1 Integers and Divisibility

In this course we primarily want to study the factorization properties of integers. So we should probably start by reminding ourselves how integers and factorization work.

Much of this material was covered in Math 210, but we shall review it so we can use it during the rest of the course, as well as perhaps putting it on a somewhat firmer foundation.

1.1 The integers and the rationals

For further reading on the material in this subsection, consult **Rosen 1.1–1.3; PMF 1.1–1.2, 2.1–2.2**.

Definition 1.1. The *integers* are elements of the set $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

The *natural numbers* are elements of the set $\mathbb{N} = \{1, 2, \dots\}$ of positive integers.

The *rational numbers* are elements of the set $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}\}$.

Remark 1.2.

1. Some sources include 0 as a natural number; in this course we will not, and none of the four suggested texts do so.

2. You may feel like these aren't really definitions, and you're not entirely wrong. A rigorous definition of the natural numbers is an extremely tedious exercise in mathematical logic; famously, Russell and Whitehead feature the proposition that "$1 + 1 = 2$" on page 379 of *Principia Mathematica*.

   We will simply trust that everyone in this course understands how to count.

The natural numbers have two very important properties.

Fact 1.3 (The Well-Ordering Property)**.** *Every subset of the natural numbers has a least element.*

This may seem obviously true, but is important for proving a number of results. (Compare the integers, the rationals, and the reals, all of which lack this property).

Fact 1.4 (The Successor Property)**.** *Every natural number n has a* successor $n + 1$*. Every natural number except 1 is the successor of some natural number. In particular there is no greatest natural number.*

This successor property underlies the principle of induction, which should be familiar to you from Math 210. It has two different but equivalent formulations:

Fact 1.5 (The Principle of Weak Induction)**.** *Let $P(n)$ be some statement about the natural number n. Then if $P(1)$ is true, and if $P(k)$ implies $P(k+1)$, then $P(n)$ is true for every natural number n.*

Fact 1.6 (The Principle of Strong Induction)**.** *Let $P(n)$ be some statement about the natural number n. Then if $P(n)$ is true whenever $P(k)$ is true for all $k < n$, then $P(n)$ is true for every natural number n.*

Remark 1.7. As stated, the principle of strong induction doesn't separately require a base case (i.e. it does not single out the case $n = 1$). Why not?

1.2 Divisibility

For further reading on the material in this subsection, consult **Rosen 1.5; PMF 3.1**.

Definition 1.8. If a and b are integers, we say that a *divides* b and write $a|b$ if there is an integer m such that $am = b$. We say a is a *divisor* or *factor* of b.

If there is no such integer, we may say that a does not divide b, and write $a \nmid b$.

Remark 1.9. The requirement that m is an integer is very important; if we allowed m to be a rational number, every integer would divide every other.

Note that if $a|b$ then $a \neq 0$. Rosen includes this in the definition but it is in fact implied by the rest of the definition.

Example 1.10.

- $2|6$
- $-2|6$
- $4 \nmid 6$
- $13|221$
- $3 \nmid 221$
- $17|0$
- $24 \nmid 12$

Much of this course will be spent studying properties related to divisibility; for now we'll prove a few basic facts about divisibility.

Lemma 1.11. *If a, b, c are integers with $a|b$ and $b|c$, then $a|c$. (In other words, the relationship $|$ is transitive).*

Proof. $a|b$ so there is some integer m with $am = b$. And $b|c$ so there is integer n with $bn = c$. Thus $amn = c$, and since mn is an integer, we have $a|c$ by definition. □

Lemma 1.12. *If a, b are natural numbers and $a|b$, then $1 \leq a \leq b$.*

Proof. Since a is a natural number, we know that $1 \leq a$. So we just need to show that $a \leq b$.

We know $a = mb$ for some integer m; since $a, b \geq 0$ we must have $m \geq 0$, and thus $1 \leq m$ (since clearly $m \neq 0$ if $a \neq 0$). Multiplying this inequality by a we have $a \leq am = b$. □

Lemma 1.13 (Linear Combinations)**.** *If a, b, c, m, n are integers, and $a|b$ and $a|c$, then $a|mb+nc$. We can say that if a divides b and c then it divides any integer linear combination of them.*

Proof. We know there are integers p and q so that $ap = b$ and $aq = c$. Then we can see $a(pm + qn) = apm + aqn = bm + cn$, and since $pm + qn$ is an integer, we have $a|mb + nc$ by definition of "divides". □

Corollary 1.14. *Let n be a natural number, and let a, b_i, n_i be integers for any $1 \leq i \leq n$. Suppose $a|b_i$ for each i. Then $a|\sum_{i=1}^{n} b_i m_i$.*

Proof. Base case: If $n = 1$ or $n = 2$, this follows from lemma 1.13 on linear combinations.

Now suppose for induction that the proposition holds for some given n. That is, fix some n and suppose that if $a|b_i$ for $1 \leq i \leq n$ then $a|\sum_{i=1}^{n} b_i m_i$. We want to prove that if $a|b_i$ for $1 \leq i + 1 \leq n$ then $a|\sum_{i=1}^{n+1} b_i m_i$.

But by inductive hypothesis we know that $a|\sum_{i=1}^{n} b_i m_i$, and we also know that $a|b_{n+1}$. So by Lemma 1.13 we know that $a|1\sum_{i=1}^{n} b_i m_i \cdot 1 + b_{n+1} m_{n+1} = \sum_{i=1}^{n+1} b_i m_i$.

Thus by the principle of weak induction, we know that whenever $a|b_i$ for each i, then $a|\sum_{i=1}^{n} b_i m_i$. □

1.3 The Greatest Common Divisor

For further reading on the material in this subsection, consult **Rosen 3.3, PMF 3.4, Stein 1.1.2**.

A useful tool for studying the divisibility and factorization properties of integers is the concept of the greatest common divisor.

Definition 1.15. If a and b are integers, then the *greatest common divisor* of a and b, written $\gcd(a, b)$ or just (a, b), is the largest (positive) integer d that divides both a and b.

We can similarly define $\gcd(a_1, a_2, \ldots, a_n)$ to be the largest (positive) integer that divides each a_i.

Remark 1.16. The notations $\gcd(a,b)$ and (a,b) are interchangeable. We'll mostly use (a,b) since it is shorter and easy to write; when we're worried about ambiguity we'll write out the full expression.

Example 1.17.

- $(4,6) = 2$
- $(4,8) = 4$
- $(2,3) = 1$
- $(23,47) = 1$
- $(-81,36) = 9$
- $(-4,4) = 4$
- $(1,a) = \gcd(a,1) = 1$ for any integer a.
- $(0,a) = (a,0) = |a|$ for any integer a.

Remark 1.18. We define $(0,0) = 0$ for boring technical reasons. This will almost never come up. (If you're familiar with the concept of an ideal, notice that the ideal generated by a and b is also the ideal generated by (a,b)–and the notation itself is suggestive.)

Fact 1.19. *For any integers a, b, $(a,b) = (b,a)$.*

Exercise 1.20. *Prove that if a and b are integers, then (a,b) exists and is unique.*

The greatest common divisor, as the name suggests, tells us how much two integers have in common (with respect to factorization). Sometimes integers have nothing in common:

Definition 1.21. If $(a,b) = 1$ then we say a and b are *relatively prime* or *coprime*.

Example 1.22.

- 2 and 3 are relatively prime. 4 and 7 are relatively prime. 12 and 35 are relatively prime.
- 4 and 6 are not relatively prime. 12 and 34 are not relatively prime. 1000 and 18 are not relatively prime.

We would like to split a pair of numbers into "the bit they have in common" and "the bit that's different." (We do this intuitively, really; we can look at 4 and 6 and see they have a 2 in common, and then factors of 2 and 3 respectively that they don't share). But we can be a bit more precise here:

Proposition 1.23. *If a, b are integers with $(a,b) = d$, then $(a/d, b/d) = 1$.*

Proof. Let a, b be integers and $(a, b) = d$. Both a/d and b/d are integers; suppose there is a positive integer e that divides both of them. Then we have integers m, n with

$$em = a/d \qquad en = b/d$$
$$dem = a \qquad den = b$$

and thus de divides both a and b.

But d is the greatest common divisor of a and b, so $d \geq de$, and since $e \geq 1$ we must have $e = 1$. So the only positive integer that divides both a/d and b/d is 1, and so $(a/d, b/d) = 1$ as desired. □

Thus given two integers a, b, we have split them into the common part (a, b), and the relatively prime parts a/d, b/d.

Corollary 1.24. *If a and $b \neq 0$ are integers, then $a/b = p/q$ for some integers p, q with $(p, q) = 1$.*

Proof. Let $d = (a, b)$ and set $p = a/d, q = b/d$. Then $(p, q) = 1$ by 1.23, and $p/q = (a/d)/(b/d) = a/b$. □

This allows us to talk about fractions being in lowest terms.

1.4 The GCD and linear combinations

For further reading on the material in this subsection, consult **Rosen 3.3, PMF 3.4–3.5, Stein 1.1.2, Shoup 1.1**.

Now that we understand how the greatest common divisor works, we want to see how it interacts with arithmetic–addition and multiplication.

Lemma 1.25. *Let a, b, c be integers. $(a + cb, b) = (a, b)$.*

Proof. Let a, b, c be integers. Suppose d is a divisor of both a and b. Then by lemma 1.13 on linear combinations we know that d divides $a + cb$. Thus d is a common divisor of a and $a + cb$.

Conversely suppose d divides both b and $a + cb$. We can see that $a = (a + cb) - c(b)$ is a linear combination of b and $a + cb$, and thus again by lemma 1.13 we see that d divides b. Thus d is a common divisor of a and b.

So we have proven that the set of common divisors of a and b is exactly the same as the set of common divisors of a and $a + cb$. Thus the greatest common divisor must be the same. □

This tells us that if we know the gcd of two numbers, we can add a multiple of the second number to the first without changing anything.

Example 1.26.
- We know that $(2,3) = 1$. Thus we also have $(5,3) = (8,3) = (11,3) = (30002,3) = 1$.
- We know that $(8,6) = 2$. Thus $(14,6) = (68,6) = 2$, and also $(8,14) = (8,86) = 2$.
- But note we can only change one thing at a time. $(15,20) = 5$ but $(15+20, 20+15) = (35,35) = 35$.

If we want to talk about addition and multiplication, it is useful to use the idea of a linear combination (which was already referenced in Lemma 1.13).

Definition 1.27. If a and b are integers, then an *integer linear combination* of a and b is a sum of the form $ma + nb$ where m, n are both integers.

Example 1.28. What are the linear combinations of 4 and 6? We clearly can get 4 and 6, as well as $8 = 2 \cdot 4$, $10 = 4 + 6$, $12 = 2 \cdot 6$. Linear combinations are not unique, as in $24 = 3 \cdot 4 + 2 \cdot 6 = 6 \cdot 4 = 4 \cdot 6$.

We can also get smaller numbers: $(-1)\cdot 4 + 6 = 2$, $(-3)\cdot 4 + 2\cdot 6 = 0$, and $(-3)\cdot 4 + (-5)\cdot 6 = -42$.

Example 1.29. What are some linear combinations of 5 and 7? We can get $10, 12, 14$ and so on. We can get $7 - 5 = 2$. So we can get $2 \cdot 7 - 2 \cdot 5 = 4$, and 6 and 8.

Is this the smallest postive result we can get? No! We see that $3 \cdot 5 - 2 \cdot 7 = 15 - 14 = 1$. Thus we can always get $3n \cdot 5 - 2n \cdot 7 = n$ and we can get any integer as a linear combination of 5 and 7.

You might notice that in both of these cases, the smallest result we can get is the greatest common denominator. This is in fact a general theorem, but we need an important (and familiar!) result first.

Lemma 1.30 (Division Algorithm)**.** *If a and b are integers and $b > 0$, then there are* unique *integers q and r such that $a = bq + r$ with $0 \leq r < b$.*

Remark 1.31. I describe this as familiar because this is just the division-with-remainder that we all learned in grade school. When we do the division b/a, then q is the quotient and r is the remainder.

Though this is traditionally called an "algorithm", the theorem itself doesn't give an algorithm. There is an algorithm presented in the proof, which is in essense division by repeated subtraction.

Proof. We use the well-ordering property.

Consider the set S of non-negative integers of the form $a - bk$ for k an integer. S is nonempty because when k is sufficiently small (possibly negative)–in particular when $k < a/b$–we will have $a - bk \geq 0$.

Since S is a set of non-negative integers, by the well-ordering property it has a least element $r = a - bq$. We will take these values as the values of r, q given in the theorem. By construction $r \geq 0$.

Suppose $r \geq b$. Then $r - b \geq 0$ and thus $r - b = a - b(q + 1)$ is an element of S which is smaller than r, contradicting minimality. Thus $0 \leq r < b$. This proves that the pair q, r exists.

(You can think of this process as conducting division by repeated subtraction. The last step is observing that if $r \geq b$ we can conduct one additional subtraction).

Now let us prove this pair is unique. Suppose we can write $a = q_1 b + r_1 = q_2 b + r_2$, giving us two representations of a as quotient and remainder. By subtracting these two equations we get

$$\begin{aligned} q_1 b + r_1 - (q_2 b + r_2) &= 0 \\ b(q_1 - q_2) &= r_2 - r_1 \end{aligned}$$

and thus b divides $r_2 - r_1$.

But since $0 \leq r_1, r_2 < b$, we know that $-b < r_2 - r_1 < b$. Since b cannot divide a number between 0 and b, we must have $r_2 - r_1 = 0$ and thus $r_2 = r_1$. Consequently $q_2 = q_1$ as well, and the quotient and remainder pair is unique. □

Proposition 1.32. *If a and b are integers and at least one is nonzero, then (a, b) is the least positive integer that is an integer linear combination of a and b.*

Proof. By the well ordering property there is a least positive integer that is a linear combination of a and b; call it $d = ma + nb$. We first wish to show that d is a common divisor of a and b—that is, that $d|a$ and $d|b$.

