after one perfect in-shuffle of the card which started at position x. Then

$$f(x) = \begin{cases} 2x & \text{if } 1 \leq x \leq 26, \\ 2x - 53 & \text{if } 27 \leq x \leq 52. \end{cases}$$

I then asked people to find one formula, using congruences, which would describe both situations. Garrett, Michelle, Sam and Trevor came up with

$$f(x) = 2x\%53.$$

To see why this formula works, notice that if $1 \leq x \leq 26$, then $2 \leq 2x \leq 52$ and so $2x\%53 = 2x$. On the other hand, if $27 \leq x \leq 52$, then $54 \leq 2x \leq 104$, and so $2x\%53 = 2x - 53$.

We then investigated successive perfect in-shuffles. In particular, we were curious about the following question:

Question: Using 52 cards, if a card starts out x spots from the bottom of the original deck, where does it end up after *two* perfect in-shuffles? three? $\ldots k$?

After a little while, we found:

Theorem 30.1 (Trevor)**.** *Using 52 cards, let $f_k(x)$ denote the position after k perfect in-shuffles of the card which started at position x in the deck. Then*

$$f_k(x) = 2^k x\%53.$$

In particular, a card which started at position x is at position $2x\%53$ after 1 perfect in-shuffle, position $4x\%53$ after 2 perfect in-shuffles, and $8x\%53$ after 3 perfect in-shuffles.

Proof. The easiest way to see this is to iterate the function. We have

$$f_2(x) = f_1(f_1(x)) = 2(2x\%53)\%53 = 4x\%53,$$
$$f_3(x) = f_1(f_2(x)) = 2(4x\%53)\%53 = 8x\%53,$$

and, in general,

$$f_k(x) = f_1(f_{k-1}(x)) = 2(2^{k-1}x\%53)\%53 = 2^k x\%53.$$

Note that, to make this completely rigorous, we really should do a (very simple) induction proof. □

Our next question dealt with varying the number of cards in the deck.

Question: What happens if we start with a deck of 50 cards? 54 cards? m cards?

Everyone quickly decided that if a card starts out at position x in a deck of m cards, then its position after k perfect in-shuffles is $2^k x \% (m+1)$. It was pointed out that this only makes sense if m is even, since otherwise we can't split the deck exactly in half and so we can't do perfect in-shuffles.

The remainder of the class focused on:

Question: Is there a positive value of k such that performing k perfect in-shuffles on a standard 52-card deck will return the deck to its original position? If so, find the smallest such k.

Theorem 30.2 (Matt)**.** *A 52-card deck will be restored to its original order after 52 perfect in-shuffles.*

Proof. We know that if a card started at position x, then it's at position $2^k x \% 53$ after k perfect in-shuffles. To restore the deck to its original order, we need $2^k x \equiv x \pmod{53}$, i.e., $2^k \equiv 1 \pmod{53}$. So we made the following table:

k	$2^k \pmod{53}$
1	2
2	4
3	8
4	16
5	32
6	11
7	22
8	44
9	35
10	17
11	34
12	15
13	30
14	7
15	14
16	28
17	3
18	6
19	12
20	24

k	$2^k \pmod{53}$
21	48
22	43
23	33
24	13
25	26
26	52
27	51
28	49
29	45
30	37
31	21
32	42
33	31
34	9
35	18
36	36
37	19
38	38
39	23
40	46
41	39
42	25
43	50
44	47
45	41
46	29
47	5
48	10
49	20
50	40
51	27
52	1

So the smallest k which restores a 52-card deck to its original order is $k = 52$, i.e.,

$$2^{52} \equiv 1 \pmod{53}$$

and

$$2^k \not\equiv 1 \pmod{53}$$

for $1 \leq k \leq 51$. □

We generalized the above proof to different numbers of cards.

Theorem 30.3 (Evan)**.** *A 50-card deck will be restored to its original order after 8 perfect in-shuffles.*

Proof. We know that if a card started at position x, then it's at position $2^k x \% 51$ after k perfect in-shuffles. To restore the deck to its original order, we need $2^k x \equiv x \pmod{51}$, i.e.,

$2^k \equiv 1 \pmod{51}$. So we start computing:

$$\begin{aligned}
2^1 &= 2 \equiv 2 \pmod{51} \\
2^2 &= 4 \equiv 4 \pmod{51} \\
2^3 &= 8 \equiv 8 \pmod{51} \\
2^4 &= 16 \equiv 16 \pmod{51} \\
2^5 &= 32 \equiv 32 \pmod{51} \\
2^6 &= 64 \equiv 13 \pmod{51} \\
2^7 &= 2^6 \cdot 2 \equiv 26 \pmod{51} \\
2^8 &= 2^7 \cdot 2 \equiv 52 \pmod{51} \\
&\equiv 1 \pmod{51}
\end{aligned}$$

Since $2^8 \equiv 1 \pmod{51}$, we see that eight perfect in-shuffles will restore the deck to its original order. Since $2^k \not\equiv 1 \pmod{51}$ for $1 \leq k \leq 7$, we see that no fewer number of perfect in-shuffles will work. □

Theorem 30.4. *A 54-card deck will be restored to its original order after 20 perfect in-shuffles.*

Proof. We know that if a card started at position x, then it's at position $2^k x \% 55$ after k perfect in-shuffles. To restore the deck to its original order, we need $2^k x \equiv x \pmod{55}$, i.e., $2^k \equiv 1 \pmod{55}$. So we made the following table:

k	$2^k \pmod{55}$
1	2
2	4
3	8
4	16
5	32
6	9
7	18
8	36
9	17
10	34
11	13
12	26
13	52
14	49
15	43
16	31
17	7
18	14
19	28
20	1

So, the smallest k which restores a 54-card deck to its original order is $k = 20$, i.e.,

$$2^{20} \equiv 1 \pmod{55}$$

and

$$2^k \not\equiv 1 \pmod{55}$$

for $1 \leq k \leq 19$. □

Incidentally, these facts are often used by magicians. They train themselves to do perfect in-shuffles. While the audience thinks the deck is getting more and more shuffled, it is in fact being restored to its original order.

31. Powers Modulo m: A Preview

We spent the last few minutes talking about the following question, inspired by our work with card shuffling:

Question: Given $a, m \in \mathbb{Z}$, will there always be an integer $k \geq 1$ such that $a^k \equiv 1 \pmod{m}$? If so, can we find a formula for the smallest such k, or even just for any k that works? If there isn't always such a k, under what conditions will there be one?

Homework: Is there a positive integer k such that $a^k \equiv 1 \pmod{m}$ if:

(1) $a = 2, m = 51$
(2) $a = 12, m = 21$
(3) $a = 2, m = 53$
(4) $a = 2, m = 6$

32. Powers Modulo m Continued

Dan brought the following quote to start our week together:

Quote: [J. L. Von Neumann] "If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is."

Our first discussion of the class period concerned the homework from Thursday. Recall that we are interested in the question:

Question: Given $a, m \in \mathbb{Z}$, will there always be an integer $k \geq 1$ such that $a^k \equiv 1 \pmod{m}$?

The homework was to answer the above question for a variety of given a and m values. For example, if $a = 2$ and $m = 51$, then when discussing card shuffling we determined that $k = 8$ works (i.e., $2^8 \equiv 1 \pmod{51}$). We also saw that when $a = 2$ and $m = 53$, we can take $k = 52$. On the other hand, using $a = 2$ and $m = 6$, we have $2^2 = 4$ and $2^3 = 8 \equiv 2 \pmod{6}$, and so $2^k \equiv 2 \pmod{6}$ when k is odd and $2^k \equiv 4 \pmod{6}$ when k is even. So there is no integer $k \geq 1$ such that $2^k \equiv 1 \pmod{6}$. Finally, we considered $a = 12$ and $m = 21$.

Example: There is no positive integer k with $12^k \equiv 1 \pmod{21}$. To see this, compute powers of 12 modulo 21:

$$\begin{aligned}
12^1 = 12 &\equiv 12 \pmod{21} \\
12^2 = 144 &\equiv -3 \pmod{21} \\
12^3 &\equiv -36 \pmod{21} \\
&\equiv 6 \pmod{21} \\
12^4 &\equiv 9 \pmod{21} \\
12^5 &\equiv -18 \pmod{21} \\
&\equiv 3 \pmod{21} \\
12^6 &\equiv 36 \pmod{21} \\
&\equiv -6 \pmod{21} \\
12^7 &\equiv 54 \pmod{21} \\
&\equiv 12 \pmod{21}
\end{aligned}$$

which means that $12^8 \equiv -3 \pmod{21}$ and so 12^k is always congruent to 12, -3, 6, 9, 3 or -6 modulo 21. In particular, it's never 1.

Kim then made a conjecture.

Conjecture 32.1 (Kim)**.** *If $a|m$ then there is no integer $k \geq 1$ such that $a^k \equiv 1 \pmod{m}$.*

Patrick noted that Kim's conjecture was not an "if and only if" statement. We agreed that we wanted to make a conjecture that was strong as possible. To get a handle on this, we made the following table. Garrett, Ethan, Dan, Blake, and Courtney put their findings on the board.

m	a's where $1 \leq a \leq m-1$ & where there exists $k \geq 1$ with $a^k \equiv 1 \pmod{m}$
2	1 (k=1)
3	1 (k=1), 2 (k=2)
4	1 (k=1), 3 (k=2)
5	1 (k=1), 2 (k=4), 3 (k=4), 4 (k=2)
6	1 (k=1), 5 (k=2)
7	1 (k=1), 2 (k=3), 3 (k=6), 4 (k=3), 5 (k=6), 6 (k=2)
8	1 (k=1), 3 (k=2), 5 (k=2), 7 (k=2)

Based on the table we made the following conjecture:

Conjecture 32.2. *Given positive integers a and m, if there exists an integer $k \geq 1$ such that $a^k \equiv 1 \pmod{m}$, then $\gcd(a, m) = 1$.*

To prove this statement we looked at its equivalent *contrapositive*.

Theorem 32.3. *Let a and m be positive integers. If $\gcd(a, m) \neq 1$, then there is no positive integer k with $a^k \equiv 1 \pmod{m}$.*

Proof. Let $d = \gcd(a, m)$. Then we can write $a = ds$ for some s and $m = dt$ for some t. Then for any positive integer r, we have $a^r = (ds)^r = d^r s^r$. If $a^k \equiv 1 \pmod{m}$, for some positive integer k, we have that m divides $a^k - 1$, i.e., m divides $d^k s^k - 1$, and so $d^k s^k - 1 = ml$ for some l. Thus, $d^k a^k - 1 = ml = dtl$. Rearranging and substituting, we get $d(d^{k-1}s^k - lt) = 1$, which says d divides 1, which says $d = 1$. This is a contradiction and so there can be no such k. □

We were then willing to strengthen Conjecture 32.2:

Conjecture 32.4 (Everyone)**.** *Let a and m be positive integers. Then $\gcd(a, m) = 1$ if and only if there is a positive integer k such that $a^k \equiv 1 \pmod{m}$.*

We decided to assume Conjecture 32.4 is true for now and investigate some related questions. The first question posed was:

Question: Assume Conjecture 32.4 is true. Let a and m be positive integers. Is there a value of $k \geq 1$, depending on m, such that $a^k \equiv 1 \pmod{m}$ for *every* a with $\gcd(a, m) = 1$?

To tackle this question we needed to collect some data. We studied the tables of powers modulo m handed out at the beginning of class. Our findings were collected in a table. The third column, labeled "k", is the smallest value of k with $a^k \equiv 1 \pmod{m}$ for all a with $\gcd(a, m) = 1$. Patrick, Michelle, Bryce, and Kai wrote their table entries on the board for the class to compare.

m	a's with $\gcd(a,m)=1$	k
3	1,2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	2
9	1,2,4,5,7,8	6
10	1,3,7,9	4
11	1,2,3,4,5,6,7,8,9,10	10
12	1,5,7,11	2
13	1,2,3,4,5,6,7,8,9,10,11,12	12
14	1,3,5,9,11,13	6
15	1,2,4,7,8,11,13,14	4
16	1,3,5,7,9,11,13,15	4

Based on this table, everyone made the same conjecture:

Conjecture 32.5 (Everyone)**.** *Let m be a positive integer. Let k be the number of positive integers $a < m$ with $\gcd(a,m)=1$. Then $a^k \equiv 1 \pmod{m}$ for every positive integer a with $\gcd(a,m)=1$.*

We noticed that the third column in the above table actually gives this count in all but four of the examples: in the row labeled by 8 and in the row labeled by 12, the entry in the third column is 2 but there are 4 values of a listed. However, if $a^2 \equiv 1 \pmod{m}$, then $a^4 \equiv 1 \pmod{m}$ since $a^4 = (a^2)^2$ and $1^2 = 1$. So the conjecture really does seem to work. Similarly, the conjecture seems to work for the rows labeled by 15 and 16.

