# Math 406 Lecture Notes

Dr. Holmes

1/27/2021: slight revision of Pythagorean triple theorem. Extension of homework assignment. 1/22/2021: redated second homework assigment (forgot to put this datestamp on) 1/15/2021: clarifications before lecture; (later) moved and revised the first homework assignment.
1/14/2021: added some proofs given in the 1/13 lecture to the notes.
1/7/2021: initial version of the Notes for Spring 2021

## 1 Welcome

Welcome to the Lecture Notes. I believe these notes include full discussion of everything I cover, though I will also refer you to sections in the book when appropriate. We may add new material to these notes if I go off in a different direction, or decide to treat a topic already covered in more depth.

I do seem to be writing notes on every class session and posting all homework assignments to the notes, so do read them!

Please read the notes: and be aware that I give *bonus points* for finding typos [to the first person who finds them, unless that person is me].

**Version notes**

I'm going to keep track of changes here to avoid version control accidents.

1/27/2021 slight revision of Pythagorean triple theorem. Extension of homework assignment.

1/22/2021 redated second homework assignment. Added refinement of algorithmic Euclidean algorithm proof. Forgot this datestamp!

1/15/2021 clarifications re the division algorithm before lecture. Later, moved and revised the first homework assignment.

1/14/2021 Added some proofs from the 1/13 lecture to the notes.

1/7/2021 This is now the Spring 2021 version. Assignment dates will be changed when assignments are actually given.

2/28/2018 corrected the stupid paragraph about 561 and its Carmichaelness.

1/12/2018 corrections and additions after a lecture.

1/3/2018 the version for Spring 2018

1/11/2016 Just showing the flag: this is the version for a new term. Homework assignments given in 2015 are still present; I may recycle them or I may write new ones, but in any case they have not been assigned yet until they have a 2016 date!

4/20/2015 corrected proofs of lemmas in the proof of the effectiveness of the Rabin Miller test for compositeness, and added a remark proving the equivalence of the two definitions of Carmichael number given in the book, which strongly suggests that the book does not succeed in giving a useful argument that Carmichael numbers do not have nontrivial square factors.

# Contents

# 2 A Starting Point

The natural numbers, the primary subject of this course, are the numbers

$$1, 2, 3 \ldots,$$

the positive whole numbers. We give a set of axioms (basic assumptions) governing these numbers.

## 2.1 Our official axioms

**basic constants and operations:** 1 is a natural number. If $a, b$ are natural numbers, $a + b$ and $a \cdot b$ (often written $ab$) are natural numbers.

**commutative laws:** $a + b = b + a$; $ab = ba$.

**associative laws:** $(a + b) + c = a + (b + c)$; $(ab)c = a(bc)$.

**distributive law:** $a(b + c) = ab + ac$

**identity of multiplication:** $a1 = a$

**cancellation laws:** $a + c = b + c$ implies $a = b$; $ac = bc$ implies $a = b$.

**Definition:** $a < b$ means "there is a natural number $c$ such that $a + c = b$".

**1 is minimal:** $a < 1$ is false for any natural number $a$.

**trichotomy:** For any $a, b$, exactly one of the following is true: $a < b$, $a = b$, $a > b$.

The final axiom is more complicated.

**Mathematical Induction:** For any sentence $P(n)$, if we can prove $P(1)$ and we can prove that for any natural number $k$, $P(k)$ implies $P(k+1)$, we can conclude that for any natural number $n$, $P(n)$ is true.

I give a short style manual for Math Induction proofs:

**Goal:** prove that for all natural numbers $n$, $P(n)$.

**Basis step:** Prove P(1)

**Induction step:** Fix an arbitrary natural number $k$.

**induction hypothesis:** Assume $P(k)$.

**induction goal:** Prove $P(k+1)$ [be sure to highlight uses of the induction hypothesis in the proof of the induction goal].

All of these axioms should be familiar to you. You may be surprised that some statements are missing (such as transitivity of order, "if $a < b$ and $b < c$ then $a < c$". The reason this is not present is that we can prove it!

We add the proof, which we gave in our lecture of 1/13/2021.

**Theorem:** For any natural numbers $a, b, c$, if $a < b$ and $b < c$ then $a < c$.

**Proof:** Let $a, b, c$ be arbitarily chosen natural numbers.

Suppose $a < b$ and $b < c$. Our goal is to prove $a < c$.

By definition of $a < b$ we can choose $x$ such that $a + x = b$.

By definition of $b < c$, we can choose $y$ such that $b + y = c$.

By definition of $a < c$, we can rephrase our goal: find $z$ such that $a + z = c$.

Now $c = b + y = (a + x) + y = a + (x + y)$ so if we define $z$ as $x + y$, we have found $z$ such that $a + z = c$, and so $a < c$ which was our goal.

This set of axioms is not minimal. For example, the commutative laws can be proved from the other given axioms.

## 2.2 A minimal set of axioms

A minimal set is the following, though you may find this hard to believe.

**basic constants and operations:** 1 is a natural number. If $a, b$ are natural numbers, $a + b$ and $a \cdot b$ are natural numbers.

**1 is minimal:** For any natural number $a$, $a + 1 \neq 1$.

**1-cancellation:** For any natural numbers $a, b$, $a + 1 = b + 1$ implies $a = b$.

**addition:** $a + (b + 1) = (a + b) + 1$

**identity of multiplication:** $a1 = a$

**multiplication:** $a(b + 1) = ab + a$

**mathematical induction:** as above.

These are basically the famous Peano axioms for arithmetic, though with some notational differences. We do not introduce a primitive operation of successor ($S(a) = a + 1$).

We give an example from our lecture of 1/13/2021, a proof of the full law of cancellation from the law of 1-cancellation.

**Theorem:** For any natural numbers $a, b, c$, if $a + c = b + c$ then $a = b$.

**Proof:** Define $P(n)$ as "for all natural numbers $a, b$, if $a + n = b + n$ then $a = b$".

Notice that "for all $n$, $P(n)$" is the same thing as the theorem we are trying to prove.

We will prove "for all $n$, $P(n)$", by math induction.

**Basis step:** We need to establish $P(1)$, that is, "for all $a, b$, if $a + 1 = b + 1$ then $a = b$". This is true because it is simply the law of 1-cancellation in our minimal axiom set.

**Induction step:** We choose a natural number $k$ arbitarily,

and assume the induction hypothesis $P(k)$ : for all $a, b$, if $a + k = b + k$ then $a = b$.

From this we need to prove the induction goal $P(k + 1)$ : for all $a, b$, if $a + (k + 1) = b + (k + 1)$ then $a = b$.

We now prove this.

Suppose $a + (k + 1) = b + (k + 1)$.

It follows by the axiom of addition that $(a + k) + 1 = (b + k) + 1$.

Then it follows by 1-cancellation that $a + k = b + k$.

Then it follows by the inductive hypothesis that $a = b$,

so we have shown " if $a + (k + 1) = b + (k + 1)$, then $a = b$", as required.

**Conclusion:** Having shown both $P(1)$ and "for any $k$, if $P(k)$ then $P(k+1)$", we have shown by mathematical induction that "for all $n$, $P(n)$", which is the full law of cancellation we are trying to prove.

## 2.3 The Well-Ordering Principle

An alternative formulation of Mathematical Induction is the following:

**Well-Ordering Principle:** Any nonempty set of natural numbers has a smallest element.

We show that this is equivalent to mathematical induction. This proof needs better formatting.

Strictly speaking, I should add that this equivalence only holds in the presence of some basic assumptions about sets of natural numbers. We state this in a very general form. The notion of *set* and the membership relation $\in$ are primitive notions for us. We assume that the set $\mathbb{N}$ of natural numbers exists (for any object $x$, $x \in \mathbb{N}$ iff $x$ is a natural number). We assume that for any set $X$ and any sentence $P(x)$ there is a set $\{x \in X : P(x)\}$ such that for any object $a$, $a \in \{x \in X : P(x)\}$ if and only if $a \in X$ and $P(a)$. We assume that sets are equal iff they have the same elements.

We begin by assuming that $P(1)$ and for any $k$, $P(k)$ implies $P(k+1)$, and the Well-Ordering Principle. Our aim is to show that for all $n$, $P(n)$.

Suppose that it isn't true that for all $n$, $P(n)$, with the aim of deriving a contradiction.

This means that the set $A = \{x \in \mathbb{N} : \neg P(x)\}$ is nonempty, so it has a smallest element $m$ by the Well-Ordering Principle.

By Trichotomy, either $m < 1$ or $1 = m$, or $1 < m$.

We deal with each case separately.

$m < 1$ is impossible by basic assumption.

$1 = m$ is impossible because $P(1)$, so $1 \notin A$, so since 1 is not an element of $A$ it cannot be the smallest element of $A$.

$1 < m$ implies by definition of $<$ that $1 + n = m$ for some natural number $n$. Now $n < m$, so $n \notin A$ (because $m$ is the smallest element of $A$) so $P(n)$ (by the definition of $A$), so $P(n+1)$ (by our assumptions), so $P(m)$, so $m \notin A$, which is a contradiction!

Since each case is impossible, we have deduced the required contradiction, and it must be the case that for all $n$, $P(n)$.

So we have shown that Mathematical Induction follows from the Well-Ordering Principle.

Now we show that the Well-Ordering Principle follows from Mathematical Induction.

Now we assume that $A$ is a nonempty set of natural numbers, and we assume Mathematical Induction. Our aim is to show that $A$ has a smallest element. For the sake of a contradiction we assume that $A$ does not have a smallest element.

We then prove that $n \notin A$ for any natural number, by induction, which gives the contradiction we want.

We will actually prove the stronger statement that for each $m \leq n, m \notin A$.

Basis step: let $n = 1$. If $m \leq 1$, then $m = 1$. $m \in A$, that is $1 \in A$, is impossible because 1 is the smallest natural number and $A$ has no smallest element: if 1 were in $A$, 1 would be the smallest element of $A$.

Induction step: Suppose (inductive hypothesis) that for all $m \leq k$, $m \notin A$. Our induction goal will be to show that for all $m \leq k+1$, $m \notin A$.

Suppose $m \leq k+1$. If $m \leq k$ we are done ($m \notin A$ by ind hyp) so we might as well assume $k < m$ (the only other possibility by trichotomy). We have $k + c = m$ and either $m = k+1$ or $m < k+1$, i.e., $m + d = k + 1$. The second case is impossible as we cannot have $k + c + d = k + 1$, which would imply $c + d = 1$. So $m = k+1$. Now if $k+1 \in A$, $k+1$ would be the smallest element of $A$, as $m < k+1$ implies $m \leq k$ ($m + c = k + 1$ implies (if $c = 1$) $m = k$ or (if $c = d + 1 > 1$) $m + d + 1 = k + 1$ so $m + d = k$ so $m < k$), and we know that for $m \leq k$, $m \notin A$. It follows than that since $A$ has no smallest element, $k + 1 \notin A$, so we have completed a proof by induction that for any $n$, for all $m \leq n$, $m \notin A$, so in particular $n \notin A$, so $A$ has no elements at all, which is a contradiction.

The technical details of the proof of this equivalence are not so very important to us, but both induction and the well-ordering principle are useful tools in number theory.

# 3 Subtraction and Division on Natural Numbers and Integers; the Euclidean Algorithm

In this section our aim is to get to the Euclidean algorithm, but there are stops on the way.

## 3.1 Subtraction and Integers

You may have noticed that some familiar operations and indeed some familiar numbers are missing from our official fundamentals.

**Observation:** For any two natural numbers $a$ and $b$, exactly one of the following things are true:

1. $a = b$,
2. or $a < b$ so there is $c$ such that $a + c = b$,
3. or $b < a$, so there is $c$ such that $b + c = a$.

If there is $c$ such that $a + c = b$, and also if $a + d = b$, then $c = d$ by cancellation. So for any $a, b$ there is at most one $c$ such that $a + c = b$.

**Definition (subtraction of natural numbers):** Fix natural numbers $a$ and $b$. We define $b - a$ as the unique $c$ such that $a + c = b$, if there is one.

Now we extend our number system in a familiar way. The *integers* consist of a new object 0, positive integers $+a$ for each natural number $a$ (which we may identify with $a$ though in most formal developments this is not done), and negative integers $-a$ for each natural number $a$.

**definition of addition of integers:** For natural numbers $a, b$, $+a + +b = +(a + b); -a + -b = -(a + b); +a + -b = -b + +a = +(a - b)$ if this makes sense, else $-(b - a)$ if this makes sense, else 0 (if $a = b$). For any integer $x$, $x + 0 = 0 + x = x$.

**definition of multiplication of integers:** For natural numbers $a, b$, $(+a)(+b) = (-a)(-b) = +ab$; $(+a)(-b) = (-a)(+b) = -ab$; for any integer $x$, $x0 = 0x = 0$.

The basic properties of the integers do not look quite the same as those of the natural numbers. 1 is of course no longer minimal. The integers $+a$ are referred to as the positive integers or the natural numbers; the definition of $<$ is rephrased: $a < b$ iff there is *positive* $c$ such that $a + c = b$. The cancellation law for multiplication ($ac = bc$ implies $a = b$) holds only if $c$ is nonzero. There are two additional properties: for every integer $x$ there is a unique integer $-x$, called the additive inverse of $x$, such that $x + -x = 0$, as well as the identity property for addition, $x + 0 = 0 + x = x$. You all know from experience that $-x$ is not necessarily a negative integer; the $-$ in names of negative integers is not precisely the same thing as the $-$ in an additive inverse expression.

Most importantly, a nonempty set of integers does not have a smallest element. But a nonempty set of integers with a lower bound does have a smallest element. Induction works perfectly well on the whole numbers (the positive integers and 0) with 0 instead of 1 as the starting point.

It is important to notice that all these properties of the integers are consequences of the stated properties of the natural numbers and the definitions of relations and operations on the integers.

## 3.2 The Division Algorithm

Notice that we are working in the natural numbers again, at least at the start of this section.

By the cancellation property for multiplication, if there is $c$ such that $ac = b$ and also $ad = b$, we have $c = d$. Thus it makes sense to make the following

**Definition (division):** If $a, b$ are natural numbers, define $b/a$ as the unique $c$ such that $ac = b$, if there is one. If we move to the integers, the only change we need to make is to stipulate that $x/0$ is never considered, since the cancellation property cannot be applied if $a = 0$ (there is either no $c$ such that $0c = x$ (if $x$ is nonzero) or every $c$ works (if $x = 0$) and either is embarrassing).

Most symbols $b/a$ remain undefined, as most integers do not go into one another evenly.

**Definition:** We define $a|b$ as meaning "there is a $c$ such that $ac = b$". It can be read "$a$ goes into $b$" or "$b$ is divisible by $a$". Notice that $a|b$ is

not a number but a *sentence*. It makes sense for natural numbers or for integers. On the natural numbers, $a|b$ is true iff $b/a$ is defined; on the integers, $a|b$ is true iff either $b/a$ is defined or $a = b = 0$. $0/0$ is not defined, but $0|0$ is true.

We are now going to explore the elementary school notion of division, under which we divide 17 by 4 and get a quotient 4 with a remainder of 1. To show that this operation works, we need to Prove a Theorem. We are going to use the Well-Ordering Principle, in the slightly modified version that any nonempty set of whole numbers has a minimal element.

**Theorem (division algorithm):** For any integer $a$ and positive integer $b$, there are unique integers $q$ and $r$ such that $a = bq + r$ and $0 \leq r < b$.

**Definition:** For a given integer $a$ and positive integer $b$, we define $a \,\mathtt{div}\, b$ as $q$ and $a \,\mathtt{mod}\, b$ as $r$ if $a = bq + r$ and $0 \leq r < b$. These are called the integer division and remainder operations: once we have proved the theorem we will know that these operations are well-defined.

**Proof of Theorem:** Fix an integer $a$ and a positive integer $b$. Define $A$ as

$$\{a - bq \mid q \in \mathbb{Z} \wedge a - bq \geq 0\}.$$

The intention is that $A$ is the set of all possible remainders, and the smallest element of $A$ will be the $r$ we are looking for. To show that there is such a smallest element, it is enough to show that $A$ is nonempty. If $a \geq 0$, $a - 0b = a$ will be in $A$. If $a < 0$, $a - ab = (-a)(b - 1) \geq 0$ will be in $A$. So in any case $A$ is nonempty and has a smallest element which we can call $r$ (and indeed we will see that this is the $r$ we are looking for).

Because $r \in A$, there is $q$ such that $r = a - bq$, and $q$ is computable uniquely as $\frac{a-r}{b}$. We clearly then have $a = bq + r$; we need to verify that $0 \leq r < b$. Suppose otherwise, that is, suppose that $r > b$. In this case $r - b \geq 0$, and $r - b = a - (q + 1)b \in A$, which is absurd because $r$ is the smallest element of $A$.

Now we need to show that $q, r$ are unique. Suppose that $a = bq + r, 0 \leq r < b$ and also $a = bq' + r', 0 \leq r' < b$. Suppose wlog that $r \geq r'$. $0 \leq r - r' = b(q' - q)$ (algebra) $< b$. But from this it is clear that

$q' - q = 0$, so $q' = q$, and from this it follows immediately that $r - r' = 0$, so $q = q', r = r'$.

The proof is complete.

**Definition:** If $a$ is an integer and $b$ is a positive integer and $a = bq + r; 0 \leq r < b$, we define $a \,\texttt{div}\, b$ as $q$ and $a \,\texttt{mod}\, b$ as $r$.

## 3.3 Common Divisors and the Euclidean Algorithm

**Definition (common divisor):** For any integers $a$ and $b$, we say that $d$ is a common divisor of $a$ and $b$ iff $d|a$ and $d|b$.

If $a = b = 0$, every integer is a common divisor of $a$ and $b$.

If $a \neq 0$ and $b = 0$, the common divisors of $a$ and $b$ are just the divisors of $a$.

For $a \neq 0$, the largest divisor of $a$ is $|a|$.

For $a, b$ both nonzero, the minimum of $|a|$ and $|b|$ is an upper bound for common divisors of $a$ and $b$.

**Lemma:** A nonempty set of integers which is bounded above has a largest element.

**Proof of Lemma:** If $A$ is a nonempty subset of $\mathbb{Z}$ (the set of integers) and $b$ is an upper bound for $A$ (that is, for any $x \in A$ we have $x \leq b$), consider the set $A' = \{b - x : x \in A\}$. All elements of $A'$ are nonnegative and $A'$ is nonempty because it has just as many elements as $A$. The smallest element of $A'$ exists by the well-ordering principle, and will be of the form $b - x$ where $x$ is the largest element of $A$.

This allows us to justify the assertion that if $a$ is nonzero, there is a greatest common divisor of $a$ and $b$: if $b = 0$, this greatest common divisor is exactly $|a|$.

**Definition:** We define $\texttt{gcd}(a, b)$ as the greatest common divisor of $a$ and $b$, where $a$ and $b$ are not both zero.

When computing $\texttt{gcd}(a, b)$ we can assume wlog that $a \geq b$ (since clearly $\texttt{gcd}(a, b) = \texttt{gcd}(b, a)$) and we can further assume that $a, b$ are both nonnegative (because $\texttt{gcd}(|a|, |b|) = \texttt{gcd}(a, b)$).

We make the further observation that if $b > 0$ we have $\texttt{gcd}(a, b) = \texttt{gcd}(b, a \,\texttt{mod}\, b)$. This is true because the set of common divisors of $a$ and $b$ is exactly the same as the set of common divisors of $b$ and $a - bq$ for any integer $q$, and $a \,\texttt{mod}\, b$ is of this form $a - bq$, being $a - b(a \,\texttt{div}\, b)$.

**Construction (the Euclidean algorithm):** We now describe the Euclidean algorithm for computing $\texttt{gcd}(a, b)$ where $a \geq b \geq 0$. If $b = 0$, the output is $|a| = a$ (or undefined if $a = 0$).

If $b > 0$, we compute $\texttt{gcd}(b, a \,\texttt{mod}\, b)$. Notice that $a \,\texttt{mod}\, b < b$: each step of this kind makes the second number in the pair smaller. This means that this process must terminate eventually with the second number equal to zero: there cannot be an infinite strictly decreasing sequence of whole numbers by the well-ordering principle. And as soon as the second number becomes 0, we are able to compute the gcd, so we have proved that this algorithm terminates and gives the gcd as the final output for any pair of numbers other than 0,0.

## 3.4 Exercises (assigned 1/15/2021):

These exercises were assigned on F 1/15/2021 and are due F 1/22/2021.