By the division algorithm, we can write $a = dq + r$ for $0 \leq r < d$. But then we can write $r = a - dq$ as a linear combination of a and q; since d is a linear combination of a and b, this

means that r is a linear combination of a and b. In particular

$$r = a - dq = a - (ma + nb)q = (1 - mq)a - (nq)b.$$

Thus r is a linear combination of a and b but $0 \leq r < d$. Since d is the least positive linear combination, we must have $r = 0$

Thus $a = dq$ and so d divides a. An identical argument shows that d divides b, so g is a common divisor of a and b.

Now we much show that d is the *greatest* common divisor. Suppose c is some integer such that $c|a$ and $c|b$. Then by lemma 1.13 on linear combinations, $c|ma + nb = d$, and thus $c \leq d$. Therefore $d = (a, b)$. □

Note that the argument at the end of this proof generalizes:

Proposition 1.33. *If a and b are non-zero integers, then a positive integer d is equal to (a, b) if and only if*

- *$d|a$ and $d|b$, and*
- *If $c|a$ and $c|b$, then $c|d$.*

Proof. Let $d = (a, b)$. Then clearly $d|a$ and $d|b$. Suppose $c|a$ and $c|b$; then by the previous result $d = ma + nb$ and $c|ma + nb = d$.

Conversely, suppose $d|a$ and $d|b$, and that whenever $c|a$ and $c|b$ then $c|d$. Then d is a common divisor of a and b. In particular set $c = (a, b)$. Then we know that $c|d$, and thus $c \leq d$. But since d is a common divisor we also know that $c \geq d$, so $c = d$. □

Remark 1.34. This gives an alternate characterization of the greatest common divisor that does not depend on the usual notion of "less than" or "greater than."

In fact, we can think of divisibility as giving a partial order on the integers; then the greatest common denominator is the greatest common divisor under this partial order as well.

Corollary 1.35. *Integers a and b are relatively prime if and only if there are integers m and n such that $ma + nb = 1$.*

Proposition 1.36. *If a and b are integers, then the set of linear combinations of a and b is the set of integer multiples of (a, b).*

Proof. Set $d = (a, b)$. We first show that every linear combination of a and b is a multiple of d: since $d|a$ and $d|b$, then d divides any linear combination of them (by lemma 1.13).

Now let us show that every multiple of d is a linear combination of a and b. We know that d is a linear combination of a and b, so write $d = ma + nb$. Let kd be some multiple of d. Then $kd = k(ma + nb) = (km)a + (kn)b$ is a linear combination of a and b. □

Corollary 1.37 (Bezout's theorem)**.** *If a and b are integers, then there are integers m and n such that $ma + nb = (a, b)$.*

Remark 1.38. Bezout's theorem is actually a much more general theorem in algebraic geometry about solutions of polynomial equations (alternatively, about the intersections of curves). It was named for Étienne Bézout, and first proved by Claude Bachet.

(Stigler's Law of Eponymy, attributed to Robert Merton, says that no scientific discovery is named after its actual discoverer).

1.5 The Euclidean Algorithm

For further reading on the material in this subsection, consult **Rosen 3.4, PMF 4.1–4.2, Stein 1.1.2**.

In the previous subsection we saw that the greatest common divisor of two numbers is the least positive linear combination of them. But this doesn't quite tell us how to find it. Fortunately, there is a simple algorithm that allows us to find the greatest common denominator of any pair of numbers quite easily.

Unlike the "division algorithm" this is actually an algorithm–which means it gives a set of steps that, when followed, reliably returns an answer. However, it uses the division algorithm to make its steps work.

The basic idea is to repeatedly subtract copies of the smaller number from the larger number, switching repeatedly, until we get to zero. Because linear combinations don't change divisibility, this won't ever change the greatest common denominator, and so we can change our starting (large) problem into a smaller, easier problem. Repeating this step gives us an answer.

To make that argument more rigorous, we need to recall the following lemma:

Lemma 1.39. *If a, b are integers and $a = bq + r$, then $(a, b) = (b, r)$*

Proof. This is precisely Lemma 1.25. □

This allows us to compute gcds easily by reducing big gcd computations to smaller ones.

Example 1.40. Suppose we want to compute $(36, 56)$. Then $56 = 1 \cdot 36 + 20$ so $(56, 36) = (20, 36)$. Now we can see that $36 = 1 \cdot 20 + 16$ and thus $(20, 36) = (20, 16)$. Then $20 = 1 \cdot 16 + 4$ so $(20, 16) = (4, 16) = 4$. Thus $(36, 56) = 4$.

Theorem 1.41 (Euclidean Algorithm)**.** *Let a, b be integers with $a \geq b > 0$. Set $r_0 = a, r_1 = b$, and inductively define r_n by the division algorithm, setting $r + n02 = r_{n-1}q_{n-1} + r_n$. We have $r_1 > r_2 > \ldots r_k > 0$, and if r_k is the last nonzero remainder obtained this way, then $r_k = (a, b)$.*

Sketch of proof: By lemma 1.39 we know that each step doesn't change the gcd. Thus the gcd at the end is the gcd at the beginning. If we repeat our step we will eventually get one value to 0, and then the gcd of the two will be the other value. □

Example 1.42. Let us compute $(20, 78)$. We have $78 = 3 \cdot 20 + 18$ so $(20, 78) = (20, 18)$. Then $20 = 1 \cdot 18 + 2$ so $(20, 18) = (2, 18)$.

We can easily see that this is 2, but if we want to keep using the algorithm we compute that $18 = 9 \cdot 2 + 0$ so $(2, 18) = (2, 0) = 2$.

In the language of the algorithm, we have $r_0 = 78, r_1 = 20, r_2 = 18, r_3 = 0 = (20, 78)$.

This might seem overly difficult–isn't it easier to just list all the factors? (Or, for those of you who are sneaking ahead, to break the numbers into their prime factors?)

And indeed for small problems this is easier; most of you could probably compute $(20, 78)$ in your heads. But as the numbers in question get larger—much larger—factorization gets much harder. And Euclid's algorithm does not.

Fact 1.43 (Lamé)**.** *For any pair of natural numbers a, b, the Euclidean algorithm takes at most $\log_2(ab)$ steps to find (a, b).*

For any pair of natural numbers $a > b$, the Euclidean algorithm takes at most $5 \log_{10}(b)$ steps to find (a, b).

2 Prime Numbers

2.1 Primes and factorizations

For further reading on the material in this subsection, consult **Rosen 3.1; PMF 3.2, Stein 1.1.1, 1.1.3**.

We've talked about relatively prime–when a number shares no divisors with another number. Is it possible to have a number that is absolutely prime–it has no common divisors with any number?

Well, not really. After all, a number has common divisors with itself. And it has common divisors with any of its multiples. But we can *almost* make this work.

Definition 2.1. A natural number $n > 1$ is *prime* if it is not divisible by any natural numbers other than 1 and itself.

A natural number $n > 1$ that is not prime is *composite*.

Example 2.2. $2, 3, 5, 11, 97, 127$ are all prime.

$4, 8, 57, 91, 255$ are all composite.

Remark 2.3. 1 is neither prime nor composite, by definition. During this course we will see how this continually makes definitions and theorems simpler to state.

Remark 2.4. It's perfectly reasonable to talk about negative numbers being prime or composite; in this context -2 and -3 would be prime, -4 composite, and -1 neither (technically, a "unit"). However, none of our references do so. We will mostly restrict ourselves to positive integers, but on occasion may (perhaps inadvertently) abuse our terminology to discuss negative primes.

Exercise 2.5. *Let p be a prime and n and integer such that p does not divide n. Prove that* $\gcd(p, n) = 1$.

We said on the first day that a major theme of this course will be understanding the distribution of the prime numbers. We will finish this section by proving that there are infinitely many prime numbers, which is the first major result on this subject.

Lemma 2.6. *Every integer greater than 1 can be written as a product of primes.*

This is a very important theorem (and in fact is half of the Fundamental Theorem of Arithmetic, which we will discuss later in this section). We can prove this either using the well-ordering property, or using strong induction. Since these are both important techniques, I will present both proofs.

Proof by well-ordering. Suppose (for contradiction) that there is an integer greater than 1 with no prime factors. Then the set of all such integers must have a least element, by the well-ordering property. So let n be the smallest integer > 1 that cannot be written as a product of primes.

If n is prime, then it can be written as a product of 1 prime; thus n must be composite. Thus it must have some other divisor, and we can write $n = ab$ with $1 < a, b < n$.

Since $1 < a, b < n$ and n is the smallest integer that cannot be written as a product of primes, we know that a and b can both be written as products of primes. Since $n = ab$ we can write n as a product of primes, yielding a contradiction. □

Proof by induction. Let $n > 1$ be a number, and suppose the lemma holds for every $k < n$. We consider two cases:

Suppose n is prime. Then n can be written as a product of one prime, n.

Now suppose $n > 1$ is not prime. Then n is composite, and we can write $n = ab$ for $1 < a, b < n$. Then by our inductive hypothesis, a and b can both be written as a product of primes, since $1 < a, b < n$.

But $n = ab$ and a and b can be written as a product of primes, so n can also be written as a product of primes.

Question for the reader: where is the base case here? □

Remark 2.7. This is stronger than Lemma 3.1 in Rosen. It is proved later, after Lemma 3.5 in Rosen, instead. But 3.1 is a clear corollary of this lemma, and the proofs are essentially the same.

Theorem 2.8 (Euclid)**.** *There are infinitely many primes.*

Proof. Suppose there are only finitely many primes; call them $p_1, \dots, p_n$. Consider the number

$$Q_n = p_1 p_2 \dots p_n + 1 = \prod_{k=1}^{n} p_k + 1.$$

By the previous lemma 2.6 we know that Q_n can be written as a product of primes, and in particular has at least one prime factor q.

Suppose $q = p_j$ for some p_j in our finite list of primes. We know that

$$Q_n - p_1 \dots p_n = 1$$

and q divides both Q_n and $p_1 \dots p_n$ (the first by hypothesis; the second because $q = p_j$. Then by lemma 1.13 on linear combinations we see that q divides 1.

But no prime divides 1, so this is a contradiction. Thus there must be infinitely primes.

Question: where did we use the assumption that the set of primes is finite? □

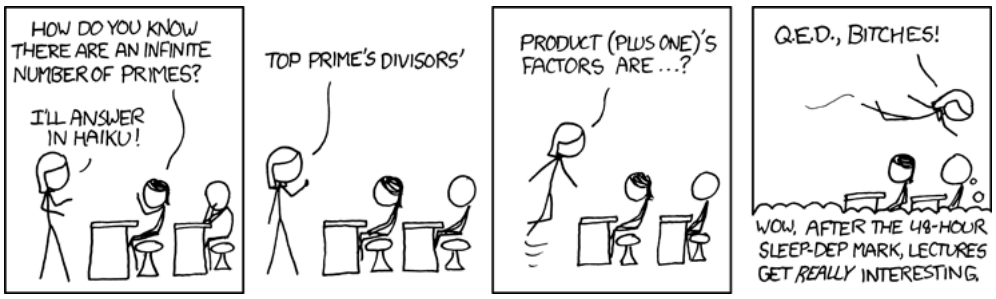

Figure 2.1: `http://xkcd.com/622`

Remark 2.9. If we have some finite list of primes $p_1, \ldots, p_n$, we do not know that $p_1 \ldots p_n + 1$ is prime. We just know that there is some prime that was not on our list.

For instance, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 * 509$.

2.2 The Fundamental Theorem of Arithmetic

For further reading on the material in this subsection, consult **Rosen 3.5, PMF 6.1–6.2, Stein 1.1.4**.

In the previous section we showed that every natural number greater than 1 can be written as a product of primes. Further, if we allow "empty products" with zero factors, then 1 is also a product of primes; and it's clear that if we allow multiplication by ± 1 we have a prime factorization of any non-zero integer.

However, if we wish to reliably decompose integers into their prime factorizations, we would like to get the same factorization every time. Thus we would like to show that there is only one possible prime factorization of any given number.

There is one roadblock we need to be careful of. We can factor $6 = 2 \cdot 3$ or $6 = 3 \cdot 2$. We can write $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$. So these numbers have two or three "different" factorizations. But we intuitively want to treat these as the same, "up to order."

Conveniently, working in the integers we can use the natural total order to remove any ambiguity.

Theorem 2.10 (Fundamental Theorem of Arithmetic)**.** *Every natural number can be written uniquely as a product of primes in non-decreasing order.*

We can write this theorem in a more general and precise form.

Theorem 2.11 (Fundamental Theorem of Arithmetic, General Form)**.** *Every non-zero integer can be written uniquely as a product*

$$n = \pm p_1^{e_1} \dots p_n^{e_n}$$

for some primes p_i with $p_i < p_{i+1}$, and $e_i \in \mathbb{N}$.

In order to prove this theorem we will first need a couple of lemmas.

Lemma 2.12 (Euclid's Lemma)**.** *Suppose a, b, c are integers such that $(a, b) = 1$ and $a|bc$. Then $a|c$.*

Proof. Because $(a, b) = 1$, there are integers m, n such that $ma + nb = 1$. Multiplying by c gives the equation $mac + nbc = c$. Then a divides mac (clearly) and divides nbc since it divides bc; by Lemma 1.13 on linear combinations we see that a divides $mac + nbc = c$. □

Lemma 2.13. *Let p be a prime number and let a, b be integers. If $p|ab$ then $p|a$ or $p|b$.*

Proof. Suppose $p|ab$. If $p|a$ we're done, so we will suppose $p \not| a$ and prove that $p|b$.

Since p is prime, $(p, a) = 1$ by exercise 2.5. Then by Euclid's Lemma 2.12, we know that $p|b$.

□

Exercise 2.14 ($\star$)**.** *Let $a_1, \dots, a_n$ be integers, and let p be a prime. Prove that if $p|a_1 \dots a_n = \prod_{i=1}^{n} a_i$, then $p|a_i$ for some i.*

Remark 2.15. We can actually take the property in Lemma 2.13 as the definition of a prime number. In the integers the two concepts are the same; in larger collections of numbers this is not the case.

In algebraic number theory, this divisibility property becomes the definition of a "prime", and our original definition becomes the definition of an "irreducible."