Based on our most recent conjecture, I introduced a definition:

Definition 32.6. The *Euler Phi Function* is the function $\phi(m)$ given by

$$\phi(m) = \#\{a \in \mathbb{Z} \mid 1 \le a \le m \text{ and } \gcd(a,m) = 1\}.$$

We also introduced the terminology:

Definition 32.7. If $\gcd(a,m)=1$, we say that a and m are *relatively prime*.

So the value of $\phi(m)$ is the number of positive integers which are less than m and relatively prime to m.

Homework: Find $\phi(3), \phi(5), \phi(8)$ and $\phi(12)$.

33. The Euler Phi Function

I sadly forgot to bring a quote to class today. Matt quickly came to my rescue though!

Quote: [A. Einstein] "Whatever you're problems in mathematics, I can assure you mine are much greater."

We started class by picking random numbers to decide on the order of the group presentations. The outcome was:

- Thursday, December 3: *Group Mathamagic* (Patrick, Blake, Michelle); *Group Epsilon* (Zach, Ethan, Matt)
- Tuesday, December 8: *Group* $\frac{2}{0}$ (Evan, Dan, TJ); *Team Wiles* (Garrett, Sam, Trevor)
- Thursday, December 10: *Group Gerbils* (Courtney, Kim); *Group Unknown* (Kai, Bryce)

We then recalled the definition of the Euler Phi Function $\phi(m)$ and its role in the following conjecture:

Conjecture 33.1 (Everyone)**.** *Let m be a positive integer. Then $a^{\phi(m)} \equiv 1 \pmod{m}$ for every positive integer a with $\gcd(a, m) = 1$.*

Our homework from last class was to find the values of $\phi(m)$ for $m = 3, 5, 8$ and 12. The solutions are collected in the next example.

Example: [Dan, Sam, Courtney, Evan] We have that $\phi(3) = 2$ since 1 and 2 are the only positive integers less than 3 which are relatively prime to 3. Similarly, $\phi(5) = 4$ since 1, 2, 3 and 4 are all relatively prime to 5. We also have that $\phi(8) = 4$ since 1, 3, 5, 7 are the only positive integers less than 8 which are relatively prime to 8. Finally, $\phi(12) = 4$ since the only positive integers less than 12 and relatively prime to 12 are 1, 5, 7 and 11.

Our next goal was to find some formulas for $\phi(m)$. We started by focusing on prime numbers.

Theorem 33.2 (Michelle)**.** *If p is prime, then $\phi(p) = p - 1$.*

Proof. We have that $\gcd(p, p) = p \neq 1$. From the definition, we know that $\phi(p)$ is the number of positive integers less than p and relatively prime to p. There are $p - 1$ positive integers strictly less than p, and since p is prime, they are all relatively prime to p. Thus $\phi(p) = p - 1$, as desired. □

It was easy to see how to push this further:

Theorem 33.3 (Zach)**.** *If p is prime, then $\phi(p^2) = p^2 - p$.*

Proof. Start by writing out the numbers from 1 to p^2. We need to cross out those numbers which are not relatively prime to p^2. Since p is prime, we have that $\gcd(a, p^2) \neq 1$ if and only if p divides a. So we need to cross out $1p$, $2p$, ..., $(p-1)p$, $(p)(p)$. There are p of these numbers we're crossing off, and so

$$\begin{aligned}\phi(p^2) &= \#\{1, 2, \ldots, p^2\} - \#\{1p, 2p, \ldots, (p)(p)\} \\ &= p^2 - p.\end{aligned}$$

□

And, in general, we have:

Theorem 33.4 (Zach, TJ)**.** *If p is prime, then $\phi(p^k) = p^k - p^{k-1}$ for every integer $k \geq 1$.*

Proof. There are p^k positive integers in the set $\{1, 2, 3, \ldots, p^k\}$. Since p is prime, for any a in this set, $\gcd(a, p^k) \neq 1$ if and only if a is a multiple of p. The multiples of p in our set are $\{1p, 2p, \ldots, (p^{k-1})(p)\}$, so there are p^{k-1} of them. Thus

$$\begin{aligned}\phi(p^k) &= \#\{1, 2, \ldots, p^k\} - \#\{1p, 2p, \ldots, (p^{k-1})(p)\} \\ &= p^k - p^{k-1}.\end{aligned}$$

□

From there, we wanted to see what happens with numbers that aren't powers of primes. The simplest case is the product of two primes. We investigated a concrete example to guess what happens in general.

Example: To compute $\phi(15)$, we can start by writing out the numbers 1 through 15. That's 15 numbers. If $\gcd(a, 15) \neq 1$, then either 3 divides a or 5 divides a. So we need to cross off the multiples of 3 and the multiples of 5. There are 5 multiples of 3 in our list: 3, 6, 9, 12 and 15. There are 3 multiples of 5 in our list: 5, 10 and 15. Since 15 appears in both of these "cross-out" lists, we need to be careful not to count it as being crossed out twice. In other words, we start with 15 numbers, we cross out 5 multiples of 3, and then we cross out the remaining $3 - 1 = 2$ multiples of 5. This means we are left with

$$15 - 5 - (3 - 1) = 15 - 5 - 3 + 1 = 8 = \phi(5) \cdot \phi(3) = (4)(2)$$

positive integers which are less than 15 and relatively prime to 15.

This generalizes to:

Theorem 33.5 (Everyone)**.** *If p and q are prime with $p \neq q$, then $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1) = pq - q - p + 1$.*

Proof. To compute $\phi(pq)$, we can start by writing out the numbers 1 through pq. That's pq numbers. If $\gcd(a, pq) \neq 1$, then either p divides a or q divides a. So we need to cross off the multiples of p and the multiples of q. There are q multiples of p in our list: $1p$, $2p$, …, $(q-1)p$, qp. There are p multiples of q in our list: $1q$, $2q$, …, $(p-1)q$, pq. Since pq appears in both of these "cross-out" lists, we need to be careful not to count it as being crossed out twice. In other words, we start with pq numbers, we cross out q multiples of p, and then we cross out the remaining $p - 1$ multiples of q. This means we are left with

$$pq - q - (p - 1) = pq - q - p + 1 = (p - 1)(q - 1) = \phi(p) \cdot \phi(q)$$

positive integers which are less than pq and relatively prime to pq. □

In fact, a similar argument shows that $\phi(rs) = \phi(r)\phi(s)$ when $\gcd(r, s) = 1$. Matt suggested that we generalize our direction of thought to prime factorizations of integers.

Theorem 33.6 (Matt)**.** *Let $n \geq 1$ be an integer with prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$. Then*

$$\phi(n) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1}).$$

We did not prove this theorem, but TJ pointed out that we would use induction on k for the argument.

For the remainder of class we worked on some specific examples.

Example: [TJ and Evan] Since $240 = 15 \cdot 16, 15 = 5 \cdot 3$ and $\gcd(15, 16) = 1 = \gcd(5, 3)$, we have

$$\phi(240) = \phi(15) \cdot \phi(16) = \phi(5) \cdot \phi(3) \cdot \phi(16) = 4 \cdot 2 \cdot 8 = 64.$$

Since $10800 = 2^4 3^3 5^2$, we know that

$$\phi(10800) = \phi(2^4)\phi(3^3)\phi(5^2) = (2^4 - 2^3)(3^3 - 3^2)(5^2 - 5) = (16 - 8)(27 - 9)(25 - 5) = 2880.$$

Homework:

(1) Find $\phi(984,021,224,766,008)$. *Hint:* $984,021,224,766,008 = 2^3 11^7 13^5 17$.
(2) Suppose a is a positive integer such that $a^3 \equiv 13 \pmod{55}$. What is a?
(3) Go back to the multiplication tables from Test 4. Come up with two conjectures by filling in the blanks below:
   (a) If _____ and $a^2 \equiv 1 \pmod{m}$, then $a \equiv 1 \pmod{m}$ or $a \equiv -1 \pmod{m}$.
   (b) If _____ and $ab \equiv ac \pmod{m}$, then $b \equiv c \pmod{m}$.

34. The Euler Phi Function: One Last Example

Class began with a quote shared by Courtney:

Quote: [R. Bott] "There are two ways to do mathematics. The first is to be smarter than everybody else. The second way is to be stupider than everybody else – but persistent."

We spent the majority of the class discussing homework exercises. The first homework exercise asked us to find $\phi(984,021,224,766,008)$. Without knowing the prime factorization of 984,021,224,766,008, finding $\phi(984,021,224,766,008)$ would be very difficult. However, I gave the information that $984,021,224,766,008 = 2^3 11^7 13^5 17$, and so computing $\phi(984,021,224,766,008)$ is very easy. TJ showed how to do this on the board:

$$\begin{aligned}\phi(984,021,224,766,008) &= \phi(2^3 11^7 13^5 17)\\ &= \phi(2^3)\phi(11^7)\phi(13^5)\phi(17)\\ &= (2^3-2^2)(11^7-11^6)(13^5-13^4)(17-1)\\ &= (4)(17715610)(342732)(16)\\ &= 388,589,212,577,280.\end{aligned}$$

The point here is that 984,021,224,766,008 is a really huge number, but we can still compute the value of $\phi(984,021,224,766,008)$ because we know its prime factorization. If we just had a huge number n but we didn't know the prime factorization of n, it would be very hard for us to compute $\phi(n)$. In fact, we would have only two options: we could try to factor n or we could write out the numbers from 1 to n and test each one to see if it's relatively prime to n. These options actually amount to the same thing, since finding numbers which aren't relatively prime to n will find us factors of n. This dilemma is the basis for why the cryptography (secret codes) system we'll be discussing later works: we'll create a very large n which is the product of two large distinct primes p and q. Since we know p and q, we can compute $\phi(n) = (p-1)(q-1)$. But if we don't tell anyone p or q then they can't compute $\phi(n)$. We'll return to this later on.

35. Solving a Modular Exponential Equation

The second homework exercise was:

Question: If a is a positive integer such that $a^3 \equiv 13 \pmod{55}$, then what is a?

Courtney explained her thoughts at the board. Her first step was to notice that we must have that 55 divides $a^3 - 13$ and so there is some integer x such that $55x = a^3 - 13$. Using trial and error, Courtney found that $a = 7$ satisfies this equation. Most people agreed that $a = 7$ works and said they also used the method of "trial and error". Everyone agreed that the method of trial and error would not work very well, however, if the numbers involved were very big. So, we decided to try to find a mathematical way of doing it. First, we recalled a recent conjecture:

Conjecture 35.1. *Let m be a positive integer. If $\gcd(b,m) = 1$, then $b^{\phi(m)} \equiv 1 \pmod{m}$.*

In our case, $m = 55 = (5)(11)$ and so $\phi(m) = \phi(55) = \phi(5)\phi(11) = (5-1)(11-1) = (4)(10) = 40$. This means that $b^{40} \equiv 1 \pmod{55}$ for every b with $\gcd(b,55) = 1$.

Next, we thought about how we would do this problem if we weren't working modulo 55. Dan and TJ shared some valuable intuition. If we were told that $a^3 = 13$ and we wanted to

know the value of a, we'd just take the cube root of both sides, i.e., we'd raise both sides to the $\frac{1}{3}$ power. So how do we do this if we're working modulo 55? The crucial observation is that, in a metaphysical sense, the point of the existence of $\frac{1}{3}$ is that it's what you need to multiply 3 by in order to get 1, i.e., it's the multiplicative inverse of 3. So, this is what we need: a multiplicative inverse of 3. More precisely, since we're talking about powers, we want a multiplicative inverse of 3 *modulo 40*. TJ noticed that

$$(3)(27) = 81 = 80 + 1 = 40(2) + 1 \equiv 1 \pmod{40}.$$

That is, 27 is the multiplicative inverse of 3 modulo 40.