1. Write out the induction proofs in exercise 7.4 on p. 53 in the book, just as you would in Math 187. There is no need to anxiously follow my minimal assumptions; you may assume standard algebra rules. You may also do inductions that start at 0, and reason in contexts involving integers and rational numbers, as usual.

2. State the definition of what it means for a natural number $n$ to be the smallest element of a set $A$ of natural numbers. You may use the notation $x \in B$ for $x$ is an element of $B$ and the notations $<$ or if you like $\leq$ for order relations.

3. The Division Algorithm theorem tells us that for each integer $a$ and positive integer $b$ there is a unique pair of integers $q, r$ such that $a = bq + r$ and $0 \leq r < b$.

   We can define $a \,\texttt{div}\, b$ as the uniquely determined $q$ here and $a \,\texttt{mod}\, b$ as the uniquely determined $r$ here.

   Find $a \,\texttt{div}\, b$ and $a \,\texttt{mod}\, b$ in each of the following cases, and write the appropriate equation $a = bq + r$.

(a) $a = 10, b = 2$ (every multi-part problem should have an absurdly easy case).

(b) $a = 100, b = 3$ (still not too hard)

(c) $a = -12, b = 5$ (careful!)

(d) $a = -100, b = 3$ (again, careful!)

Computer languages are notably inconsistent in defining the div and mod operations where negative numbers are involved.

Why is there a problem with trying to define $a \,\texttt{div}\, b$ and $a \,\texttt{mod}\, b$ when $b < 0$? If you can see a way to restate the division algorithm theorem in a way which makes sense when $b < 0$ ($b = 0$ is of course hopeless), do so, and use your theorem (and associated definitions of div and mod) to answer two more parts with the same instructions as above:

(a) $a = 100, b = -3$

(b) $a = -100, b = -3$

We will not give an official definition for the case $b < 0$; this is just a thought experiment.

4. (hard; it's a challenge problem, your grade won't suffer horribly if you can't do it) Prove the commutative law of addition "for any natural numbers $a$ and $b$, $a + b = b + a$" using just the minimal assumptions.

   Hints: first prove by induction that $1+a = a+1$ for any natural number $a$ (this is a separate induction proof)

   Then assume "for any $a$, $a + k = k + a$" for a fixed $k$, and deduce "for any $a$, $a + (k + 1) = (k + 1) + a$".

   To prove this, you will need to prove the identity $(k+a)+1 = (k+1)+a$, again by induction.

   Part of the reason that this is hard is that you will constantly need to watch yourself to make sure you are only using the minimal assumptions!

   It is definitely possible to find proofs of the commutativity of addition from the Peano axioms on the web or in resources on my web page. You will learn more if you don't.

# 4 The Euclidean Algorithm and Linear Equations; Prime Factorization

In this section we will refine the Euclidean algorithm to get more information, then we will apply this to prove the theorem that each natural number can be uniquely factored into primes.

## 4.1 The Euclidean Algorithm and Linear Equations

In this subsection, we show that for each pair of natural numbers $a, b$, there is a pair of integers $x, y$ such that $ax + by = \texttt{gcd}(a, b)$. We show how to compute this by refining the calculation of the Euclidean algorithm.

Suppose $a \geq b \geq 0$ and $a$ is nonzero. Notice that $a = a1 + b0$. Notice that $b = a0 + b1$.

Suppose that in the course of our calculation we have reduced the problem of computing $\texttt{gcd}(a, b)$ to computing that of $\texttt{gcd}(c, d)$ and also we have $c = ap + bq$ and $d = au + bv$.

At the next step of the Euclidean algorithm we reduce computing $\texttt{gcd}(c, d)$ to computing $\texttt{gcd}(d, c \,\texttt{mod}\, d) = \texttt{gcd}(d, c - (c \,\texttt{div}\, d)d)$. This is just as above. But in addition we can record the information that $d = au + bv$ and $c - (c \,\texttt{div}\, d)d = a(p - (c \,\texttt{div}\, d)u) + b(q - (c \,\texttt{div}\, d)v)$.

So we can carry out the entire Euclidean algorithm preserving the condition that each number in a pair for which we compute the gcd is a linear combination of $a$ and $b$ with integer coefficients. This condition will be preserved at the last step, the computation of a $\texttt{gcd}(e, 0)$ where $e$ turns out to be $\texttt{gcd}(a, b)$, which is thus seen to be a linear combination of $a$ and $b$ with integer coefficients.

In class I gave a very formal description of this procedure, which I will now summarize.

Let $a \geq b \geq 0$ with $a$ positive.

We give recursive definitions of three finite sequences.

$A_0$ is defined as $a$, $A_1$ is defined as $b$, and $A_{i+2}$ is defined as $A_i \,\texttt{mod}\, A_{i+1} = A_i - (A_i \,\texttt{div}\, A_{i+1})A_{i+1}$, as long as this is nonzero: if $A_{i+1}$ goes evenly into $A_i$, $A_{i+2}$ is undefined.

$B_0$ is defined as 1, $B_1$ as 0, and $B_{i+2}$ as $B_i - (A_i \,\texttt{div}\, A_{i+1})B_{i+1}$, as long as $A_{i+1}$ does not evenly go into $A_i$, in which case $B_{i+2}$ is undefined.

$C_0$ is defined as 0, $B_0$ as 1, and $C_{i+2}$ as $C_i - (A_i \,\mathtt{div}\, A_{i+1})C_{i+1}$, as long as $A_{i+1}$ does not evenly go into $A_i$, in which case $C_{i+2}$ is undefined.

Notice that $A_{i+2} < A_{i+1}$ for every $i$. This is because $A_i \mathtt{mod} A_{i+1} < A_{i+1}$.

This means that the set of all $A_i$'s has a smallest element $A_k$, and it must be the case then that $A_k$ goes evenly into $A_{k-1}$, or we would be able to define $A_{k+1} < A_k$ and $A_k$ would not be smallest. In other words, the sequences must be finite.

We have $\mathtt{gcd}(A_{i+1}, A_{i+2}) = \mathtt{gcd}(A_{i+1}, A_i \mathtt{mod} A_{i+1}) = \mathtt{gcd}(A_i, A_{i+1})$ for each $i$, so in fact for each $i$ we have $\mathtt{gcd}(A_{i+1}, A_{i+2}) = \mathtt{gcd}(A_0, A_1) = \mathtt{gcd}(a, b)$. And further if $A_k$ is the smallest of the $A_i$'s we have $\mathtt{gcd}(a, b) = \mathtt{gcd}(A_{k-1}, A_k) = \mathtt{gcd}(A_k, A_{k-1} \mathtt{mod} A_k) = \mathtt{gcd}(A_k, 0) = A_k$.

So there is a smallest $A_i$, call it $A_k$, and $A_k = \mathtt{gcd}(a, b)$.

Further, we prove by induction that for each $i$ we have $A_i = B_i a + C_i b$.

For $i = 0$ we have $A_0 = a = 1a + 0b = B_0 a + C_0 b$.

For $i = 1$, we have $A_1 = b = 0a + 1b = B_1 a + c_1 b$.

This completes the basis step.

Our induction hypothesis is that $A_i = B_i a + C_i b$ and $A_{i+1} = B_{i+1} a + C_{i+1} b$.

Then

$$A_{i+2} = A_i \mathtt{mod} A_{i+1} = A_i - (A_i \mathtt{div} A_{i+1}) A_{i+1} =$$

[ind hyp]

$$(B_i a + C_i b) - (A_i \mathtt{div} A_{i+1})(B_{i+1} a + C_{i+1} b) =$$

[algebra]

$$(B_i - (A_i \mathtt{div} A_{i+1}) B_{i+1}) a + (C_i - (A_i \mathtt{div} A_{i+1}) C_{i+1}) b = B_{i+2} a + C_{i+2} b.$$

This completes the proof by induction that $A_i = B_i a + C_i b$ for each $i$. It might require a little thought to see that this is a proof by induction: this is the pattern found in many induction proof involving the Fibonacci numbers.

This then implies that $\mathtt{gcd}(a, b) = A_k = B_k a + C_k b$, so there are as desired integers $x, y$ such that $ax + by = \mathtt{gcd}(a, b)$. Moreover, we are presented with an explicit computation procedure to find these integers.

I'll provide a spreadsheet implementing this (there is already a link to it above).

It is further worth noting that $\mathtt{gcd}(a, b)$ is the smallest natural number which can be expressed in the form $ax + by$ where $x$ and $y$ are integers. To see this, notice that every number of the form $ax + by$ must be divisible by $\mathtt{gcd}(a, b)$, because both $a$ and $b$ are so divisible. We have just shown that

$\texttt{gcd}(a, b)$ is a linear combination of $a$ and $b$ with integer coefficients, and if there were a smaller natural number which was such a linear combination, it would be a natural number smaller than $\texttt{gcd}(a, b)$ but also divisible by $\texttt{gcd}(a, b)$, which is impossible.

There is a proof that $\texttt{gcd}(a, b)$ can be expressed in the form $ax+by$ which follows this path.

**Alternative Proof:** Fix $a \geq b \geq 0$ with $a$ nonzero.

> Consider the set $A = \{ax + by : x, y \in \mathbb{Z} \wedge ax + by > 0\}$. This set is nonempty because $a = a1+b0$ belongs to it, so it has a smallest element $d$. We claim that for any $e \in A$, we have $d|e$. Suppose otherwise: then for some $e \in A$, $e \,\texttt{mod}\, d \neq 0$. $e = au+bv$ for some $u, v$ because it is in $A$. $d = ap+bq$ for some $p, q$ because $d \in A$. Now $e \,\texttt{mod}\, d = e-(e \,\texttt{div}\, d)d = a(u - (e \,\texttt{div}\, d)p) + b(v - (e \,\texttt{div}\, d)q)$. $e \,\texttt{mod}\, d$ is greater than 0 by our assumptions so it belongs to $A$, being a positive linear combination of $a$ and $b$. But it is also less than $d$, which is the smallest positive linear combination of $a$ and $b$. This is a contradiction. So we see that $d$ is a common divisor of $a$ and $b$ (since $a, b$ both belong to $A$, or else $b = 0$). Because $d$ is a linear combination of $a$ and $b$, any common divisor of $a$ and $b$ also goes into $d$, so it must be the greatest common divisor of $a$ and $b$.

The alternative proof has the disadvantage that it is nonconstructive: it does not indicate a way to compute the coefficents $x$ and $y$, merely shows that they must exist.

## 4.2 Factorization into Primes

In this subsection, we show that each natural number can be factored into primes in one and only one way.

We begin by proving a Lemma which shows the relevance of the previous subsection.

**Definition:** A natural number $p$ is *prime* iff it has exactly two factors, $p$ and 1. Notice that this implies $p \neq 1$. A natural number $c$ is composite iff there is $a$ such that $1 < a < c$ and $a|c$. Notice that 1 is neither prime nor composite (it is said to be a *unit*).

**Lemma:** If $p$ is a prime and $p|ab$ then either $p|a$ or $p|b$.

**Proof of Lemma:** Either $p|a$ or $p \not| a$. If $p|a$ we are done so we might as well assume $p \not| a$. We show that in this case $p|b$. Because $p \not| a$, we have $\texttt{gcd}(p, a) = 1$: the gcd must be either $p$ or 1 as these are the only factors of $p$, and it cannot be $p$ because $p$ is not a factor of $a$. So we have integers $x, y$ such that $px+ay = 1$. Now $b = b1 = b(px+ay) = bpx+bay$. $p$ obviously goes into $bpx$ and it goes into $bay$ because by assumption it goes into $ab$. Thus $p|(bpx + bay) = b$. This completes the proof that $p$ must go into either $a$ or $b$.

**Lemma 2:** If $p|a_1 \cdot a_2 \cdot \ldots \cdot a_n$, then $p|a_i$ for some index $i$.

**Proof:** Prove this by induction on the length $n$ of the product. For $n = 2$ this is just the previous Lemma. Assume that the Lemma is true for products of $k$ numbers. If $p|a_1 \cdot a_2 \cdot \ldots \cdot a_k \cdot a_{k+1}$ then either $p|a_1 \cdot a_2 \cdot \ldots \cdot a_k$ or $p|a_{k+1}$ by the previous Lemma, and if $p|a_1 \cdot a_2 \cdot \ldots \cdot a_k$ then $p|a_i$ for some $i \leq k$ by inductive hypothesis.

**Theorem (existence of prime factorizations):** Every natural number other than 1 is either a prime or a finite product of primes.

**Proof of Theorem:** Suppose there is a natural number $x \neq 1$ which is neither a prime nor a finite product of primes. Then there is a *smallest* such natural number which we will call $m$. We know by assumption that $m$ is not prime, so $m$ is composite: there are $a, b$ such that $1 < a, b < m$ and $ab = m$. Since $a, b$ are both greater than one and less than $m$, each of them is either a prime or a finite product of primes, so their product $ab = m$ is a finite product of primes, which is a contradiction.

**Theorem (uniqueness of prime factorizations):** Every natural number other than 1 can be expressed as a prime or finite product of primes in exactly one way (we stipulate that products of primes are written in nondecreasing order).

**Proof:** Let $m$ be the *smallest* natural number for which this is not the case. We have $m = p_1 p_2 \ldots p_M = q_1 q_2 \ldots q_N$.

No $p_i$ can be equal to any $q_j$: if this were the case, we could divide $m$ by $p_i = q_j$ to obtain a smaller number with two different prime factorizations.

Now $p_1|m = q_1q_2 \dots q_N$, so by Lemma 2 $p_1|q_i$ for some index $i$, and the only way this can be true, since $p_1$ and $q_i$ are both primes, is for the two to be equal, which is a contradiction.

This proof is quite elaborate! So now you really know something you "learned" in elementary school. Or is that a fair statement? What do we know in mathematics?

### 4.3 Exercises, assigned 1/22/2021

These are assigned Friday 1/22/2021 and due Wednesday 2/3/2021 (this is an extension; originally I had "Wed 2/9", but of course 2/29 is Fri!). These are all problems from the book.

5.3, 5.5, 6.1, 6.6, 7.2, 7.5 (I might have some words to say about this problem on Wednesday: the definitions are in chapter 7, pp. 48-49).

Get to work on these problems promptly: some of them involve independent investigations into things I haven't talked about. I will give an overview of the background of question 7.5 as part of the lecture next Wednesday, but there is a sufficient discussion on the indicated pages.

## 5 What is Number Theory (with an extended example)?

This lecture was on chapters 1 and 2 in the book.

### 5.1 What is Number Theory?

They don't give a formal definition of what makes a mathematical question number-theoretical, but a list of typical questions in number theory which should give an impression. I remarked that my formalized theory of natural numbers (a version of Peano arithmetic) is more an exercise in logic than an exercise in number theory, though of course it is a theory of exactly the same objects and can be used as the foundation for number theory.

**sums of squares:** Can the sum of two squares be a square? When? See next subsection.

**sums of higher powers:** Can the sum of two $n$th powers be an $n$th power? No. This is the very hard Fermat-Wiles Theorem, far beyond our scope. The case $n = 4$ is in the book. The case $n = 3$ might possibly not be beyond our reach. This is a good example of the general situation in number theory: it is easy to recognize that situations are (probably) true by experiment without having any access to *why* they are true: proving that our observations can be generalized can be very hard.

**infinitude of primes:** I proved that there are infinitely many primes.

**Theorem:** There are infinitely many primes.

**Proof:** Suppose otherwise. Then there are finitely many primes $p_1, \ldots, p_n$. Consider the number $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$, the product of all the primes plus one. This is not divisible by any of the primes $p_i$ (if it were, 1 would be), but it has to have a prime factor (we showed above that every natural number is a prime or product of primes). This is a contradiction.

Generalizing this question, are there infinitely many primes in given arithmetic progressions? We know there are infinitely many primes of the form $2n + 1$ (odd primes) and only one of the form $2n + 0$.

Are there infinitely many primes of the form $4n+1$? of the form $4n+3$?

**Theorem (NOT IN BOOK):** There are infinitely many primes of the form $4n + 3$.

**Proof:** A product of numbers of the form $4n + 1$ must be of the form $4n + 1$. So suppose we only had finitely many primes of the form $4n + 3$. Multiply all of them together, getting a number of one of the forms $4n + 1$ or $4n + 3$, then add either 2 or 4 to get a number of the form $4n + 3$. This number must have a prime factor of the form $4n + 3$, and cannot be divisible by any of the primes of the form $4n + 3$ that are given on our finite list. So there must be infinitely many primes of the form $4n + 3$.

When I say it is not in the book, I mean it is not in Chapter 1. I think that it is very likely that this appears later in the book. This is the result I had on the tip of my tongue in class (I thought it was the $4n+1$ case which was relatively easy, but I had it backwards).

Dirichlet proved the following theorem which is both "obviously true" and very hard. If $a$ and $b$ are relatively prime natural numbers, there are infinitely many primes of the form $an + b$: any arithmetic progression that isn't made up of composite numbers for obvious reasons contains infinitely many prime numbers.

**which numbers can be sums of squares?** It is an interesting result that the odd primes which are sums of squares are exactly the ones of the form $4n + 1$. Who ordered that?

**numbers from shapes (see pictures in the book):** The Greeks were interested in numbers derived from arrays of dots of particular shapes. The square number $n^2$ are familiar. The triangular numbers $T_n = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ might be less familiar.

A question you will explore in the homework is, which numbers are both square and triangular? $36 = T_8 = 6^2$ is an example.

**are there infinitely many twin prime pairs?** A pair of twin primes is a pair of odd primes $p$ and $p + 2$. We all believe that there are infinitely many of them. This is a brutally hard problem.

**are there infinitely many primes of the form $n^2 + 1$?** Experiment suggests that there are. This has not been proved.

A characteristic of number theory is that we look for patterns by observation and experiment much as in the natural sciences, because in this area there are lots of patterns which can be observed from which we can form deceptively simple looking conjectures (guesses). But this is mathematics: we want to prove our conjectures.

Another characteristic of number theory is that the proofs we do obtain are often quite strange. There is a toolkit of methods we can *try* for proving theorems in number theory, but the proofs are often eccentric and sometimes come from what seem to be quite different areas of mathematics.

## 5.2 A Problem Solved: Pythagorean Triples

**Definition:** A *Pythagorean triple* is a triple of natural numbers $a, b, c$ such that $a^2 + b^2 = c^2$.

**Geometric Motivation:** For any Pythagorean triple $a, b, c$ , there is a right triangle with legs $a, b$ and hypotenuse $c$. The 3,4,5 Pythagorean triple can be used as a practical method to form a right angle.

**Example:** $3^2 + 4^2 = 5^2$

**Definition:** A *primitive Pythagorean triple* is a Pythagorean triple with no common factors other than 1.

**Motivation:** If $a, b, c$ are a Pythagorean triple and $d \neq 1$ is a common factor of $a, b, c$, so $a'd = a, b'd = b, c'd = c$, then $(a'd)^2 + (b'd)^2 = (c'd)^2$ implies $a'^2 + b'^2 = c'^2$ (divide both sides by $d^2$). If we further let $d$ be the greatest common divisor of $a, b, c$, then $a', b', c'$ will be a primitive Pythagorean triple. So if we know all the primitive triples, we can obtain all the triples by multiplying by constants.

**Lemma:** In a primitive Pythagorean triple $a, b, c$, the numbers $a, b$ will neither both be odd nor both be even.

**Proof:** if $a, b$ were both even, then $a^2 + b^2 + c^2$ would be even, so $c$ would be even and $a, b, c$ would not be a primitive triple.

If $a, b$ were both odd, then $a = 2x+1$, $b = 2y+1$, and since $a^2+b^2 = c^2$ would be even, $c^2$ and so $c$ are even, so we can set $c = 2z$. Now $a^2+b^2 = (2x+1)^2+(2y+1)^2 = 4x^2+4x+4y^2+4y+2$ is not divisible by 4, while $(2z)^2 = 4z^2$ is divisible by 4. But these two quantities are supposed to be equal. So this situation is impossible.

**Observations:** Let $a, b, c$ be a primitive Pythagorean triple. We may safely assume that $a$ is odd and $b$ is even (if not we could switch them), and $c$ is thus odd.

Since $a^2 + b^2 = c^2$ we have $a^2 = c^2 - b^2 = (c + b)(c - b)$.

$c + b$ and $c - b$ have no common factors. Both are odd numbers. If $d$ were a prime factor of both, $d$ would be odd and $d$ would also be a factor of $2c$ (their sum) and $2b$ (their difference) and so would be a factor of both $c$ and $b$ which is impossible as we have a primitive triple.