Exercise 2.16. *Let $p > 1$ be an integer with the following property: whenever a, b are integers and $p|ab$, then $p|a$ or $p|b$. Prove that p is prime.*

We are now ready to prove the Fundamental Theorem. We will prove the simpler version; the more general version is an obvious extension.

Proof of the Fundamental Theorem of Arithmetic. Let $n > 1$ be a natural number. In Lemma 2.6 we showed that n can be written as a product of primes, so we only need to show that any factorization is unique.

Suppose n can be written as a product of nondecreasing primes in two different ways; that is, suppose

$$n = p_1 \dots p_s = q_1 \dots q_t$$

with p_i, q_i prime, and $p_i \leq p_{i+1}, q_i \leq q_{i+1}$. (We cannot guarantee $p_i < p_{i+1}$ since some numbers have repeated factors; for instance we would write $36 = 2 \cdot 2 \cdot 3 \cdot 3$.)

We may divide through by all the common factors in the two lists, and get an equation

$$p_{i_1} \dots p_{i_e} = q_{j_1} \dots q_{j_f}$$

which still holds, and has no prime present on both sides of the equation. But then we have

$$p_{i_1} | q_{j_1} \dots q_{j_f}$$

and by Exercise 2.14 we see that $p_{i_1} | q_{j_k}$ for some k. Since q_{j_k} is prime, it is divisible only by 1 and itself; since $p_{i_1} \neq 1$, we must have $p_{i_q} = q_{j_k}$, which is a contradiction.

Thus we cannot have two distinct such prime factorizations, and the prime factorization must be unique. □

2.3 Where are the primes?

For further reading on the material in this subsection, consult **Rosen 3.1-2, PMF 3.3**.

We've now proven that multiplicatively, we can reduce all natural numbers uniquely into primes. Thus, if we understand the prime numbers completely, we will understand the multiplicative structure of the natural numbers. Unfortunately, understanding of the primes has been notoriously elusive.

2.3.1 The Sieve of Eratosthenes

One of the earliest attempts to find the prime numbers was by Eratosthenes of Cyrene in the third century BCE. Eratosthenes realized that we can make a list of prime numbers by an iterative process.

We make a list of the first, say, hundred numbers, and cross off one because it a unit. The first uncrossed on the list, 2, is prime; we write it down, and then discard it and all its multiples (which of course aren't prime since they're divisible by 2).

Now the first uncrossed number, 3, is prime, since it's not divisible by any smaller prime. Now we can cross 3 and all its multiples. The first uncrossed number, 5, is prime, and we can repeat the process; at the end we will know all the primes on our list.

A process like this is called a "sieve" because it sifts the primes out of a larger set of numbers. There is a substantial body of research known as "sieve theory" which formulates better sieves and arguments based on sieves. Some of these more sophisticated sieves and sieve arguments could make a good paper. These advanced sieving methods have allowed us to build large lists of primes; as of August 2019, the largest known prime is the *Mersenne Prime* $2^{74,207,281} - 1$.

Unfortunately, sieve theory has a major weakness known as the "parity problem":

Fact 2.17 (Parity Problem)**.** *It is not possible for a purely sieve-theory-based argument to differentiate primes from numbrs which are the product of two primes.*

We shall discuss an example problem where this is an issue shortly. Of course, there is a great deal of work trying to get around this limitation of sieve theory.

This technique also gives us a (very!) rough estimate for how many primes there are up to a given number. In the first step of the sieve of Eratosthenes, we throw away about half of our numbers. In the second step, we throw away a third–but wait, we've counted some of them twice, so add a sixth of our numbers back in. In the third step we throw out a fifth, but then we need to add back in a tenth and a fifteenth, but then we have to throw out a thirtieth again.

In the limit, we expect the fraction of numbers which are prime to be roughly

$$1 - \sum_p \frac{1}{p} + \sum_{p \neq q} \frac{1}{pq} - \sum_{p \neq q \neq r} \frac{1}{pqr} + \dots$$

Unfortunately, error terms in this approximation build quickly enough that getting good data out of this is hard–in particular we run up against the parity problem very hard.

2.3.2 Counting Primes and the Prime Number Theorem

Based on data from algorithms like the sieve of Eratosthenes, mathematicians in the 1700s and 1800s wished to estimate the density of primes.

Definition 2.18. The function $\pi(x)$ is the number of prime numbers less than or equal to x. Thus $\pi(10) = 4$ and $\pi(100) = 25$.

Legendre (1798) used counts of prime numbers by Vega to estimate that $\pi(x)$ was approximated by

$$\frac{\log x}{x - 1.08366}.$$

This was not quite correct, and Gauss came up with a more accurate conjecture, that

$$\pi(x) \sim \frac{x}{\log x} \sim Li(x) = \int_2^x \frac{dt}{\log t}.$$

Chebyshev (1850) produced a great deal of work towards this, but the result was not proven until Hadamard and de la Vallée-Poussin (1896) independently proved the Prime Number Theorem:

Theorem 2.19 (Prime Number Theorem)**.**

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

2.3.3 Riemann Zeta Function

Though several proofs exist today, including elementary proofs by Selberg and Erdős (1949), the Prime Number Theorem was originally proved using results from complex analysis. Riemann (1859) defined the *Riemann Zeta Function*

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p \frac{1}{1-p^{-s}}$$

(and the equality of the two formulas can be proved using the Fundamental Theorem of Arithmetic).

The Riemann Zeta Function underlies a number of the most sought-after results in number theory today. It controls and describes a great deal of the "deep structure" of the distribution of prime numbers, and I hope to return later in the course and discuss it in more detail. Of particular note is the famous Riemann Hypothesis:

Conjecture 2.20. *If s is a complex number with $\zeta(s) = 0$, then either s is a negative even integer, or the real part of s is equal to $1/2$.*

Proving this result would imply a number of important facts about the primes; in particular, it would imply that the error in the approximation given in the Prime Number Theorem is very small. People often say that the Riemann Hypothesis would essentially imply that the primes are distributed randomly.

2.3.4 Arithmetic Progressions

Let's examine this idea of random distribution a bit more. It's pretty clear that there are very few primes that are, say, multiples of three. However, if the primes are "random" we shouldn't expect there to be more primes of the form $3n+1$ than $3n+2$. Similarly, there

are no primes of the forms $4n$ or $4n+2$ but we would expect "equally many" of the forms $4n+1$ and $4n+3$. Indeed, our data seem to imply this.

There are some very precise formulations of this idea (and again, exploring these could make a good paper). But the simplest version of the idea would simply expect all of these sets to be infinite. This was indeed proven by Dirichlet in 1837.

Theorem 2.21 (Dirichlet)**.** *If $a, b \in \mathbb{N}$ with $(a,b) = 1$, then the set $\{an+b : n \in \mathbb{N}\}$ has infinitely many primes.*

An *arithmetic progression* is just a set of this form $\{an+b : n \in \mathbb{N}\}$, in which the difference between consecutive elements is constant. Thus Dirichlet proved that all non-trivial arithmetic progressions that don't start at 0 have infinitely many primes. Note we could also phrase this in terms of modular arithmetic: the set of primes equivalent to b mod a is infinite if $(a,b) = 0$.

We can also turn this question around and approach from the other angle. Dirichlet proved that every (reasonable) arithmetic progression contains infinitely many primes. We can ask instead whether the set of primes contains arithmetic progressions.

Green and Tao (2004) proved that the set of primes contains arithmetic progressions of any length–thus if you want a set of thirty consecutive primes which are equal distances apart, you can find one.

2.3.5 Prime Gaps

We just said that there are infinitely many times when the primes are spaced reasonably closely. But if each number has a $1/\log n$ chance of being prime, then *on average* we would expect the space p_n and p_{n+1} to be about $\log(p_n)$.

However, there is dramatic variance in both directions. It's clear that the smallest possible gap that can occur regularly is of size 2. In fact, we suspect that this happens infinitely often.

Conjecture 2.22 (Twin Primes)**.** *There are infinitely many prime numbers p such that $p+2$ is also prime.*

Sieve theory has gotten us halfway to proving this result:

Theorem 2.23 (Chen)**.** *There are infinitely many primes p such that $p+2$ is either prime or the product of two primes.*

You might note that this is as close as we can get before running into the parity problem again.

We do know that twin primes are considerably rarer than primes. In particular, the sum of the reciprocals of the primes $\sum \frac{1}{p}$ diverges, similar to the harmonic series. But the sum of the reciprocals of the twin primes converges–thus while they may be infinite, they are not very infinite.

Recently, it was proven that there is some constant c so that there are infinitely many pairs of primes $p, p+N$. The polymath project has proven the smallest such N is at most 246.

Notice that we can't really look for triples $p, p+2, p+4$, since one of those will be divisible by 3. Thus any triple of such primes must contain 3, and the only one is $3, 5, 7$.

We can also look in the other direction: how *large* can the gaps between consecutive primes get? It turns out that these gaps also get infinitely large, as you will prove on your homework.

Exercise 2.24. *Prove that for any $n \in \mathbb{N}$, there are at least n consecutive composite integers. Hint: consider $(n+1)! + 2$.*

2.4 Primality Testing and Factorization

For further reading on the material in this subsection, consult **Rosen 3.1,3.6**.

The previous subsection stated a lot of results about the general distribution of prime numbers. Now we will scale down a bit and figure out how to look at individual numbers–to determine if they are primes, and factor them if they are not.

If we want to factor a natural number n, or just tell whether it's prime, the obvious idea is to try dividing by all the numbers smaller than n; an obvious optimization is to just divide by all the primes, if we have a list of primes, since every composite number has a prime factor.

One more optimization is not too hard to see:

Lemma 2.25. *If n is a composite number, then n has a prime factor no larger than $\sqrt{n}$.*

Proof. Since n is composite, we can write $n = ab$ for $1 < a \leq b < n$. Then if $a > \sqrt{n}$ then $ab \geq a^2 > (\sqrt{n})^n = n$. Thus $a \leq \sqrt{n}$, and a has at least one prime factor p (which might be the same as a). Thus $1 < p \leq a \leq \sqrt{n}$. □

Thus to test if n is prime, or to attempt to factor it, we only need to try dividing by every prime smaller than $\sqrt{n}$.

2.4.1 Fermat Factorization

Fermat developed a factorization technique that is often better than the naive approach, although substantially limited. The basic idea comes from the following lemma:

Lemma 2.26. *If n is an odd positive integer, then there is a one-to-one correspondence between factorizations of n into two positive integers, and pairs of squares whose difference is n.*

Proof. Let n be an odd positive integer, and suppose $n = s^2 - t^2$. Then we can factor $n = (s-t)(s+t)$ and thus we have a factorization into two positive integers.

Conversely, let$n = ab$ be a factorization into two positive integers. Then we can observe that if we set $s = (a+b)/2$ and $t = (a-b)/2$, then

$$s^2 - t^2 = \frac{a^2 + 2ab + b^2}{4} - \frac{a^2 - 2ab + b^2}{4} = \frac{ab}{2} - \frac{-ab}{2} = ab = n.$$

□

Thus if we can write $n = x^2 - y^2$ as a difference of squares, we have a factorization. This might not seem like a huge advance, since we've replaced one non-obviously-easy problem with another, but it leads to a more straightforward algorithm:

Set t to be the least integer greater than $\sqrt{n}$ so that t^2 is the least square larger than n. Then start computing the sequence

$$t^2 - n, (t+1)^2 - n, (t+2)^2 - n, \dots$$

and examine it for squares; if we find a square s^2 in this sequence, we have a factorization of $n = t^2 - s^2 = (t-s)(t+s)$.

This algorithm always terminates, because it will eventually reach $t = (n+1)/2$ and yield the equations

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = n \cdot 1.$$

Example 2.27. Let's factor 16899. We use a calculator to compute that $\sqrt{16899} \approx 129.996$, so we start at 130. We compute

$$130^2 - n = 16900 - 16899 = 1 = 1^2$$

So we have

$$16899 = 130^2 - 1^2 = (130-1)(130+1) = 129 \cdot 131.$$

Example 2.28. Let's factor 3827. We compute $\sqrt{3827} \approx 61.8$, so we start at 62. We compute

$$62^2 - 3827 = 3844 - 3827 = 17$$
$$63^2 - 3827 = 3969 - 3827 = 142$$
$$64^2 - 3827 = 4096 - 3827 = 269$$
$$65^2 - 3827 = 4225 - 3827 = 398$$
$$66^2 - 3827 = 4356 - 3827 = 529 = 23^2$$

so we have $t = 66, s = 23$, and thus

$$3827 = 66^2 - 23^2 = (66 - 23)(66 + 23) = 43 \cdot 89.$$

Unfortunately, the worst-case performance of this algorithm is actually pretty bad; in the worst case, we have to check $(n+1)/2 - \sqrt{n}$ integers. But this algorithm works well in "good" cases where our integer n has two factors of similar size. And many more advanced factorization techniques are based on this idea.

2.4.2 Efficient Factorization Algorithms

There are of course more efficient factorization methods, some of which we will see later in the course, after we study modular arithmetic. There are a few that are outside of the scope of this course, but which I want to mention now.

The second most efficient known classical algorithm is the *quadratic sieve* of Carl Pomerance (1981), which takes approximately $e^{\sqrt{\log n \log\log n}}$ operations to factor an integer n. This algorithm is basically a method for making Fermat factorization efficient by trying many possible square differences in parallel. Explaining this algorithm would probably make a good paper. This algorithm is in fact the most efficient for numbers smaller than 10^{100} and is still in wide use.

The most efficient known classical algorithm is the *general number field sieve* of Buhler, Lenstra, Pomerance. This takes approximately

$$e^{\sqrt[3]{64/9}(\log n)^{1/3}(\log\log n)^{2/3}}$$

operations to factor an integer n. This algorithm holds the record for the largest computed prime factorization; in 2009 a group of researchers used hundreds of computers to factor a 232-digit number called "RSA-768" used for some cryptographic applications.

Remark 2.29. Note that you could write both of these as polynomials in n, but for complexity reasons we actually want to count the number of *bits* it takes to represent n, which is approximately $\log n$. So rather than writing the times as polynomial in n we write them as exponential in $\log n$.

Thus there is no known classical algorithm that factors a large integer in polynomial time; we say that we do not believe integer factorization is "in P".