The point here is that, using the above conjecture, if $\gcd(a, 55) = 1$ then

$$\begin{aligned}(a^3)^{27} = a^{81} = a^{80+1} = a^{80}a^1 = (a^{40})^2 a^1 &\equiv 1^2 a^1 \pmod{55} \\ &\equiv a \pmod{55}.\end{aligned}$$

In summary, we see that $a \equiv (a^3)^{27} \pmod{55}$.

Now we can finish the problem: We start with $a^3 \equiv 13 \pmod{55}$. Raising both sides to the 27^{th} power, we get that $(a^3)^{27} \equiv 13^{27} \pmod{55}$. From the previous paragraph, we get that $(a^3)^{27} \equiv a \pmod{55}$, and so we have $a \equiv 13^{27} \pmod{55}$. All that remains is to compute $13^{27} \pmod{55}$. Garrett showed us that we can compute this using *fast exponentiation*:

$$\begin{aligned}13^1 &\equiv 13 \pmod{55} \\ 13^2 &= 169 \equiv 4 \pmod{55} \\ 13^4 &= (13^2)^2 \equiv 4^2 \pmod{55} \\ &\equiv 16 \pmod{55} \\ 13^8 &= (13^4)^2 \equiv 16^2 \pmod{55} \\ &\equiv 256 \pmod{55} \\ &\equiv 36 \pmod{55} \\ 13^{16} &= (13^8)^2 \equiv (36)^2 \pmod{55} \\ &\equiv 1296 \pmod{55} \\ &\equiv 31 \pmod{55}\end{aligned}$$

and so

$$\begin{aligned}13^{27} = 13^{16+8+2+1} = 13^{16}13^8 13^2 13^1 &\equiv (31)(36)(4)(13) \pmod{55} \\ &\equiv 58032 \pmod{55} \\ &\equiv 7 \pmod{55},\end{aligned}$$

which is (thankfully!) the same solution we got earlier by our brute force methods.

Courtney mentioned that this second method was much harder than the method of trial and error. The hope now is that we can apply this method to solve *any* modular exponential equation, assuming that we know the prime factorization of the modulus so that we can compute the value of the Euler Phi Function. To convince ourselves that trial and error would be difficult with large numbers we gave ourselves another equation to consider in the homework at the end of class.

36. Multiplication Theorems

The other homework problem for today was to complete two fill-in-the-blank conjectures.

Theorem 36.1 (Mike & Garrett's Square Root Theorem)**.** *Suppose p is a prime number and $a^2 \equiv 1 \pmod{p}$. Then $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.*

Proof. Since $a^2 \equiv 1 \pmod{p}$, we know that $a^2 - 1$ is divisible by p. Factoring, we get that p divides $(a-1)(a+1)$. Since p is prime, we know that either p divides $a-1$ or p divides $a+1$ (see Theorem 14.2 from September 17). In the first case, we have $a \equiv 1 \pmod{p}$, and in the second case we have $a \equiv -1 \pmod{p}$. □

The second fill-in-the-blank conjecture was: If _____ and $ab \equiv ac \pmod{m}$, then $b \equiv c \pmod{m}$. The class generated 4 possible conjectures for the fill-in-the-blank space. The following were the suggested entries for the fill-in-the-blank:

- (TJ) $a \equiv c \pmod{m}$.
- (Trevor) $ab < m$.
- (Dan) m does not divide $a-1$.
- (Courtney and Evan) $\gcd(a, m) = 1$.

We took a vote and decided to try to prove the 4th suggested conjecture.

Theorem 36.2 (Courtney & Evan's Cancellation Theorem)**.** *Let a and m be integers such that $\gcd(a, m) = 1$ and $ab \equiv ac \pmod{m}$. Then $b \equiv c \pmod{m}$.*

Proof. Suppose $\gcd(a, m) = 1$ and $ab \equiv ac \pmod{m}$. Then m divides $ab - ac$. Pulling out the a, we get that m divides $a(b-c)$. By Corollary 12.1 on September 15, since $\gcd(a, m) = 1$, we know that m divides $b-c$. But then this means that $b \equiv c \pmod{m}$ and we're done. □

37. Euler's Theorem

Our next goal was to prove our outstanding conjecture involving congruence powers and the Euler Phi Function (Conjecture 33.1). However, before we can do so we need to work out some preliminary notation that will be handy.

Notation: Let $m \geq 1$ be an integer.

(1) Let
$$P(m) = \{x \in \mathbb{Z} \mid 1 \leq x \leq m \quad \text{and} \quad \gcd(x, m) = 1\}.$$
We know that there are $\phi(m)$ elements of $P(m)$ (this is just the definition of $\phi(m)$), and so we can write
$$P(m) = \{r_1, r_2, \ldots, r_{\phi(m)}\}.$$

(2) Let a be any integer with $\gcd(a, m) = 1$. Define
$$aP(m) := \{ar\%m \mid r \in P(m)\} = \{ar_1\%m, ar_2\%m, \ldots, ar_{\phi(m)}\%m\}.$$

At this point I assigned a task to be completed within our table groups.

Task: Let $m = 15$ and $a = 11$. Find $\phi(m), P(m), \#P(m)$ and $aP(m)$.

Homework:

(1) Complete the above Task. Blake agreed to share his solution on the board next class period.

(2) Suppose a is a positive integer such that $a^{2725} \equiv 1451 \pmod{3071}$. What is a? *Hint:* $3071 = (37)(83)$.
(3) What is "Fermat's Little Theorem"?

38. Modular Exponential Equations: A Second Example

Kim brought the following quote to class:

Quote: [Unknown] "A tragedy of mathematics is a beautiful conjecture ruined by an ugly fact."

For the first part of class we looked at Tuesday's homework problem involving a modular exponential equation. There was some confusion on how to get started and so we initiated the work together as a class.

Example: Suppose we know $a^{2725} \equiv 1451 \pmod{3071}$ and wish to find the value of a. We're also given the hint that $3071 = (37)(83)$.

By Conjecture 33.1, we believe that if $\gcd(a, 3071) = 1$ then $a^{\phi(3071)} \equiv 1 \pmod{3071}$. Since $3071 = (37)(83)$, we know that $\phi(3071) = \phi(37) \cdot \phi(83) = (36)(82) = 2952$. We then noted, via trial and error, that

$$(2725)(13) = (2952)(12) + 1 \equiv 1 \pmod{2952}.$$

Thus, if $\gcd(a, 3071) = 1$, then

$$(a^{2725})^{13} = a^{(2952)(12)}a^1 = (a^{2952})^{12}a^1 \equiv (1)^{12}a^1 \pmod{3071} \equiv a \pmod{3071}.$$

Therefore, if $a^{2725} \equiv 1451 \pmod{3071}$ and $\gcd(a, 3071) = 1$ then

$$(a^{2725})^{13} \equiv (1451)^{13} \pmod{3071} \implies a \equiv (1451)^{13} \pmod{3071}.$$

Using fast exponentiation we can find $(1451)^{13} \pmod{3071}$. Trevor put the details on the board for us:

$$\begin{aligned}
1451^1 = 1451 &\equiv 1451 \pmod{3071} \\
1451^2 = 2105401 &\equiv 1766 \pmod{3071} \\
1451^4 = (1451^2)^2 &\equiv (1766)^2 \pmod{3071} \\
&\equiv 3118756 \pmod{3071} \\
&\equiv 1691 \pmod{3071} \\
1451^8 = (1451^4)^2 &\equiv (1691)^2 \pmod{3071} \\
&\equiv 2859481 \pmod{3071} \\
&\equiv 380 \pmod{3071}
\end{aligned}$$

Therefore,

$$\begin{aligned}
1451^{13} = 1451^{8+4+1} = 1451^8 \cdot 1451^4 \cdot 1451 &\equiv 380 \cdot 1691 \cdot 1451 \pmod{3071} \\
&\equiv 932383580 \pmod{3071} \\
&\equiv 341 \pmod{3071}
\end{aligned}$$

Observe that $\gcd(341, 3071) = 1$. So $a = 341$ is the solution to $a^{2725} \equiv 1451 \pmod{3071}$.

Trevor pointed out that we should have a method to do this without using trial and error at all. Let's back up to where we used trial and error. We had gotten to the point where we needed to find integers l and k such that $2725l = 2952k + 1$. We can do this by applying

the Extended Euclidean Algorithm. Start with the Euclidean Algorithm and rewrite the equations:

$$\begin{aligned} 2952 = 2725(1) + 227 &\implies 227 = 2952 - 2725(1) \\ 2725 = 227(12) + 1 &\implies 1 = 2725 - 227(12) \end{aligned}$$

Now back-substitute:

$$\begin{aligned} 1 &= 2725 - 227(12) \\ &= 2725 - (2952 - 2725(1))(12) \\ &= 2725(13) - 2952(12) \end{aligned}$$

Rewriting this equation shows that $2725(13) - 1 = 2952(12)$, and so $2725(13) \equiv 1 \pmod{2952}$.

39. Back to Euler's Theorem

We next returned to our discussion on "Euler's Theorem". In particular, we completed the task started at the end of Tuesday's class. We continue with the notation set out on Tuesday.

Example: (Blake) Take $m = 15$ and $a = 11$. We have $\phi(15) = \phi((3)(5)) = \phi(3)\phi(5) = (3-1)(5-1) = 8$, $P(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$, and $\#P(15) = 8 = \phi(15)$. Also,

$$\begin{aligned} 11P(15) = \{&(11)(1)\%15, (11)(2)\%15, (11)(4)\%15, (11)(7)\%15, (11)(8)\%15, \\ &(11)(11)\%15, (11)(13)\%15, (11)(14)\%15\} \\ = \{&11, 7, 14, 2, 13, 1, 8, 4\}. \end{aligned}$$

We observed that in this example, $aP(m) = P(m)$ (as sets — the order is mixed up but both sets have exactly the same elements).

Our next goal was to prove that $P(m)$ and $aP(m)$ are always equal as sets. To do so we needed a preliminary fact.

Lemma: Let $m \geq 1$ be an integer and a be an integer such that $\gcd(a, m) = 1$. Let r be a number in $P(m)$. Then $\gcd(ar, m) = 1$.

Proof. By definition of $P(m)$, we know that $\gcd(r, m) = 1$. Theorem 11.1 on September 10 says, since $\gcd(a, m) = 1 = \gcd(r, m)$, that there are integers u, v, x and y with $au + mv = 1$ and $rx + my = 1$. Multiplying the two equations together, we have

$$\begin{aligned} (au + mv)(rx + my) &= (1)(1) \\ aurx + aumy + mvrx + mvmy &= 1 \\ ar(ux) + m(auy + vrx + vmy) &= 1, \end{aligned}$$

which shows that $\gcd(ar, m) = 1$ (again by Theorem 11.1). □

Theorem 39.1. *Let a and m be integers such that $m \geq 1$ and $\gcd(a, m) = 1$. Then $aP(m) = P(m)$.*

Proof. Since $P(m)$ has $\phi(m)$ elements, we can write $P(m) = \{r_1, r_2, \ldots, r_{\phi(m)}\}$. We first show that $aP(m) \subseteq P(m)$. That is, we first show that every element of $aP(m)$ is also an element of $P(m)$. We have that $\gcd(a, m) = \gcd(r, m) = 1$ for all $r \in P(m)$. So, by our most recent Lemma, $\gcd(ar, m) = 1$ for all $r \in P(m)$. Now by Euclid's Lemma, there exist integers q and b such that $ar = mq + b$ where $0 \leq b < m$. Since $\gcd(ar, m) = 1$, we see that $b \neq 0$. By the GCD Reduction Theorem, we also have that $1 = \gcd(ar, m) = \gcd(m, b)$. Thus $b = ar\%m$ satisfies $0 < b < m$ and $\gcd(m, b) = 1$, showing that $b = ar\%m$ is in $P(m)$. Thus, for all r in $P(m)$, the integer $ar\%m$ is in $P(m)$. This shows that $aP(m) \subseteq P(m)$.