$a^2$ is a perfect square, so every prime in its factorization has an even exponent. Any prime which goes into $a^2$ goes into only one of $c + b$ and $c - b$, and in fact we can see that the exponent of each such prime

must be the same as its exponent in the expansion of $a$, and so even. And so $c+b$ and $c-b$ are perfect squares.

Set $c+b=s^2$ and $c-b=t^2$. Notice that $s$ and $t$ have no common prime factors, as any common prime factor of these would be a common factor of $b$ and $c$ by reasoning already given.

Algebra gives $c=\frac{s^2+t^2}{2}$ and $b=\frac{s^2-t^2}{2}$. $a^2=(c+b)(c-b)=s^2t^2$ so $a=st$.

**Theorem:** Every primitive Pythagorean triple is of the form $st$, $\frac{s^2-t^2}{2}$, $\frac{s^2+t^2}{2}$, where $\texttt{gcd}(s,t)=1$ and $s,t$ are both odd.. Moreover, all such triples are primitive Pythagorean triples.

**Proof:** The first sentence has been shown to be true in the observations above. The second sentence requires slightly more work.

That for any $s,t$ at all ($s>t$, both odd or both even) $st$, $\frac{s^2-t^2}{2}$, $\frac{s^2+t^2}{2}$ is a Pythagorean triple is just algebra.

What remains is to shown that if $\texttt{gcd}(s,t)=1$, then this triple is primitive. It is enough to show that $\frac{s^2-t^2}{2}$, $\frac{s^2+t^2}{2}$ have no common factors. Any prime common factor of these two numbers would be a prime factor of $s^2$, the sum of these two numbers, and $t^2$, their absolute difference. But any prime which goes into $s^2$ and $t^2$ also goes into $s,t$ (by the lemma on prime factorizations proved earlier), and $s,t$ have no common prime factor.

To my mind, this is an example of the fact that proofs in number theory are often rather odd and indirect. Others might not think so.

# 6 More about Pythagorean Triples Than You Ever Wanted To Know

In this section we continue the investigation of Pythagorean triples.

## 6.1 The tree of primitive Pythagorean triples

The theorem we will prove in this subsection is not so much very hard to prove as very surprising. How did someone think of this? The theorem is that the

set of primitive Pythagorean triples has the structure of a ternary tree. The root of the tree is the PPT $(3, 4, 5)$, which we treat as the vector $[3, 4, 5]^T$. There are three $3 \times 3$ matrices $A, B, C$ which we will specify. The three children of any node $[a, b, c]^T$ in the tree are $A[a, b, c]^T$, $B[a, b, c]^T$, $C[a, b, c]^T$. Every PPT appears in the tree, and every PPT appears in just one place.[1]

The matrices $A, B, C$ are

$$A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}$$

$$C = \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}$$

We are going to take a hint from the Wikipedia page on the subject and prove an analogous result using not PPT's $[a, b, c]^T$ but pairs $[s, t]^T$ with $s, t$ coprime and both odd, and $s > t$. We know from the previous section that these correlate exactly with the PPT's: $[st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2}]^T$ is a PPT for each such pair $[s, t]^T$, the pair can be recovered from the triple (so the representation of the triple is unique) and every PPT has a correlated pair.

What we do is show that the pairs $[s, t]^T$ form a ternary tree in exactly the same way with $[3, 1]^T$ as the root of the tree and the three matrices generating the tree being

$$D = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$E = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$$

$$F = \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix}$$

We show that each of the pairs $[s, t]^T$ with the appropriate properties appears in the ternary tree exactly once.

[1]The $T$ in $[a, b, c]^T, [s, t]^T$ is the transpose operator. These vectors are column vectors!

Then we show that the action of $D, E, F$ respectively on pairs $[s,t]^T$ corresponds to the action of $A, B, C$ respectively on the corresponding PPT's. This proves the theorem.

First of all, it is straightforward to see that if $[s,t]^T$ has $s > t$, $s, t$ both odd and coprime, then $D[s,t]^T = [s+2t, t]^T$, $E[s,t]^T = [2s+t, s]^T$, and $F[s,t]^T = [2s-t, s]^T$ satisfy the same conditions. Thus all the pairs in the tree satisfy the conditions.

The three matrices are invertible:

$$D^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$$

$$E^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}$$

$$F^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 2 \end{bmatrix}$$

We will show that for each pair $[s,t]^T$ other than $[3,1]^T$, exactly one of $D^{-1}[s,t]^T, E^{-1}[s,t]^T, F^{-1}[s,t]^T$ will satisfy the conditions, and moreover its first component will be less than $s$. This means that repeated application of the correct one of the three inverse matrices must terminate (otherwise we would have an infinite decreasing sequence of first components) and the only way we can stop is to reach $[3,1]^T$. So each pair satisfying the condition is in the ternary tree built on $[3,1]^T$ using the matrices $D, E, F$, and appears in the tree just once with the downward path in the tree to the root computed in the way we just described.

For any pair $[s,t]^T$ satisfying the conditions and different from $[3,1]^T$, we certainly have that each of $D^{-1}[s,t]^T, E^{-1}[s,t]^T, F^{-1}[s,t]^T$ has its components coprime and both odd. The issue is whether the components are positive and in the right order.

$D^{-1}[s,t] = [s-2t, t]^T$ will satisfy the conditions iff $s-2t > 0$ and $s-2t > t$. The first condition implies the second, which is equivalent to $s > 3t$.

$E^{-1}[s,t]^T = [t, s-2t]^T$ will satisfy the conditions iff $s - 2t > 0$ and $t > s - 2t$, that is, iff $s > 2t$ and $s < 3t$.

$F^{-1}[s,t]^T = [t, -s+2t]^T$ will satisfy the conditions iff $-s + 2t > 0$ and $t > -s+2t$. The first is equivalent to $s < 2t$ and the second is a consequence of $s > t$ and so simply holds.

The three sets of conditions are mutually exclusive and exhaustive. We cannot have $s = 2t$ because $s$ is odd, and we cannot have $s = 3t$ because we excluded $[3, 1]^T$ and $s, t$ are coprime. So exactly one of these triples will satisfy the conditions. And the first components $s - 2t$ and $t$ are both less than $s$.

Thus, we have completed the proof that we have described a ternary tree of pairs $[s, t]^T$ which includes all the pairs satisfying the conditions.

Now we show that the action of $D, E, F$ on pairs corresponds to the action of $A, B, C$ on triples.

$[a, b, c]^T$ in all cases is $[st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2}]^T$.

Let $[s', t']^T = D[s, t]^T = [s + 2t, t]^T$.

$$[a', b', c']^T = [(s + 2t)t, \frac{(s + 2t)^2 - t^2}{2}, \frac{(s + 2t)^2 + t^2}{2}]^T$$

$$= [st+2t^2, \frac{s^2 + 4st + 3t^2}{2}, \frac{s^2 + 4st + 5t^2}{2}] = [a-2b+2c, 2a-b+2c, 2a-2b+3c]^T = A[a, b, c]^T$$

Let $[s', t']^T = E[s, t]^T = [2s + t, s]^T$.

$$[a', b', c']^T = [(2s + t)s, \frac{(2s + t)^2 - s^2}{2}, \frac{(2s + t)^2 + s^2}{2}]^T$$

$$= [st+2s^2, \frac{3s^2 + 4st + t^2}{2}, \frac{5s^2 + 4st + t^2}{2}]^T = [a+2b+2c, 2a+b+2c, 2a+2b+3c]^T = B[a, b, c]^T$$

Let $[s', t']^T = F[s, t]^T = [2s - t, s]^T$.

$$[a', b', c']^T = [(2s - t)s, \frac{(2s - t)^2 - s^2}{2}, \frac{(2s - t)^2 + s^2}{2}]^T$$

$$= [-st + 2s^2, \frac{3s^2 - 4st + t^2}{2}, \frac{5s^2 - 4st + t^2}{2}]^T$$

$$= [-a - 2b + 2c, -2a + b + 2c, -2a + 2b + 3c]^T = C[a, b, c]^T$$

And this completes the proof that we have a tree of PPT's exactly parallel to the tree of pairs, and proves the theorem of the section.

## 6.2 Rational numbers

Just because I am the sort of mathematician I am, I'll say a couple of words about how the rational numbers can be implemented before the next topic of rational points on the unit circle.

A pair of natural numbers $(a, b)$ will be written $\frac{a}{b}$ when we are using it to represent a rational number. A pair of natural numbers $\frac{m}{n}$ such that $\texttt{gcd}(m, n) = 1$ we will call a *fraction*. Fractions implement the positive rational numbers: this is very familiar.

For a general pair $\frac{a}{b}$, we define $\texttt{simplify}(\frac{a}{b})$ as $\frac{a/\texttt{gcd}(a,b)}{b/\texttt{gcd}(a,b)}$, which will be the equivalent fraction in our sense. This is the familiar process of reducing a fraction to simplest form.

We can then define $\frac{a}{b}+\frac{c}{d}$ as $\texttt{simplify}(\frac{ad+bc}{bd})$ and define $\frac{a}{b}\cdot\frac{c}{d}$ as $\texttt{simplify}(\frac{ac}{bd})$. We define $\frac{a}{b}-\frac{c}{d}$ as $\texttt{simplify}(\frac{ad-bc}{bd})$ when this is defined, and we define order on fractions in the same way we defined it on natural numbers.

We then extend the fractions (positive rational numbers) to the complete system of rational numbers in the same way that we extended the natural numbers to the integers: rational numbers are of the form $+\frac{m}{n}$, 0, or $-\frac{m}{n}$, and we define addition and multiplication of fractions with signs attached just as we defined addition and multiplication of natural numbers with signs attached.

A lot of work is not done here: verifying that the rationals as I have defined them have the properties we all know they have takes some effort!

One thing that is clear is that the theory of the rational numbers is part of number theory: a rational number is a structure built quite directly from natural numbers. Another point is that we have given a standard notation for each rational number. For the reals the situation is much more complicated: in fact, it is a theorem that there are more real numbers than there are possible finite notations, so we cannot write a unique finite notation for each real!

## 6.3 Rational points on the unit circle

We aren't going to insist that notations $\frac{a}{b}$ for fractions are in simplest form; that is a technicality suiting the purposes of the previous subsection.

If $(x, y)$ is a point on the unit circle (whose equation is $x^2 + y^2 = 1$) then we can write $x = \frac{a}{c}$ and $y = \frac{b}{c}$ for suitable integers $a, b, c$. We can then write $\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$, from which we can deduce $a^2 + b^2 = c^2$. Observe that we

can assume without loss of generality that $a, b, c$ are non-negative (we could replace them with their absolute values without changing the situation in this equation). We then see that if neither $x$ or $y$ is 0, so neither $a$ nor $b$ is 0, we have associated a Pythagorean triple with the point $(x, y)$.

Now for any two points with rational coordinates, the slope of the line between them is rational. We consider points $(x, y)$ on the unit circle, with $x$ $y$ both positive, such that the slope $m$ of the line from $(-1, 0)$ is rational: $m = \frac{u}{v}$ where $u, v$ are natural numbers (that $m$ is positive is clear). We have discussed above why we can restrict our attention to points with positive rational coordinates.

It is clear that if $(x, y)$ is rational, the slope of the line from $(-1, 0)$ to $(x, y)$ will be positive. What is much less obvious is that the converse is also true: any line with rational slope through $(-1, 0)$ intersects the circle in a point with rational coordinates (this is *not* true if we use the origin $(0, 0)$ instead of $(-1, 0)$, for example).

The equation $y = m(1 + x)$ holds because $m$ is the slope of the line through $(-1, 0)$ and $(x, y)$. The equation $x^2 + y^2 = 1$ holds because $(x, y)$ is on the unit circle (Pythagorean theorem). We get the equation

$$x^2 + (m(1 + x))^2 = 1$$

by substitution, which algebra

$$x^2 + m^2(1 + 2x + x^2) = 1$$

converts into the quadratic equation

$$(m^2 + 1)x^2 + 2m^2x + (m^2 - 1) = 0$$

I solved this in class by polynomial long division. Here I am going to use the quadratic formula.

$$x = \frac{-2m^2 \pm \sqrt{(2m^2)^2 - 4(m^2 + 1)(m^2 - 1)}}{2(m^2 + 1)} =$$

$$\frac{-2m^2 \pm \sqrt{4m^4 - 4(m^4 - 1)}}{2(m^2 + 1)} =$$

$$\frac{-2m^2 \pm 2}{2(m^2 + 1)},$$

from which we see the solutions are $x = -1$ (the point $(-1, 0)$ is on the given line and circle no matter what $m$ is) and

$$x = \frac{1 - m^2}{1 + m^2}.$$

In the latter case

$$y = m(\frac{1 - m^2}{1 + m^2} + 1) = \frac{2m}{1 + m^2}.$$

We have not so far used the equation $m = \frac{u}{v}$ (nothing in this algebra depends on $m$ being rational, in fact).

$$x = \frac{1 - (\frac{u}{v})^2}{1 + (\frac{u}{v})^2} = \frac{v^2 - u^2}{v^2 + u^2}; y = \frac{2(\frac{u}{v})}{1 + (\frac{u}{v})^2} = \frac{2uv}{v^2 + u^2}$$

Geometry tells us that $x > 0$, because $m < 1$ is clear so $v > u$.

This demonstration shows that every Pythagorean triple without exception must be of the form

$$(v^2 - u^2, 2uv, v^2 + u^2).$$

Unlike our previous argument, it makes explicit use of the geometric motivation for Pythagorean triples related to the Pythagorean Theorem.

## 6.4 Exercises

I'm assigning 1.1, 1.3, 2.1, 2.3 (investigate and report, no expectation of a final answer), 2.4, 2.5 (optional), 2.8, 3.1, 3.5, 4.2 (optional) on 2/5 (should have done this earlier!) and making it due 2/12.

# 7 Basics of Congruences (Modular Arithmetic)

**Definition:** We define $a \equiv b \,\texttt{mod}\, m$ as holding iff $m|(a - b)$. We read this "$a$ is congruent to $b$ mod $m$". It is straightforward to show that this is an equivalence relation. It is also straightforward to show that this is equivalent to $a \,\texttt{mod}\, m = b \,\texttt{mod}\, m$ (where `mod` is the remainder operator).

It is natural when considering a fixed modulus $m$ to regard numbers which are congruent mod $m$ as identified: in mod $m$ arithmetic the only numbers are 0,1,2,... $m - 1$, as it were.

**Theorem:** We need to show that addition and multiplication are well-defined operations on equivalence classes under congruence mod $m$. That is, if $a \equiv a' \bmod m$ and $b \equiv b' \bmod m$, then $a + b \equiv a' + b' \bmod m$ and $a \cdot b \equiv a' \cdot b' \bmod m$.

**Proof:** If we assume $a \equiv a' \bmod m$ and $b \equiv b' \bmod m$, then we can choose integers $p$ and $q$ such that $a + pm = a'$ and $b + qm = b'$. Then $a' + b' = (a + pm) + (b + qm) = a + b + (p + q)m$, which is congruent to $a + b$ mod $m$. Further, $a'b' = (a + pm)(b + qm) = ab + aqm + bpm + pqm^2 = ab + m(aq + bp + pqm)$, which is congruent to $ab$ mod $m$.

Subtraction is also a well-defined operation: it is straightforward to show that $a + c \equiv b + c \bmod m$ implies $a = b \bmod m$: $m|(a + c) - (b + c)$ is equivalent to $m|a - b$ because $(a + c) - (b + c) = a - b$. If we consider 0,1,2,. . . , $m - 1$ as the mod $m$ numbers, then the additive inverse of $a$ is easily computed as $m - a$.

Division (or the existence of multiplicative inverses) is a more complex issue. If $ac \equiv bc \bmod m$ ($c \not\equiv 0 \bmod m$), we cannot necessarily deduce $a \equiv b \bmod m$. $ac \equiv bc \bmod m$ is equivalent to $m|ac - bc$, and so equivalent to $m|(a - b)c$. We can further deduce $m|(a - b)$ if we know that $m$ and $c$ have no common factors, that is, if $\gcd(c, m) = 1$. The condition $\gcd(c, m) = 1$ is only equivalent to the extra condition $c \not\equiv 0 \bmod m$ if $m$ happens to be a prime, and if $m$ is prime we *do* get the cancellation law for multiplication and the ability to compute multiplicative inverses. But if $m = uv$ with $1 < u, v < m$ (that is, if $m$ is composite) then observe that $u \equiv 0 \bmod m$ is false, but $uv \equiv 0v \bmod m$ is true (the latter equation being $m \equiv 0 \bmod m$), though $v$ is not congruent to 0 mod $m$, so we have a counterexample to cancellation for multiplication, and we also have a failure of the Zero Property of multiplication: $uv = m \equiv 0 \bmod m$, but $u \not\equiv 0, v \not\equiv 0 \bmod m$.

We can use the extended Euclidean algorithm to compute multiplicative inverses mod a prime $p$. If $c$ is not congruent to 0 mod $p$ then $c$ is not divisible by $p$, so $\gcd(c, p) = 1$, from which we find that there are integers $u$ and $v$ such that $cu + pv = 1$, from which it follows that $cu \equiv 1 \bmod p$. Now suppose that $ac \equiv bc \bmod p$. It then follows that $acu \equiv bcu \bmod p$, from which it follows that $a \equiv b \bmod p$, since $cu$ is congruent to 1 mod $p$. We can solve equations $cx \equiv d \bmod p$ by multiplying both sides by $u$: from $cxu \equiv du \bmod p$ we deduce that $x = du$ will work because $cu$ is congruent to 1.

The solution of such equations when we are in a modulus which is not prime will be discussed in the next lecture.

# 8 Solving Equations in Modular Arithmetic

In this section we do some algebra in modular arithmetic. The results we get will be more familiar-looking if the modulus is prime.

## 8.1 Linear Equations in Modular Arithmetic

Solving an equation $ax + b \equiv c \bmod m$ reduces to solving $ax \equiv c - b \bmod m$, so it is enough to solve equations of the form $ax \equiv b \bmod m$.

We solve $ax \equiv b \bmod m$.

Let $g = \gcd(a, m)$.

Note first that if $ax \equiv b \bmod m$ then there is $k$ such that $ax + km = b$, and it follows that there can be no solution to the congruence unless $g|b$, since clearly $g|ax + km$ for any $x$ and $k$.

So suppose that $g|b$, so $gh = b$ for some integer $h$. We know by a theorem proved earlier that there are integers $u$ and $v$ such that $au+mv = g$. Multiply both sides of this equation by $h$ to get $auh + mvh = gh = b$. $x = uh$ gives us a solution to the equation.

The solution is not unique. Suppose $ax \equiv ay \equiv b \bmod m$. It follows that $m|(ax - ay) = a(x - y)$. If $a$ had no common factors with $m$, it would follow that $m|(x - y)$ which would imply the uniqueness of the solution up to congruence mod $m$. In the more general situation, we analyze things as follows. $a = a'g$ and $m = m'g$ where $a'$ and $m'$ have no common factors. $m'g|a'g(x - y)$ implies $m'|a'(x - y)$ which implies (since $m'$ and $a'$ have no common factors) that $m'|(x - y)$. Moreover, if we have $ax \equiv b \bmod m$ then we will also have $a(x + km') \equiv b \bmod m$, because $a(x + km') = ax + akm' = ax + a'gkm' = ax + a'km$, which is congruent to $ax$ mod $m$. $x + km' \equiv x + nm' \bmod m$ iff $(k - n)m'$ is divisible by $m$, which will be true iff $k - n$ is divisible by $g$, that is, iff $k \equiv n \bmod g$. So there are $g$ solutions up to congruence mod $n$, obtained by plugging in $0, 1, \ldots, g-1$ in for $k$ in $x+km'$.

We summarize the solution. If $\gcd(a, m) \not| b$, then there is no solution to the congruence. If $\gcd(a, m)|b$, find $u$ and $v$ such that $au + mv = \gcd(a, m)$. $\frac{ub}{\gcd(a,m)}$ is a solution to the congruence, and the full set of $\gcd(a, m)$ distinct solutions up to congruence mod $m$ is obtained as $\frac{ub}{\gcd(a,m)} + \frac{km}{\gcd(a,m)}$ where $0 \leq k < g$.

## 8.2 Roots of Polynomials in Modular Arithmetic

In this subsection we prove that in mod $p$ arithmetic, where $p$ is prime, a polynomial of degree $d$ has no more than $d$ incongruent solutions. This is analogous to a familiar result about factoring polynomials in the reals.