The most efficient known algorithm at all is Shor's Algorithm, formulated by Peter Shor in 1994. This algorithm runs only on quantum computers, and takes approximately $(\log n)^2(\log\log n)(\log\log\log n)$ steps to factor an integer n. Thus *on a quantum computer* it is possible to to factor an integer in polynomial time (we say the integer factorization problem is "in BQP").

2.4.3 Prime testing and prime certificates

While it is generally difficult to factor a large number, it turns out that it is much easier if we just want to know whether a number is prime. We can in fact (somewhat frustratingly) prove a number is or isn't prime, while having no idea what its factors are if it is composite.

In 2002, Agrawal, Kayal, Saxena found an algorithm that can prove an integer to be prime in about $(\log n)^{12}$ operations. In fact this algorithm has been improved to work in $(\log n)^{6+\epsilon}$ operations for any $\epsilon > 0$; if a certain widely believed conjecture is true, it in fact works in $(\log n)^6$ operations.

A different algorithm by Miller (1975) will in fact work in $(\log n)^5$ operations, if the Generalized Riemann Hypothesis is true.

Remark 2.30. These results imply that the prime factorization problem is definitely in NP, which roughly means that a proposed solution can be *checked* in polynomial time, even if it takes longer to generate a solution. Given a factorization of a large integer, it is easy to check it is correct by multiplying all the numbers together, and by these results we can also confirm that every factor is in fact prime in polynomial time.

However, prime factorization is *not* (known to be) NP-complete. Many researchers believe that it is simultaneously impossible to solve in polynomial time, but easier in some sense than problems like the Travelling Salesman or the Shortest Vector Problem.

In all of this section, we've been studying "deterministic" algorithms, that definitely return the correct answer. But if we only want answers that are "probably" right, then prime testing becomes much easier. In order to understand this, we need to develop some tools from modular arithmetic.

3 Modular arithmetic

For further reading on the material in this subsection, consult **Rosen 4.1, PMF 7.1-2, Stein 2.1, Shoup 2.1-2,2.5**.

Modular arithmetic is a powerful tool that lets us do arithmetic while preserving information about divisibility, and has a broad range of number theory applications. We'll be studying various aspects of it for the next few sections.

3.1 Congruences

Definition 3.1. Let m be a positive integer. If a, b are integers, we say that a is congruent to b modulo m, and write $a \equiv b \mod m$, if m divides $a - b$.

Proposition 3.2. *The congruence* $\mod m$ *relation is an equivalence relation; that is:*

- *(Reflexive Property) If a is an integer, then $a \equiv a \mod m$.*
- *(Symmetric Property) If a, b are integers and $a \equiv b \mod m$ then $b \equiv a \mod m$.*
- *(Transitive property) If a, b, c are integers, and $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.*

Proof.

- We see that $m|0 = (a - a)$ so $a \equiv a \mod m$.
- If $a \equiv b \mod m$ then $m|a - b$, which means that there is an integer k such that $km = a - b$. Then $(-k)m = b - a$ so $m|b - a$ so $b \equiv a \mod m$.
- If $a \equiv b \mod m$ and $b \equiv c \mod m$ then $m|a - b$ and $m|b - c$. By the lemma on linear combinations, $m|(a - b) + (b - c) = a - c$, so $a \equiv c \mod m$.

□

You should recall from Math 210 that an equivalence relationship partitions a set into *equivalence classes*, which in this case are called *congruence classes* $\mod m$. Two integers are in the same congruence class $\mod m$ if they are congruent to each other. For a fixed integer m, there are precisely m congruence classes $\mod m$. For example, if $m = 2$, the two congruence classes are even integers (congruent to $0 \mod m$) and odd integers (congruent to $1 \mod m$).

We'd like to pick canonical representatives of each equivalence class. There are a few different ways to do this.

Definition 3.3. Let a be an integer and m a positive integer. By the Division Algorithm, there is a unique r with $0 \leq r < m$ such that $a = mq + r$ for some integer q. We call this r the *reduction of $a \mod m$.*

Proposition 3.4.
- *The reduction of $a \mod m$ is congruent to $a \mod m$.*
- *The reduction of $a \mod m$ is an element of the set $\{0, 1, \ldots, m-1\}$.*

Proof.
- Let r be the reduction of $a \mod m$. Then $a = mq + r$ for some integer q, so $a - r = mq$ is divisible by m. Thus $a \equiv r \mod m$.
- We know that r is an integer with $0 \leq r < m$ from the division algorithm.

□

Definition 3.5. We say a set S is a *complete system of residues* $\mod m$ if any integer a is congruent $\mod m$ to exactly one element of S.

Corollary 3.6. *The set $\{0, 1, \ldots, m-1\}$ is a complete system of residues* $\mod m$. *We sometimes call it the set of* least nonnegative residues $\mod m$. *I will sometimes write $\mathbb{Z}/m\mathbb{Z}$ for this set.*

Example 3.7. The set $\{1, 5, 9\}$ is a complete system of residues $\mod 3$.

Example 3.8. If m is an odd positive integer, then the set

$$\left\{-\frac{m-1}{2}, -\frac{m-2}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}\right\}$$

is a complete system of residues $\mod m$. We sometimes call it the set of *absolute least residues* $\mod m$.

Exercise 3.9. *Let S be a set of m integers such that no element of S is congruent to any other element of $S \mod m$. Prove that S is a complete system of residues.*

Possibly the most useful fact about congruences is that they behave well with respect to basic arithmetic operations.

Theorem 3.10. *If a, b, c, d, m are integers with $m > 0$, and $a \equiv b \mod m$ and $c \equiv d \mod m$, then*

1. $a + c \equiv b + d \mod m$
2. $a - c \equiv b - d \mod m$

3. $ac \equiv bd \mod m$.

Proof. Since $m|a-b$ and $m|c-d$, there are integers k, ℓ such that $km = a-b$ and $\ell m = c-d$. Then

1. $(a+c)-(b+d) = (a-b)+(c-d) = km + \ell m = (k+\ell)m$. Thus $m|(a+c)-(b+d)$ and $a+c \equiv b+d \mod m$ by definition.
2. The same proof holds here.
3. $ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d) = ckm + b\ell m = m(ck + b\ell)$. Thus $m|ac-bd$ and $ac \equiv bd$ by definiton.

□

Remark 3.11. For those of you who have taken algebra: we can interpret these results as showing that the set of integers $\mod m$ form an abelian group under addition, and in fact form a ring under the usual addition and multiplication. Then the reduction modulo m map is a group (or ring) homomorphism from the integers to the integers modulo m. And in this case we can interpret $\mathbb{Z}/m\mathbb{Z}$ as the quotient of the integers with respect to the kernel of this homomorphism. See PMF 8.1-2, or Stein or Shoup for more on this perspective.

Remark 3.12. Note that division is *not* on this list. Division in modular arithmetic is in fact somewhat subtle, in contrast to the straightforwardness of addition and multiplication.

For instance, we see that $7 \cdot 2 = 14 \equiv 8 = 4 \cdot 2 \mod 6$. But it is not true that $7 \cdot 4 \mod 6$.

Exponentiation, however, works as well as we'd like.

Lemma 3.13. *Let a, b, k, m be integers with $k, m > 0$, and $a \equiv b \mod m$. Then $a^k = b^k \mod m$.*

Proof. Recall that

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}) = (a-b)\prod_{i=0}^{k-1} a^{k-1-i}b^i.$$

Thus since $m|(a-b)$, we also know that $m|a^k - b^k$ and so $a^k \equiv b^k \mod m$ by definition. □

Remark 3.14. The converse is not actually true, which is easy to see: e.g. $1^2 \equiv 2^2 \mod 3$.

Remark 3.15. When computing the reduction mod p of some large exponent, it's hopelessly inefficient to do the entire exponentiation and then do a division. It's moderately more efficient to see what power you need to raise the base to to get a reduction, and then iterate: e.g. if I want to compute $2^{100} \mod 5$ I will observe that $2^4 = 16 \equiv 1 \mod 5$, and thus $2^{100} = (2^4)^{20} \equiv 1^{20} \equiv 1 \mod 5$.

Rosen covers a more efficient way still towards the end of §4.1, which turns the problem mostly into a huge bitwise XOR.

Corollary 3.16. *Let n be an integer. Then $3|n$ if and only if 3 divides the sum of the (base ten) digits of n.*

Proof. Write $n = n_0 + n_1 \cdot 10^1 + n_2 \cdot 10^2 + \cdots + n_k \cdot 10^k$ (with $0 \leq n_i \leq 9$). We notice that $10 \equiv 1 \mod 3$ and thus for any $\ell > 0$, $10^\ell \equiv 1^\ell = 1 \mod 3$. Thus

$$n \equiv n_0 + n_1 + \cdots + n_k \mod 3$$

and the right-hand side is the sum of the decimal digits.

Then in particular $n \equiv 0 \mod 3$ if and only if the sum of the digits is congruent to 0 mod 3, as desired. □

Remark 3.17. Similar arguments can be made for divisibility by other integers, like 9 or 11.

3.2 Linear Congruences and Modular Division

For further reading on the material in this subsection, consult **Rosen 4.1-2, PMF 8.3, Stein 2.1.1, Shoup 2.3**.

Modular division is a bit trickier to understand than other modular arithmetic. Recall our earlier example:

Example 3.18. $8 \equiv 2 \mod 6$ but $4 \not\equiv 1 \mod 6$.

However, you might notice that $4 \equiv 1 \mod 3$; we have essentially divided the *modulus* by 2 as well as the two equivalent integers. It turns out that this is basically what's going on.

Proposition 3.19 (Modular cancellation law)**.** *Let a, b, c, m be integers with $m > 0$, and set $d = (c, m)$. Then if $ac \equiv bc \mod m$ then $a \equiv b \mod m/d$.*

Proof. If $ac \equiv bc \mod m$ then $m|ac - bc = c(a - b)$, so there is a k with $km = c(a - b)$. Dividing through by d gives $km/d = c/d(a - b)$. Thus $m/d|(c/d)(a - b)$.

But $(m/d, c/d) = 1$, so we know that $m/d|a - b$ and thus $a \equiv b \mod m/d$. □

Corollary 3.20. *Let a, b, c, m are integers with $m > 0$ and $(c, m) = 1$. Then if $ac \equiv bc \mod m$ then $a \equiv b \mod m$.*

But often we would really like not to change the modulus. Thus we ask ourselves how division works with respect to a fixed modulus.

To answer this question, let's think about what division really means. Division is in essence undoing multiplication. So when we compute b/a, we are actually solving the equation $ax = b$ for x. Similarly, if we want to understand modular division, we should study the congruence $ax \equiv b \mod m$.

Definition 3.21. A congruence of the form $ax \equiv b \mod m$, where a, b are constant integers and x is unknown, is a *linear congruence in one variable.*

First notice that if this congruence has any solution, it has infinitely many. Suppose x_0 is a solution to this equation, and x_1 is an integer such that $x_1 \equiv x_0 \mod m$. Then $ax_1 \equiv ax_0 \equiv b \mod m$ so x_1 is another solution.

Thus if x_0 solves a linear congruence $\mod m$, any element of its congruence class will. (This will generally be the case for solving congruences, whether linear or not). But in modular arithmetic we tend to want to treat elements of the same congruence class as being the same.

The next question we might ask is *how many* solutions a given congruence has? Non-modularly, a linear equation $ax = b$ has either zero solutions (when b is not divisible by a), or exactly one solution (when it is). The modular situation is a bit more complicated; fortunately, we have already done some work towards solving this problem in another form.

Lemma 3.22 (Linear Diophantine Equations)**.** *Let a, b be integers with $d = (a, b)$. Then the equation $ax + by = c$ has solutions if and only if $d \mid c$.*

Further, if $d|c$ then there are infinitely many solutions, all of which have the following form: if x_0, y_0 is some particular solution, the set of all solutions is given by

$$x = x_0 + (b/d)t, \qquad y = y_0 - (a/d)t$$

where t is an integer.

Proof. The first statement was show in Homework 2 problem 1.

Suppose $d|c$ and let (x_0, y_0) be a solution. Then

$$\begin{aligned} a(x_0 + (b/d)t) + b(y_0 - (a/d)t) &= ax_0 + abt/d + by_0 - abd/t \\ &= ax_0 + by_0 = c. \end{aligned}$$

Thus every pair of this form is a solution, and there are infinitely many solutions.

Finally, we prove every solution is of this form. Suppose x, y are integers with $ax+by = c$. Then subtracting $ax_0 + by_0 = c$ from this equation gives

$$\begin{aligned} a(x - x_0) + b(y - y_0) &= 0 \\ a(x - x_0) &= b(y - y_0) \\ (a/d)(x - x_0) &= (b/d)(y - y_0). \end{aligned}$$

Since $(a, b) = d$, we know that $(a/d, b/d) = 1$ and thus $(a/d)|(y - y_0)$. Thus there is an integer t with $(a/d)t = y - y_0$, which we can rewrite $y = y_0 + (a/d)t$.

Plugging this in to our earlier equation gives

$$\begin{aligned} a(x - x_0) &= b(a/d)t \\ x - x_0 &= (b/d)t \\ x &= x_0 + (b/d)t \end{aligned}$$

as desired. □

Proposition 3.23. *Let a, b, m be integers with $m > 0$, and set $(a, m) = d$. If $d \nmid b$, then $ax \equiv b \mod m$ has no solutions. If $d|b$, then $ax \equiv b \mod m$ has exactly d "distinct" or incongruent solutions modulo m.*

Proof. The key step here is to turn our linear congruence in one variable into a linear equation in two variables. We know that $ax \equiv b \mod m$ if $m|ax - b$, which is true precisely when there is some integer y such that $my = ax - b$. Thus x is a solution to $ax \equiv b \mod y$ if and only if there is a y such that (x, y) is a solution to $ax - my = b$.

We showed in homework 2 problem 1 that $ax - my = b$ has solutions if and only if $d = (a, m)|b$. This proves the first claim.

If $d|b$, then $ax - my = b$ has infinitely many solutions, all of which are given by the formulas

$$x = x_0 + (m/d)t, \qquad y = y_0 - (a/d)t$$

Thus the values $x = x_0 + (m/d)t$ are the infinitely many solutions of the linear congruence.