Now we show that $aP(m) = P(m)$ by counting the elements in each of the sets. Since $\gcd(a, m) = 1$, Courtney and Evan's Cancellation Theorem tells us that if $ar_i\%m = ar_j\%m$, then $r_i = r_j$. Because of this, we see that $aP(m)$ has $\phi(m)$ elements. But this is the same number of elements in $P(m)$, and so since $aP(m) \subseteq P(m)$, we must actually have $aP(m) = P(m)$. □

We are now in a position to prove Euler's Theorem:

Theorem 39.2 (Euler's Theorem)**.** *Let a and m be integers such that $m \geq 1$. If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Proof. Let $P(m) = \{r_1, r_2, \ldots, r_{\phi(m)}\}$. By Theorem 39.1, $aP(m) = P(m)$. This means that if we multiply all the elements of $aP(m)$ together, what we get must be the same (modulo m) as what we get if we multiply all the elements of $P(m)$ together. In symbols, we have

$$(ar_1)(ar_2)\cdots(ar_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Rewriting the expression on the left, we get

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Since $\gcd(r_i, m) = 1$ for each i, repeatedly applying Courtney and Evan's Cancellation Theorem, we can cancel r_1, r_2, …, $r_{\phi(m)}$ from both sides, and we get

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

as desired. □

In the special case where the modulus is prime, Euler's Theorem is called *Fermat's Little Theorem* (not to be confused with *Fermat's Last Theorem*). More precisely we have:

Corollary 39.3 (Fermat's Little Theorem)**.** *If p is prime and p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. We know that $\phi(p) = p - 1$. We also know that p does not divide a if and only if $\gcd(a, p) = 1$. Now applying Euler's Theorem directly completes the proof. □

Homework: Prove the general form of *Fermat's Little Theorem*: If p is prime, then for every integer a we have $a^p \equiv a \pmod{p}$. *Hint:* It might be helpful to consider two cases: (1) $\gcd(a, p) = 1$ and (2) $\gcd(a, p) \neq 1$.

40. Fermat's Little Theorem

Courtney and Kai shared the following quote to start the week:

Quote: [A. Einstein] "Not everything that counts can be counted. Not everything that can be counted counts."

We first discussed the homework problem from Thursday's class. The goal was to prove the general version of Fermat's Little Theorem. Matt put the first part on the board. However, we needed some time to work through the second part. After some hints and time working in groups, Blake put the proof of the second case on the board.

Theorem 40.1 (Fermat's Little Theorem)**.** *If p is prime, then $a^p \equiv a \pmod{p}$ for every integer a.*

Proof. If $\gcd(a, p) = 1$, then, by Euler's Theorem, we have $a^{\phi(p)} \equiv 1 \pmod{p}$. Since p is prime, $\phi(p) = p - 1$ and we have $a^{p-1} \equiv 1 \pmod{p}$. We also know that $a \equiv a \pmod{p}$. Multiplying the two congruence equations gives $a^p \equiv a \pmod{p}$.

Now assume $\gcd(a, p) \neq 1$. Then, since p is prime, we have that $\gcd(a, p) = p$. Thus p divides a and p divides a^p. This says that $a \equiv 0 \pmod{p}$ and $a^p \equiv 0 \pmod{p}$. We conclude that $a^p \equiv a \pmod{p}$. □

41. Cryptography

We then moved to an introductory discussion of cryptography. The science of *cryptography* deals with sending and receiving coded messages. Not only governments, but also financial institutions and businesses need frequently to transfer sensitive information from one user or from one computer to another in such a way that even if a message is intercepted by the wrong party, it cannot be read. The general public also needs secure methods of transmitting information, so that, for example, a credit card purchase made over the Internet does not allow one's name and credit card number to fall into the hands of an unscrupulous thief. (Unfortunately, there are such bad people in our world.)

We use the term *cipher* to mean a system for encoding and decoding messages. We use the terms *encipher* or *encode* or *encrypt* to denote the process of transforming a plain text message into a coded message and the terms *decipher* or *decode* or *decrypt* to denote the process of transforming the coded message back into the original plain text message. All modern ciphers are based on mathematics and many are based on techniques and results from number theory. We shall focus for the next several classes on some of these.

The United States government (for obvious reasons) has a very strong interest in cryptography, both for devising break-proof codes and for cracking the codes of others. In fact, the National Security Agency is the largest employer of Ph.D. mathematicians in the world.

Historically, people have not only used ciphers to keep their messages secret, but they also have devised ways to keep people from knowing that a message was even being sent. For example, there is an old story about a king who wanted to send a message to his brother. He shaved the head of a servant, tattooed the message on the servant's scalp, waited for the servant's hair to grow back, and gave the servant instructions to find the brother and request a haircut.

One of the oldest methods of secret communication can be traced back about 2500 years to ancient Sparta, where the Spartan government needed to communicate with its generals in private. As with the haircut story above, the idea was to disguise the fact that a message

was even being sent. Every general had a cylinder (perhaps a cane or a spear) of exactly the same radius. A narrow ribbon was wrapped around the cylinder and then the message was written across the ribbon. When the ribbon was unwound, the letters of the message were transposed. To the untrained eye (especially since so few people could read then!) this ribbon did not contain a message but instead was just decorated with attractive symbols which happened to be letters. The ribbon could then be worn as a belt by a messenger while in transit. This method, often referred to as the **Spartan scytale**, is an example of a **transposition cipher**. The letters of the original message remain the same, but their order is changed.

An example of a very old and very simple cipher, based on number theory and purportedly used by Julius Caesar, is the so-called **Caesar Cipher**. The idea of the Caesar cipher was to use a simple shift of letters. Replace every letter in the plain text message by the letter three letters to the right to get the coded message. To decode the coded message, one needs only replace each letter in the coded message by the letter three places to the left. The correspondence is shown in the table below.

Plain Text:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher Text:	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

For simplicity in our examples, we shall just run the words together with no encoding of spaces or punctuation. For example, we worked in groups to encode the phrase "I LOVE MATH". Using the Caesar cipher, Michelle showed that "ILOVEMATH" would be encoded to read as the message "loryhpdwk". Similarly, Kim showed that the encoded message "uhwxuqkrph" would be decoded into the plain text message "RETURN HOME". The Caesar cipher is obviously not a very sophisticated system and would be relatively easy to crack.

Note that the Caesar cipher amounts to adding 3 and working modulo 26. For example, the letter "U" is the number 21 because it is the 21st letter of the alphabet. Enciphering it, we add 3 and get 24, which corresponds to "x", because "x" is the 24th letter of the alphabet. If we start with the letter "Y", we think of that as 25. Adding 3, we get 28, and modulo 26, this is 2. The second letter of the alphabet is "b", so "Y" is enciphered as "b".

At this point, we really need some mathematical context for our discussion. When discussing cryptography, one usually makes some standard assumptions. One assumption that we'll make is that letters are always translated to numbers via the following scheme:

Letters:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Numbers:	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

Letters:	Q	R	S	T	U	V	W	X	Y	Z
Numbers:	16	17	18	19	20	21	22	23	24	25

Notice that this is just a *translation*, not an encryption.

Also, to make discussing what's going on easier, you assume there are two individuals — Alice and Bob — who are wanting to communicate privately, without their opponent — Oscar — knowing what they are saying to each other. We assume that Oscar has full access to the encrypted messages, however. Of course, we also assume that Oscar knows how to translate letters into numbers and conversely. We also assume Oscar knows the *scheme* for encryption but not the *key*. This last sentence will make more sense later.

To make the mathematics of cryptography precise, let's introduce some notation and terminology. The *encryption* function is denoted by ϵ, and the *decryption* function is denoted by δ. For example, the encryption function for the Caesar cipher is given by

$$\epsilon_{\text{Caesar}}(\alpha) = (\alpha + 3)\,\%26$$

and the decryption function for the Caesar cipher is given by

$$\delta_{\text{Caesar}}(\beta) = (\beta - 3)\,\%26.$$

(Recall that $a\,\%26$ is the smallest non-negative integer which is congruent to a modulo 26.) Notice that δ_{Caesar} is the *inverse function* for ϵ_{Caesar}. In other words, for any message α, we have

$$\delta_{\text{Caesar}}(\epsilon_{\text{Caesar}}(\alpha)) = \delta_{\text{Caesar}}((\alpha + 3)\,\%26) = ((\alpha + 3) - 3)\,\%26 = \alpha.$$

This is true in general — decrypting an encrypted message should always return the original message.

The Caesar cipher is an example of a **shift cipher**. In general, a shift cipher is described mathematically by $\epsilon(\alpha) = (\alpha + \beta)\,\%26$ for some chosen integer β. The decryption function is then given by $\delta(\alpha) = (\alpha - \beta)\,\%26$. You can check for yourself that $\delta(\epsilon(\alpha)) = \alpha$ for any message α. Note that in the example of a Caesar cipher, the *scheme* is that it's a shift cipher and the *key* is the value of the integer β.

Shift ciphers are far from secure for several reasons. First, there are only 26 possible shift ciphers, so if we assume that Oscar knows that Alice and Bob are using a shift cipher, it is very easy for him to figure out which one it is. Additionally, shift ciphers are a special case of **substitution ciphers**, where the cipher text alphabet is just some (possibly random) permutation of the plain text alphabet. This is bad because one can use common knowledge about the English language (for example, the fact that "e" is by far the most common letter) to make guesses about what the various letters stand for. The "CRYPTOQUOTES" puzzles you find in the newspaper are examples of substitution ciphers. If Oscar makes just one educated guess about a shift cipher, he has found the value of the "shift" β in the encoding function $\epsilon(\alpha) = (\alpha + \beta)\,\%26$, and so he knows the formula for δ, and hence the values of *all* the letters.

We can build on shift ciphers and consider **affine ciphers**. The idea here is that the encoding function ϵ has two parameters: γ and β, so that $\epsilon(\alpha) = (\gamma\alpha + \beta)\,\%26$. What is the decoding function δ in this case? We decided to look at example. We took the affine cipher described by $\epsilon(\alpha) = (5\alpha + 11)\,\%26$, and encrypted the word "EXAMPLE". To do this, we first translated it to numbers to get 4, 23, 0, 12, 15, 11, 14. Now encrypting each of these numbers gives the sequence 5, 22, 11, 19, 8, 14, 5, which translates to "FWLTIOF". The question now is: how do we decipher?

Homework: Each table group is to choose a word and encode it using the affine cipher $\epsilon(\alpha) = (5\alpha + 11)\,\%26$.

42. Affine Ciphers

Kai brought us the following quote:

Quote: [P. Pastoret] "If you don't think dogs can count, try putting 3 dog biscuits in your pocket and then giving Fido only 2 of them."

We began class by recalling our last example with affine ciphers from Tuesday's class. We had the affine cipher described by the encryption function $\epsilon(\alpha) = (5\alpha + 11)\,\%26$ and encrypted the word "EXAMPLE" as "FWLTIOF". We closed with the question: how do we decipher this cipher? To do this we need to discuss inverses in the "modular world". In general, if we weren't working modulo 26, we would just take our encrypted message α, subtract 11, and divide by 5. It's this division by 5 which poses the problem.

Definition 42.1. Let a and m be integers with $m > 1$. We say that an integer b is an *inverse* for a modulo m if $ba \equiv 1 \pmod{m}$.

Example: $(2)(6) \equiv 1 \pmod{11}$ and so 2 is an inverse for 6 modulo 11.

Example: There is no integer k such that $6k \equiv 1 \pmod{4}$ and so 6 has no inverse modulo 4.

This brought up the obvious question:

Question: When does an integer a have an inverse modulo m?

We made the conjecture on Take-Home Test 4 that given integers a and $m > 1$, there is an integer x such that $ax \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$. This is indeed true!

Theorem 42.2. *Let a and m be integers with $m \geq 2$. Then a has an inverse modulo m if and only if* $\gcd(a, m) = 1$.

Proof. Assume that $\gcd(a, m) = 1$. Then there exist integers x and y such that $ax + my = 1$. So $my = 1 - ax$. That is, m divides $1 - ax$. We can express this by writing $ax \equiv 1 \pmod{m}$. Thus, x is an inverse of a modulo m.