Suppose otherwise. Then there will be a polynomial $F(x)$ of smallest degree $d$ for which this fails (i.e., a degree $d$ polynomial with at least $d+1$ distinct roots (roots no two of which are congruent mod $p$).

For any fixed $r$, $F(x) - F(r)$ can be factored. $F(x)$ is a sum of terms $a_n x^n$ for $n \leq d$, and $F(x) - F(r)$ is a sum of terms $a_n(x^n - r^n)$, and $x - r$ is a factor of $x^n - r^n = (x-r)(x^{n-1} + x^{n-2}r + \ldots + xr^{n-2} + r^{n-1})$. But this means that $F(x) = (x-r)G(x)$ where $G(x)$ is some polynomial of degree $d-1$ (whose exact shape depends on $r$). Now let $r$ be a root $r_1$ of $F(x)$ and let $s$ be any other root of $F(x)$. $F(s)$ is congruent to 0 mod $p$ (because it is supposed to be a root); $F(s) = (s-r)G(s)$: $s - r$ is not divisible by $p$ so $G(s)$ must be, so every root of $F(x)$ other than $r$ is a root of $G(x)$, so this $d-1$ degree polynomial has $d$ roots, which means that $d$ was not the smallest degree of a counterexample, which is a contradiction.

Notice that at a crucial point the argument depended on $d$ being a prime. We should go hunting for counterexamples in composite moduli.

I construct an example with too many roots to a polynomial $x^2 - a$. Suppose $x$ and $y$ are both roots to $x^2 - a$. Then $x^2 - y^2 = (x-y)(x+y) = 0$, and in the real world we use the Zero Property to conclude that either $x+y = 0$ or $x - y = 0$, so $x = \pm y$ and there are no more than two solutions. But in modular arithmetic we can arrange for bad things to happen. Set $x = 2$, $y = 4$ and set the modulus $m$ to $(4-2)(4+2) = 12$. What I have done is forced $4^2 = 2^2$ in mod $m$. And indeed in mod 12 arithmetic, $2^2 = 4^2 = 4$ and moreover the additive inverses of 2 and 4 have the same square for the usual algebraic reason, so $2^2 = 4^2 = 8^2 = 10^2 = 4$, and $x^2 - 4$ has four roots in mod 12 arithmetic! This is a concrete example but should suggest a general technique.

## 8.3 Exercises (assigned 2/2/2018 and due 2/9/2018)

8.3, 8.4 (optional and fun), 8.5, 8.7 (optional), 8.9, 8.10 (hint, think about my method for getting more than two square roots that I demonstrated in class)

# 9 Theorems about Modular Exponentiation: Fermat's Little Theorem and Euler's Theorem

This section has a variety of things in it, generally having to do with computing exponentiation in modular arithmetic: $a^b = ???\,\texttt{mod}\,m$

## 9.1 Computing Exponentials using Repeated Squaring

It is true that $a \equiv b \,\texttt{mod}\, m$ implies $a^n \equiv b^n \,\texttt{mod}\, m$, but it is **not** true that $a \equiv b \,\texttt{mod}\, m$ and $p \equiv q \,\texttt{mod}\, m$ imply $a^p \equiv b^q \,\texttt{mod}\, m$: you can reduce the base of an exponentiation problem in mod $m$ arithmetic to its remainder on division by $m$, but you cannot do this with the exponent.

Nonetheless, we can compute $a^n \,\texttt{mod}\, m$ fairly efficiently: my algorithm for doing this is to write the sequence of numbers $n_i$ where $n_1 = n$ and $n_{i+1} = n_i\texttt{div2}$. Of course some $n_k = 1$. $k$ will be approximately the base 2 logarithm of $n$. Now it is clear that we can compute $a^{n_k}\texttt{mod}m = a\texttt{mod}m$ quite directly. When we have computed $a^{n_i}\texttt{mod}m$ we indicate how to compute $a^{n_{i-1}}\texttt{mod}m$: it is either the case that $n_{i-1} = 2n_i$ or $n_{i-1} = 2n_i + 1$. In the first case we compute $a^{n_{i-1}}\texttt{mod}m$ by squaring $a_{n_i}\texttt{mod}m$ and taking the remainder mod $m$. In the second case, we compute $a_{n_{i-1}}\texttt{mod}m$ by squaring $a_{n_i}\texttt{mod}m$, multiplying by $a$, then taking the remainder mod $m$. At each step we deal with no number larger than $m^3$, and we take a number of steps related to the logarithm to the base 2 of $n$ (so roughly proportional to the number of digits in $n$), which means that we can compute $a^n\texttt{mod}m$ in situations where we absolutely would not wish to attempt to compute $a^n$ itself!

## 9.2 Fermat's Theorem and Euler's Theorem

**Theorem (Fermat's Little Theorem):** $a^{p-1} \equiv 1 \,\texttt{mod}\, p$, where $a$ is not divisible by $p$.

**Proof:** Consider all the nonzero remainders on division by $p$, the numbers $1, 2, 3, \ldots, p-1$. Now consider the numbers obtained by multiplying each of these by $a$ in mod $p$ arithmetic, namely $a, 2a, 3a, \ldots, a(p-1)$ (really, $a\texttt{mod}p, 2a\texttt{mod}p, (p-1)a\texttt{mod}p$). Because we are in a prime modulus, the numbers in the second list are all distinct mod $p$ and so

are in fact exactly the same numbers in a different order. The product of the numbers in the first list is $(p-1)!$. The product of the numbers in the second list is $a^{p-1}(p-1)!$. We thus have $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$. Since $p$ is prime it shares no factors with $(p-1)!$, so $a^{p-1} \equiv 1 \bmod p$ follows by the cancellation property of multiplication in prime moduli.

**Alternative Proof:** Here is another quite different proof of Fermat's Little Theorem. The number of open chains of $p$ beads of $a$ colors (where we do have a distinguished beginning and end of the chain) is $a^p$. We consider counting closed necklaces of $p$ beads of $a$ colors, where we do not care about where we start on a necklace or which direction we go on it (we are allowed to flip a necklace over and consider it the same necklace).

There are $a$ monochromatic necklaces, each of which corresponds to exactly one open chain.

Ecah non-monochromatic necklace corresponds to either $p$ or $2p$ open chains, depending on whether it is symmetric or not. But this means that the size $a^p - a$ of the collection of non-monochromatic open chains is divisible by $p$, from which it follows that $a^p \equiv a \bmod p$ from which it further follows if $a \not\equiv 0 \bmod p$ that $a^{p-1} \equiv 1 \bmod p$, which is what was to be proved.

**Annoying question:** Is there a similar counting argument for Euler's theorem presented below? Counting necklaces of composite length is a much harder problem, as repetitive patterns in chains then come into play.

**Observation about exponentiation:** It is not true that exponentiation is well-defined in modular arithmetic: it is not true that $a = a' \bmod m$ and $b = b' \bmod m$ imply $a^b = a'^{b'} \bmod m$. But it is true for a prime $p$ that $a = a' \bmod p$ and $b = b' \bmod p - 1$ imply $a^b = a'^{b'} \bmod p$: one uses a different modulus for the exponent.

There is a similar result for composite moduli, which requires a new concept. Note first that if we are to have $a^n \equiv 1 \bmod m$ that $a^n$ is relatively prime to $m$, and so of course is $a$. Fix an $a$ which is relatively prime to $m$. Now list all the numbers $b_1, b_2, \ldots, b_n$ which are greater than 0, less than $m$ and relatively prime to $m$. Then list all the numbers $ab_1, \ldots, ab_n$ (in the sense

of mod $m$ arithmetic: one really lists $ab_1 \texttt{mod} m, \ldots, ab_n \texttt{mod} m$). The numbers $ab_1, \ldots, ab_n$ are each relatively prime to $m$ and are distinct from one another mod $m$, and so must be exactly the same numbers that were on the original list (up to congruence). So $b_1 \cdot \ldots \cdot b_n$ is congruent to $a^n(b_1 \cdot \ldots \cdot b_n)$ mod $m$, and since $b_1 \cdot \ldots \cdot b_n$ is relatively prime to $m$, we can cancel and obtain $a^n \equiv 1 \,\texttt{mod}\, m$. All that remains is to talk about what the exponent $n$ is: it is simply the number of remainders mod $m$ which are relatively prime to $m$, and we call it the Euler $\phi$ function and denote it by $\phi(m)$. The theorem then is that

**Euler's Theorem:** If $a$ is relatively prime to $m$, $a^{\phi(m)} \equiv 1 \,\texttt{mod}\, m$.

About the Euler $\phi$ function, we will hear much more.

One doesn't immediately get such a nice theorem about modular exponentiation for composite moduli, because one has to worry about bases $a$ which are not relatively prime to $m$: in the prime case, the only such modulus is 0, and for 0 the theorem stated above is true.

## 9.3 Computing the Euler $\phi$ function, and the Chinese Remainder Theorem

The formal definition of the Euler $\phi$ function is

**Definition:** For any natural number $m$,

$$\phi(m) = |\{a : 0 < a < m \wedge \texttt{gcd}(a, m) = 1\}|,$$

the size of the set of remainders mod $m$ which are relatively prime to $m$.

It is possible to compute the value of $\phi(m)$ given the prime factorization of $\phi$. The reason for this is that it is easy to compute $\phi(p^k)$ and $\phi$ has a number-theoretic property which is important enough to have a name:

**Definition:** A function $f$ with domain the natural numbers is *multiplicative* iff $f(mn) = f(m)f(n)$ whenever $\texttt{gcd}(m, n) = 1$.

**Lemma 1:** $\phi(p^k) = p^k - p^{k-1}$ for any prime $p$ and natural number $k$.

**Proof:** The remainders mod $p^k$ which are not relatively prime to $p^k$ are the ones which are divisible by $p$, and there are $p^{k-1}$ of these, so there are $p^k - p^{k-1}$ remainders mod $p^k$ which are relatively prime to $p^k$.

**Lemma 2:** $\phi$ is multiplicative.

**Proof** : Let $\texttt{gcd}(m, n) = 1$. We show the result by exhibiting a set of size $\phi(m, n)$ and a set of size $\phi(m)\phi(n)$ and a bijection between them.

The set of size $\phi(mn)$ is the obvious one, the set of remainders mod $mn$ which are relatively prime to $mn$.

The set of size $\phi(m)\phi(n)$ is also the obvious one: it is the set of all pairs $(b, c)$ where $b$ is a remainder mod $m$ which is relatively prime to $m$ (there are $\phi(m)$ of these) and $c$ is a remainder mod $n$ which is relatively prime to $n$ (there are $\phi(n)$ of these). This set is of size $\phi(m)\phi(n)$ because it is the cartesian product of a set of size $\phi(m)$ and a set of size $\phi(n)$.

The function which we claim is a bijection is the map which sends a remainder $a$ in the first set to the pair $(a\texttt{mod}m, a\texttt{mod}n)$. Notice that if $a\texttt{mod}m$ had a common factor with $m$, $a$ would have a common factor with $m$, and so $a$ would have a common factor with $mn$, which is impossible, and similarly $a\texttt{mod}n$ cannot have a common factor with $n$: if $a$ is in the first set, $F(a)$ is in the second set.

Now we argue that $F$ is one-to-one: suppose $F(a) = F(a')$: we need to show that $a = a'$ follows. Since $F(a) = F(a')$ we have $a\texttt{mod}m = a'\texttt{mod}m$ and $a\texttt{mod}n = a'\texttt{mod}n$, so $a - a'$ is divisible by both $m$ and $n$. But since $m$ and $n$ are relatively prime, this implies that $a - a'$ is divisible by $mn$, and since it is less than $mn$ in absolute value it must be 0, so $a = a'$.

Now we argue that $F$ is onto: Given $(b, c)$ in the second set, we want to find $a$ in the first set such that $F(a) = (b, c)$, that is, $a\texttt{mod}m = b$ and $a\texttt{mod}n = c$. We show that this pair of simultaneous equations has a solution. Because $a\texttt{mod}m = b$, we can write $b + mk = a$. We then need to solve $b + mk\texttt{mod}n = c$, for which it is sufficient to solve $mk \equiv c - b \,\texttt{mod}\, n$. Let $m^{-1}\texttt{mod}n$ denote the multiplicative inverse of $m$ in mod $n$ arithmetic (which exists because $m$ and $n$ are relatively prime). We can then solve for $k$ as $(m^{-1}\texttt{mod}n)(c - b)$ and for $x$ as $b + m(m^{-1}\texttt{mod}n)(c - b)$, which is clearly congruent to $b$ mod $m$ and to $b + 1(c - b) = c$ mod $n$.

The result that $F$ is a bijection is usually called the Chinese Remainder Theorem, and we give it separately:

**Chinese Remainder Theorem:** If $\texttt{gcd}(m, n) = 1$, then any system of equations

$$x \equiv a \bmod m$$

$$x \equiv b \bmod n$$

has a unique solution up to congruence mod $mn$.

It should now be clear that we can compute $\phi(m)$ for any $m$ directly from the prime factorization of $m$. Note the method for computing $\phi(m)$ which you are supposed to verify in problem 11.3: if $p_1, \ldots, p_n$ are the primes going into $m$, $\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_n})$.

## 9.4 Exercises – assigned 2/11/2018, due next Friday, 2/16/18.

A Test is planned for 2/23/2018.

9.1, 9.2 and 9.3 (9.2 and 9.3 both optional investigations), 10.1 (think about reciprocals in modular arithmetic), 11.3, 11.5, 11.6 and11.7 (both optional but fun), 11.11, 16.2 (optional but recommended) , 16.3.

As I am developing the test, I may decide to recommend additional exercises for test review!

# 10 Finding $k$th roots mod $m$ and the RSA algorithm

We have seen above how we can very efficiently compute $a^k \bmod m$ for any reasonable $a, k, m$ using repeated squaring.

We now look into finding $k$th roots, that is, solving equations $x^k = a \bmod m$. We will be able to do this in many interesting cases, but we will find that conditions are not ideal.

Suppose that $\texttt{gcd}(a, m) = 1$ and $\texttt{gcd}(k, \phi(m)) = 1$. We can find $s$ such that $sk \texttt{mod} \phi(m) = 1$ (multiplicative inverses exist in any modular arithmetic for numbers relatively prime to the modulus). We claim that $a^s$ is a solution to our equation, a $k$th root of $a$ mod $m$. For $(a^s)^k \texttt{ mod } m = a^{sk} \texttt{ mod} m = a^1 \texttt{ mod } m = a \texttt{ mod } m$. The fact that $\gcd(a, m) = 1$ is used to ensure that $sk \equiv 1 \texttt{ mod } \phi(m)$ implies $a^{sk} \equiv a^1 \texttt{ mod } m$ by Euler's Theorem.

Efficient computation of these roots is blocked by the fact that $\phi(m)$ is not easy to find for large numbers, as prime factorizations are not easy to find.

We now describe the RSA algorithm.

The public information which you distribute for RSA encryption is a large number $N$ and an exponent $r$. Individual blocks of a message to you are to be encrypted thus $M' = M^r \texttt{ mod } N$. This can be computed by repeated squaring.

The secret information you have is this. You know that $N = pq$, where $p, q$ are two large primes known only to you. Thus $\phi(N) = (p - 1)(q - 1)$ is again known only to you. You know that $\texttt{gcd}(r, \phi(N)) = 1$. You compute $s$ such that $rs = 1 \bmod (p - 1)(q - 1)$ (multiplicative inverse property in modular arithmetic) and you can then decrypt messages because $M'^s \texttt{ mod } N = (M^r)^s \texttt{ mod } N = M^{rs} \texttt{ mod } N = M \texttt{ mod } N$ by Euler's theorem as above.

As long as it is fairly easy to find huge primes and very hard to factor a large number which is a product of two primes, this gives a secure method of communication.

For examples, see the Sage file (once I have functions and examples ready).

# 11 Primality testing: testing with Fermat's theorem; Carmichael numbers; the Rabin-Miller test

Fermat's little theorem $a^{p-1} \equiv 1 \texttt{ mod } p$ (for $p$ prime) gives a test for compositeness: if $a^{m-1} \texttt{mod} m \neq 1$, then $m$ is composite! This isn't quite as good as it seems, as for many $a < m$ it may nonetheless be true that $a^{m-1} \texttt{mod} m = 1$, but it shows the potential for testing a number for compositeness when you have no idea what its factorization might be. The test example $2^{110} \texttt{ mod } 111 = 4$ shows that 111 is not prime (if we hadn't known this already!).

Fermat's little theorem does not give the best compositeness test, due to the existence of Carmichael numbers $m$, which have an unreasonably large number of $a < m$ such that $a^{m-1} \,\texttt{mod}\, m = 1$. Clearly if $a^{m-1} \equiv 1 \texttt{mod} m$, then $\texttt{gcd}(a, m) = 1$. A Carmichael number is a number $m$ such that for every $a < m$ with $\texttt{gcd}(a, m) = 1$, we have $a^{m-1} \,\texttt{mod}\, m = 1$.

561 is the smallest example of a Carmichael number. Since 561 has the small factor 3, there are lots of counterexamples to $a^{m-1} \,\texttt{mod}\, m = 1$, but a number with only very large prime factors has very few $a < m$ such that $\texttt{gcd}(a, m) \neq 1$: if such a number is a Carmichael number, it will give a very good impression of being prime by the Fermat test.

$561 = (3)(11)(17)$ is a Carmichael number because $a^{560} = 1 \bmod 3$ unless $3|a$, because $3 - 1 = 2|560$, $a^{560} = 1 \bmod 11$ unless $11|a$, because $11 - 1 = 10|560$, and $a^{560} = 1 \bmod 17$ unless $17|a$, because $17 - 1 = 16|560$, by applications of Fermat's Little Theorem. Fermat's Little Theorem tells us that for any $a$ relatively prime to 561, and so to 3,11,17, we have $a^{560} = 1 \bmod 3,11$, and 17, because 3-1, 11-1, and 17-1 all go into 560, and so $a^{560} = 1 \bmod 561$ by the Chinese Remainder Theorem. The reason that all of this works is that 3-1, 11-1, and 17-1 all go into 561-1 = 560. [This should now be correct, though rather repetitive!]

In general, if we have an $m$ such that for each of its prime factors $p$, we have $p^2 \not| m$ (so $p - 1|\phi(m)$) and $p - 1|m - 1$, then by the argument outlined above in the case of 561, $m$ will be a Carmichael number. The converse is also the case: all Carmichael numbers are like this (a fact which I may yet lecture; the proof is in the book, and will be supplied here if I lecture it). This is called Korselt's Criterion.

The book gives two different definitions of Carmichael number! In the problem where they first introduce them, they have given the one above. In the section they give as the defining condition $a^m \equiv a \texttt{mod} m$ for every $a$. I still have an open question in my mind about equivalence of this with the condition stated above – I gave an argument for it in class but I think it was wrong.

From the second definition, I can deduce readily that if $p^2|m$ ($p$ an odd prime) $m$ is not a Carmichael number. Let $p^{e+1}$ be the largest power of $p$ dividing $m$. We must have $p^{em} \equiv p^e$ by the second definition of Carmichael number. So $m$ goes into $p^{em} - p^e$, so $p^{e+1}$ goes into $p^{em} - p^e$, and $\frac{p^{em} - p^e}{p^{e+1}}$ differs from $p^{em-e-1}$ by $\frac{1}{p}$, which is only possible for an integer if $e = 0$, so the largest power of $p$ going into $m$ is $p$ itself.

I will return obsessively to the question of equivalence of the two definitions. The other part of the converse part of Korselt's Criterion is shown using the Primitive Root Theorem below.

We cast about for a better compositeness test. And lo, there is one.

**Theorem (Rabin and Miller):** If $p$ is an odd prime and $p-1 = 2^k q$ with $q$ odd, and $p \not| a$, then either $a^q = 1$ mod p or $a^{2^i q} = -1$ mod $p$ for some $i$ with $0 \leq i < k$.

**Proof:** We know that $a^{p-1} = a^{2^k q} = 1$ mod $p$ by Fermat's Little Theorem. The sequence of numbers $a^q, a^{2q}, a^{4q}, \ldots, a^{2^i q}, \ldots, a^{2^k q} = a^{p-1} = 1$ mod p is generated by repeated squaring. A 1 in this sequence must be preceded either by a 1 or a $-1$ (by the prime modulus polynomial roots theorem). There is a 1 in the sequence (the last term) so either a 1 or a -1 appears among the earlier terms of the sequence. The only way that no -1 will appear is if the first term is 1. This completes the proof.