Finally, we wish to prove that there are d incongruent solutions. Let $x_1 = x_0 + (m/d)t_1$ and $x_2 = x_0 + (m/d)t_2$ be two solutions; they are congruent modulo m if and only if $(m/d)t_1 \equiv (m/d)t_2 \mod m$.

But $(m, m/d) = m/d$, so by the modular cancellation law of proposition 3.19, this holds if and only if $t_1 \equiv t_2 \mod (m/(m/d)) = d$.

Thus we have two incongruent solutions when we have solutions whose t are congruent modulo d but not modulo m. In particular, the set of solutions $\{x = x_0 + (m/d)t : 0 \leq t < d\}$ is a set of d mutually incongruent solutions, □

Corollary 3.24. *If a, b, m are integers with $m > 0$ and $(a, m) = 1$, then the linear congruence $ax \equiv b \mod m$ has a unique solution modulo m.*

This tells us that division is not, in general, unique modulo m; sometimes b is not divisible by a, but sometimes b/a gives multiple reasonable answers. But if $(a, m) = 1$, then division by a modulo m *always* gives one solution, thus every number is uniquely divisble by a.

In even more particular, if p is a prime number, then every number is uniquely divisible by every non-zero number modulo p. We will use this fact a lot during the rest of the course.

Example 3.25. Let's compute $10/4 \mod 14$. I.e. let's find solutions to $4x \equiv 10 \mod 14$. We first note that $(10, 14) = 2$ and $2|10$, so there are exactly 2 incongruent solutions.

We first need to find a particular solution. In small cases like this it's easy enough to just plug numbers in; a more general approach is to use the Euclidean algorithm to write the $2 = -3 \cdot 4 + 1 \cdot 14$ as a linear combination of 4 and 14. We then use this to solve the equation $4x - 14y = 10$, giving us

$$10 = 5 \cdot 2 = 5 \cdot (-3 \cdot 4 + 1 \cdot 14) = -15 \cdot 4 + 5 \cdot 14$$

and thus one solution is given by $x_0 = -15 \equiv 13 \mod 14$ and $y_0 = 10$.

Then a complete set of incongruent solutions is given by

$$x = x_0 + (m/d)t = 13 + (14/2)t = 13 + 7t$$

and thus we have $x = x_0 = 13$ and $x = x_0 + 7 = 20 \equiv 6$.

We can somewhat simplify this process by understanding how reciprocals work.

Definition 3.26. Given an integer a with $(a, m) = 1$, an integer solution x to $ax \equiv 1 \mod m$ is called an *inverse of a modulo m*.

Remark 3.27. Note that we never have a modular inverse if $(a, m) \neq 1$.

Example 3.28. What is a modular inverse of $9 \mod 29$?

We use the Euclidean algorithm:

$$\begin{aligned} 29 &= 3 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 = 4(29 - 3 \cdot 9) + 1 \\ 1 &= 9 - (4 \cdot 29 - 12 \cdot 9) = 13 \cdot 9 - 4 \cdot 29 \end{aligned}$$

thus $(13, 4)$ is a solution to $9x - 29y = 1$ and we see that $9 \cdot 13 \equiv 1 \mod 29$. (In particular, $9 \cdot 13 = 117 = 116 + 1 = 4 \cdot 29 + 1$).

Importantly, if we have a an inverse of $a \mod m$ we can use this to solve other linear congruences of the form $ax \equiv b \mod m$. In particular, if a^{-1} is an inverse of $a \mod m$, then $aa^{-1} \equiv 1 \mod m$ and thus $a(a^{-1}b) \equiv b \mod m$.

Example 3.29. Solve the linear congruence $9x \equiv 5 \mod 29$.

We know that 13 is an inverse for $9 \mod 29$. Thus the unique up to congruence solution for this congruence is $13 \cdot 5 = 65 \equiv 7 \mod 29$.

Notice that every (non-zero) number has a modular inverse modulo p if p is a prime number. We state one result for these special cases.

Lemma 3.30. *Let p be prime. The positive integer a is its own inverse modulo p if and only if $a \equiv 1 \mod p$ or $a \equiv -1 \mod p$.*

Proof. If $a \equiv \pm 1 \mod p$ then $a^2 \equiv (\pm 1)^2 = 1 \mod p$.

Conversely, suppose $a^2 \equiv 1 \mod p$. Then $p | a^2 - 1 = (a+1)(a-1)$, and since p is prime, either $p|(a+1)$ or $p|(a-1)$. In the first case, $a \equiv -1 \mod p$, and in the second case, $a \equiv 1 \mod p$. □

3.3 Multiple Moduli and the Chinese Remainder Theorem

For further reading on the material in this subsection, consult **Rosen 4.1,4.3, PMF 7.4, Stein 2.2, Shoup 2.4**.

All of our results so far, except for a few results on division, have kept the modulus m unchanged. But it is useful sometimes to combine congruences with different moduli, and this is in fact quite possible.

Exercise 3.31. *Let a, b, m, n be integers with $m, n > 0$ and $m|n$. If $a \equiv b \mod n$, then $a \equiv b \mod m$.*

Proposition 3.32. *If $a \equiv b \mod m_1, a \equiv b \mod m_2, \dots, a \equiv b \mod m_k$, then*

$$a \equiv b \mod \operatorname{lcm}(m_1, m_2, \dots, m_k).$$

Proof. We know that $m_1|a-b, m_2|a-b, \dots, m_k|a-b$. Thus the LCM of $m_1, \dots, m_k$ also divides $a-b$ (by e.g. Exercise 5 of HW2), and $a \equiv b \mod \operatorname{lcm}(m_1, \dots, m_k)$ by definition. □

In the past section we solved single congruences. Now we want to turn our attention to solving systems of multiple congruences. The first known discussion of this problem comes from Sunzi Suanjing (also known as Sun Tzu, but not the one who wrote *The Art of War*) in the third century:

"There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there? "

We can rephrase this in our language:

Question 3.33. Suppose we have the following system of congruences:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 2 \mod 7. \end{aligned}$$

What are the possible values of x?

This question was studied by many mathematicians in China, India, the Middle East, and Europe; the first known algorithm to solve the question is due to Aryabhata in the sixth century, and the first known complete solution is due to Qin Jiushao in 1247.

Theorem 3.34 (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \dots, m_r$ be pairwise prime positive integers. Then the system*

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

has a unique solution modulo $M = m_1 m_2 \dots m_r$. Further there is an algorithm for finding the solution.

Proof. First we will present an algorithm that will always find a solution, proving existence. Then we will prove uniqueness modulo M.

For each k, set $M_k = M/m_k = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r$. We see that $(M_k, m_k) = 1$ since m_k is relatively prime to m_j for each $j \neq k$. Thus by modular division we can find an inverse of M_k modulo m_k, which we shall call y_k. Thus $y_k M_k \equiv 1 \mod m_k$.

Now set

$$x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_rM_ry_r.$$

We know that if $i \neq j$, then $M_j \equiv 0 \mod m_i$. Thus we see that for each i, we have

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + \cdots + a_rM_ry_r \\ &\equiv 0 + 0 + \cdots + 0 + a_iM_iy_i + 0 + \cdots + 0 \mod m_i \\ &\equiv a_i(M_iy_i) \mod m_i \\ &\equiv a_i \cdot 1 \mod m_i \end{aligned}$$

and thus x satisfies each congruence.

Now we prove that this solution is unique modulo M. Suppose x_0 and x_1 are both solutions to the system of congruences. Then for each i we know that $x_0 \equiv a_i \mod m_i$ and $x_1 \equiv a_i \mod m_i$ and thus $x_0 \equiv x_1 \mod m_i$.

But then $x_0 \equiv x_1 \mod \operatorname{lcm}(m_1, m_2, \ldots, m_r)$, and since the m_i are all relatively prime $\operatorname{lcm}(m_1, m_2, \ldots, m_r) = m_1m_2 \ldots m_r = M$. □

Example 3.35. Let's solve the system of congruences given earlier:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 2 \mod 7. \end{aligned}$$

Then we have $M = 3 \cdot 5 \cdot 7 = 105$. Then we compute

$$\begin{aligned} M_1 &= 5 \cdot 7 = 35 \equiv 2 \mod 3 & y_1 &= 2 \\ M_2 &= 3 \cdot 7 = 21 \equiv 1 \mod 5 & y_2 &= 1 \\ M_3 &= 3 \cdot 5 = 15 \equiv 1 \mod 7 & y_3 &= 1 \end{aligned}$$

and thus

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233.$$

We can check that 233 satisfies the three equivalences (and in particular, $3 \cdot 77 = 231, 5 \cdot 46 = 230, 7 \cdot 33 = 231$).

A possible last step is to notice that the solution is unique modulo $M = 105$. Thus the least nonnegative solution is $233 = 210 = 23$, which we can easily see satisfies the congruences.

3.4 Systems of linear congruences

For further reading on the material in this subsection, consult **Rosen 4.5, PMF 8.3, Stein 2.3**.

So far we have solved congruences in one variable; we can also try to solve systems of congruences in two or more variables.

In this subsection we will study systems of two linear congruences in two variables. We can generalize this theory to larger systems of linear congruences in more variables, but this requires a substantial dose of linear algebra (similar to the linear algebra involved in solving large systems of linear equations), so we shall pass over it here. If you're interested, this can make a good course paper.

Theorem 3.36. *Let a, b, c, d, e, f, m be integers with $m > 0$. Set $\Delta = ad - bc$ (notice this is the determinant of a 2×2 matrix). Then if $(\Delta, m) = 1$, the system of congruences*

$$\begin{aligned} ax + by &\equiv e \mod m \\ cx + dy &\equiv f \mod m \end{aligned}$$

has a unique solution modulo m, given by

$$\begin{aligned} x &\equiv \Delta^{-1}(de - bf) \mod m \\ y &\equiv \Delta^{-1}(af - ce) \mod m \end{aligned}$$

where Δ^{-1} is a multiplicative inverse of Δ modulo m.

Proof. We can solve these just like we normally solve linear equations. To remove y we see

$$\begin{aligned} adx + bdy &\equiv de \mod m \\ bcx + bdy &\equiv bf \mod m \\ adx - bcx &\equiv de - bf \mod m \\ \Delta x &\equiv de - bf \mod m \end{aligned}$$

Then since $(\Delta, m) = 1$, we know Δ has a multiplicative inverse Δ^{-1}; multiplying by this gives

$$x \equiv \Delta^{-1}(de - bf) \mod m.$$

Thus any solution must satisfy this relation, as claimed.

We can similarly eliminate y from these equations via

$$\begin{aligned} acx + bcy &\equiv ce \mod m \\ acx + ady &\equiv af \mod m \\ ady - bcy &\equiv af - ce \mod m \\ \Delta y &\equiv af - ce \mod m \\ y &\equiv \Delta^{-1}(af - ce) \mod m. \end{aligned}$$

Again, this is the relation we claimed was necessary. Thus we have proven uniqueness.

Now we just need to check that any pair like this is a solution. But then

$$\begin{aligned} ax + by &\equiv a\Delta^{-1}(de - bf) + b\Delta^{-1}(af - ce) \\ &\equiv \Delta^{-1}(ade - abf + abf - bce) \\ &\equiv \Delta^{-1}(ad - bc)e \\ &\equiv \Delta^{-1}\Delta e \equiv e \mod m \end{aligned}$$

and similarly

$$\begin{aligned} cx + dy &\equiv c\Delta^{-1}(de - bf) + d\Delta^{-1}(af - ce) \\ &\equiv \Delta^{-1}(cde - bcf + adf - cde) \\ &\equiv \Delta^{-1}(ad - bc)e \\ &\equiv \Delta^{-1}\Delta e \equiv e \mod m. \end{aligned}$$

□

This analysis could be extended to solve systems with more equations and more variables, but it's mostly an exercise in linear algebra, so we won't do it here.

Example 3.37. Consider the system

$$\begin{aligned} 2x + 3y &\equiv 7 \mod 13 \\ 5x + 2y &\equiv 3 \mod 13 \end{aligned}$$

We have $\Delta = 2 \cdot 2 - 3 \cdot 5 = -11 \equiv 2 \mod 13$, and thus $\Delta^{-1} \equiv 7 \mod 13$. Then the system has a unique solution $\mod 13$, given by

$$\begin{aligned} x &\equiv \Delta^{-1}(de - bf) \equiv 7(2 \cdot 7 - 3 \cdot 3) \equiv 35 \equiv 9 \mod 13 \\ y &\equiv \Delta^{-1}(af - ce) \equiv 7(2 \cdot 3 - 5 \cdot 7) \equiv 7 \cdot (-29) \equiv -21 \equiv 5 \mod 13. \end{aligned}$$

We can check our work by plugging these in:

$$2 \cdot 9 + 3 \cdot 5 \equiv 18 + 15 \equiv 33 \equiv 7 \mod 13$$
$$5 \cdot 9 + 2 \cdot 5 \equiv 45 + 5 \equiv 55 \equiv 3 \mod 13.$$

3.5 Solving Polynomial Congruences

For further reading on the material in this subsection, consult **Rosen 4.4**.

So far we've been looking only at linear congruences. But we can also solve congruences with polynomial equations in the variable.

We can break this problem up into two pieces (as we can with all congruence problems in the future). If we have a congruence modulo $m = p_1^{n_1} \dots p_r^{n_r}$, we can use the Chinese Remainder theorem to split this up into a system of r congruences, modulo each prime power

Example 3.38. Suppose we want to solve the congruence

$$2x^3 + 12x + 4 \equiv 0 \mod 100.$$

We see that $200 = 2^3 5^2$ so we need to solve

$$2x^3 + 12x + 4 \equiv 0 \mod 4$$
$$2x^3 + 12x + 4 \equiv 0 \mod 25.$$

The first we can solve easily enough by testing numbers; we see that it holds when $x \equiv 0$ or $x \equiv 2 \mod 4$. As we shall see below, the second equivalence holds when $x \equiv 19 \mod 25$.