Now suppose that b is an inverse of a modulo m. Also, let $d = \gcd(a, m)$. We want to show that $d = 1$. By the definition of an inverse, $ba \equiv 1 \pmod{m}$. Thus, m divides $ba - 1$. So there exists an integer y such that $my = ba - 1$. Rearranging this equation, we see that $1 = ba - my$. Now, $d|a$ and $d|m$, and so $d|ba$ and $d|my$. Thus, $d|(ba - my)$. That is, $d|1$. Since $d > 0$, this means that $d = 1$ which completes the proof. □

Example: Let's find the inverse of 13 modulo 1000. First note that $\gcd(13, 1000) = 1$, and so we know that an inverse exists. We use the Extended Euclidean Algorithm to find this inverse. We have

$$\begin{aligned} 1000 &= 13(76) + 12 \\ 13 &= 12(1) + 1 \end{aligned}$$

Applying back-substitution yields

$$\begin{aligned} 1 &= 13 - (1)(12) \\ &= 13 - (1)(1000 - 13(76)) \\ &= 13 - 1000 + 13(76) \\ &= 13(77) - 1000. \end{aligned}$$

This says that $1000 = 13(77) - 1$ which means that $(77)(13) \equiv 1 \pmod{1000}$. We conclude that 77 is an inverse of 13 modulo 1000.

Example: Solve the following equation for x:

$$13x + 88 \equiv 762 \pmod{1000}$$

First, we subtract 762 from both sides of the equation to obtain:

$$13x \equiv 674 \pmod{1000}.$$

In the previous example, we saw that 77 is an inverse of 13 modulo 1000. We now multiply both sides of the equation by 77:

$$\begin{aligned} 13x &\equiv 674 \pmod{1000} \\ (77)(13)x &\equiv (77)(674) \pmod{1000} \\ (1)(x) &\equiv 51898 \pmod{1000} \\ x &\equiv 51898 \pmod{1000}. \end{aligned}$$

Hence, $x \equiv 51898 \pmod{1000}$ is the solution.

We can now return to our discussion of affine ciphers.

Example: Consider the affine cipher with encoding function $\epsilon(x) = (5x + 11)\,\%26$. We want to find the decoding function δ. We start with

$$y = \epsilon(x) = (5x + 100)\,\%26.$$

The next step is to interchange the roles of x and y:

$$x = (5y + 11)\,\%26$$

or

$$5y + 11 \equiv x \pmod{26}.$$

We want to solve for y in terms of x. First, we subtract 11 from both sides of the equation to obtain:

$$5y \equiv (x - 11) \pmod{26}.$$

To find y, we need to find an inverse of 5 modulo 26. Note that $\gcd(5, 26) = 1$ and so we know an inverse exists. We have,

$$26 = 5(5) + 1 \implies 1 = 26 + 5(-5).$$

This says that

$$5(-5) \equiv 1 \pmod{26}.$$

But $-5 \equiv 21 \pmod{26}$ and so

$$5(21) \equiv 1 \pmod{26}.$$

That is, 21 is an inverse of 5 modulo 26.

We now return to the equation we are trying to solve: $5y \equiv (x-11) \pmod{26}$. Multiplying both sides by 21 gives

$$(21)(5)y \equiv (21)(x - 11) \pmod{26}$$

or

$$y \equiv 21(x - 11) \pmod{26}.$$

Distributing the 21 gives

$$y \equiv (21x - 231) \pmod{26} \equiv (21x - 23) \pmod{26} \equiv (21x + 3) \pmod{26}.$$

Therefore, our decoding function is

$$\delta(x) = (21x + 3)\,\%26.$$

To make sure our work was correct, we decoded the encoding of "EXAMPLE". We saw before that "EXAMPLE" is encoded to "FWLTIOF". To decode "FWLTIOF" we first translated each letter to its corresponding number which yielded the sequence 5, 22, 11, 19, 8, 14, 5. Next, we applied $\delta(x) = (21x + 3)\,\%26$ to each of these numbers. For example, $\delta(5) = (21 \cdot 5 + 3)\,\%26 = 4$. This gave the sequence 4, 23, 0, 12, 15, 11, 4. Finally, we translated this last sequence of numbers into letters and obtained "EXAMPLE".

We then exchanged encoded messages between table groups and practiced decoding them.

43. Block Affine Ciphers

Of course, what we've been doing so far with affine ciphers really just boils down to a mathematical description of some substitution ciphers. Further, they're really not much better than shift ciphers. Just like knowing one value with a shift cipher tells you everything you could want to know about the cipher, knowing two values with an affine cipher tells you everything you could want to know about it. (This is because there are now two parameters in the encrypting function ϵ.) The common knowledge about the most frequently used letters in the English language still applies.

However, one might consider encoding more than one letter at a time. For example, suppose we wish to encode 4 letters as one "block". We can still translate each letter into a two-digit number as above, but then we consider the four letters together as an eight-digit number m. Such a number is certainly less than 10^8, so we can use 10^8 as our modulus and proceed as before with our affine cipher. (Note that we might not, however, always be able to represent the cipher text as letters.) Choose parameters a and b with $\gcd(a, 10^8) = 1$, and set $\epsilon(m) = (am + b)\,\%10^8$. The frequencies for blocks of four letters are not nearly so well known as they are for individual letters, and so this type of affine cipher is much more secure.

Example: Consider the block affine cipher given by $\epsilon(x) = (2547x + 2723)\%100,000,000$. Here, we are taking each block to consist of four letters. Our first goal was to encode the clear text "ARE WE HAVING FUN YET". To do this, we first broke the clear text into blocks of four letters, adding three "A"s onto the end to make it come out evenly. Next, we translated the letters into numbers using our standard translation system which makes "A" into "00", "B" into "01", and so on. Finally, we used the function $\epsilon(x) = (2547x + 2723)\,\%10^8$ to encrypt the blocks of numbers. We obtained:

block	AREW	EHAV	INGF	UNYE	TAAA
translate	00170422	04070021	08130605	20132404	19000000
encrypt	34067557	66346210	8653658	77235711	93002723

Our next task was to find the decoding function δ by mimicking our previous work with affine ciphers. We ran out of time for this second part and so left it as homework.

Homework:

(1) Complete the last example by finding the decryption function δ.

(2) Decode the message "PDQZPSFA" using the affine cipher with decoding function $\delta(x) = (21x + 3)\,\%26$.
(3) Consider the block affine cipher given by $\epsilon(x) = (12939x + 3456)\%1,000,000$. Here, we are taking each block to consist of three letters.
   - Encode the clear text "MICHIGAN WILL BEAT OSU". (Use any "dummy" letter you like to get the clear text to break up evenly into blocks of three letters.)
   - Find the deciphering function δ for this ϵ.

44. One More Example of an Affine Cipher

Our week started with a quote shared by Patrick.

Quote: [Unknown] "The human mind has never invented a labor saving machine equal to algebra."

The majority of our class was spent on homework from the previous class. There was confusion and so we first worked in groups before sharing solutions at the board. The first exercise we tackled involved an affine cipher.

Example: We want to decode the message "PDQZPSFA" using the affine cipher with decoding function $\delta(x) = (21x + 3)\,\%26$. Dan and Bryce showed us how to do this. The first task was to translate each of the encoded letters to numbers. Using the scheme where "A" translates to "00", "B translates to "01", etc., we obtain the sequence of numbers 15, 03, 16, 25, 15, 18, 05, 00. Now we apply the decoding function δ to each of these numbers. We obtain:

$$\begin{aligned}
\delta(15) &= ((21)(15) + 3)\,\%26 = 318\,\%26 = 6\\
\delta(3) &= ((21)(3) + 3)\,\%26 = 66\,\%26 = 14\\
\delta(16) &= ((21)(16) + 3)\,\%26 = 339\,\%26 = 1\\
\delta(25) &= ((21)(25) + 3)\,\%26 = 528\,\%26 = 8\\
\delta(15) &= ((21)(15) + 3)\,\%26 = 318\,\%26 = 6\\
\delta(18) &= ((21)(18) + 3)\,\%26 = 381\,\%26 = 17\\
\delta(5) &= ((21)(5) + 3)\,\%26 = 108\,\%26 = 4\\
\delta(0) &= ((21)(0) + 3)\,\%26 = 3\,\%26 = 3
\end{aligned}$$

We next translate the sequence of numbers 06, 14, 01, 08, 06, 17, 04, 03 into letters. This gives "GO BIG RED".

45. Block Affine Codes, Revisited

Our next task was to complete the last example from our previous class.

Example: Consider the block affine cipher given by $\epsilon(x) = (2547x + 2723)\%100,000,000$. Here, we are taking each block to consist of four letters. Last class we encoded the clear text "ARE WE HAVING FUN YET". We obtained:

block	AREW	EHAV	INGF	UNYE	TAAA
translate	00170422	04070021	08130605	20132404	19000000
encrypt	34067557	66346210	8653658	77235711	93002723

Today we wanted to compute the decryption function $\delta(s)$. To find the inverse of 2547 modulo 10^8 we need to apply the Extended Euclidean Algorithm. Matt shared the details at the board:

$$\begin{aligned} 100000000 = 2547(39261) + 2233 &\implies 2233 = 100000000 - 2547(39261) \\ 2547 = 2233(1) + 314 &\implies 314 = 2547 - 2233(1) \\ 2233 = 314(7) + 35 &\implies 35 = 2233 - 314(7) \\ 314 = 35(8) + 34 &\implies 34 = 314 - 35(8) \\ 35 = 34(1) + 1 &\implies 1 = 35 - 34(1). \end{aligned}$$

Now back-substitution gives:

$$\begin{aligned} 1 &= 35 - 34(1) \\ &= 35 - (314 - 35(8))(1) = 35(9) - 314(1) \\ &= (2233 - 314(7))(9) - 314(1) = 2233(9) - 314(64) \\ &= 2233(9) - (2547 - 2233(1))(64) = 2233(73) - 2547(64) \\ &= (100000000 - 2547(39261))(73) - 2547(64) = 100000000(73) - 2547(2866117) \end{aligned}$$

We end up with the equation $1 = 100000000(73) + 2547(-2866117)$. Trevor pointed out that this says

$$(2547)(-2866117) \equiv 1 \pmod{100000000}.$$

Dan noted that

$$-2866177 \equiv 97133883 \pmod{100000000}$$

and so we also have

$$(2547)(97133883) \equiv 1 \pmod{100000000}.$$

So, to solve for δ, we write the equation

$$2547x + 2723 \equiv y \pmod{100000000}.$$

We next reverse the roles of x and y:

$$2547y + 2723 \equiv x \pmod{100000000}$$

and solve for y. Our first step is to subtract 2723 from both sides of the equation:

$$2547y \equiv (x - 2723) \pmod{100000000}.$$

Now we multiply both sides of the equation by 97133883 to obtain

$$(97133883)(2547)y \equiv (97133883)(x - 2723) \pmod{100000000}$$

which simplifies to

$$y \equiv (97133883)(x - 2723) \pmod{100000000}$$

or

$$y \equiv (97133883x - 264495563409) \pmod{100000000}.$$

But, since $264495563409 \equiv 95563409 \pmod{100000000}$, we could also write

$$y \equiv (97133883x - 95563409) \pmod{100000000}.$$

Therefore, we can take

$$\delta(s) = (97133883s - 95563409)\%100000000.$$

We then worked on the third homework exercise from last class.

Example: We first wish to encode "MICHIGAN WILL BEAT OSU" using the block affine cipher given by $\epsilon(m) = (12939m + 3456)\%1,000,000$ with blocks of 3.