This gives us the Rabin-Miller test for compositeness: if $m$ is odd and $m-1 = 2^k q$ with $q$ odd, and $a^q \neq 1$ mod $m$ and no $a^{2^i q}$ for $0 \leq i < k$ is equal to $-1$ mod $m$, then $m$ is composite. An $a$ for which this test shows that $m$ is composite is called a Rabin-Miller witness for $m$. There is no analogue to Carmichael numbers for this test: if $m$ is composite, at least three-quarters of positive $a < m$ are witnesses to $m$ being composite by the test above.

Repeated application of this test to a number $m$ for random $a < m$ will give rapidly increasing probabilities that $m$ is in fact prime. Primes are fairly common: near a large number $N$, roughly one in $\ln(N)$ numbers is prime. So if one chooses a number near $10^{100}$ (whose natural logarithm is about 300) and applies 50 iterations of the Rabin-Miller test to each successive odd number (going up by 2 each time you get compositeness confirmed) you will fairly rapidly find a number that you can be essentially certain is prime (within about 300 numbers). Do this twice and you have a nice candidate for an RSA key $N$. Watch for implementations in my Sage project!

# 12 The effectiveness of the Rabin-Miller test (a coming attraction, but not yet)

I am going to read and lecture on a proof that at least 75 percent of numbers $a$ less than a composite odd $m$ are Rabin-Miller witnesses for $m$. Not until later – a lot of prerequisites!

# 13 Exercises assigned (a little belatedly) 2/18/2018

Due Friday 2/30/2015, a week after the test. I'll have more to say about some parts (notably the Carmichael numbers), and I will be introducing my computer functions to assist with these, I hope on Wednesday.

17.1, 17.2, 17.3a (parts b and c optional: I have never quite been able to prove the part b result to my own satisfaction, and I may work on this term.), 17.5 (optional), 18.1, 18.4 (optional), 19.2 (I dont know the answer!), 19.3, 19.4, 19.7, 19.8 (optional, easy with my Sage functions)

Practice some of these calculations manually or with a TI-89. Your own computer programs to execute these processes, in whatever language, would be of interest to me. I fyou write your own code, please attach it to your paper.

# 14 Mersenne primes and perfect numbers

## 14.1 Mersenne primes

We ask the question, what primes are of the form $a^n - 1$?

The key to answering this question is the factorization rule $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$. If $n \geq 2$ (which is required for the question to be interesting) the second factor is at least 2, so the only hope for such a difference to be prime is for $a - b$ to be 1. In the case of $a^n - 1$, this means that for this difference to be prime, we must have $a = 2$.

**Definition:** A *Mersenne prime* is a prime of the form $2^n - 1$.

Notice that if $n$ is composite, say $n = ab$ (neither $a$ nor $b$ being 1), $2^{ab} - 1$ is a composite number, divisible by $2^a - 1$ because it is the difference of the $b$th powers of $2^a$ and 1. The same factoring rule is at work.

So every Mersenne prime is of the form $2^p - 1$ where $p$ is prime. Not all numbers of this form are prime (many are composite) and it is an open question whether there are infinitely many Mersenne primes.

## 14.2 Perfect numbers

The Mersenne primes have an intimate relation to the ancient mathematical problem of *perfect numbers*

**Definition:** A number is perfect if it is the sum of its proper divisors. Examples are 6=1+2+3 and 28=1+2+4+7+14.

Euclid gives a proof of the following proposition.

**Theorem:** If $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number.

**Proof:** It is more convenient to add up *all* the divisors of the number $n = 2^{p-1}(2^p - 1)$ and verify that you get $2n$. The divisors are the numbers of the form $2^i$ for $0 \leq i \leq (p-1)$, which add up to $2^p - 1$ (geometric series formula) and the numbers of the form $2^i(2^p - 1)$ for $0 \leq i \leq (p-1)$ which add up to $(2^p - 1)(2^p - 1)$. Now $(2^p - 1) + (2^p - 1)(2^p - 1) = 2^p(2^p - 1) = 2n$. This completes the proof.

Euler proved the following converse

**Theorem:** Every even perfect number is of the form $2^{p-1}(2^p - 1)$ where $2^p - 1$ is prime.

**Proof:** This proof has independently interesting concepts embedded in it.

**Definition:** $\sigma(n)$ is defined as the sum of all the divisors of $n$.

**Observation:** $n$ is perfect iff $\sigma(n) = 2n$.

**Lemma:** $\sigma(p^k) = 1 + p + \ldots + p^k = \frac{p^{k+1}-1}{p-1}$ by the geometric series formula. If $\texttt{gcd}(m, n) = 1$ then $\sigma(mn) = \sigma(m)\sigma(n)$. A quick idea of why this latter formula is true is this: the product of the sum of all the factors of $m$ and the sum of all the factors of $n$ is the sum of all products $ab$ where $a|m$ and $b|n$. Every such product $ab$ is a factor of $mn$ (this is obvious): because $m$ and $n$ have no common factors, it is pretty clear that each factor of $mn$ appears

once in this sum so it is also equal to $\sigma(mn)$. This would fail if $m, n$ were not relatively prime because some factors of $mn$ could then be written in more than one way as a factor of $m$ times a factor of $n$. I may assign an actual proof of this lemma.

Suppose that $n$ is an even perfect number. We can write $n$ in the form $2^k q$ where $k \geq 1$ and $q$ is odd.

We have $2n = \sigma(n) = \sigma(2^k)\sigma(q) = (2^{k+1} - 1)\sigma(q)$.

Since $(2^{k+1} - 1)$ is odd, we must have $2^{k+1} | \sigma(q)$, so for some integer $c$ we have $\sigma(q) = 2^{k+1}c$.

$2n = \sigma(n) = \sigma(2^k)\sigma(q) = (2^{k+1} - 1)\sigma(q) = (2^{k+1} - 1)2^{k+1}c$.

If $c = 1$ we have $2n = (2^{k+1} - 1)\sigma(q) = (2^{k+1} - 1)2^{k+1}(1)$ from which we can conclude $n = 2^k(2^{k+1} - 1)$ whence $q = 2^{k+1} - 1$, and $\sigma(q) = 2^{k+1}(1) = q + 1$ from which it follows that $q = 2^{k+1} = 1$: if $c = 1$ the even perfect number is of the claimed form $2^{p-1}(2^p - 1)$ where $p = k+1$, and $(2^p - 1)$ is prime as claimed.

If $c > 1$, observe that $2n = \sigma(n) = \sigma(2^k)\sigma(q) = (2^{k+1} - 1)\sigma(q) = (2^{k+1} - 1)2^{k+1}c$ implies that $2^k q = n = (2^{k+1} - 1)2^k c$, so $q = (2^{k+1} - 1)c$ so $c | q$.

Thus $\sigma(q) \geq 1 + c + q = 1 + c + (2^{k+1} - 1)c = 1 + 2^{k+1}c = 1 + \sigma(q) > \sigma(q)$ which is absurd.

**Question:** Euler and Euclid together completely settle the question of what the even perfect numbers are (mod identifying Mersenne primes). Are there any odd perfect numbers? No one knows; if there are, they are very large.

## 14.3 A little more about perfect numbers

**Theorem:** The base 10 representation of any even perfect number ends with 6 or 8.

**Proof:** Such a number is of the form $2^{p-1}(2^p - 1)$. The powers of 2 in mod 10 arithmetic are 1,2,4,8,6,2,4,8,6,2,4,8,6,... So in mod 10 arithmetic we are looking at (2)(4-1) = 6 or (4)(6-1) = 0 or (6)(4-1)=8 (a pair of consecutive powers of 2 will be 2,4 or 4,6 or 6,2 in mod 10). The only way that $2^{p-1}(2^p - 1)$ could be divisible by 10 is if $2^p - 1$ were divisible

by 5, and 5 is not a Mersenne prime. So 6 and 8 are the only possible values (and we see both of them).

The question of whether there are any odd perfect numbers remains. We prove a theorem about odd perfect numbers.

**Theorem:** An odd perfect number must be of the form $p^{4m+1}q^2$, where $p$ is an odd prime of the form $4k+1$ and $q$ is an odd integer relatively prime to $p$.

**Proof:** Let $n$ be an odd perfect number. The prime factorization of $n$ can be written $p_1^{n_1}p_2^{n_2}\ldots p_k^{n_k}$. We know that $\sigma(n) = 2n$. Now $\sigma(n) = (1+\ldots+p_1^{n_1})(1+\ldots+p_2^{n_2})\ldots(1+\ldots+p_k^{n_k})$. A term $(1+\ldots+p_i^{n_i})$ is even iff $n_i$ is odd. So since $\sigma(n) = 2n$ has exactly one factor of 2 in its prime factorization ($n$ being odd) it follows that just one term $(1+\ldots+p_i^{n_i})$ is even, and that term is not divisible by 4. Without loss of generalization let $i = 1$: $n_1$ is then odd while all other $n_i$'s are even. In order to avoid $4|(1+\ldots+p_1^{n_1})$, we must have $p \equiv_4 1$ and also $n_i \equiv_4 1$: recall that $n_1$ is odd, and if $p_1$ is congruent to $-1$ mod 4 we get $1+p_1+\ldots p_1^{n_1-1}+p_1^{n_1}$ congruent to $1+(-1)+\ldots+1+(-1) \equiv 0$ mod 4, and if $p_1$ is congruent to 1 mod 4 we get a term congruent to 0 mod 4 if $n_1+1$ is divisible by 4, that is, if $n_1 \equiv_4 3$.

The desired odd prime $p$ is then $p_1$, $4m+1$ is $n_1$, and $q$ is $p_2^{\frac{n_2}{2}}\ldots p_k^{\frac{n_k}{2}}$

# 15 Primitive Roots in Prime Moduli

We interest ourselves in solutions to equations $a^n \equiv 1 \mathtt{mod} p$.

**Definition:** For any $a$, $m$ with $\mathtt{gcd}(a,p) = 1$, we define the order of $a$ in mod $p$ arithmetic (which we will write $o(a)$, leaving $p$ understood) as the smallest positive $k$ such that $a^k \equiv 1 \mathtt{mod} p$.

**Observation:** There is such an $k$: it is clear that for some two numbers $m > n$ we have $a^m \equiv a^n \mathtt{mod} p$ because there are only finitely many possible remainders mod $p$, and then we have $a^m \equiv a^n(a^{m-n}) \equiv a^n$, from which we have $a^{m-n} \equiv 1$ by multiplying both sides by the mod $p$ reciprocal of $a^n$.

**Lemma:** If $a^n = 1$ then $o(a)|n$.

**Proof of Lemma:** By the division algorithm, $n = o(a)q + r$ for some $q$ and some $r < o(a)$. Thus $a^n = a^{o(a)q+r} \equiv (a^{o(a)})^q a^r \equiv a^r$. Since $a^r \equiv 1$, we must have $r = 0$, because if $0 < r < o(a)$ $a^r$ cannot be 1 by definition of $o(a)$.

**Corollary:** By Fermat's Little Theorem, $o(a)|p-1$.

**Definition:** For each $d$, define $\psi(d)$ as the number of remainders $a$ mod $p$ which are of order $d$. We know that $\psi(d) = 0$ if $d$ is not a divisor of $p-1$.

**Observation:** For any $n$, the number of roots of $x^n - 1 \equiv 0 \mathtt{mod} p$ among the remainders mod $p$ is the sum of $\psi(d)$ over all divisors of $n$. This is true because any root of $x^n - 1 \equiv 0$ has $x^n \equiv 1 \mathtt{mod} p$ whence its degree goes into $n$.

**Lemma:** For any $n|p-1$, $x^n - 1 \equiv 0 \mathtt{mod} p$ has exactly $n$ roots.

**Proof of Lemma:** $x^{p-1} - 1 \equiv 0$ has exactly $p-1$ roots by Fermat's Little Theorem. If $p - a = mn$ then $x^{p-1} - 1 = x^{mn} - 1 = (x^n - 1)(x^{n(m-1)} + x^{n(m-2)} + \ldots + x^{n2} + x^n)$. Since we are in arithmetic in a prime modulus, we have the Zero Property, and any root of $x^{p-1} - 1$ in mod $p$ arithmetic is a root of one of the two factors. The first factor has no more than $n$ roots by our Polynomial Roots theorem for prime moduli; the second has no more than $n(m-1) = nm - n = (p-1) - n$ roots. But the total number of roots of the two factors must be exactly $p-1$, which is only possible of the first term has $n$ roots, the second has $(p-1) - n$, and they share no roots.

**Corollary of the Lemma:** The sum for all $d|n$ of $\psi(d)$ is $n$, for any $n|(p-1)$.

**Observation:** The assertion $\sum_{d|n} f(d) = n$ is actually a recursive definition of the function $f$ (if we assume it true for all $n$). To see this, rewrite it as $f(n) = n - \sum_{d|n \wedge d \neq n} f(d)$. Notice that this allows us to evaluate $f(1)$ as $1 - \sum_{d \in \emptyset} f(d) = 1 - 0 = 1$: this is the hardest case. In every other case, we can clearly compute $f(n)$ once we know all smaller values of $f$. The condition above shows us that $\psi$ coincides with this function $f$ on all divisors of $p-1$. So what is the function $f$?

**Theorem:** $\sum_{d|n} \phi(d) = n$, where $\phi$ is the Euler $\phi$ function ($\phi(n)$ is the size of the collection of natural numbers in the interval $[1, n]$ which are relatively prime to $n$).

$\phi(1) = 1$ and the sum over all the divisors $d$ of 1 if $\phi(d)$ is just $\phi(1) = 1$.

For any prime $p$, the sum over all divisors $d$ of $p^k$ of $\phi(d)$ is $\phi(1) + \phi(p) + \phi(p^2) + \phi(p^3) + \ldots + \phi(p^k) = 1 + (p-1) + (p^2 - p) + (p^3 - p^2) + \ldots + (p^k - p^{k-1})$, which is a telescoping sum: everything cancels but the final $p^k$ so the result holds for $p^k$.

If $\texttt{gcd}(m, n) = 1$, the product of the sum over all divisors $d$ of $m$ of $\phi(d)$ and the sum over all divisors $d$ of $n$ of $\phi(d)$ is the sum over all divisors $d$ of $mn$ of $\phi(d)$:

$$\sum_{d|mn} \phi(d) = (1) \sum_{d_1|m, d_2|n} \phi(d_1 d_2)$$

$$= (2) \sum_{d_1|m, d_2|n} \phi(d_1)\phi(d_2) = (3)(\sum_{d_1|m} \phi(d_1)) \cdot (\sum_{d_2|n} \phi(d_2))$$

Thus if we have $\sum_{d_1|m} \phi(d_1)) = m$ and $\sum_{d_2|n} \phi(d_2) = n$ we have $\sum_{d|mn} \phi(d) = mn$.

Equation 1 holds because each $d|mn$ can be expressed as a product of $d_1|m$ and $d_2|n$ in exactly one way (I suggest writing out a proof of this). Equation 2 holds because the Euler function itself is multiplicative. Equation 3 holds by many applications of the distributive law.

Anything which is true for 1, for powers of primes, and is true for the product of a pair of relatively prime numbers if it is true for the two numbers is true for all numbers (by the prime factorization theorem).

**Theorem:** For each $d|p-1$, $\psi(d) = \phi(d)$.

**Proof of Theorem:** This follows from the previous theorem and the preceding Observation directly.

**Definition:** $a$ is a *primitive root* for $p$ iff the order of $a$ in mod $p$ arithmetic is $p - 1$. Notice that this implies that all nonzero remainders mod $p$ are powers of $a$ in mod $p$ arithmetic.

**Corollary (Primitive Root Theorem):** There is a primitive root for every prime $p$. In fact, there are $\phi(p-1)$ primitive roots for $p$.

We give one application, proving part of Korselt's Criterion which we did not prove correctly in class. Suppose that $m$ is a Carmichael number. We want to show that for any prime $p|m$ we have $p-1|m-1$. Let $a$ be relatively prime to $m$ *and a primitive root for* $p$ (this is the essential missing ingredient. We can do this because we can choose $m$ to be equal to a primitive root mod $p$ and then equal to 1 mod each other prime factor of $m$ by the CRT.) We have $a^{m-1} \equiv 1 \bmod m$ because $m$ is a Carmichael number. We then have $a^{m-1} \equiv 1 \bmod p$. Now **because $a$ is a primitive root so its order goes into** $m-1$ we can conclude $p-1|m-1$.

## 15.1 An application of the Primitive Root Theorem: safe primes and the El Gamal cryptosystem

Although for any odd prime $p$ there are $\phi(p-1)$ generators (a lot of them) it is actually rather hard to identify a generator for a general prime $p$.

The characteristic a generator needs to have is that $g^d \not\equiv_p 1$ for each proper divisor $d$ of $p-1$. This is straightforward to check...if you know the factorization of $p-1$, and finding that is in general quite a hard problem.

However, it is easy to find a generator for an odd prime $p$ of the form $2q+1$ where $q$ is prime. Such primes $p$ are called *safe primes*, and they are fairly easy to find computationally (in the vicinity of a large number $N$, about in in every $\ln(N)^2$ numbers will be a safe prime, or so we guess on the assumption that primes are distributed fairly randomly).

If $p$ is a safe prime, then $p = 1 = 2q$. A number$g$ between 2 and $p-2$ (inclusive) will be a generator iff $g^q \not\equiv_p 1$ (it will be $-1$, can you see why?). $p-1$ is ruled out because it is the only residue mod $p$ which is of order 2.

An application of safe primes and the ability to compute generators for them is the El Gamal public key cryptosystem, which we now describe.

Let $p$ be a large safe prime (my son tells me that 700 digits is the current state of the art: I think my Sage functions might take a while to find one).

Let $g$ be a generator for $p$ (identified using the procedure above: choose a random $g$ in $[2, p-2]$ and compute $g^q$ mod $p$ (recalling that $q = 2p-1$ is also prime): you have a 50 percent chance of getting 1 ($g$ is not a generator) or -1 ($g$ is a generator!).

Choose a random exponent $x$ less than $p-1$. $x$ is your private key. Compute $y = g^x \texttt{mod} p$ and supply $p, g$, and $y$ to the world as your public key.

If someone wishes to send you a message $M$, they compute a random number $r < p-1$ (which they use only once!) and send you the pair $(My^r \texttt{mod} p, g^r \texttt{mod} p)$. Notice that all the ingredients used are things you have made known to the world.

When you receive a message $(M_1, M_2)$, you compute $(M_1)((M_2)^x)^{-1} \texttt{mod} p$, and lo and behold, this is $M$.

We verify this. $(My^r)((g^r)^x)^{-1} \texttt{mod} p = (M((g^x)^r)((g^r)^x)^{-1} \texttt{mod} p = M \texttt{mod} p$ (presumably $M < p$ so this is simply $M$). It is worth noting that we can compute $(M_2^x)^{-1}$ by computing $M_2^{p-1-x}$: it can all be done with modular exponentiation without a separate step of computing a modular inverse. You should be able to verify this with some reasoning using Fermat's Little Theorem.

The reason that we believe this to be secure is that we believe that the *discrete logarithm problem* (finding $x$ given $g^x \texttt{mod} p$) is hard for large $p$. This is not a theorem: it is what is currently believed.

# 16 Exercises assigned 3/9/2018

Computer assignment: Please create a public key for yourself on the RSA system and on the ElGamal system and send them to me. I will post public keys for myself for both systems. Send me a message using each of the public keys I post. You may send me any integer as a message, but I will try to provide functions for translations from character strings to integers and back so that you can send me actual messages, this weekend, in the Sage project. The due dates for these activities are flexible, but get started on them.

Here is my public RSA key:

```
N=1158578239535814371728242725027210069219496
5163491261272377101209382678022050630045065066 19
7231120570388023589460469884035534325138525302 03
7264345694940772524281195509356174290011054338 80
625266197995857983

r=528039247239604140554813796777721818725103530
```

```
79807200403160934955517025668240778596447295403 9
74962442219337961003259765710010909491585638232 63
11947429908568798093527948216702687523432131918 2
17238045167443
```

Here is my ElGamal key (my son tells me it is not secure, but I think it would be a challenge for you to break it).

```
p=877057057304731785499646978 53
17847316475161855791457914477950607 79

g=113745909997444291047402158204
00718516078300120535164370850733347 7

y=831190032931693344127951428008 76
54276498731635553579795399619643 31
```

Here $p$ is my safe prime, $g$ is my generator, and $y = g^x \mathtt{mod} p$ is my public key. Of course I know $x$ and you don't (I hope!)