Then by the Chinese Remainder theorem, the congruence $\mod 100$ holds if and only if

$$x = 0 \cdot 25 \cdot 1 + 19 \cdot 4 \cdot 19 = 1444 \equiv 44 \mod 100$$
$$x2 \cdot 25 \cdot 1 + 19 \cdot 4 \cdot 19 = 1494 \equiv 94 \mod 100$$

So we can reduce the problem of solving congruences in general to the problem of solving congruences modulo a prime power (i.e. p^n for some integer n). Fortunately, we can approach these congruences $\mod p^n$ by an even simpler step, by simply solving them $\mod p$.

Example 3.39. We wish to find the solutions to

$$2x^3 + 12x + 4 \equiv 0 \mod 25.$$

First we solve

$$2x^3 + 12x + 4 \equiv 0 \mod 5$$

which we can do by the guess-and-check method:

$$\begin{aligned}
2(0)^3 + 12(0) + 4 &\equiv 4 \mod 5 \\
2(1)^3 + 12(1) + 4 &\equiv 13 \equiv 3 \mod 5 \\
2(2)^3 + 12(2) + 4 &\equiv 1 + 4 - 1 \equiv 4 \mod 5 \\
2(3)^3 + 12(3) + 4 &\equiv 4 + 6 - 1 \equiv 4 \mod 5 \\
2(4)^3 + 12(4) + 4 &\equiv -2 + 8 - 1 \equiv 0 \mod 5
\end{aligned}$$

So this has a solution if and only if $x \equiv 4 \mod 5$.

So what about $\mod 25$? Well, we know any solution must be equivalent to $4 \mod 5$, so we only need to test solutions of the form $4 + 5t$. Plugging this in gives

$$\begin{aligned}
2(4 + 5t)^3 + 12(4 + 5t) + 4 &\equiv 0 \mod 25 \\
2(64 + 240t + 300t^2 + 125t^3) + 48 + 60t + 4 &\equiv 0 \mod 25 \\
3 + 5t + 23 + 10t + 4 &\equiv 0 \mod 25 \\
15t + 5 &\equiv 0 \mod 25
\end{aligned}$$

which holds only if $t \equiv 3 \mod 5$. Thus the only solution $\mod 25$ is 19.

We call this process "lifting", where we start with a solution in some small modulus, and then lift it up to a power of that modulus. We'd like to systematize this, which will require some tools that are annoyingly familiar.

Definition 3.40. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. We define the *derivative* of $f(x)$ to be

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

We use the notation $f^{(k)}(x)$ to denote the result of repeating the derivative k times.

Remark 3.41. This should be familiar from calculus, but the definition doesn't actually require calculus; this is useful, because it means we can use it even when we're not working with real numbers. We can do the same trick with functions like log and exp that can be represented by power series, but we won't worry about those here.

Lemma 3.42. *If $f(x), g(x)$ are polynomials and c is a constant, then $(f+g)'(x) = f'(x) + g'(x)$ and $(cf)'(x) = cf'(x)$. Further, $(f+g)^{(k)}(x) = f^{(k)}(x) + g^{(k)}(x)$ and $(cf)^{(k)}(x) = cf^{(k)}(x)$.*

Lemma 3.43. *If m, k are positive integers, and $f(x) = x^m$, then*

$$f^{(k)} = m(m-1)\dots(m-k+1)x^{m-k} = \frac{m!}{(m-k)!}x^{m-k}.$$

Lemma 3.44 (Taylor expansions)**.** *If $f(x)$ is a polynomial of degree n, and $a, b \in \mathbb{R}$, then*

$$f(a+b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)b^k}{k!} = f(a) + f'(a)b + \frac{f''(a)b^2}{2} + \dots + \frac{f^{(n)}(a)b^n}{n!}.$$

and this is a polynomial in b whose coefficients are polynomials in a with integer coefficients.

Proof. We will prove this for $f_m(x) = x^m$. This is sufficient to prove it for any polynomial $f(x)$, since any polynomial is the sum $a_0 f_0(x) + \dots + a_n f_n(x)$ of scalar multiples of x^m for various m, and derivatives commute with addition and scalar multiplication.

By the binomial theorem,

$$(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k}b^k.$$

But $f_m^{(k)}(a) = \frac{m!}{(m-k)!}a^{m-k} = k!\binom{m}{k}a^{m-k}$, so

$$f_m(a+b) = \sum_{k=0}^{m} \binom{m}{k} a^{m-k}b^k = \frac{f_m^{(k)}(a)b^k}{k!}.$$

We can see these coefficients must be integers because $\frac{f^{(k)}(a)}{k!} = \binom{m}{k}a^{m-k}$ and $\binom{m}{k}$ is an integer. □

Now we're ready to prove the key lemma about lifting, known as Hensel's Lemma after Kurt Hensel, who studied a field known as p-adic analysis. This lemma is complicated to state and annoyingly technical (that's why we say it's a lemma!), but is exceptionally useful for studying polynomial congruences.

Theorem 3.45 (Hensel's Lemma)**.** *Suppose $f(x)$ is a polynomial with integer coefficients, k is an integer with $k \geq 2$, and p is a prime. Suppose r is a solution to $f(x) \equiv 0 \mod p^{k-1}$ (that is, $f(r) \equiv 0 \mod p^{k-1}$). Then*

1. *If $f'(r) \not\equiv 0 \mod p$, then there is a unique integer t with $0 \leq t < p$ such that $f(r + tp^{k-1}) \equiv 0 \mod p^k$. Further, t is given by the formula*

$$t \equiv -(f'(r))^{-1}(f(r)/p^{k-1}) \mod p$$

where $(f'(r))^{-1}$ is an inverse of $f'(r)$ modulo p.

2. *If* $f'(r) \equiv 0 \mod p$ *and* $f(r) \equiv 0 \mod p^k$*, then* $f(r + tp^{k-1}) \equiv 0 \mod p^k$ *for any integer* t*.*

3. *If* $f'(r) \equiv 0 \mod p$ *and* $f(r) \not\equiv 0 \mod p^k$*, then* $f(x) \equiv 0 \mod p^k$ *has no solutions with* $x \equiv r \mod p^{k-1}$*.*

In particular, this tells us that if the derivative is 0, then a solution modulo p^{k-1} lifts to a unique solution modulo p^k; if the derivative is not zero, it lifts either to p different solutions modulo p^k, or to none at all.

Proof. Notice that every solution modulo p^k is also a solution modulo p^{k-1}. That is, if $f(x) \equiv 0 \mod p^k$ then $f(x) \equiv 0 \mod p^{k-1}$. Therefore, if $f(x) \equiv 0 \mod p^k$, then $x = r + tp^{k-1}$ for some r which satisfies $f(r) \equiv 0 \mod p^{k-1}$, and some integer t. We just need to determine the conditions on t.

So suppose $f(r + tp^{k-1}) \equiv 0 \mod p^k$. By the lemma on Taylor expansions,

$$f(r+tp^{k-1}) = \sum_{i=1}^{n} \frac{f^{(i)}(r)(tp^{k-1})^i}{i!} = f(r) + f'(r)tp^{k-1} + \frac{f''(r)}{2}(tp^{k-1})^2 + \cdots + \frac{f^{(n)}(r)}{n!}(tp^{k-1})^n,$$

with $f^{(i)}(r)/i!$ an integer for $1 \leq i \leq n$. But when we reduce this modulo p^k, we see that all but the first two terms will disappear, since $i(k-1) \geq k$ for $i \geq 2$, and thus $p^k | p^{i(k-1)}$. So we have

$$f(r + tp^{k-1}) \equiv f(r) + f'(r)tp^{k-1} \mod p^k.$$

But since $r + tp^{k-1}$ is a solution to $f(x) \equiv 0 \mod p^k$, we thus know that

$$f'(r)tp^{k-1} \equiv -f(r) \mod p^k.$$

Since by hypothesis $f(r) \equiv 0 \mod p^{k-1}$, we know that $p^{k-1} | f(r)$ (considered as integers). So we can cancel out the p^{k-1} on both sides of the congruence by the cancellation law, and get

$$f'(r)t \equiv -f(r)/p^{k-1} \mod p. \tag{1}$$

So far we've shown that if $f(r) \equiv 0 \mod p^{k-1}$, and $r + tp^{k-1}$ is a lift of r to a solution modulo p^k so that $f(r + tp^{k-1}) \equiv 0 \mod p^k$, then t must satisfy this (linear!) congruence in equation (1). We know proceed to analyze it in the three cases given in the lemma.

1. Suppose $f'(r) \not\equiv 0 \mod p$. Then $f'(r), p) = 1$, there is a unique t modulo p satisfying equation (1), given by

$$t \equiv (-f(r)/p^{k-1})(f'(r))^{-1} \mod p.$$

2. Suppose $f'(r) \equiv 0 \mod p$, so that $(f'(r), p) = p$. Suppose further that $f(r) \equiv 0 \mod p^k$, implying that $p | f(r)/p^{k-1}$. Again by our results on linear congruences, if $p | f(r)/p^{k-1}$ then the equation (1) has p solutions, and thus all values of t are solutions.

3. Finally, suppose $f'(r) \equiv 0 \mod p$, so that $(f'(r), p) = p$, but that $f(r) \not\equiv 0 \mod p^k$ so that $p \nmid f(r)/p^{k-1}$. Then equation (1) has no solutions.

□

Example 3.46. Find the solutions of $f(x) = x^3 + x^2 + 29 \equiv 0 \mod 25$.

We first find the solutions $\mod 5$. By plugging in values we see the only solution is $x \equiv 3 \mod 5$. We compute $f'(3) = 27 + 6 = 33 \equiv 3 \not\equiv 0 \mod 5$, and thus Hensel's lemma tells us there is a unique solution $\mod 25$ given by $x_2 \equiv 3 + 5t$ where

$$t \equiv -(f'(3))^{-1}(f(3)/5) \equiv -3^{-1}(65/5) \equiv -2 \cdot 13 \equiv -26 \equiv 4 \mod 5$$

and thus $x_2 \equiv 23 \mod 25$ is a unique solution $\mod 25$.

Example 3.47. Find the solutions of $x^2 + x + 7 \equiv 0 \mod 27$.

Let $x(x) = x^2 + x + 7$. We check for solutions modulo 3 and find the only one is when $x \equiv 1 \mod 3$. We compute $f'(1) = 3 \equiv 0 \mod 3$. Thus $f(x)$ will have either 3 or 0 solutions modulo 9; we see that $f(1) = 9 \equiv 0 \mod 9$ and thus $1 + 3t$ is a solution modulo 9 for all integers t; thus the solutions modulo 9 are $1, 4, 7$.

We may try to lift again to 27, but we still have $f'(1) = 3 \equiv 0 \mod 3$, so each solution either lifts to three solutions or does not lift at all. $f(1) = 9 \not\equiv 0 \mod 27$ so $1 + 9t$ is not a solution modulo 27 for any intger t. $f(4) = 27 \equiv 0 \mod 27$ so $4 + 9t$ is a solution modulo 27 for any integer t. $f(7) = 63 \not\equiv 0 \mod 27$ so $7 + 9t$ is not a solution modulo 27 for any integer t.

Thus the solutions modulo 27 are $x \equiv 4, 13, 22$.

Example 3.48. Find solutions of $x^3 + x^2 + 23 \equiv 0 \mod 125$.

We first find solutions modulo 5. We observe that the solutions are all congruent to 1 or 2 modulo 5. We calculate $f'(x) = 3x^2 + 2x$ so $f'(1) = 3 + 2 \equiv 0 \mod 5$ and $f'(2) = 12 + 4 \equiv 1 \mod 5$; we have to handle these two cases separately.

First let's try to lift 1. We see that $f'(1) \equiv 0 \mod 5$ so either $f(1) \equiv 0 \mod 25$ or 1 has no lifts to roots $\mod 25$. In fact we see that $f(1) = 1 + 1 + 23 \equiv 0 \mod 25$, so every possible lift of 1 is a root modulo 25. Thus $1, 6, 11, 16, 21$ are all solutions to $f(x) \equiv 0 \mod 25$.

Now we need to test if each of these lifts to a root modulo 125. We know the derivatives are all equivalent to 0 modulo 5, so each solution modulo 25 has either 5 lifts or zero. We compute

$$\begin{aligned} f(1) &= 25 \equiv 25 \mod 125 \\ f(6) &= 275 \equiv 25 \mod 125 \\ f(11) &= 1475 \equiv 100 \mod 125 \\ f(16) &= 4375 \equiv 0 \mod 125 \\ f(21) &= 9725 \equiv 100 \mod 125 \end{aligned}$$

Thus 1, 6, 11, and 21 all lack lifts, but 16 has a lift and thus has five lifts. So $16, 41, 66, 91, 116$ are all solutions of $f(x) \equiv 0 \mod 125$.

Now let's return to considering the root 2. We have $f'(2) = 12 + 4 = 16 \equiv 1 \mod 5$ which has 1 as an inverse modulo 5. Thus there is a unique root modulo 25, and by Hensel's lemma we have a lift $r_2 \equiv 2 + t \cdot 5 \mod 25$ with

$$t \equiv -(f'(2))^{-1} \left(\frac{f(r)}{5} \right) \equiv -1 \cdot \frac{35}{5} \equiv -2 \equiv 3 \mod 5$$

and thus our lift $r_2 \equiv 2 + 3 \cdot 5 = 17 \mod 25$ is a root of $f(x) \equiv 0 \mod 25$. Now we wish to lift this again, but our derivative modulo 5 is still 1, so by Hensel's lemma we have a unique root modulo 125 given by $r_3 \equiv 17 + 25t \mod 125$ with

$$t \equiv -(f'(17))^{-1} \frac{f(17)}{25} \equiv -1 \cdot \frac{5225}{25} \equiv -249 \equiv 1 \mod 5$$

so $r_3 \equiv 17 + 25 \equiv 42 \mod 125$.

Thus the complete set of solutions to $f(x) \equiv 0 \mod 125$ is the set $\{x : x \equiv 16, 41, 42, 66, 91, 116 \mod 125\}$.