We break the clear text into blocks, each of which must be smaller than our modulus. Since our modulus has 7 digits, we can use 6-digit blocks. So we use blocks of three letters, adding two "A"s onto the end to make it come out evenly. Next, we translate the letters into numbers using our standard translation system which makes "A" into "00", "B" into "01", and so on. Finally, we use the function $\epsilon(m) = (12939m + 3456)\,\%10^6$ to encrypt the blocks of numbers. Garrett put the resulting encryption on the board:

block	MIC	HIG	ANW	ILL	BEA	TOS	UAA
translate	120802	070806	001322	081111	010400	191418	200000
encrypt	060534	162290	108814	498685	569056	760958	803456

Next, we were to compute the decryption function $\delta(s)$ using the Extended Euclidean Algorithm. Kim provided the following details:

$$\begin{aligned} 1000000 = 12939(77) + 3697 &\implies 3697 = 1000000 - 12939(77) \\ 12939 = 3697(3) + 1848 &\implies 1848 = 12939 - 3697(3) \\ 3697 = 1848(2) + 1 &\implies 1 = 3697 - 1842(2). \end{aligned}$$

Now we back-substitute:

$$\begin{aligned} 1 &= 3697 - 1842(2) \\ &= 3697 - (12939 - 3697(3))(2) = 3697(7) - 12939(2) \\ &= (1000000 - 12939(77))(7) - 12939(2) = 1000000(7) + 12939(-541). \end{aligned}$$

So we see that

$$12939(-541) \equiv 1 \pmod{1000000}.$$

Michelle then worked out the decoding function for us. We have

$$-541 \equiv 999459 \pmod{1000000}$$

and so we also have

$$(12939)(999459) \equiv 1 \pmod{1000000}.$$

So, to solve for δ, we write the equation

$$12939x + 3456 \equiv y \pmod{1000000}.$$

We next reverse the roles of x and y:

$$12939y + 3456 \equiv x \pmod{1000000}$$

and solve for y. Our first step is to subtract 3456 from both sides of the equation:

$$12939y \equiv (x - 3456) \pmod{1000000}.$$

Now we multiply both sides of the equation by 999459 to obtain

$$(999459)(12939)y \equiv (999459)(x - 3456) \pmod{1000000}$$

which simplifies to

$$y \equiv (999459)(x - 3456) \pmod{1000000}$$

or

$$y \equiv (999459x - 3454130304) \pmod{1000000}.$$

But, since $3454130304 \equiv 130304 \pmod{1000000}$, we could also write

$$y \equiv (999459x - 130304) \pmod{1000000}.$$

Therefore, we can take

$$\delta(s) = (999459s - 130304)\%1000000.$$

Homework: Read the handout on public key cryptography and RSA. The details of the handout will be included later in the notes.

46. Public Key Cryptography and RSA

Michelle contributed to our daily quotes with:

Quote: [Unknown] "Mathematics is the science which uses easy words for hard ideas."

Affine ciphers using "blocks" of four letters (8 digits) are reasonably secure. There are still problems with affine ciphers, however. The main problem is that before Alice and Bob can communicate using this affine cipher, they must decide on the values of the two parameters a and b in the encryption function. (These values are called the "key" for the cipher.) They can't just send these values to each other unencrypted, because then Oscar could read them and he would know the formula for ϵ. Moreover, Oscar could just use the Extended Euclidean Algorithm to figure out the formula for the decryption function δ! So how do Alice and Bob decide on their key?

One solution is to use *public key cryptography*. The basic idea of a public key system is that even if Oscar knows ϵ, he can't figure out δ. Each user sets up two sets of keys: one *public* and one *private*. The public keys are "very" public — they are published in some location so that everyone who wants to can find them. If Bob wants to send Alice a message, he goes to this public location and looks up Alice's public keys. He then knows Alice's encryption function $\epsilon_A(m)$, and he uses it to send Alice a message. Note that anyone in the world can find Alice's public keys, so anyone in the world can send Alice a message. On the other hand, the private keys need to be kept "very" private. Alice's private keys are used in her decryption function $\delta_A(s)$, and since only she knows them, only she can decrypt a message sent to her using her public encryption function $\epsilon_A(m)$.

Again, the key fact here is that even though everyone, including Oscar, knows Alice's public keys, this is not enough information for them to compute Alice's private keys. This is why it's so important that Alice keeps her private keys private. If anyone (besides Alice) has access to them, then that person can read any secret messages sent to Alice.

For *RSA cryptography*, the public keys are integers n and e, and the encryption function is

$$\epsilon(m) = m^e \% n.$$

The private key is an integer d, and the decryption function is

$$\delta(s) = s^d \% n.$$

To see that the RSA system works we will need to show two things:

(1) Decryption recovers the original message. In other words, $\delta(\epsilon(m)) = m$. In this case, this means that n, d, and e must be chosen in such a way that

$$m^{de} \equiv m \pmod{n}.$$

(2) The system is secure. In other words, even though Oscar will know n and e (because *everyone* knows n and e), it must be "impossible" for Oscar to find d.

First, let's discuss how a user, Alice, would go about setting up her keys, giving an example at each step.

Pick primes: The first step for Alice is to pick two prime numbers p and q. In practice, these primes need to be *very large* — about 150 digits each.

- We'll take $p = 11$ and $q = 13$.

Calculate n and $\phi(n)$: Next Alice simply sets $n = pq$. Since Alice knows the factorization of n, she can compute $\phi(n) = (p-1)(q-1)$. Notice that in practice n will have about 300 digits. This means that computing $\phi(n)$ would be very difficult without knowing the factorization of n, and factoring n would also be very difficult.

- In our example, we have $n = (11)(13) = 143$ and $\phi(n) = (10)(12) = 120$.

Choose e — the encoding exponent: The next step is to pick a value of e at random, making sure that $\gcd(e, \phi(n)) = 1$. Alice does this by first selecting a value for e and then performing the Euclidean Algorithm to calculate $\gcd(e, \phi(n))$. If this gcd is 1, great. Otherwise, Alice simply chooses a new value of e.

- We'll take $e = 23$. It is "obvious" that $\gcd(23, 120) = 1$, but let's do the Euclidean Algorithm anyway:

$$\begin{aligned} 120 &= 23(5) + 5 \\ 23 &= 5(4) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \end{aligned}$$

Find d — the decoding exponent: Now, Alice needs to find a value of d so that $de \equiv 1 \pmod{\phi(n)}$. She can do this through the Extended Euclidean Algorithm.

- We have

$$\begin{aligned} 1 &= 3 - 2(1) \\ &= 3 - (5 - 3(1))(1) = 3(2) - 5(1) \\ &= (23 - 5(4))(2) - 5(1) = 23(2) - 5(9) \\ &= 23(2) - (120 - 23(5))(9) = 23(47) - 120(9), \end{aligned}$$

and so $d = 47$.

When all is said and done, Alice's public keys are n and e, and her private key is d. The encoding function, which anyone in the world can use to send a message to Alice, is $\epsilon(m) = m^e \,\%n$. The decoding function, which only Alice knows, is $\delta(s) = s^d \,\%n$. Alice should also destroy her records of p, q, and $\phi(n)$. These bits of information are no longer needed by her, and if anyone else finds them, they will be able to figure out her (private) decoding exponent d by using the Extended Euclidean Algorithm on e and $\phi(n)$.

We still need to verify two things about RSA:

(1) Decryption recovers the original message. In other words, $\delta(\epsilon(m)) = m$. In this case, this means that n, d, and e must be chosen in such a way that $m^{de} \equiv m \pmod{n}$.
(2) The system is secure. In other words, even though Oscar will know n and e (because *everyone* knows n and e), it must be "impossible" for Oscar to find d.

We already saw why (2) is true: In order for the RSA system to be secure, it needs to be true that even if Oscar knows the encryption function $\epsilon(m)$ and has access to some encrypted message s, he cannot find the decrypted, original message m. The only way that anyone (not just in this class) knows for Oscar to be able to find m is if he can figure out d, the decoding exponent. Remember that d needs to satisfy $de \equiv 1 \pmod{\phi(n)}$, so to figure out d, Oscar would need to know the value of $\phi(n)$. There are two ways Oscar can find $\phi(n)$. First, he could factor n into the primes p and q and then use the formula $\phi(n) = (p-1)(q-1)$. However, factoring n is computationally infeasible for a 300-digit n (unless n has special

properties, which Alice was certain to avoid!). Alternatively, he can make a list of the integers from 1 to n and test each one to see if it's relatively prime to n. But this is actually equivalent to factoring n by brute-force, and so it too is infeasible.

We are left needing to prove (1).

Theorem 46.1. *Let p and q be distinct primes and set $n = pq$. Suppose d and e are integers chosen so that $de \equiv 1 \pmod{\phi(n)}$. Then $m^{de} \equiv m \pmod{n}$ for any integer m. Hence, if $\epsilon(m) = m^e \,\%n$ and $\delta(s) = s^d \,\%n$, then $\delta(\epsilon(m)) = m$, i.e., RSA cryptography works.*

Proof. Let p and q be distinct primes and set $n = pq$. We begin with two observations:

Note 1: If $\gcd(m, n) \neq 1$, then $\gcd(m, n) = p$, q, or n. To see this, let $d = \gcd(m, n)$. Then, by the Fundamental Theorem of Arithmetic, d can be factored into a product of primes. Let r be any prime divisor of d. Then $r|d$ and $d|n$ implies that $r|n$. Thus, $r|pq$. Since r is a prime number, this implies that $r|p$ or $r|q$. So, since r, p and q are prime numbers, we conclude that either $r = p$ or $r = q$. This says that the prime factorization of d is $d = p$ or $d = q$ or $d = pq = n$.

Note 2: If x is any integer such that $p|x$ and $q|x$, then $pq|x$. To see this, note that there exist integers l and t such that $x = pl$ and $x = qt$. Thus, $pl = qt$ showing that p divides qt. Since p is prime, we can conclude that $p|q$ or $p|t$. But p and q are distinct primes, and so p does not divide q which implies that $p|t$. Thus, there exists an integer w such that $t = pw$. Substitution then gives $x = qt = qpw$. That is, pq divides x as desired.

We can now prove the theorem. We have $\phi(n) = (p-1)(q-1)$. Suppose d and e satisfy $de \equiv 1 \pmod{\phi(n)}$. Thus, $\phi(n)$ divides $de - 1$. So, there exists an integer k such that $\phi(n)k = de - 1$, or $de = \phi(n)k + 1$. Let m be any integer. We consider two cases.

Case 1: Suppose $\gcd(m, n) = 1$. Then, by Euler's Theorem,

$$\begin{aligned} m^{de} = m^{\phi(n)k+1} = (m^{\phi(n)})^k m &\equiv 1^k m \pmod{n} \\ &\equiv m \pmod{n}, \end{aligned}$$

as desired.

Case 2: Suppose $\gcd(m, n) \neq 1$. Then, by Note 1, we know that $\gcd(m, n) = p$, q, or n. We consider three sub-cases.

Case 2a: Assume $\gcd(m, n) = n$. Then $n|m$ and $n|m^{de}$. In congruence language, this says that $m \equiv 0 \pmod{n}$ and $m^{de} \equiv 0 \pmod{n}$, and so $m^{de} \equiv m \pmod{n}$ as desired.

Case 2b: Assume that $\gcd(m, n) = p$. This means that p divides m, but $\gcd(q, m) = 1$. By Euler's Theorem, we have

$$\begin{aligned} m^{de} = m^{\phi(n)k+1} = m^{(p-1)(q-1)k+1} = (m^{q-1})^{(p-1)k} m &\equiv 1^{(p-1)k} m \pmod{q} \\ &\equiv m \pmod{q}, \end{aligned}$$

which shows that q divides $m^{de} - m$. But since p divides m, we know that p divides m^{de}, and so p also divides $m^{de} - m$. We now apply Note 2 which says that $m^{de} - m$ is a multiple of $n = pq$. Thus, $m^{de} \equiv m \pmod{n}$, as desired.

Case 2c: Assume $\gcd(m, n) = q$. Then the result holds by an argument similar to that made for Case 2b. □

47. History

Here's a little history of the Public Key Cryptography system which we've been discussing. The system is called RSA Public Key Cryptography after the three MIT mathematicians who invented it – Rivest, Shamir, and Adelman. It was introduced in 1977, and at that time, the authors published a secret message which was encoded using a modulus n which had 129 digits. This n was called $RSA129$ and was finally factored (thus allowing the secret message to be read) in 1994 by an international group of people who had their computers work on the problem when the computer wasn't doing anything else. Most recently, the 193-digit number $RSA640$ was factored in November 2005 using a similar approach. The "RSA Factoring Challenge" is interesting to learn about; see `http://www.rsasecurity.com/rsalabs/node.asp?id=2092` for more information.

48. An Example of Using RSA

We next worked through an example using RSA cryptography.