Problems from the book: 14.1, (14.2 opt), 14.3, (explore), 15.2,15.3, 15.8, 15.9 (optional – if you can do later parts I will be impressed), 27.1 (optional), 28.1, 28.2, 28.4 (do 28.4 for a prime other than 13 (and larger) since we did 13 in class), 28.5, 28.6 (opt ) There are several other exercises in 28 which would make good computer explorations.

This is due on Friday, March 16 (the problems from the book; the RSA messages are more flexible, and the problems from the book are flexible if I hear lots of distress – meaning active questions on Wednesday!).

Please read the proof of the Primitive Root Theorem in the notes, carefully, and tell me about any problems you have with it (either trouble you have understanding it or potential mental slips on my part!)

# 17 Quadratic Residues

We investigate perfect squares in mod $p$ arithmetic, where $p$ is an odd prime.

**Definition:** By a residue mod $p$ we simply mean a number $a$ with $0 < a < p$ (a residue is nonzero). A residue $a$ mod $p$ is a quadratic residue iff there is $x$ such that $x^2 \equiv a \bmod p$.

**Counting quadratic residues:** We show that there are $\frac{p-1}{2}$ quadratic residues mod $p$. Note that $a^2$ is congruent to $(p-a)^2$, so the squares of the numbers in the range $1, \ldots, \frac{p-1}{2}$ and in the range $\frac{p-1}{2}, \ldots, p-1$ make up the same set. This means there are no more than $\frac{p-1}{2}$ quadratic residues. Now observe that if $a$ is congruent to $b^2$, the numbers which have $a$ as a square in mod $p$ arithmetic are solutions to $x^2 - b^2 = 0$, which has the obvious solutions $b$ and $p - b$, one in the range $1, \ldots, \frac{p-1}{2}$ and one in the range $\frac{p-1}{2}, \ldots, p-1$, and by the Polynomial Roots theorem mod $p$ there are just these two roots. This shows that all the squares of numbers in the range $1, \ldots, \frac{p-1}{2}$ are distinct. So there are exactly $\frac{p-1}{2}$ quadratic residues, and exactly $\frac{p-1}{2}$ non-quadratic residues. We abbreviate quadratic residue as QR and non-quadratic residue as NR.

**Multiplication of residues and non-residues:** The product $ab$ of two quadratic residues is congruent to some $c^2d^2 = (cd)^2$ and so is a quadratic residue.

The product of a QR $a$ and an NR $b$ is an NR: suppose otherwise. Then we can choose $a$ congruent to $c^2$ and $b$ an NR such that $ab$ is a QR, so congruent to $d^2$ for some $d$. Then $b$ is congruent to $(ab)a^{-1}$ and so to $d^2(c^2)^{-1}$ and so to $(dc^{-1})^2$ which makes it a QR which is a contradiction.

The product of two NR's is a QR. Consider a fixed $a$ which is an NR. The products $a1, a2, \ldots, a(p-1)$ are congruent to $p-1$ distinct residues (all of them). The $\frac{p-1}{2}$ products of $a$ with QR's are NR's by the previous result. Since there are $\frac{p-1}{2}$ NR's, these products are all the NR's. So the $\frac{p-1}{2}$ remaining products of $a$ with NR's are the QR's.

**Definition (Legendre symbol):** We define $\left(\frac{a}{p}\right)$ as 1 if $a$ is a QR mod $p$ and $-1$ if $a$ is an NR. Note that the results above show that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. This follows much more directly from the following result.

**Euler's Criterion:** $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$. We prove this: Notice that because $(a^{\frac{p-1}{2}})^2 = a^{p-1} = 1 \bmod p$ by FLT, we have $a^{\frac{p-1}{2}}$ equal to 1 or $-1$. If $a = c^2$ is a QR, we have $a^{\frac{p-1}{2}} = (c^2)^{\frac{p-1}{2}} = c^{p-1} = 1 \bmod p$ by FLT. So all the QRs satisfy the Criterion: there are $\frac{p-1}{2}$ of these as we keep observing. Any number $x$ such that $x^{\frac{p-1}{2}}$ is equal to 1 is a root of

$x^{\frac{p-1}{2}} - 1 = 0$, which has no more than $\frac{p-1}{2}$ roots. But that means it has exactly $\frac{p-1}{2}$ roots, all the QR's. For any NR $a$, we have $a^{\frac{p-1}{2}}$ equal to 1 or $-1$, and we have just seen that it cannot equal 1 so it must equal $-1$. This completes the proof.

**is $-1$ a perfect square?:** We now investigate the question of whether $-1$ is a QR mod $p$. This will be true iff $(-1)^{\frac{p-1}{2}} = 1$, that is, iff $\frac{p-1}{2}$ is even, so for some $n$, we have $2n = \frac{p-1}{2}$, thus $4n = p - 1$, thus $p$ is of the form $4n + 1$, or more briefly, congruent to 1 mod 4. So $-1$ is a QR iff $p$ is congruent to 1 mod 4 and $-1$ is an NR iff $p$ is congruent to 3 mod 4.

**is 2 a perfect square?:** We further investigate the question of whether 2 is a QR mod $p$. We adapt the trick we used to prove the FLT.

Consider the product of all the even numbers from 2 to $p - 1$. Notice that this is $2^{\frac{p-1}{2}}(\frac{p-1}{2})!$ and the first factor is what interests us if we plan to apply Euler's Criterion.

We consider expressing the product of all the even numbers from 2 to $p - 1$ mod $p$ in a different way: we can express it as the product of all the even numbers $x$ less than or equal to $\frac{p-1}{2}$ and the numbers $-x$ (congruent to the actual even number $p-x$ in the original product) for even numbers greater than $\frac{p-1}{2}$ and no greater than $p-1$. The absolute values of these numbers $x$ and $-x$ are all the natural numbers, both even and odd, in the interval $(0, \frac{p-1}{2}]$, so that the same product is congruent to $(-1)$ to the power of (the number of even numbers in the interval $(\frac{p-1}{2}, p-1]$) times $(\frac{p-1}{2})!$.

There are $\frac{p-1}{2}$ numbers greater than $\frac{p-1}{2}$ and $\leq p - 1$. If $\frac{p-1}{2}$ is even, half of these are even, so the number we are interested in is $\frac{p-1}{4}$. If this is even, say $2m$, then $8m = p - 1$ so $p = 8m + 1$. If this is odd, say $2m + 1$, then $8m + 4 = p - 1$, so $p = 8m + 5$. If $\frac{p-1}{2}$ is odd, $\frac{1}{2}$ more than half of these are even so the number that interests us is $\frac{p+1}{4}$. If $\frac{p+1}{4} = 2m$, $8m = p+1$, so $p = 8m-1$. If $\frac{p+1}{4} = 2m+1$, $p+1 = 8m+4$, so $p = 8m + 3$. This allows us to determine whether 2 is a QR mod $p$ by considering the residue class of $p$ mod 8: if $p = 1$ or 7 (equivalently $-1$ mod 4, 2 is a QR, and otherwise it is not.

We now state the full Quadratic Reciprocity Theorem, two parts of which

we have proved, and discuss how to use it, deferring the Proof of the third part.

**Quadratic Reciprocity Theorem:** The Legendre symbol $\left(\frac{a}{p}\right)$, where $p$ is an odd prime, can be computed using the rule $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ and the following clauses (the first one is really not used until the generalization stated below is given).

1. $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \mathtt{mod} 4$; $\left(\frac{-1}{p}\right)$ = -1 iff $p \equiv -1 \mathtt{mod} 4$.
2. $\left(\frac{2}{p}\right) = 1$ iff $p \equiv 1 \mathtt{mod} 8$ or $p \equiv 7 \mathtt{mod} 8$; $\left(\frac{2}{p}\right)$ = -1 iff $p \equiv 3 \mathtt{mod} 8$ or $p \equiv 5 \mathtt{mod} 8$
3. $\left(\frac{q}{p}\right)$ (where $q$ is an odd prime) $= \left(\frac{p}{q}\right)$ iff $p \equiv 1 \mathtt{mod} 4$ or $q \equiv 1 \mathtt{mod} 4$; $\left(\frac{q}{p}\right)$ (where $q$ is an odd prime) $= -\left(\frac{p}{q}\right)$ iff $p \equiv 3 \mathtt{mod} 4$ and $q \equiv 3 \mathtt{mod} 4$

To compute $\left(\frac{a}{p}\right)$ ($a < p$, otherwise we replace it with $a \mathtt{mod} p$ first), factor $a$ into primes, notice that $\left(\frac{q^k}{p}\right)$ where $q$ is any prime will be 1 when $k$ is even and equal to $\left(\frac{q}{p}\right)$ when $k$ is odd. Use the second formula above to handle $q = 2$; use the third formula (flipping $\left(\frac{q}{p}\right)$ to $\pm\left(\frac{p}{q}\right)$ and then (since $p > q$) converting this to $\pm\left(\frac{p \mathtt{mod} q}{q}\right)$, factoring $p \mathtt{mod} q$ and continuing recursively!

Notice that this appears to require us to factor $a$ into primes. But in fact we don't have to!

**Definition:** Define $\left(\frac{a}{b}\right)$ where $b$ is an odd integer equal to $p_1 p_2 \ldots p_r$, a product of not necessarily distinct primes, as the product $\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_r}\right)$.

**Generalized QR Theorem:** The Legendre symbol $\left(\frac{a}{c}\right)$, where $c$ is an *odd integer*, can be computed using the rule $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$ and the following clauses This computation will agree with the one above when $c$ is prime.

1. $\left(\frac{-1}{c}\right) = 1$ iff $c \equiv 1 \mathtt{mod} 4$; $\left(\frac{-1}{p}\right)$ = -1 iff $c \equiv -1 \mathtt{mod} 4$.

2. $\left(\frac{2}{c}\right) = 1$ iff $c \equiv 1 \mathtt{mod} 8$ or $c \equiv 7 \mathtt{mod} 8$; $\left(\frac{2}{c}\right)$ = -1 iff $c \equiv 3 \mathtt{mod} 8$ or $c \equiv 5 \mathtt{mod} 8$
3. $\left(\frac{b}{c}\right)$ (where $b, c$ are odd and positive) $= \left(\frac{c}{b}\right)$ iff $b \equiv 1 \mathtt{mod} 4$ or $c \equiv 1 \mathtt{mod} 4$; $\left(\frac{c}{b}\right)$ (where $b, c$ are odd and positive) $= -\left(\frac{b}{c}\right)$ iff $b \equiv 3 \mathtt{mod} 4$ and $c \equiv 3 \mathtt{mod} 4$

Of course this generalization has to be justified. Once we know it works (to be explained) we can compute Legendre symbols without prime factorization of the top number. It still isn't clear to me why the first rule would ever have to be used, though certainly it might be useful.

# 18 A few more exercises (also assigned 3/10/2015):

20.1, [20.2/21.6(optional exploration)], 20.3, 21.1, 21.3, 21.5, 22.1, 22.2. This set is due Thursday before the break. It might be augmented with one or two more non-test-relevant questions after the Wednesday lecture.

# 19 Things to Come

My top level goals are to get to quadratic reciprocity and to get to the result about Rabin-Miller witnesses (and do other stuff, this probably won't take the whole rest of the term). I'm being very high level here because I'm not sure what Im going to start on on Wednesday. You are welcome to express a preference! I do still owe you some more details in the notes.

I omitted to give the proof in chapter 21 that there are infinitely many primes of the form $4n + 1$! It will appear! My immediate goal is to prepare and deliver a set piece lecture giving the proof of Quadratic Reciprocity. I am still **wrong** in my proof of the infamous 17.3b; I'm working on it!

# 20 Apology for being late!

I do apologize for getting behind on the notes!

# 21 There are infinitely many primes of the form $4n+1$

Recall that we proved above that there are infinitely many primes of the form $4n+3$; subtler methods are needed for the case of primes of the form $4n+1$.

Suppose that there are finitely many primes of this form, $p_1, \ldots, p_n$. Let $P = p_1 \cdot p_2, \ldots, \cdot p_{n-1} \cdot p_n$, the product of all the primes of the form $4n+1$.

Let $Q = (2P)^2 + 1$. $Q$ has no prime factor other than odd primes of the form $4n+3$, by construction. $Q$ does have some prime factor $q$. Now observe that $Q = (2P)^2 + 1 \equiv 0 \bmod q$, so $(2P)^2 \equiv -1 \bmod q$ so $-1$ is a quadratic residue mod $q$, so $q$ is of the form $4n+1$, which is a contradiction!

# 22 The proof of the third part of Quadratic Reciprocity

[3/10/2015: I believe I have corrected the typos. I still plan to try to amend the style a bit.]

The Third Part is expressible in this way:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Why does this say the same thing? $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ will be $-1$ (equivalently, $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ will have opposite signs) iff $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are both odd, which is equivalent to $p, q$ both being of the form $4n+3$.

Define $P$ as $\frac{p-1}{2}$ and $Q$ as $\frac{q-1}{2}$.

Define $\mu(a,p)$ as the cardinality of $\{i : 1 \leq i \leq P \wedge ai \bmod p > P\}$, or equivalently the size of the set of $i$'s between 1 and $P$ inclusive for which $ai$ becomes negative when reduced mod $p$ to a number between $-P$ and $P$ inclusive.

**Gauss's Criterion:** $\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$

**Proof:** Let $a$ not be divisible by $p$. We claim that the numbers $ai$ for $i$ between 1 and $P$ exclusive, when reduced mod $p$ to numbers between $-P$ and $P$ inclusive, all have distinct absolute values (so have all the absolute values from 1 to $P$).

Suppose that $ia = \pm ja$ for $i, j$ both between 1 and $P$ inclusive. $ia \pm ja$ is then divisible by $p$. Thus $p|i \pm j$ (as $p$ does not go into $a$). But the absolute values of both $i + j$ and $i - j$ are less than or equal to $\frac{P+1}{2} = p - 1$, so the only possibility is $i = j$.

Now the product $a \cdot 2a \cdot \ldots \cdot Pa$ is equal to $a^P P!$.

It is also equal mod $p$ to a product $(\pm 1)(\pm 2)\ldots(\pm P)$ where the number of minus signs is $\mu(a, p)$. Thus $a^P P! \equiv (-1)^{\mu(a,p)} P!$ in mod $p$ arithmetic, and since $P!$ is not divisible by $p$ we can cancel to obtain Gauss's Criterion.

**Weird Lemma (Eisenstein):** Let $p$ be an odd prime. Let $P = \frac{p-1}{2}$. Let $p$ not go into the odd number $a$. It follows that $\sum_{k=1}^{P} \lfloor \frac{ka}{p} \rfloor \equiv \mu(a, p) \bmod 2$.

**Proof:** Write each $ka$ as $q_k p + r_k$ with $r_k$ between $-P$ and $P$ inclusive.

$\frac{ka}{p} = q_k + \frac{r_k}{p}$ where $|\frac{r_k}{p}| < \frac{1}{2}$.

$\lfloor \frac{ka}{p} \rfloor$ is $q_k$ if $r_k \geq 0$, $q_k - 1$ if $r_k < 0$.

Now we see that $\sum_{k=1}^{P} \lfloor \frac{ka}{p} \rfloor = \sum_{k=1}^{P} q_k - \mu(a, p)$

We have $ka = q_k p + r_k$ and both $a, p$ odd. Thus $k = q_k + r_k$ in mod 2 arithmetic.

$\sum_{k=1}^{P} k = \sum_{k=1}^{P} r_k$ in arithmetic mod 2, because these are the same sum in a different order if minus signs are dropped (this is an appeal to the point already established under Gauss's criterion that the first $P$ multiples of $a$, when shoved into $[-P, P]$, all have different absolute values, so the numbers which occur as $r_k$'s are just the numbers from 1 to k, sometimes adorned with minus signs), and in mod 2 minus signs can be dropped.

$\sum_{k=1}^{P} k = \sum_{k=1}^{P} q_k + r_k \mod 2$ implies that $\sum_{k=1}^{P} q_k = 0 \mod 2$, so $\sum_{k=1}^{P} \lfloor \frac{ka}{p} \rfloor = \sum_{k=1}^{P} q_k - \mu(a, p) = -\mu(a, p) = \mu(a, p)$ in arithmetic mod 2, which is what was to be shown.

We now prove the third part of the Quadratic Reciprocity theorem by counting points with positive integer coordinates with $x < \frac{p}{2}$ and $y < \frac{q}{2}$ (the points with integer coordinates in the interior of the rectangle aligned with the axes with opposite corners at the origin and at $(\frac{p}{2}, \frac{q}{2})$. It is clear that there are $PQ$ such points total.

We now consider the points below the diagonal $y = \frac{q}{p}x$. In the column for each value $x = k$ there are $\lfloor \frac{kq}{p} \rfloor$ points with integer coordinates. So there are $\sum_{k=1}^{P} \lfloor \frac{kq}{p} \rfloor$ total points below the diagonal. The same argument using rows $y = k$ shows that there are $\sum_{k=1}^{Q} \lfloor \frac{kp}{q} \rfloor$ points above the diagonal. There are no integer points on the diagonal, so $\frac{p-1}{2}\frac{q-1}{2} = \sum_{k=1}^{P} \lfloor \frac{kq}{p} \rfloor + \sum_{k=1}^{Q} \lfloor \frac{kp}{q} \rfloor$. Then by the weird lemma of Eisenstein, $\frac{p-1}{2}\frac{q-1}{2} \equiv \mu(q, p) + \mu(p, q) \mod 2$. From

this it follows that $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\mu(p,q)}(-1)^{\mu(q,p)} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$.

It is rumored that all proofs of this theorem have strange qualities.

# 23 Exercises, drafted 3/28/18

20.1, 20.2 (notice the hint about using a formula for the sum of the first $n$ squares), 20.3, 21.1, 21.5, 22.1 (remember my remarks in class about carefully documenting such calculations), 22.3, 22.7, 22.8. If you are tempted by another problem in these sections, feel free to try it (or them) out and report. I will award extra credit to anyone who comes up with a tidy Python implementation of the procedure for computing Legendre symbols using the Generalized QR Theorem before I release one (probably sometime in the second week after break).

I will probably release a new exponent part of my RSA public key, since I leaked the one I was using in class; in the meantime you are welcome to use the publicly posted one.

These problems are due notionally on the Friday after Spring Break (April 6th) though you are aware of my flexibility in these regards. Do start working on them!

# 24 Which natural numbers are sums of two squares?

We interest ourselves the question as to which numbers can be expressed as the sum of two squares.

You can verify the identity $(u^2+v^2)(A^2+B^2) = (uA+vB)^2+(vA-uB)^2$ algebraically. It is worth noting that this is equivalent to the assertion that the magnitude of the complex number $(u+vi)(A-Bi)$ is equivalent to the product of the magnitudes of the complex numbers $u+vi$ and $A+Bi$. This implies that if two numbers can each be expressed as the sum of two squares, their product can be expressed as the sum of two squares. In class I was concerned about the possibility that $vA-uB=0$: this can be resolved cheaply by stipulating that we count a square as a sum of two squares (one of them being $0^2$). Notice that when we show that primes of the form $4k+1$ are sums of two squares in this sense, we have actually shown that they are sums of two positive squares, since they are certainly not squares themselves!

Further, we observe that no number of the form $4n+3$ can be expressed as the sum of two squares. For any square is congruent to either 0 or 1 mod 4, and so any sum of squares is congruent to 0,1, or 2.

We now exhibit Fermat's method of descent. If $c$ is any number and $M$ is relatively prime to $c$, and we can express $Mc$ as the sum of two squares, and if $M \geq 2$, we show how to express $rc$ as the sum of two squares for some $r$ with $1 \leq r < M$.

We have assumed $A^2 + B^2 = Mc$.

Let $u \equiv A \bmod M$ and let $v \equiv B \bmod M$, with $-\frac{M}{2} \leq u, v \leq \frac{M}{2}$.

We show that $u^2 + v^2$ is divisible by $M$: $A^2 + B^2 = Mc$ is divisible by $M$ and $u^2 \equiv A^2$, $v^2 \equiv B^2 \bmod M$ are obvious.

Thus $u^2 + v^2 = rM$ for some $r$.

Now $(u^2 + v^2)(A^2 + B^2) = M^2rc$ so $(uA + vB)^2 + (vA - uB)^2 = M^2rc$

Notice that my resolution to accept sums of two nonnegative squares removes any need for me to worry about whether $|vA - uB|$ is nonzero.