Corollary 3.49. *Suppose $f(x)$ is a polynomial and r is a solution to the polynomial congruence $f(x) \equiv 0 \mod p$ for a prime number p. If $f'(r) \not\equiv 0 \mod p$, then for each integer*

$k \geq 1$ there is a solution r_k to the congruence $f(x) \equiv 0 \mod p^k$, such that $r_k \equiv r \mod p$. Further, this r_k is unique modulo p^k. In particular, $r_1 = r$ and for $k > 1$ we have

$$r_k = r_{k-1} - f(r_{k-1})(f'(r))^{-1}.$$

Proof. We prove this by induction. For $k = 1$ it is given that there is a unique solution that is equivalent to $r \mod p$, and $f'(r) \not\equiv 0 \mod p$.

Suppose we have proven that this property for n–that is there is a r_n, unique modulo p^n, such that $r_n \equiv r \mod p$ and $f(r_n) \equiv 0 \mod p^n$, and further $f'(r_n) \equiv f'(r) \not\equiv 0 \mod p$.

Then by Hensel's lemma, since $f'(r_n) \not\equiv 0 \mod p$, there is a unique integer t with $0 \leq t < p$ such that $f(r_n + tp^n) \equiv - \mod p^{n+1}$, and $t \equiv -(f'(r_n))^{-1}(f(r_n)/p^{kn}) \mod p$.

Then there is a unique solution to $f(x) \equiv 0 \mod p^{n+1}$ that is equivalent to $r_n \mod p^n$, given by

$$r_{n+1} = r_n - (f'(r_n))^{-1} f(r_n).$$

Since $r_n \equiv r \mod p$ and $r_{n+1} \equiv r_n \mod p^n$ we know that $r_{n+1} \equiv r \mod p$.

Finally, we see that

$$\begin{aligned} f'(r_{n+1}) &= f'(r_n - (f'(r_n))^{-1} f(r_n)) \equiv f'(r_n - (f'(r_n))^{-1} \cdot 0) \mod p \\ &\equiv f'(r_n) \equiv f'(r) \not\equiv 0 \mod p. \end{aligned}$$

□

Example 3.50. Find the solutions of

$$x^3 + x^2 + 2x + 26 \equiv 0 \mod 7^k.$$

We first solve $x^3 + x^2 + 2x + 26 \equiv 0 \mod 7$, and see that the only solution is $x \equiv 2 \mod 7$. We see that $f'(x) = 3x^2 + 2x + 2$ so $f'(2) = 12 + 4 + 2 = 18 \equiv 4 \mod 7 \not\equiv 0 \mod 7$. Thus by the corollary, we can find solutions modulo 7^k for $k \in \mathbb{N}$.

We compute $(f'(2))^{-1} \equiv 4^{-1} \equiv 2 \mod 7$. Thus we have

$$\begin{aligned} r_2 &\equiv 2 - f(2)(f'(2))^{-1} \equiv 2 - 42 \cdot 2 = -82 \equiv 16 \mod 49 \\ r_3 &\equiv 16 - f(16)(f'(2))^{-1} = 16 - 4410 \cdot 2 = -8804 \equiv 114 \mod 343 \\ r_4 &\equiv 114 - f(114)(f'(2))^{-1} = 114 - 1494794 \cdot 2 = -2989474 \equiv 2172 \mod 2401 \quad \vdots \end{aligned}$$

4 Exponential Congruences and Pseudoprimes

In this section we will develop a couple of important tools that rely on congruences and modular arithmetic, and use them to understand the primes a bit better–and come up with a quick test that will "usually" tell us if a number is prime.

4.1 Fermat's Little Theorem

For further reading on the material in this subsection, consult **Rosen 6.1, PMF 9.1, Stein 2.1.3, 2.4, Shoup 2.7**.

In this section we will prove a few results about congruences modulo a prime number. We already know one such result: if p is a prime, then every number not equivalent to 0 modulo p has a multiplicative inverse modulo p (and this is true *only* if p is prime or 1).

We will start with another result proved by Joseph Lagrange in 1771:

Theorem 4.1 (Wilson's Theorem)**.** *If p is prime, then $(p-1)! \equiv -1 \mod p$.*

Example 4.2. If $p = 5$, then $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \equiv 1 \mod 25$.

If $p = 7$ then $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$. We could multiply this out (it's 720, in fact), but we probably don't want to. It's easier to write

$$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6(4 \cdot 2)(5 \cdot 3) \equiv (-1)(1)(1) \mod 7.$$

That is, we can pair every number with its modular inverse modulo 7, except for $6 \equiv -1$ which is left "stranded." This gives us the idea for the proof.

Proof. When $p = 2$ we can check directly that $1! = 1 \equiv 1 \mod 2$. So let's assume p is an odd prime. Then consider the list of numbers $1, 2, \ldots, p-1$. We know that each such integer a has a modular inverse a^{-1}, which must also be on this list.

But we proved that the only numbers which are their own inverses modulo p are 1 and $p - 1 \equiv -1$. (see Lemma 3.30). Thus each integer on the list $2, 3, \ldots, p-2$ is the modular inverse of exactly one other integer on the list, and thus we have

$$\prod_{i=2}^{p-2} i = 2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \mod p$$

$$(p-1) = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2)(p-1) \equiv 1(p-1) \equiv -1 \mod p.$$

□

Importantly, the converse of this theorem is true–any number with this property is prime.

Theorem 4.3. *If $n \geq 2$ is an integer and $(n-1)! \equiv -1 \mod n$ then n is prime.*

Proof. Suppose n is a composite integer. Then $n = ab$ for some integers a, b with $1 < a, b < n$. From here we can take two approaches:

1. If $a \neq b$ then $ab|(n-1)!$ and thus $(n-1)! \equiv 0 \mod n$, and since $n > 1$ we know that $0 \not\equiv -1 \mod n$. Thus we only need to consider the case where $a = b$.

   If $a = b = 2$ then we can see easily that $(n-1)! = 3! = 6 \equiv 2 \mod 4$ and thus $(n-1)! \not\equiv -1 \mod 4$. So assume $a = b > 2$. Then $ab > 2a$ so $2a$ is a factor in the product $(n-1)!$, and thus $2ab|(n-1)!$ and so does $ab = n$. Thus $(n-1)! \equiv 0 \mod n$.

2. Alternatively, we can suppose that $(n-1)! \equiv -1 \mod n$, implying that $n|(n-1)!+1$ and thus $a|(n-1)!+1$. But $a|(n-1)!$ as well and thus $a|(n-1)!+1-(n-1)! = 1$ and thus $a = 1$, which is a contradiction.

□

Thus we can use Wilson's Theorem to test whether a given number is prime: just compute $(p-1)! \mod p$ and see if the result is $p-1$. Unfortunately, this isn't really a *good* or efficient prime test, since it takes a large amount of computation.

Similar to Wilson's Theorem is Fermat's Little Theorem (which is *not* Fermat's Last Theorem!). The first published proof is due to Leonhard Euler.

Theorem 4.4 (Fermat's Little Theorem)**.** *If p is prime and a is an integer with $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.*

Proof. Consider the $p-1$ integers $a, 2a, \ldots, (p-1)a$. We know that none of these integers are equivalent mod p, since if $ia \equiv ja \mod p$ then since $(p, a) = 1$ we know that $i \equiv j \mod p$. Similarly none of these are divisible by p, since if $p|ja$ then $p|j$.

Thus our list contains one representative of every non-zero equivalence class modulo p. So the product of these $p-1$ integers is equivalent to the product of the first $p-1$ non-zero integers modulo p, and thus we have

$$\prod_{k=1}^{p-1} ka \equiv \prod_{k=1}^{p-1} k \mod p$$

$$a^{p-1} \prod_{k=1}^{p-1} \equiv \prod_{k=1}^{p-1} k = (p-1)! \mod p$$

But since $p \not| (p-1)!$, we know that $((p-1)!, p) = 1$, so we can cancel the $(p-1)!$ from both sides and get

$$a^{p-1} \equiv 1 \mod p.$$

□

Remark 4.5. From the perspective of group theory, this says that the order of any element of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ divides $p-1$ which is the order of this group.

Corollary 4.6. *If p is prime and a is an integer, then $a^p \equiv a \mod p$.*

Proof. If $p \not| a$, then by Fermat's little theorem, $a^{p-1} \equiv 1 \mod p$. Multiplying both sides by a gives $a^p \equiv a \mod p$.

If $p|a$ then $a^p \equiv 0 \equiv a \mod p$. □

Example 4.7. This makes it easy to compute large powers of numbers modulo primes. For instance, suppose we want to compute $2^{700} \mod 7$. We know that $2^6 \equiv 1 \mod 7$ and thus $(2^6)^{(116)} = 2^{696} \equiv 1 \mod 7$, so $2^{700} \equiv 2^4 \equiv 16 \equiv 2 \mod 7$

Corollary 4.8. *If p is a prime and a is an integer with $p \not| a$ then a^{p-2} is an inverse of a modulo p.*

Example 4.9. What is the inverse of 5 modulo 7? It is

$$5^5 \equiv 25 \cdot 25 \cdot 5 \equiv 4 \cdot 4 \cdot 5 \equiv 16 \cdot 5 \equiv 2 \cdot 5 \equiv 3 \mod 7.$$

What is the inverse of 7 modulo 11? It is

$$7^9 \equiv (-4)^9 \equiv -4^9 \equiv - \equiv (4^2)^4 \cdot 4 \equiv -16^4 \cdot 4 \equiv -5^4 \cdot 4 \equiv -25^2 \cdot 4 \equiv -3^2 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \mod 11.$$

Recall that when we were trying to solve linear congruences, we reduced many questions to simply the task of finding modular inverses. Thus we can use Fermat's little theorem to make solving linear congruences easier.

Corollary 4.10. *If a, b are integers and p is prime with $p \not| a$, then the solutions to the congruence $ax \equiv b \mod p$ are the integers $x \equiv a^{p-2}b \mod p$.*

4.2 Pseudoprimes

For further reading on the material in this subsection, consult **Rosen 6.2, Stein 2.4**.

In the last subsection we proved two results about congruences modulo a prime number. Wilson's theorem holds if and only if a number is prime, and thus gives us a (very inefficient) prime test.

Fermat's little theorem also holds for congruences modulo any prime, so we can use it to prove a number is not prime.

Example 4.11. We can show 63 is not prime by calculating

$$2^{62} = 2^{60} \cdot 2^2 = (2^6)^{10} \cdot 2 = 64^{10} \cdot 4 \equiv 1^{10} \cdot 4 \equiv 4 \mod 63.$$

Thus 63 cannot be prime, since $2^{p-1} \equiv 1 \mod p$ for any prime.

Unfortunately, Fermat's little theorem doesn't give a very clear prime test, since the converse is *not* true.

Example 4.12. Let $n = 341 = 11 \cdot 31$. But $2^{340} = 2 \cdot (2^{10})^{34}$ and we know that $2^{10} \equiv 1 \mod 11$ by Fermat's little theorem, so

$$2^{340} \equiv (2^{10})^{34} \equiv 1^3 4 \equiv 1 \mod 341.$$

Thus $2^{341-1} \equiv 1 \mod 341$ even though 341 is not prime.

Remark 4.13. This result is due to Pierre Sarrus in 1919; it was not known that the converse to Fermat's little theorem was false until relatively recently.

Definition 4.14. If b is a positive integer, we say an integer n is *pseudoprime to the base b* if n is composite but $b^n \equiv b \mod n$.

Note that if $(b, n) = 1$ then this is equivalent to $b^{n-1} \equiv 1 \mod n$

Example 4.15. We showed that $341 = 11 \cdot 31$ is pseudoprime to base 2. We can also check that $561 = 3 \cdot 11 \cdot 17$ and $645 = 3 \cdot 5 \cdot 43$ are as well.

Remark 4.16. These are somtimes called "Fermat pseudoprimes" because they pass this particular prime test. There are other tests that can generate false positives; we should discuss Euler pseudoprimes towards the end of the course.

For any given base, there are more primes than there are pseudoprimes by a wide margin; pseudoprimes are fairly rare. However, there are infinitely many pseudoprimes for any base. We prove this for base 2 (Proving it for other bases requires more work but is totally possible).

Lemma 4.17. *If d, n are positive integers with $d|n$, and $b > 1$ is an integer, then $b^d - 1 | b^n - 1$.*

Proof. We know that for any t,

$$x^t - 1 = (x-1)(1 + x + x^2 + \cdots + x^{t-2} + x^{t-1}.$$

Thus

$$b^n - 1 = (b^d - 1)(1 + b^d + b^{2d} + \cdots + b^{n-d}).$$

□

Theorem 4.18. *There are infinitely many pseudoprimes to the base 2.*

Proof. Let $n_1 = 341$ be a pseudoprime to the base 2. Recursively define $n_{k+1} = 2^{n_k} - 1$. We claim that n_k is a pseudoprime to the base 2 for each natural number k.

First we prove by induction that n_k is composite. $n_1 = 11 \cdot 31$ is composite. Assume (for induction) that n_i is composite. Then we can write $n_i = a_i b_i$ with $1 < a_i, b_i < n_i$, and we can write

$$n_{i+1} = 2^{n_i} - 1 = (2^a - 1)(1 + 2^a + \cdots + 2^{n_i - a}).$$

Since $2^a - 1 > 1$ and $1 + 2^a + \cdots + 2^{n_i - a} > 1$, we know that n_{i+1} is composite. Thus, by induction, n_k is composite for each natural number k.

Now we show that $2^{n_k} \equiv 2 \mod n_k$. Again, we use induction. We showed, $2^{n_1} \equiv 2 \mod n_1$. So assume (for induction) that $2^{n_i} \equiv 2 \mod n_i$. This means there is an integer m with $2^{n_i} - 2 = m n_i$.

Then we see that $2^{n_{i+1}-1} = 2^{2^{n_i}-2} = 2^{m n_i}$. Then

$$n_{i+1} = 2^{n_i} - 1 | 2^{m n_i} - 1 = 2^{n_{i+1}-1} - 1.$$

Thus $2^{n_{i+1}-1} \equiv 1 \mod n_{i+1}$, so n_{i+1} is a pseudoprime to the base 2. □

The simplest version of the Fermat test therefore does not work to test whether a number is prime, because it has (admittedly rare) counterexamples.