Example: Suppose Alice has public keys $n = 1537$ and $e = 47$. Our first task was to find the corresponding private key d. We quickly factored n as $n = (29)(53)$ and found $\phi(n) = (28)(52) = 1456$. We noted that $\gcd(e, \phi(n)) = \gcd(47, 1456) = 1$. We then used the Extended Euclidean Algorithm to find an integer d such that $de \equiv 1 \pmod{\phi(n)}$. The calculations were:

$$\begin{aligned} 1456 &= 47(30) + 46 \\ 47 &= 46(1) + 1 \end{aligned}$$

and

$$\begin{aligned} 1 &= 47 - 46 \\ &= 47 - (1456 - 47(30)) \\ &= 47(31) + 1456(-1) \end{aligned}$$

showing that $d = 31$ satisfies $de \equiv 1 \pmod{1456}$. Thus, our encryption function ϵ and decryption function δ are:

$$\begin{aligned} \epsilon(m) &= m^{47} \,\%1537 \\ \delta(s) &= s^{31} \,\%1537. \end{aligned}$$

Our second task was to decode an actual encrypted message! Suppose Alice receives the message "0708 1341" from Bob. In order to read the message, she performs the following steps:

Decode the blocks: First, Alice must apply her decoding function $\delta(s) = s^{31} \,\%1537$ to each block separately, using fast exponentiation to actually do the computations. We worked this out in groups. Trevor and TJ put their answers on the board. They were:

$$\delta(0708) = 708^{31} \,\%1537 = 220$$
$$\delta(1341) = 1341^{31} \,\%1537 = 24$$

Translate to numbers: Next, Alice translates the output of the decoding function into letters, using the usual system where "00" becomes "A", "01" becomes "B", and so on. Since 220 has only 3 digits and we are looking for a letters corresponding

to 2 digits we decided that there must have been a "dummy variable" placed at the end of the block when being encoded. Thus we really just concentrate on "22" which corresponds to "W". Also, the number "24" really represents the 4-digit block "0024" giving the two letters "AY". Thus, the message Bob was sending Alice was "WAY".

Our next task involved encoding a function using RSA. Suppose Bob wants to send Alice the message "SOPHIE". Bob needs to follow these steps:

Look up Keys: His first step is to look up Alice's public keys, n and e. He then knows that $\epsilon(m) = m^e \,\%n$ is the encoding function he should use.

- Bob finds $n = 1537$, $e = 47$ and so he knows that the encoding function he should use is $\epsilon(m) = m^{47} \,\%1537$.

Translate: Next, Bob needs to translate his message into numbers, using the usual system where "A" becomes "00", "B" becomes "01", and so on.

- He translates "SOPHIE" as "181415070804".

Break into blocks: Since the encoding function works modulo n, Bob needs to break up his message into *blocks*, each of which is less than n. The easiest way to do this is to break it into blocks which have one fewer digit than n does, since any such number is clearly less than n.

- Since $n = 1537$, Bob breaks the message into 3-digit blocks. He gets 181, 415, 070, 804.

Encode: Now, Bob simply encrypts each block separately (using fast exponentiation to do the computations). We didn't finish this work and left it for homework.

Comments. Even though the numbers used with the RSA system in practice are huge, it is important to realize that the fast exponentiation algorithm is so efficient that computers can "easily" do the necessary computations.

Homework: Complete the encoding of "SOPHIE" from the last example.

49. The Conclusion of a RSA Example

Class started with a quote by S. Gudder.

Quote: [S. Gudder] "The essence of mathematics is not to make simple things complicated, but to make complicated things simple."

Our first task of the day was to complete the RSA example from last class. All details are included here for completion.

Example: Bob needs to complete the following steps to encode the message "SOPHIE" using Alice's public keys $n = 1537$ and $e = 47$.

Look up Keys: His first step is to look up Alice's public keys, n and e. He then knows that $\epsilon(m) = m^e \,\%n$ is the encoding function he should use.

- Bob finds $n = 1537$, $e = 47$ and so he knows that the encoding function he should use is $\epsilon(m) = m^{47} \,\%1537$.

Translate: Next, Bob needs to translate his message into numbers, using the usual system where "A" becomes "00", "B" becomes "01", and so on.

- He translates "SOPHIE" as "181415070804".

Break into blocks: Since the encoding function works modulo n, Bob needs to break up his message into *blocks*, each of which is less than n. The easiest way to do this is to break it into blocks which have one fewer digit than n does, since any such number is clearly less than n.

- Since $n = 1537$, Bob breaks the message into 3-digit blocks. He gets 181, 415, 070, 804.

Encode: Now, Bob simply encrypts each block separately (using fast exponentiation to do the computations). This part was homework. Michelle, Kai, Courtney, and Bryce shared their answers with us. They were:

$$\epsilon(181) = 181^{47} \,\%1537 = 480$$
$$\epsilon(415) = 415^{47} \,\%1537 = 121$$
$$\epsilon(070) = 70^{47} \,\%1537 = 481$$
$$\epsilon(804) = 804^{47} \,\%1537 = 462$$

This means that the final message Bob sends to Alice is 480, 121, 481, 462.

As we've mentioned, in order for the RSA system to actually be useful in practice, it must be relatively easy to find large prime numbers but relatively hard to factor large integers. We've talked about factoring some already, and we decided to return to the general problem of finding large primes.

50. Primality Testing & Carmichael Numbers

We started by recalling the general version of Fermat's Little Theorem:

Theorem 50.1. *If p is prime, then $a^p \equiv a \pmod{p}$ for every integer a.*

Note that this is a consequence of an application of Euler's Theorem which states that if p is a prime number and a is any integer then $a^{p-1} \equiv 1 \pmod{p}$ (since $\phi(p) = p - 1$).

Question: Is the converse of this theorem true? In other words, if $a^n \equiv a \pmod{n}$ for every integer a, can we conclude that n is prime?

We decided to vote on the possible truth of this question. Sam was the only person who thought the answer would be "no". Unfortunately, the answer to this question is indeed "no".

Definition 50.2. An integer n which is composite (i.e., not prime) and for which $a^n \equiv a \pmod{n}$ for all integers a is called a *Carmichael number*.

It turns out that there are infinitely many Carmichael numbers. (This was just proven in 1994!) The smallest Carmichael number is 561. The proof that 561 is a Carmichael number is kind of a fun set of calculations. I did about a third of it, and then we finished it off in groups with Evan and Patrick putting the solutions on the board.

Proposition 50.3. *The number* 561 *is not prime, but* $a^{561} \equiv a \pmod{561}$ *for every integer* a*. That is, 561 is a Carmichael number.*

Proof. Since $561 = 3 \cdot 11 \cdot 17$, it is clear that 561 is not prime. We need to show that $a^{561} \equiv a \pmod{561}$ for every integer a. This is the same as showing that 561 divides $a^{561} - a$ for every integer a, which is the same as showing that 3, 11 and 17 all divide $a^{561} - a$ for every integer a, which is the same as showing three things:

$$\begin{aligned} a^{561} &\equiv a \pmod{3} \\ a^{561} &\equiv a \pmod{11} \\ a^{561} &\equiv a \pmod{17} \end{aligned}$$

We attacked each of these statements separately, using laws of exponents and Fermat's Little Theorem repeatedly. For the first one, we have:

$$\begin{aligned} a^{561} &= (a^3)^{11 \cdot 17} \\ &= (a^3)^{187} \\ &\equiv a^{187} \pmod{3} \\ &\equiv (a^3)^{62} a \pmod{3} \\ &\equiv a^{62} a \pmod{3} \\ &\equiv a^{63} \pmod{3} \\ &\equiv (a^3)^{21} \pmod{3} \\ &\equiv a^{21} \pmod{3} \\ &\equiv (a^3)^7 \pmod{3} \\ &\equiv a^7 \pmod{3} \\ &\equiv (a^3)^2 a \pmod{3} \\ &\equiv a^2 a \pmod{3} \\ &\equiv a^3 \pmod{3} \\ &\equiv a \pmod{3}. \end{aligned}$$

In groups we also found

$$\begin{aligned} a^{561} &= (a^{11})^{3\cdot 17} \\ &= (a^{11})^{51} \\ &\equiv a^{51} \pmod{11} \\ &\equiv (a^{11})^4 a^7 \pmod{11} \\ &\equiv a^4 a^7 \pmod{11} \\ &\equiv a^{11} \pmod{11} \\ &\equiv a \pmod{11} \end{aligned}$$

and

$$\begin{aligned} a^{561} &= (a^{17})^{3\cdot 11} \\ &= (a^{17})^{33} \\ &\equiv a^{33} \pmod{17} \\ &\equiv (a^{17}) a^{16} \pmod{17} \\ &\equiv a a^{16} \pmod{17} \\ &\equiv a^{17} \pmod{17} \\ &\equiv a \pmod{17}. \end{aligned}$$

This completes the proof. □

The existence of Carmichael numbers means that we're going to need to try something else for primality testing.

51. Miller's Primality Test

Recall (from Test 4) that if p is prime, then there are only two possible solutions to the equation

$$a^2 \equiv 1 \pmod{p},$$

namely $a \equiv 1 \pmod{p}$ and $a \equiv p - 1 \equiv -1 \pmod{p}$. This means that if there is an integer a with $2 \leq a \leq n-2$ and $a^2 \equiv 1 \pmod{n}$, then the integer n cannot be prime. In 1975, Miller turned this observation into a primality test. Here it is:

Miller's Test: To see if the odd integer $n > 2$ is prime, perform the following algorithm:

Step 0: Pick a *base* b with $1 < b < n$. Use the Euclidean Algorithm to compute $d := \gcd(b, n)$. If $d = 1$, proceed to Step 1. Otherwise, n cannot be prime because d is a non-trivial divisor of n.

Step 1: Use Fast Exponentiation to compute $a_1 := b^{n-1} \,\%n$. We know from Fermat's Little Theorem that *if* n is prime, then we must have $a_1 = 1$. So if $a_1 \neq 1$ then n cannot be prime and we're done. If $a_1 = 1$, then go to Step 2.

Step 2: Use Fast Exponentiation to compute $a_2 := b^{\frac{n-1}{2}} \% n$. Since we already know that $b^{n-1} \equiv 1 \pmod{n}$ (by Step 1), we have

$$\begin{aligned} a_2^2 &\equiv \left(b^{\frac{n-1}{2}}\right)^2 \pmod{n} \\ &\equiv b^{n-1} \pmod{n} \\ &\equiv 1 \pmod{n}. \end{aligned}$$

This means that *if* n is prime, then a_2 must be either 1 or -1. So if $a_2 \neq \pm 1$, then n cannot be prime and we're done. If $a_2 = -1$, then there's nothing more we can do. We declare that n is a *strong pseudo-prime* to the base b and stop. If $a_2 = 1$ and $\frac{n-1}{2}$ is odd, then there's again nothing more we can do. We declare that n is a *strong pseudo-prime* to the base b and stop. Finally, if $a_2 = 1$ and $\frac{n-1}{2}$ is even, we proceed to Step 3.

Step 3: Replace the exponent just used in Step 2 by half that exponent and repeat Step 2 with the new exponent. (That is, replace $\frac{n-1}{2}$ by $\frac{n-1}{4}$, and then next replace $\frac{n-1}{4}$ by $\frac{n-1}{8}$, etc., as long as you keep getting to this step.)

Some observations:

(1) Every prime p passes Miller's Test for every base b.
(2) Composites which pass Miller's Test are rare.

In fact, one can show that the smallest composite which passes Miller's Test for the base $b = 2$ is $n = 2047$, and the smallest composite which passes Miller's Test for both of the bases $b = 2$ and $b = 3$ is 1,373,653. In fact, there is only one composite less than 25,000,000,000 which passes Miller's Test to all four of the bases 2, 3, 5, and 7, namely 3,215,031,751.

We decided to work through a few examples applying Miller's Test.

Example: Let $n = 2047$.

Step 0: We pick the base $b = 2$. It is clear that $d := \gcd(2, 2047) = 1$. Since $d = 1$, we proceed to Step 1.

Step 1: We use Fast Exponentiation to compute $a_1 := 2^{2046} \% 2047$. We have

$$\begin{aligned} 2 &\equiv 2 \pmod{2047} \\ 2^2 &\equiv 4 \pmod{2047} \\ 2^4 &\equiv 16 \pmod{2047} \\ 2^8 &\equiv 256 \pmod{2047} \\ 2^{16} &\equiv 32 \pmod{2047} \\ 2^{32} &\equiv 1024 \pmod{2047} \\ 2^{64} &\equiv 512 \pmod{2047} \\ 2^{128} &\equiv 128 \pmod{2047} \\ 2^{256} &\equiv 8 \pmod{2047} \\ 2^{512} &\equiv 64 \pmod{2047} \\ 2^{1024} &\equiv 2 \pmod{2047}. \end{aligned}$$

Thus,

$$\begin{aligned} 2^{2046} &= 2^{1024} \cdot 2^{512} \cdot 2^{256} \cdot 2^{128} \cdot 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^8 \cdot 2^4 \cdot 2^2 \\ &\equiv 1 \pmod{2047}. \end{aligned}$$

That is, $a_1 = 1$ and hence we go to Step 2.