$uA + vB \equiv A^2 + B^2 \equiv 0 \bmod M$ and $vA - uB \equiv BA - AB \equiv 0 \bmod M$

so $(\frac{uA+vB}{M})^2 + (\frac{vA-uB}{M})^2 = rc$

$r = \frac{u^2+v^2}{M} \leq \frac{(\frac{M}{2})^2+(\frac{M}{2})^2}{M} = \frac{M}{2}$

If $r = 0$ then $u^2 + v^2 = 0$ so $u, v = 0$ so $M$ goes into both $A$ and $B$, so $M^2$ goes into $A^2 + B^2 = Mc$, so $M|c$, which is only possible if $M = 1$, in which case $A^2 + B^2 = c$. In any case $M = 1$ is contrary to our assumption above.

What we have shown is that if we can express $Mc$ ($M$ relatively prime to $c$ and greater than 1) as a sum of two squares, then we can find $r \leq \frac{M}{2}$ greater than 0 such that $rc$ can be expressed as a sum of two squares.

Now we apply this to a special case.

If $p$ is a prime of the form $4n + 1$, then $-1$ is a quadratic residue mod $p$, so we have a number $x^2 + 1$ ($1 \leq x < P - 1$ which is a multiple of $p$, say $Mp$, and further $M = \frac{x^2+1}{p} \leq \frac{(p-1)^2+1}{p} < p$ (check the details yourself) so $M < p$ is relatively prime to $p$ because $p$ is prime. Now by descent since $Mp$ is a sum of two squares, so is $p$: we can repeat the application of descent as many times as desired, because if $M < p$ is relatively prime to $p$, so is $r < M < p$, and we must eventually arrive at $r = 1$.

If $n$ is divisible by a prime of the form $p = 4n + 3$ then if $n = x^2 + y^2$, $x$ and $y$ must have a common factor, and in fact must have a common factor of $p$. Suppose otherwise. If $n = x^2 + y^2$, $n$ is divisible by $p$ and neither $x$ nor $y$ is divisible by $p$, so $x^2 + y^2 = 0$ in mod $p$ arithmetic, while $x, y$ are not zero, so $1 + (yx^{-1})^2 = 0$ in mod $p$ arithmetic, so $(yx^{-1})^2 = -1$ in mod

$p$ arithmetic, which is impossible because $-1$ cannot be a quadratic residue mod $p$. This means that if any number $n$ with a factor $p = 4k + 3$, a prime, is written in the form $x^2 + y^2$, then $p$ is a factor of both $x$ and $y$, so $p^2$ is a factor of $n$, and further $\frac{n}{p^2} = (\frac{x}{p})^2 + (\frac{y}{p})^2$ is a sum of two squares as well. We can thus argue that no number of the form $Mp^{2k+1}$ (where $p$ does not go into $M$) can be a sum of two squares, if $p$ is of the form $4k + 3$: by applying the result above $k$ times (if we know that $Mp^{2k+1}$ is a sum of two squares, we use the previous argument to show that $\frac{Mp^{2k+1}}{p^2} = Mp^{2(k-1)+1}$ is a sum of two squares, and repeat), we see that $Mp$ must be a sum of two squares, and it is not divisible by $p^2$.

We can now state exactly which natural numbers can be expressed as the sum of two squares, by considering their prime factorizations. Each $p_i^{k_i}$ in the factorization must either have $k_i$ even or $p_i$ either $2 = 1^2 + 1^2$ or a prime of the form $4n + 1$.

This works based on two points: any prime of the form $4n + 1$ and so any product of primes of the form $4n + 1$ can be expressed as the sum of two squares, and so can 2. Further, any product of a sum of two squares and a square is the sum of two squares: $d^2(A^2 + B^2) = (dA)^2 + (dB)^2$. This is enough to see that any prime factorization in which all exponents on primes of the form $4n + 3$ are even can be expressed as a sum of two squares; we have seen above that if the exponent on a specific prime of the form $4n+3$ in the prime factorization is odd, the number cannot be a sum of two squares.

We further investigate the question of which numbers can be expressed as the sum of two positive squares. The product of two sums of positive squares can only fail to be a sum of two positive squares in the $vA - uB = 0$ case, in which the two sums must have a common divisor. This means that a product of distinct primes not of the form $4k + 3$ (this is carefully phrased to include 2 as a possibility) will be a sum of positive squares, and so any number obtained from such a number by multiplication by any perfect square is a sum of positive squares. The only numbers left which can be expressed as the sum of two non-negative squares but might not be expressible as sums of two positive squares are perfect squares all of whose prime factors are of the form $4k+3$. And indeed I can give an example: $49 = 7^2$ can be expressed as a sum of two non-negative squares, because it is a square, but cannot be expressed as a sum of two positive squares. I do not know a full solution to this question of which numbers can be expressed as the sum of two positive squares.

I include my example of the procedure of descent.

We set out to express 137, a prime of the form $4n+1$ as the sum of two squares.

Find $x$ such that $x^2+1 \equiv 0 \bmod 137$. The book suggests computing values $a^{\frac{p-1}{4}}$, about half of which will be witnesses to this.

In this case, $100^2+1^2 = (73)(100)$

$A = 100; B = 1; M = 73$

$u = 100\%73 = 27; v = 1\%73 = 1$ (Im using Sage notation for remainder)

$(\frac{uA+vB}{M})^2 + (\frac{vA-uB}{M})^2 = 37^2+1^2 = (10)(137)$

$A = 37; B = 1; M = 10$

$u = 37\%10 = 7; v = 1\%10 = 1$ (Im using Sage notation for remainder)

$(\frac{uA+vB}{M})^2 + (\frac{vA-uB}{M})^2 = 26^2+3^2 = (5)(137)$

$A = 26; B = 3; M = 5$

$u = 26\%5 = 1; v = 3\%5 = 3$ (Im using Sage notation for remainder)

$(\frac{uA+vB}{M})^2 + (\frac{vA-uB}{M})^2 = 7^2+15^2 = (2)(137)$ $A = 7; B = 15; M = 2$

$u = 7\%2 = 1; v = 15\%2 = 1$ (Im using Sage notation for remainder)

$(\frac{uA+vB}{M})^2 + (\frac{vA-uB}{M})^2 = 11^2+4^2 = 137$

There will be computational exercises of this kind in the next homework.

# 25 Effectiveness of the Rabin-Miller Test

This section is my personal folly; I wanted to know why 75 percent of numbers below a composite $n$ are Rabin-Miller witnesses to its compositeness, so with the assistance of Mr Elbakri I found this result in another book. It didn't take as long as I expected to present, but it is definitely a good example of the weirdly arbitrary nature of proofs in number theory!

Let $n \in \mathbb{N}$ be odd and composite.

Our aim is to show that there are at most $\frac{1}{4}(n-1)$ Rabin-Miller misleaders for $n$.

Suppose first that $n$ is divisible by the square of some prime $p$.

We claim that for any $n \in \mathbb{N}$ and $p$ an odd prime such that $p^2|n$, the number of Fermat misleaders (and so the number of Rabin-Miller misleaders) for $n$ is at most $\frac{1}{4}(n-1)$, which would establish our result in this case.

let $S$ be the set $\{a < p \mid a^{n-1} \equiv 1 \bmod n\}$ of Fermat misleaders for $n$.

For a specific $b$ let $S_b$ be $\{a \in S : a \equiv b \bmod p\}$.

We claim that $S_b$ has at most $\frac{n}{p^2}$ elements.

To prove this we need a couple of lemmas.

**Lemma:** If $x \equiv y \bmod p$ then $x^p \equiv y^p \bmod p^2$

**Proof:** $x^p - y^p = (x-y)(x^{p-1} + x^{p-2}y + \ldots xy^{p-2} + y^{p-1})$: the first factor is divisible by $p$ by explicit hypothesis, and the second is divisible by $p$ because it is the sum of $p$ terms each congruent to $x^{p-1} \bmod p$, so this difference is divisible by $p^2$ and the conclusion follows.

**Lemma:** If $x$ and $y$ are Fermat misleaders for $n$ and $p^2|n$ ($p$ prime) and $x \equiv y \bmod p$ then $x \equiv y \bmod p^2$.

**Proof:** $x^{n-1} = 1 \bmod n$ so $x^n \equiv x \bmod p^2$ and similarly $y^n \equiv y \bmod p^2$. $x^p \equiv y^p \bmod p^2$ by the previous Lemma, so $x \equiv (x^p)^{\frac{n}{p}} \equiv (y^p)^{\frac{n}{p}} \equiv y \bmod p^2$

From the second Lemma it follows that all elements of $S_b$ are congruent to $b$ mod $p^2$, and there at most $\frac{n}{p^2}$ elements of $S$ in an congruence class mod $p^2$.

There are at most $p-1$ classes $S_b$, so there are at most $\frac{(p-1)n}{p^2}$ Fermat misleaders, or at most $\frac{2}{9}n$ misleaders (taking $p$ to be 9, as small as possible), and further $\frac{2}{9}n \leq \frac{1}{4}(n-1)$ for all $n \geq 9$, and $n$ is at least 9 because it has an odd prime square as a factor.

Thus we can assume that $n$ has no square factors in the main theorem.

**An Intermission**

We discuss the two definitions of "Carmichael number" in the book.

**Definition 1:** An odd composite number $m$ is a Carmichael number iff $a^{m-1} \equiv_m 1$ for each $a$ relatively prime to $m$.

**Definition 2:** An odd composite number $m$ is a Carmichael number iff $a^m \equiv_m a$ for every $a$.

**2 implies 1:** Suppose that $m$ satisfies Definition 2. Our aim is to show that it satisfies Definition 1. Let $a$ be chosen relatively prime to $m$, where $m$ is a Carmichael number according to Definition 2. We then have $a^m \equiv_m a$ because $m$ is a Def 2 Carmichael number. $a$ has a multiplicative inverse mod $m$ because $a$ is relatively prime to $m$. It follows that $a^{m-1} \equiv_m 1$ by multiplying both sides of the previous congruence by the mod $m$ reciprocal of $a$. We have thus shown that $m$ is a Def 1 Carmichael number.

**1 implies 2, under restricted conditions:** Suppose that $m$ is a Definition 1 Carmichael number and is a product of distinct primes (for no prime $p$ does $p^2|m$). For each prime $p_i|m$ and each $a$ we do have $a^{p_i} \equiv_{p_i} a$, because either $p_i|a$ and so $a^{p_i} \equiv_{p_i} 0 \equiv_{p_i} a$, or $p_i \not| a$ and we have $a^{p_i-1} \equiv_{p_i} 1$, so again $a^{p_i} \equiv_{p_i} a$. It thus follows that $a^m \equiv_{p_i} a$ for each $p_i$, since $m$ is a multiple of each $p_i$, from which it follows that $a^m \equiv_m a$ by the Chinese Remainder Theorem.

**No Definition 1 Carmichael number has a nontrivial square factor:** Suppose that $m$ is a Definition 1 Carmichael number and $p$ is a prime with $p^k|m$ and $p^{k+1} \not| m$, $k \geq 2$. Suppose that $a$ is relatively prime to $m$. $(a + p^{k-1})^p \equiv_{p^k} a^p$: expand this by the Binomial Theorem and the first term will be $a^p$ and each subsequent term will be divisible by $p^k$, as it contains a power of $p^{k-1}$ and a binomial coefficient divisible by $p$. If $m = p^k q$, choose numbers $a_1$ and $a_2$ with $a_1 \equiv_{p^k} a$, $a_2 \equiv_{p_k} a + p^{k-1}$ and $a_1 \equiv_q a_2 \equiv_q 1$ (Chinese Remainder Theorem). $a_1$ and $a_2$ are not congruent mod $m$ and are relatively prime to $m$, and $(a_1^{-1}a_2)^{p^k} \equiv_m 1$, because $a_1$ and $a_2$ have been engineered to have the same $p^k$ powers mod $m$. But this means that $a_1^{-1}a_2$, which is relatively prime to $m$ and is not 1, has order $p^i$, for some positive $i \leq k$, which cannot go into $m - 1 = p^k q - 1$, so it cannot be the case that $(a_1^{-1}a_2)^{m-1} \equiv_m 1$.

It then follows that a Definition 1 Carmichael number has to be a Definition 2 Carmichael number, completing the proof of equivalence. The nature of this argument makes it clear that the author's assumption that the two definitions are equivalent is not harmless!

We resume the proof of the main result.

We claim that for any product $n = p_1 \ldots p_s$ of distinct primes, the number of Rabin-Miller misleaders for $n$ is no more than $\frac{1}{2^{s-1}}(n-1)$. This is enough to establish our main result if $n$ has at least three distinct prime factors.

A Rabin-Miller misleader $a < n$, where $n - 1 = 2^k q$, $q$ odd, will satisfy either $a^q \equiv 1 \bmod n$ (and so $a^q \equiv 1 \bmod p_i$ for each $i$) or $a^{2^j q} \equiv -1 \bmod n$ for some $j < k-1$ (and so $a^{2^j q} \equiv -1 \bmod p_i$ for each $i$). A number cannot satisfy more than one of these equations for any $i$, so any misleader will satisfy one of these congruences (the same one) in mod $p_i$ arithmetic for each $i$.

Now we need two Lemmas.

**Lemma:** If $m$ is odd and $p$ is an odd prime, $x^m \equiv 1 \bmod p$ has no more than

$\frac{p-1}{2}$ solutions. If in addition $\frac{p-1}{2}$ does not go into $m$, then there are no more than $\frac{p-1}{4}$ solutions.

**Proof:** A solution of $x^m \equiv 1 \bmod p$ has order a divisor of $m$ and a divisor of $p-1$, so has order some divisor of $\gcd(m, p-1)$, so is a solution of $x^{\gcd(m,p-1)} \equiv_p 1$. There are no more than $\gcd(m, p-1)$ such solutions by the Polynomial Roots Theorem, and $\gcd(m, p-1) \leq \frac{p-1}{2}$ (in fact $\gcd(m, p-1) | \frac{p-1}{2}$) because $m$ is odd and $p-1$ is even. If there are more than $\frac{p-1}{4}$ solutions then we must have $\gcd(m, p-1) = \frac{p-1}{2}$ from which $\frac{p-1}{2} | m$, and the contrapositive gives the last part of the result.

**Lemma:** If $p$ is an odd prime, $x^m \equiv -1 \bmod p$ has no more than $\frac{p-1}{2}$ solutions. If in addition $\frac{p-1}{2}$ does not go into $m$, then there are no more than $\frac{p-1}{4}$ solutions.

**Proof:** A solution of $x^m \equiv -1 \bmod p$ will have order dividing $2m$ and order dividing $p-1$ (notice that we are not assuming $m$ odd here). It will certainly satisfy $x^{\gcd(2m,p-1)} \equiv_p 1$, from which it must satisfy $x^{\gcd(m,p-1)} \equiv_p -1$ (if this were 1, the only other alternative, then $x^m$ would be 1 as well), whence $m$ has fewer factors of 2 than $p-1$. This equation has no more than $\gcd(m, p-1)$ solutions by the Polynomial Roots Theorem. If $\gcd(m, p-1)$ were $p-1$ (or any $\frac{p-1}{2k+1}$), it would follow that $m$ has as many factors of 2 as $p-1$, which we see from above is impossible, so $\gcd(m, p-1) \leq \frac{p-1}{2}$, being a proper divisor of $p-1$. If there are more than $\frac{p-1}{4}$ solutions, then $\gcd(m, p-1) = \frac{p-1}{2}$ or $\frac{p-1}{3}$. The latter is impossible because $m$ has strictly fewer factors of 2 than $p-1$. The former implies $\frac{p-1}{2} | m$, and the contrapositive gives us the last part of the theorem.

Now consider for any $b$ the collection $S_b$ of misleaders for $n$ congruent to $b$ mod $p_1$. The number of possible values mod $p_i$ ($i > 1$) for an element of $S_b$ is no more than $\frac{p_i-1}{2}$, so the total number of possible values mod $n$ for an element of $S_b$ is no more than the product of all $\frac{p_i-1}{2}$ for $i > 1$, by the fact that $n$ has no squared prime factors and the Chinese Remainder Theorem. Thus the total number of misleaders is no more than the product of $p_1 - 1$ (for the number of possible values of $b$) and the product of all $\frac{p_i-1}{2}$ for $i > 1$, and this is less than or equal to $\frac{1}{2^{s-1}}(n-1)$, which gives the desired upper bound $\frac{1}{4}(n-1)$ if $s$ is at least 3.

There only remains the case $s = 2$, $n = p_1p_2$. A product of two primes is not a Carmichael number, so we do not have both $p_1-1|n-1$ and $p_2-1|n-1$. wlog assume $p_2 - 1$ does not go into $n - 1$.

Define $S_b$ exactly as in the previous case. Because $p_2 - 1$ does not go into $n - 1$, $\frac{p_2-1}{2}$ does not go into $\frac{n-1}{2}$ and so does not go into any $2^jq$ (that is, it does not go into the relevant $m$ in our application of the appropriate Lemma). Thus each $S_b$ has no more than $\frac{p_2-1}{4}$ elements by the appropriate Lemma, and there are no more than $(p_1 - 1)\frac{p_2-1}{4}$ misleaders in all, which is less than or equal to $\frac{1}{4}n - 1$, completing the proof.

# 26 Square triangular numbers clarified

This is quite similar to the development in chapter 31 of the book. My use of division is a little different.

A square number is a number of the form $n^2$.

A triangular number is a number of the form $\frac{m(m+1)}{2}$.

So we get a square triangular number when we see a solution in integers to $n^2 = \frac{m(m+1}{2}$.

Multiply both sides by 8 and we get $8n^2 = 4m^2 + 4m = (2m + 1)^2 - 1$.

So if we set $y = 2n$, $x = 2m + 1$, solutions of $2y^2 = x^2 - 1$ yield square triangular numbers. This can be written $x^2 - 2y^2 = 1$.

To show that this is completely general, we need to show that if $x^2-2y^2 = 1$, it follows that $x$ is odd and $y$ is even. It is evident that $x$ is odd. Now if $y$ were odd, it is straightforward to show that $x^2 - 2y^2$ would be congruent to $-1$ mod 4.

So if we have integer solutions to $x^2-2y^2 = 1$, we get integer solutions to $n^2 = \frac{m(m+1}{2}$ with $n = \frac{y}{2}$, $m = \frac{x-1}{2}$, so there is an exact correlation between solutions to these equations.

We know one solution $(3, 2)$: $3^2 - 2(2^2) = 1$.

If we have a solution $(x, y)$ to $x^2 - 2y^2 = 1$, then it is a solution to the equation $(x - y\sqrt{2})(x + y\sqrt{2}) = 1$. Squaring both sides, then expanding the left side, gives $((x^2+2y^2)-2xy\sqrt{2})((x^2+2y^2)+(2xy)\sqrt{2})$, so $(x^2+2xy, 2xy)$ is a solution, from which we can get another solution to the equation in $m$ and $n$, and another square triangular number.

More generally, we can take any solution $(x, y)$ and find another one $(u, v)$ by expressing $(x+y\sqrt{2})^k$ in the form $u+v\sqrt{2}$ where $u$ and $v$ are integers and

$k$ is any natural number, which is clearly always possible by multiplication in the usual way and collection of like terms.

At this point we have shown that there are infinitely many square triangular numbers, namely the ones obtained from $(3+2\sqrt{2})^k$ in the way indicated. We also might feel weird because we solved this problem in number theory using a fact about irrational real numbers! Get used to it; this is common in number theory.

Now we show that *all* the solutions to the equation $x^2 - 2y^2 = 1$ are obtained in this way, using Fermat's method of descent.

Suppose $(u, v)$ is a solution, $u$ and $v$ positive. If $u = 3$, then $v = 2$ and we are done. It is straightforward to show that there are no smaller solutions other than $(1, 0)$, which also corresponds to a power of $(3 + 2\sqrt{2})$.

Now suppose that $u > 3$. We show that there is another solution $(s, t)$ such that $(3 + 2\sqrt{2})(s + t\sqrt{2}) = (u + v\sqrt{2})$ and $s < u$. But then it is clear that we can apply this process repeatedly and the first component must eventually descend to 3, as we cannot have an infinite descending sequence of first components of solutions.

Since we are in the realm of reals anyway, I proceed boldly to use division.

$s + t\sqrt{2}$ must be

$$\frac{u + v\sqrt{2}}{3 + 2\sqrt{2}} = \frac{(u + v\sqrt{2})(3 - 2\sqrt{2})}{(3 + 2\sqrt{2})(3 - 2\sqrt{2})}) = (3u - 4v) + (3v - 2u)\sqrt{2}.$$

So we know that $s = 3u - 4v$ and $t = 3v - 2u$ must be true if there is a solution.

We need to show that $s$ and $t$ are positive and that $s < u$.

$u^2 = 1 + 2v^2 > 2v^2$ so $u > \sqrt{2}v$ so $s = 3u - 4v > (3\sqrt{2} - 4)v > 0$.