Step 2: We now use Fast Exponentiation to compute $a_2 := 2^{1023} \,\%2047$. Most of the work was completed in Step 1. We have

$$\begin{aligned} 2^{1023} &= 2^{512} \cdot 2^{256} \cdot 2^{128} \cdot 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^8 \cdot 2^4 \cdot 2^2 \cdot 2 \\ &\equiv 1 \pmod{2047}. \end{aligned}$$

That is, $a_2 = 1$. Since $a_2 = 1$ and $\frac{n-1}{2} = 1023$ is odd, there's nothing more we can do and 2047 passes Miller's Test with base 2. We declare that 2047 is a *strong pseudo-prime* to the base 2 and stop.

Example: Let $n = 2047$.

Step 0: This time we pick the base $b = 3$. It is clear that $d := \gcd(3, 2047) = 1$. Since $d = 1$, we proceed to Step 1.

Step 1: We use Fast Exponentiation to compute $a_1 := 3^{2046} \,\%2047$. We have

$$\begin{aligned} 3 &\equiv 3 \pmod{2047} \\ 3^2 &\equiv 9 \pmod{2047} \\ 3^4 &\equiv 81 \pmod{2047} \\ 3^8 &\equiv 420 \pmod{2047} \\ 3^{16} &\equiv 358 \pmod{2047} \\ 3^{32} &\equiv 1250 \pmod{2047} \\ 3^{64} &\equiv 639 \pmod{2047} \\ 3^{128} &\equiv 968 \pmod{2047} \\ 3^{256} &\equiv 1545 \pmod{2047} \\ 3^{512} &\equiv 223 \pmod{2047} \\ 3^{1024} &\equiv 601 \pmod{2047}. \end{aligned}$$

Thus,

$$\begin{aligned} 3^{2046} &= 3^{1024} \cdot 3^{512} \cdot 3^{256} \cdot 3^{128} \cdot 3^{64} \cdot 3^{32} \cdot 3^{16} \cdot 3^8 \cdot 3^4 \cdot 3^2 \\ &\equiv 1013 \pmod{2047}. \end{aligned}$$

That is, $a_1 = 1013 \neq 1$. So $n = 2047$ fails Miller's Test with base 3. We conclude that 2047 is not a prime number. In fact, $2047 = (23)(89)$.

Homework: We decided to work with one final RSA example. Using the public keys $n = 143$ and $e = 23$ for Alice do each of the following.

(1) Explain how Bob would encode the message "HELLO" to send to Alice.
(2) Decode Bob's message if Alice receives "85, 27, 126, 75".

Happy Thanksgiving Break!!!!

52. One Last RSA Example

We returned from the Thanksgiving Break to the following quote.

Quote: [L. Euler] "Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the mind will never penetrate."

We began class with reminders about the group presentations which will begin next class. We then shared our solutions to our last homework problem which served as a last example of RSA cryptography. We were given Alice's public keys: $n = 143$ and $e = 23$. The homework was to figure out how Bob would send the message "HELLO", and to figure out how Alice would decrypt the message "85, 27, 126, 75". A variety of people were called upon for answers. It was noted that Alice's private key is $d = 47$. The details of the involved calculations to find d can be found in the notes from November 19.

Example: Suppose Bob wants to send Alice the message "HELLO". Bob needs to follow these steps:

Look up Keys: His first step is to look up Alice's public keys, n and e. He then knows that $\epsilon(m) = m^e \,\%n$ is the encoding function he should use.

- Bob finds $n = 143$, $e = 23$ and so he knows that the encoding function he should use is $\epsilon(m) = m^{23} \,\%143$.

Translate: Next, Bob needs to translate his message into numbers, using the usual system where "A" becomes "00", "B" becomes "01", and so on.

- He translates "HELLO" as "0704111114".

Break into Blocks: Since the encoding function works modulo n, Bob needs to break up his message into *blocks*, each of which is less than n. The easiest way to do this is to break it into blocks which have one fewer digit than n does, since any such number is clearly less than n.

- Since $n = 143$, Bob breaks the message into two-digit blocks. He gets 07, 04, 11, 11, and 14.

Encode: Now, Bob simply encrypts each block separately (using fast exponentiation to do the computations).

- In our example, we get

$$\epsilon(07) = 7^{23} \,\%143 = 02$$
$$\epsilon(04) = 4^{23} \,\%143 = 75$$
$$\epsilon(11) = 11^{23} \,\%143 = 110$$
$$\epsilon(11) = 11^{23} \,\%143 = 110$$
$$\epsilon(14) = 14^{23} \,\%143 = 27.$$

This means that the final message Bob sends to Alice is 02, 75, 110, 110, 27.

Example: Suppose Alice receives the message "85, 27, 126, 75" from Bob. In order to read the message, she performs the following steps:

Decode the Blocks: First, Alice must apply her decoding function $\delta(s) = s^d \,\%m$ to each block separately, using fast exponentiation to actually do the computations.

- In our example, we have $\delta(s) = s^{47}\,\%143$, and so

$$\delta(85) = 85^{47}\,\%143 = 02$$
$$\delta(27) = 27^{47}\,\%143 = 14$$
$$\delta(126) = 126^{47}\,\%143 = 03$$
$$\delta(75) = 75^{47}\,\%143 = 04$$

Translate to Numbers: Next, Alice translates the output of the decoding function into numbers, using the usual system where "00" becomes "A", "01" becomes "B", and so on.

- We have that "02" means "C", "14" means "O", "03" means "D", and "04" means "E". Thus, the message Bob was sending Alice was "CODE".

53. The Chinese Remainder Theorem

We next had a brief discussion of another application to Euler's Theorem. This was a proof of the famous *Chinese Remainder Theorem*.

Theorem 53.1 (The Chinese Remainder Theorem)**.** *Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution which is unique modulo $n = n_1 n_2 \cdots n_r$.

Proof. We prove the existence of the solution x and leave the proof of the uniqueness of x.

Let $n = n_1 n_2 \cdots n_r$ and $N = \dfrac{n}{n_i}$ for all $i = 1, 2, \ldots, r$.

Claim: $x = a_1 N_1^{\phi(n_1)} + a_2 N_2^{\phi(n_2)} + \cdots + a_r N_r^{\phi(n_r)}$ is a solution to the system.

To see this, note that when $i \neq j$, $N_j \equiv 0 \pmod{n_i}$. Thus $x \equiv a_i N_i^{\phi(n_i)} \pmod{n_i}$ for all $i = 1, \ldots, r$. But, $\gcd(N_i, n_i) = 1$ for each i and so Euler's Theorem can be applied to obtain $N_i^{\phi(n_i)} \equiv 1 \pmod{n_i}$. Therefore, for each i, we see that $x \equiv a_i \pmod{n_i}$ as desired. □

Example: (Garrett, Dan, Kim, Patrick, Bryce, Kai, Evan) We want to find the solution x which simultaneously satisfies the equations

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

Using the notation from the proof of the Chinese Remainder Theorem, we have $n_1 = 3, n_2 = 5, n_3 = 7$ and $a_1 = 2, a_2 = 3, a_3 = 2$. Thus, $n = n_1 n_2 n_3 = (3)(5)(7) = 105$ and so

$$N_1 = \frac{105}{3} = 35$$
$$N_2 = \frac{105}{5} = 21$$
$$N_3 = \frac{105}{7} = 15.$$

Note that $\phi(n_1) = \phi(3) = 2, \phi(n_2) = \phi(5) = 4$ and $\phi(n_3) = \phi(7) = 6$. Thus,

$$\begin{aligned} x &= a_1 N_1^{\phi(n_1)} + a_2 N_2^{\phi(n_2)} + a_3 N_3^{\phi(n_3)} \\ &= (2)(35)^2 + (3)(21)^4 + (2)(15)^6 \\ &= 23367143. \end{aligned}$$

Indeed,

$$\begin{aligned} 23367143 &\equiv 2 \pmod 3 \\ 23367143 &\equiv 3 \pmod 5 \\ 23367143 &\equiv 2 \pmod 7. \end{aligned}$$

54. Rabin's Probabilistic Primality Test

We next returned to our discussion of primality testing.

Recall that a composite odd integer n which passes Miller's Test to the base b is called a *strong pseudo-prime* to the base b. One can prove that there are no integers which are strong pseudo-primes to every base, so there is no analogue of Carmichael numbers for strong pseudo-primes. In fact, one can even prove a result which gives a bound on the number of bases for which an odd integer n can pass Miller's Test. The precise statement is given in the following theorem.

Theorem 54.1. *If n is a composite odd integer, then the number of bases b between 1 and n for which n passes Miller's Test is less than $n/4$.*

This theorem means that, depending on which base b we choose, Miller's Test could tell us that a composite n is prime up to $1/4$ of the time! This seems bad, but Rabin made the observation that the theorem can be interpreted probabilistically: Given a composite odd integer and a base b which is chosen at random, the probability that n passes Miller's Test to the base b is less than $1/4$. Given two randomly chosen bases, the probability that n passes Miller's Test to both of these bases is then less than $(1/4)(1/4) = 1/4^2$. More generally given k randomly chosen bases, the probability that n passes Miller's Test for all k bases is less than $1/4^k$.

Theorem 54.2 (Rabin's Probabilistic Primality Test)**.** *Let n be an odd positive integer. Pick k different bases less than n and perform Miller's Test for all of these k different bases. If n is composite, then the probability that n passes all these tests is less that $1/4^k$.*

This gives a very quick and efficient test for primality which is not absolutely certain, but almost. For example, if we find that some odd integer n passes Miller's Test for 100 different bases, we have overwhelming evidence that n is prime, since the probability that a composite n could pass all 100 tests would be less than $1/4^{100}$, which is approximately $1/10^{60}$.

Since roughly 1 in every 115 odd 100 digit numbers is a prime (this follows from the Prime Number Theorem which we discuss below), one would not have to test too many different 100 digit odd numbers n before getting one which passes Miller's Test to 100 different bases. Using the technique of successive squarings that we have used to compute big powers, this takes only a few minutes on a computer. This n is almost certain to be prime.

55. The Prime Number Theorem

It is natural to wonder about the distribution of the prime numbers. One law that governs the behavior is:

Theorem 55.1 (Bertrand-Chebyshev Theorem)**.** *If $n > 1$ is an integer then, then there exists at least one prime number p with $n < p < 2n$.*

In the same spirit of prime distribution, we have the *Prime Number Theorem*. Given a real number x, this result allows one to predict how many prime numbers there are which are less than x.

Definition 55.2. Let x be a real number. The *prime-counting function* is $\pi(x)$ which gives the number of primes less than or equal to x.

Example: Together we completed the following table.

x	$\pi(x)$
7	4
10	4
36.5	11
100	25

One way to say that there are infinitely many primes is to write $\lim_{x\to\infty} \pi(x) = \infty$.

Question: Is there a formula for the number $\pi(x)$?

Example: To get a feel for the above question, we worked in groups to complete the following table. Matt, Trevor, and TJ wrote their answers on the board.

x	$\pi(x)$	$\dfrac{\pi(x)}{x/\ln x}$
10	4	0.921
10^2	25	1.151
10^3	168	1.161
10^4	1,229	1.132
10^5	9,592	1.104
10^6	78,498	1.084
10^7	664,579	1.071
10^8	5,761,455	1.061
10^{23}	1,925,320,391,606,803,968,923	1.020

We noticed that all the numbers in the last column of the above table are quite close to 1. This is essentially the key observation for the Prime Number Theorem.

Theorem 55.3 (The Prime Number Theorem)**.** *Let x be a real number. Then*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

This can be rephrased as

$$\pi(x) \approx \frac{x}{\ln x}.$$

As a consequence, we have:

Corollary 55.4. *If p_n is the nth prime number, then*

$$p_n \approx (n)(\ln n).$$

Example: $p_{21} = 73$ is the 21st prime number. Note that $(21)(\ln 21) \approx 63.93$.

Example: $p_{25} = 97$ is the 25th prime number. Note that $(25)(\ln 25) \approx 80.47$.

Example: $p_{14} = 43$ is the 14th prime number. Note that $(14)(\ln 14) \approx 36.95$.

Example: $p_{1000} = 7919$ is the 1000th prime number. Note that $(1000)(\ln 1000) = 6907.755$.