$u > 3$ so $u^2 > 9$ so $9u^2 > 9 + 8u^2$ so $9u^2 - 9 > 8u^2$ so $u^2 - 1 > \frac{8}{9}u$ so $2v^2 > \frac{8}{9}u^2$ so $v > \frac{2}{3}u$.

Thus $t = 3v - 2u > 3\frac{2}{3}u - 2u > 0$.

Since $s$ and $t$ are positive, we have $s < 3s+4t = (9u-12v)+(12v-8u) = u$. This completes the proof.

Thus we have a recipe for the $k$th square triangular number. Use a CAS to compute $(3 + 2\sqrt{2})^k$ in the form $(x + y\sqrt{2})$ where $x$ and $y$ are integers. We then have $\frac{y}{2} = n$ so the square triangular number is $\frac{y^2}{4}$.

# 27 $a^4 + b^4 \neq c^4$

In this section, we produce a proof of the case $n = 4$ of Fermat's Last Theorem, closely following the development in chapter 30 in the book. This is usually ascribed to Fermat himself.

The exact strategy is to assume that we have a solution $(x, y, z)$ of the equation $x^4 + y^4 = z^2$ with $xyz \neq 0$ (a solution of $x^4 + y^4 = z^4$ with $xyz \neq 0$ would give a solution to this equation), and from this construct a smaller solution $(X, Y, u)$ (smaller in the sense that $u < z$). This is absurd, because we could then iterate this process endlessly to get a decreasing infinite sequence of positive integers.

$(x^2, y^2, z)$ may be assumed to be a primitive Pythagorean triple. If it is not, we can find a common prime factor $p$ in $(x, y, z)$ and $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2})$ will be a smaller solution.

We know already that we can find relatively prime odd integers $s, t$ such that (after possibly switching $x, y$) we have $x^2 = st$, $y^2 = \frac{s-t}{2}$ and $z = \frac{s^2+t^2}{2}$, from our earlier analysis of primitive Pythagorean triples.

Since $st$ is an odd square, $st$ is congruent to 1 mod 4. This further implies that $s$ and $t$ are congruent mod 4.

We know that $2y^2 = s^2 - t^2 = (s-t)(s+t)$. $s$ and $t$ are odd and relatively prime, so the only common factor of $(s - t)$ and $(s + t)$ is 2. $s$ and $t$ are congruent mod 4 so we know that $s - t$ is divisible by 4. This tells us that $s + t$ is twice an odd number. We then have $s - t = 4a$ and $s + t = 2b$ where $2a$ and the odd $b$ are relatively prime. But also $(4a)b = y^2$, and since $4a$ and $b$ have no common factors they must both be perfect squares, so $s - t = 4v^2$ and $s + t = 2u^2$ for some relatively prime $u$ and $v$.

Solving for $s, t$ we find $s = u^2 + 2v^2$ and $t = u^2 - 2v^2$ so $x^2 = st = u^4 - 4v^4$, so $x^2 + 4v^4 = u^4$.

This gives us $A = x, B = 2v^2, C = u^2$ a primitive Pythagorean triple. We repeat the application of the analysis of primitive Pythagorean triples: we have $x = A = ST$. $2v^2 = B = \frac{S^2-T^2}{2}$, and $u^2 = C = \frac{S^2+T^2}{2}$.

We have $4v^2 = S^2 - T^2 = (S - T)(S + T)$. Since $S$ and $T$ are odd and relatively prime, the only common divisor of $S - T$ and $S + T$ is 2. Their product is a square so we must have $S + T = 2X^2$, $S - T = 2Y^2$ for some integers $X$ and $Y$.

Solving, we find that $S = X^2 + Y^2$ and $T = X^2 - Y^2$.

Then $u^2 = \frac{S^2+T^2}{2} = \frac{(X^2+Y^2)^2+(X^2-Y^2)^2}{2} = X^4 + Y^4$.

So $(X, Y, u)$ is a solution to the original equation. Earlier equations tell us that

$$z = \frac{s^2 + t^2}{2} = \frac{(u^2 + 2v^2)^2 + (u^2 - 2v^2)^2}{2} = u^4 + 4v^4$$

so $u < z$, completing the proof that we have a smaller solution.

# 28 $a^3 + b^3 \neq c^3$

Eventually I want to craft my own version of this in the correct order, but for the moment I am going to transcribe my notes in the perhaps strange order in which I presented them. Proving the $n = 3$ case of Fermat's Last Theorem turned out to be more than I bargained for!

## 28.1 The Euler Proof

This is Euler's proof of 1770, basically as presented in the Wikipedia article with some comments of mine made in the course of digesting it.

Assume a solution $(x, y, z)$ to the equation $x^3+y^3+z^3 = 0$ where $xyz \neq 0$. Our aim is to construct a new solution which is smaller in a suitable sense, thus showing by the method of descent that there cannot be any solution. We may assume that $x, y, z$ have no common factor, because otherwise we could divide through by the common factor and get a smaller solution. Further, we can assume that they are pairwise coprime, because the form of the equation ensures that a common factor of two of them would be a common factor of all three.

Two of the numbers are odd and one is even; assume without loss of generality that $z$ is even. $x$ is not equal to $y$; if they were equal, they would both be 1, and 2 is not a cube.

$x + y$ and $x - y$ are both even, so we may set $2u = x + y$, $2v = x - y$. $u$ and $v$ are coprime and of opposite parities (one is even, one is odd).

Now $x = u + v$ and $y = u - v$ so

$$-z^3 = (u + v)^3 + (u - v)^3 = 2u(u^2 + 3v^2)$$

$u^2 + 3v^2$ is odd, so, since $2u(u^2 + 3v^2)$. being $-z^3$, must be divisible by 8 since $z$ is even, so $u$ is divisible by 4 and $v$ is odd.

Since $u$ and $v$ are coprime, the greatest common divisor of $2u$ and $u^2+3v^2$ is either 1 (Case A) or 3 (case B).

### 28.1.1 Case A

We assume that $\texttt{gcd}(2u, u^2 + 3v^2) = 1$. Note that this implies that 3 is not a factor of $u$. We have $-z^3 = 2u(u^2 + 3v^2)$; if we factor a perfect cube into two coprime factors, they must also be perfect cubes, so we may set $r^3 = 2u$, $x^3 = u^2 + 3v^2$.

Now, like magic, we introduce the Key Lemma.

**The Key Lemma:** For any $s, u, v$ integers, if $u, v$ are coprime, $s$ is odd, and $s^3 = u^2 + 3v^2$, then for some coprime integers $e, f$, $s = e^2 + 3f^2$, where $u = e(e^2 - 9f^2)$ and $v = 3f(e^2 - f^2)$.

Euler's published proof of this Lemma is wrong.

Having mercy on my reader, I point out that the Lemma actually says that any $u + v\sqrt{-3}$ with $u, v$ coprime and $|u + v\sqrt{-3}|^2$ a perfect cube is equal to $(e + f\sqrt{-3})^3$ for some coprime $e, f$. Euler knew this. Notice the algebra of larger domains peeping in as it did in our account of the square triangular numbers!

We return to the proof of Case A.

By the Key Lemma we have coprime $e, f$ such that $u = e(e^2 - 9f^2)$ and $v = 3f(e^2 - f^2)$.

Since $u$ is even and $f$ odd, we must have $e$ even and $f$ odd.

$$r^3 = 2u = 2e(e - 3f)(e + 3f)$$

The factors $2e$, $e + 3f$, $e - 3f$ are coprime: the only common factor they could have is 3, and $e$ goes into $u$ which does not have 3 as a divisor. Thus each of these factors is a perfect cube, and $-2e = k^3; e - 3f = l^3; e + 3f = m^3$ gives a solution $k^3 + l^3 + m^3 = 0$.

Further

$$|k^3| = |2e| < |r^3| = |2u| < |z^3|,$$

so the even term of the new solution is smaller than the even term of the original solution.

### 28.1.2 Case B

We assume that $\texttt{gcd}(2u, u^2 + 3v^2) = 3$. This implies that 3 is a factor of $u$, so we can set $u = 3w$ and get

$$-z^3 = 6w(9w^2 + 3v^2) = 18w(3w^2 + v^2)$$

$v, w$ are coprime and 3 does not go into $v$, so $18w$ and $3w^2 + v^2$ are also coprime, so both are perfect cubes. Set $r^3 = 18w$ and $s^3 = 3w^2 + v^2$.

By the Key Lemma we have $s = e^2 + 3f^2$ where $e, f$ are coprime,

$$v = e(e^2 - f^2); w = 3f(e^2 - f^2).$$

$e$ is odd and $f$ is even, because $v$ is odd.

$$r^3 = 18w = 54f(e^2 - f^2) = 54f(e + f)(e - f) = 3^3(2f)(e + f)(e - f)$$

Let $t = \frac{r}{3}$, which is an integer since $27|r^3$: $t^3 = (2f)(e + f)(e - f)$.

Since $e, f$ are coprime, so are $2f$, $e + f$, $e - f$ so each of them is a perfect cube.

$-2f = k^3; e + f = l^3; e - f = m^3$ gives a solution to our equation, $k^3 + l^3 + m^3 = 0$. Further,

$|k^3| = |2f| < |r^3| = |18w| < |z^3|$, so the even term of the new solution is smaller in absolute value than the even term of the original solution.

### 28.1.3 Not quite done...

This completes the proof, except for the Key Lemma.

## 28.2 Macys's Proof of the Key Lemma

This section proves the Key Lemma. The argument is taken from J. J. Macys, "On Euler's Hypothetical Proof", Mathematical Notes, 2007, vol. 82, no 3, pp 395-400. Macys is arguing that Euler really did know how to prove the Key Lemma, so his presentation is deliberately elementary in the sense that he avoids even mentioning numbers of the form $a + b\sqrt{-3}$. My aim is just to prove the Lemma, so I shall be less pure in my approach. (I think Macys adapted his proof from another source, and it is likely that my version looks more like the version he was working from, due to his aim of making the proof look less "complex").

We repeat the statement of

**The Key Lemma:** For any $s, u, v$ integers, if $u, v$ are coprime, $s$ is odd, and $s^3 = u^2 + 3v^2$, then for some coprime integers $e, f$, $s = e^2 + 3f^2$, where $u = e(e^2 - 9f^2)$ and $v = 3f(e^2 - f^2)$.

Having mercy on my reader, I point out that the Lemma actually says that any $u + v\sqrt{-3}$ with $u, v$ coprime and $|u + v\sqrt{-3}|^2$ a perfect cube

is equal to $(e+f\sqrt{-3})^3$ for some coprime $e, f$. Euler knew this. Notice the algebra of larger domains peeping in as it did in our account of the square triangular numbers!

Macys presents a sequence of Propositions. Our propositions will parallel his; our presentation will not be the same, because we will explicitly mention complex numbers of the form $a+b\sqrt{-3}$, $a, b$ integers, which we will call Euler integers.

**Definition:** We say a number is representable if it can be expressed in the form $a^2 + 3b^2$.

**Proposition 1:** The product of two representable numbers is representable.

**Proof of Proposition 1:** $(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$ can be verified by direct calculation.

Notice that this can be expressed in terms of complex numbers in a way that makes it clear that it is true:

$$(a^2 + 3b^2)(c^2 + 3d^2) = |a + b\sqrt{-3}|^2|c + d\sqrt{-3}|^2 =$$
$$|(a+b\sqrt{-3})(c+d\sqrt{-3})|^2 = |(ac-3bd)+(ad+bc)\sqrt{-3}|^2 = (ac-3bd)^2+3(ad+bc)^2$$

Of course this is cheating.

**Definition:** A representative factorization of a number $a^2 + 3b^2$ is a factorization of $a + b\sqrt{-3}$ into Euler integers. Of course a representative factorization of $a^2 + 3b^2$ induces a factorization of the representable integer $a^2 + 3b^2$ into representable integers in the obvious way.

**Proposition 2:** In a representative factorization, the order and grouping of the factors is immaterial.

**Proof:** This is obvious. It is less obvious for Macys as he avoids talking about complex numbers.

**Proposition 3:** $(a^2 + 2b^2)^3$ is representable.

**Proof:** $(a^3-9ab^2)^2+3(3a^2b-3b^3)^2$, which can be verified directly, and which is obtained from the representative factorization $(a + b\sqrt{-3})^3$.

**Proposition 4:** If $a, b$ are coprime, then each odd divisor of $a^2 + 3b^2$ is representable.

**Proof:** Macys just gives a reference for this. We found a proof on the web, whcih we give in the next subsection.

**Proposition 5:** If $a, b$ are coprime integers, and $P = p^2 + 3q^2$ is a representable prime factor of $a^2 + 3b^2$, then there is a representive factorization $(p + q\sqrt{-3})(u + v\sqrt{-3})$ of $a^2 + 3b^2$, where $u, v$ are coprime.

**Note:** We state this differently from Macys, who uses Prop. 4 here to observe that any odd prime factor of $a^2 + 3b^2$ is in fact representable, as we will use our modified Prop. 5 in our proof of Prop. 4 below.

**Proof:**

$$\frac{a + b\sqrt{-3}}{p + q\sqrt{-3}} = \frac{(a + b\sqrt{-3})(p - q\sqrt{-3})}{(p + q\sqrt{-3})(p - q\sqrt{-3})} =$$

$$\frac{(ap + 3bq) + (pb - aq)\sqrt{-3}}{p^2 + 3q^2} =$$

$$\frac{ap + 3bq}{p^2 + 3q^2} + \frac{pb - aq}{p^2 + 3q^2}\sqrt{-3},$$

which we would like to claim is the desired Euler integer $u + v\sqrt{-3}$.

This is not necessarily the case if we proceed naively, but we can make it the case.

$$(pb - aq)(pb + aq) = b^2(p^2 + 3q^2) - q^2(a^2 + 3b^2)$$

can be verified by direct computation, and the right side is divisible by the prime $p^2 + 3q^2$, so one of the factors of the left side is. The signs of $p$ and $q$ can be chosen freely: we note that in representing primes we will always choose $p$ positive; choose $q$ so that $(p^2 + 3q^2)|(pb - aq)$, and we see that the second coefficient in the quotient above is an integer, and the first one must be as well because the square of the magnitude of the given quotient is also an integer, and a rational square root of an integer is an integer (if $A^2 + 3B^2$ is an integer, and $B$ is an integer, and $A$ is rational, then $A^2$ is an integer, so $A$ is an integer).

$u = \frac{ap+3bq}{p^2+3q^2}$ and $v = \frac{pb-aq}{p^2+3q^2}$ are coprime because their denominators must be coprime, as we can check that $a = pu - 3qv$ and $b = pv + qu$.

This proof is different from what I gave in class, which followed Macys more closely; as in the section on square triangular numbers above, I decided to bring in the more powerful operations possible in the larger domain I am working in.

**Proposition 6:** If a prime is representable, its representation is unique up to signs of its coefficients.

**Proof:** Suppose $P$ is a representable prime. It will be odd, since 2 is not representable. Give a representation $p^2 + 3q^2$ and another representation $a^2 + 3b^2$. Clearly the coefficients $a, b$ are coprime. By the previous proposition, we can express $a+b\sqrt{-3} = (p+q\sqrt{-3})(u+v\sqrt{-3})$ in a way which might involve changing the signs of $p$ and $q$. Then $a = pu - 3qv$ and $b = pv + qu$. But $u + v\sqrt{-3}$ must have magnitude 1, so $u = \pm 1$ and $v = 0$. It follows that $a = \pm p$ and $b = \pm q$.

**Proposition 7:** Suppose $a$ and $b$ are coprime and $a^2 + 3b^2$ is odd. Then we can factor $a + b\sqrt{-3}$ as a product of numbers of the form $p + q\sqrt{-3}$ for which $p$ is positive and $p^2 + 3q^2$ is prime, and a final factor $\pm 1$. Moreover, if $c + d\sqrt{-3}$ appears in this factorization, $c + d\sqrt{-3}$ does not.

**Proof:** $a^2 + 3b^2$ factors uniquely into odd primes. Each odd prime in its factorization is representable (Prop. 4) and can be factored out using the procedure of Prop. 5, and the sign of the first coefficient of each factor can be chosen to be positive. This process can be repeated. If the factors $c+d\sqrt{-3}$ and $c-d\sqrt{-3}$ both appeared, then $a$ and $b$ would both be divisible by $c^2 + 3d^2$, which is impossible.

**Proof of the Key Lemma:** If $a, b$ are coprime, $a^2 + 3b^2 = s^3$ is odd, then we can factor $a + b\sqrt{-3}$ as indicated in Proposition 7. Then it is clear that the factors will occur in groups of three identical factors, so we can write $a+b\sqrt{-3} = (e+f\sqrt{-3})^3$ and this has already been observed to be equivalent to the Lemma. If $e, f$ were not coprime, neither would $a, b$ be.

## 28.3 A Final Lemma

We still need to show that Macys's Prop. 4 holds.

**Proposition 4:** If $a, b$ are coprime, then each odd divisor of $a^2 + 3b^2$ is representable.

Our source for this is on a blog about the FLT; the proof I am using is at

`http://fermatslasttheorem.blogspot.com/2005/05/fermats-last-theorem-n-3-a2-3b2.html`

Assume that $a, b$ are coprime, and that $x$ is a odd factor of $a^2 + 3b^2$. Our aim is to show that $x$ is representable. If $x = 1$, $x$ is representable, so we can assume $x > 1$.

We can find $m, n, c, d$ such that $a = mx \pm c$ and $b = nx \pm d$, and $|c|, |d| < \frac{x}{2}$, by the division algorithm (with a small tweak to get remainders between $-\frac{x-1}{2}$ and $\frac{x-1}{2}$ rather than between 0 and $x - 1$).

$a^2 + 3b^2 = (mx \pm c)^2 + 3(nx \pm d)^2 = c^2 + 3d^2$ plus factors divisible by $x$, so $c^2 + 3d^2$ is divisible by $x$. Note also that neither $c$ nor $d$ is 0, as neither $a$ nor $b$ can be divisible by $x$, as they are supposed coprime.

$c^2 + 3d^2 = xy$ for some $y$. Note that $c^2 + 3d^2 < (\frac{1}{2}x)^2 + 3(\frac{1}{2}x)^2 = x^2$, so $y < x$.

Now let $C = \frac{c}{\gcd(c,d)}$ and $D = \frac{d}{\gcd(c,d)}$ and $z = \frac{y}{\gcd(c,d)}$. Computation reveals that $xz = C^2 + 3D^2$.

Now we show that if $x$ is not representable then $C^2 + 3D^2$ has an odd factor which is not representable.

Suppose on the contrary that every odd factor of $z$ was representable. Then observe that by Macys's Prop. 5 above we can divide $C^2 + 3D^2$ ($C, D$ are coprime!) by any odd prime factor of $z$ (since all odd factors of $z$ are assumed representable) obtaining a representable number still of the form $xz'$ with all odd factors of $z'$ representable. This process can be iterated.

Further, any factor of 2 can be handled as well, as the following Lemma shows:

**Lemma:** If $a^2 + 3b^2$ is even, with $a, b$ coprime, it is divisible by 4 and $\frac{a^2+3b^2}{4}$ is representable with coprime coefficients.

**Proof:** That $a, b$ are both odd is evident. $a^2$ and $b^2$ are both congruent to 1 mod 4, so $a^2 + 3b^2$ is congruent to 0 mod 4.

Now either $a + b$ or $a - b$ is divisible by 4.

If $4|(a + b)$ set $u = \frac{a-3b}{4}$ and $v = \frac{a+b}{4}$.

If $4|(a - b)$ set $u = \frac{a+3b}{4}$ and $v = \frac{a-b}{4}$.

In both cases, we can verify that $u, v$ are integers, are coprime, and $4(u^2 + 3v^2) = a^2 + 3b^2$.

So all factors of $z$ can be eliminated and we see that $x$ is representable contrary to assumption. So $z$ must have some odd factor which is not representable if $x$ is not representable.

Now we complete the proof by descent. If $C^2 + 3D^2$ is less than our original $a^2 + 3b^2$, we have a smaller bad number. If $C^2 + 3D^2 = a^2 + 3b^2$ (not on the face of it impossible, if $m = n = 1$), then we have a factor of $z < x$ which is an odd factor of our original number and not representable, so we have a smaller bad factor of the same number. We can iterate this process one way or the other and get a steadily decreasing sequence of counterexamples from any counterexample, which is impossible.

And this fills the last gap, completing our proof of Fermat's Last Theorem in the case $n = 3$.