There is still some hope we can use this Fermat test to test whether a number is prime, by using multiple bases, as follows:

Example 4.19. Let us test the primality of 341 using the base 7. We observe that $7^3 = 343 \equiv 2 \mod 341$, which makes this an eaqy base to work with, especially since we already know facts about 2, like that $2^{10} \equiv 1 \mod 341$. Then we see that

$$7^{340} = (7^3)^{113} \cdot 7 \equiv 2^{113} \cdot 7 \equiv (2^{10})^{11} \cdot 2^3 \cdot 7 \equiv 1^{11} \cdot 8 \cdot 7 \equiv 56 \not\equiv 1 \mod 341.$$

Thus we can see that 341 is not prime because $7^{340} \not\equiv 1 \mod 341$.

This approach usually works, but unfortunately it does not always work.

4.2.1 Carmichael Numbers

Definition 4.20. If n is a positive integer such that $b^{n-1} \equiv 1 \mod n$ for all positive integers b with $(b,n) = 1$, we say n is a *Carmichael number* or an *absolute (Fermat) pseudoprime.*

Example 4.21. We claim that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. Suppose $(b, 561) = 1$. Then $(b,3) = (b,11) = (b,17) = 1$. Thus by Fermat's little theorem, $b^2 \equiv 1 \mod 3, b^{10} \equiv 1 \mod 11$, and $b^{16} \equiv 1 \mod 17$.

Then we see that $b^{560} = (b^2)^{280} \equiv 1 \mod 3$, $b^{560} = (b^{10})^{56} \equiv 1 \mod 11$, and $b^{560} = (b^{16})^{35} \equiv 1 \mod 17$. Thus by the Chinese Remainder Theorem, $b^{560} \equiv 1 \mod 561$.

Carmichael conjectured that there were infinitely many Carmichael numbers in 1912; in 1992, Alford, Granville, and Pomerance proved that if $C(x)$ is the number of Carmichael numbers less than x, then for large x we have $C(x) > x^{2/7}$. We wont' prove this result, but we will prove the easy half of it.

Theorem 4.22. *If $n = \prod_{i=1}^{k} q_i$ for $k > 2$, where the q_i are all distinct primes, and $(q_i - 1)|n-1$ for all i, , then n is a Carmichael number.*

Proof. We can see the proof following from the computation we just did for 561. Suppose b is a positive integer with $(b,n) = 1$. Then $(b, q_i) = 1$ for each i, and thus $b^{q_i - 1} \equiv 1 \mod q_i$ by Fermat's Little Theorem. Since $(q_i - 1)|n-1$, we then have that $b^{n-1} \equiv 1 \mod q_i$ for each i, and the Chinese Remainder Theorem tells us that $b^{n-1} \equiv 1 \mod \prod_{i=1}^{k} q_i$. □

Remark 4.23. The converse of this theorem is also true, but we're not ready to prove it yet.

Thus the proof that there are infinitely many Carmichael numbers reduces to proving that there are infinitely many numbers $n = \prod q_i$ where $q_i - 1 | n - 1$ for each q_i.

Fact: there are 43 Carmichael numbers $\leq 10^6$, and 105,202 that are $\leq 10^{15}$. (That seems like a lot, but 10^{15} is a very large number).

4.2.2 The Miller test

We can push all these arguments a bit farther. We know from your homework that if $x^2 \equiv 1 \mod p$ then $x \equiv \pm 1 \mod p$. So suppose we have some number b such that $b^{n-1} \equiv 1 \mod n$. We can compute $b^{(n-1)/2} \mod n$; if this quantity is not congruent to $\pm 1 \mod n$ then n must not be prime.

Example 4.24. Let $n = 561$ and let $b = 5$. Then we compute that $5^{560} \equiv 1 \mod 561$ as before. But $5^{280} \equiv 67 \not\equiv \pm 1 \mod 561$ so we know that 561 is not prime.

(Note: we can do this by hand but we'd really like a computer).

Definition 4.25. Let n be an integer with $n > 2$ and $n - 1 = 2^s t$ for $s \in \mathbb{N}$ and t odd. We say n passes the *Miller test for the base b* if either $b^t \equiv 1 \mod n$ or if $b^{2^j t} \equiv -1 \mod n$ for some $0 \leq j \leq s - 1$.

Our previous example showed that 561 does not pass the Miller test for the base 5. We now show that $2047 = 23 \cdot 89$ passes the Miller test for the base 2.

Example 4.26. We have $2^{2046} = (2^{11})^{186} = (2048)^{186} \equiv 1 \mod 2047$, so 2047 is pseudoprime to the base 2. Further, we have $2046 = 1023 \cdot 2$, and $2^{1023} = (2^{11})^{93} = (2048)^{93} \equiv 1 \mod 2047$, and thus 2047 passes the Miller test for the base 2.

Theorem 4.27. *If n is prime and b is a positive integer with $n \not| b$, then n passes the Miller test for the base b.*

Proof. Set $n - 1 = 2^s t$ for t odd. Let $x_k = b^{(n-1)/2^k} = b^{2^{s-k}t}$ for $0 \leq k \leq s$, and thus $x_0 = b^{n-1}$. Since n is prime, by Fermat's Little Theorem, we know that $x_0 = b^{n-1} \equiv 1 \mod n$.

We prove the rest by induction (sort of). Fix some $k \leq s$ and suppose (for induction) that $x_1 \equiv 1 \mod n$ for each $i < k$. Then since $(x_k)^2 = (b^{(n-1)/2^k})^2 = b^{(n-1)/2^{k-1}} = x_{k-1} \equiv 1$, we know that $x_k \equiv \pm 1 \mod n$. Thus by induction, either $x_k \equiv 1 \mod n$ for every $k < s$, or $x_k \equiv -1 \mod n$ for some $k \leq s$.

Thus in particular, either $b^{(n-1)/2^k} = b^{t2^k} \equiv -1 \mod n$ for some k, or $b^{(n-1)/2^s} - b^t \equiv 1 \mod n$, so n passes the Miller test for the base b. □

Notice that if n passes the Miller test for the base b, then in particular $b^{n-1} \equiv 1 \mod n$, and thus n is a pseudoprime to the base b. But passing the Miller test is in fact harder, leading us to define:

Definition 4.28. If n is composite and passes the Miller test for the base b, we say n is a *strong pseudoprime to the base b.*

Thus we saw that 2047 is a strong pseudoprime to the base 2.

Theorem 4.29. *There are infinitely many strong pseudoprimes to the base 2.*

Proof. We will claim something more specific: if n is a pseudoprime to the base 2, then $N = 2^n - 1$ is a strong pseudoprime to the base 2. Since there are infinitely many pseudoprimes, there are thus infinitely many strong pseudoprimes.

Suppose n is an odd pseudoprime to the base 2. That is, n is composite and $2^{n-1} \equiv 1 \mod n$. Thus $2^{n-1} - 1 = nk$ for some odd integer k. Then

$$N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2nk$$

is the factorization of N into an odd integer and a power of 2.

But we compute now that $2^n \equiv 1 \mod N$ and thus

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \mod N.$$

Thus $2^{(N-1)/2} \equiv 1 \mod N$, and $(N-1)/2$ is the largest odd factor of $N - 1$, so N passes the Miller test for the base 2.

Now we only need to show that N is composite. But we showed in the proof of Theorem 4.18 that if n is composite then so is $N = 2^n - 1$. Thus N is composite but passes the Miller test for the base 2, and thus is a strong pseudoprime to the base 2. Because there are infinitely many pseudoprimes, there are thus infinitely many strong pseudoprimes. □

Theorem 4.30. *If n is an odd composite positive ingeter, then n passes the Miller test for at most $(n-1)/4$ bases b with $1 \leq b \leq n-1$.*

We need more tools before we can prove this. We can use this result to prove that a number is prime, but it takes far longer than simple trial division. But it produces a good probabilistic primality test:

Theorem 4.31 (Rabin's Probabilistic Primality Test)**.** *Let n be a positive integer. Pick k different postiive integers less than n and perfom the Miller test on n for each of these bases. If n is composite, the probability that n passes all k tests is less than $(1/4)^k$.*

This generates an extremely efficient *probabilistic* test; The odds of a composite number n passing 100 Miller tests are less than 10^{-60}. (Note: always be careful reasoning about p-values: this doesn't mean that a number that passes 100 Miller tests has less than 10^{-60} chance of being composite. The chances are still quite small).

However, if we assume the Generalized Riemann Hypothesis, we can get a good deterministic prime test.

Conjecture 4.32. *For every composite positive integer n, there is a base $b < 2(\log n)^2$ such that n fails the Miller test for the base b.*

If this conjecture is true, the Miller test gives us a very good deterministic primality test, which takes $O((\log n)^5)$ operations.

4.3 Euler's Theorem and composite moduli

For further reading on the material in this subsection, consult **Rosen 6.3, PMF 9.3, Stein 2.1.2, Shoup 2.6-7**.

All the work we've done so far only applies to prime moduli. We'd like to extend or adapt these results to composite moduli. To do this we need to tweak everything slightly.

Definition 4.33. Let n be a positive integer. We define the *Euler phi-function* $\phi(n)$ to be the number of positive integers $\leq n$ that are relatively prime to n.

Example 4.34. $\phi(7) = 6$, since 7 is relatively prime to $1, 2, 3, 4, 5, 6$. $\phi(8) = 4$ since 8 is relatively prime to $1, 3, 5, 7$. $\phi(9) = 6$ since $1, 2, 4, 5, 7, 8$ are relatively prime to 9. $\phi(10) = 4$ since $1, 3, 7, 9$ are relatively prime to 10.

Definition 4.35. A *reduced residue system modulo n* is a set of $\phi(n)$ integers such that each element of the set is relatively prime to n, and no congruence class modulo n is represented more than once.

Example 4.36. $\{1, 2, 3, 4, 5, 6\}$ is a reduced residue system modulo 7. So is $\{2, 4, 6, 8, 10, 12\}$.

$\{1, 3, 5, 7\}$ is a reduced residue system modulo 8. So is $\{-3, -1, 1, 3\}$.

Lemma 4.37. *If $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ is a reduced residue system modulo n and $(a, n) = 1$, then the set $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ is also a reduced residue system modulo n.*

Proof. Suppose $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ is a reduced residue system modulo n, and $(a, n) = 1$.

First we have to prove that $(ar_j, n) = 1$. Suppose $(ar_j, n) > 1$. Then there is some prime p that divides both n and ar_j. But then either $p|a$ or $p|r_j$, so either $p|n$ and $p|a$ and thus $(a, n) \neq 1$; or $p|n$ and $p|r_j$ and thus $(r_j, n) \neq 1$. Either way is a contradiction. Thus $(ar_j, n) = 1$ for each j.

Now we wish to show that if $ar_j \equiv ar_i \mod n$ then $i = j$. But suppose $ar_j \equiv ar_i \mod n$. Then since $(a, n) = 1$, by modular cancellation we know that $r_j \equiv r_i \mod n$, and since $\{r_1, \ldots, r_{\phi(n)}\}$ is a reduced residue system, we know that $r_j \equiv r_i \mod n$ only if $j = i$. □

Theorem 4.38 (Euler's Theorem)**.** *If a, n are natural numbers and $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.*

Proof. Let $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ be the reduced residue system made up of integers less than n that are relatively prime to n. Then since $(a, n) = 1$, we know the set $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$

is a reduced residue system. Thus the set of least positive residues

$$\{ar_1 \mod n, ar_2 \mod n, \dots, ar_{\phi(n)} \mod n\}$$

must be the set $\{r_1, r_2, \dots, r_{\phi(n)}\}$ in some order (because each set has exactly one representative of each equivalence class).

If we multiply them all together, this tells us that

$$r_1 r_2 \dots r_{\phi(n)} \equiv (ar_1)(ar_2)\dots(ar_{\phi(n)}) \equiv a^{\phi(n)}(r_1 r_2 \dots r_{\phi(n)}) \mod n.$$

But since $(r_i, n) = 1$, we know that $(r_1 r_2 \dots r_{\phi(n)}, n) = 1$, and thus by modular cancellation we have $a^{\phi(n)} \equiv 1 \mod n$ as desired. □

Corollary 4.39. *If a, m are natural numbers with $(a, m) = 1$, then $a^{\phi(m)-1}$ is a multiplicative inverse for a modulo m.*

Example 4.40. Compute $5^{200} \mod 9$.

We know that $5^6 = 5^{\phi(9)} \equiv 1 \mod 9$. Thus

$$5^{100} = 5^{198} \cdot 5^2 = (5^6)^{33} \cdot 25 \equiv 1 \cdot 25 \equiv 7 \mod 9.$$

These results look *suspiciously similar* to Fermat's little theorem and its corollary. In fact Fermat's little theorem is a special case if $\phi(p) = p - 1$, which is in fact the case.

Exercise 4.41. *$\phi(n) = n - 1$ if and only if n is prime.*

Remark 4.42. There are a lot more results we can prove about computing $\phi(n)$, and basically the next big chunk of material will be devoted to that.

5 Multiplicative Functions

For further reading on the material in this subsection, consult **Rosen 7.1, Stein 2.2**.

Definition 5.1. An *arithmetic function* is a function defined for all natural numbers.

A function is *multiplicative* if it has the property that $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$. It is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all natural numbers m, n.

Example 5.2. The functions $f(n) = 1$ and $g(n) = n$ are completely multiplicative.

We will see that $\phi(n)$ is multiplicative but not completely multiplicative. (Example: $\phi(4) = 2 \neq 1 \cdot 1 = \phi(2) \cdot \phi(2)$).

Completely multiplicative functions are easy to understand, but we can get a good grasp even of regularly multiplicative functions.

Proposition 5.3. *If f is multiplicative and $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s} = \prod_{i=1}^{s} p_i^{a_i}$ is the prime factorization of n, then*

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \dots f(p_s^{a_s}) = \prod_{i=1}^{s} f(p_i^{a_i}).$$

Proof. We prove by induction on s, the number of distinct prime factors of n. If $s = 1$ then $n = p_1^{a_1}$ and then $f(n) = f(p_1^{a_1})$ is trivially true.

Suppose the proposition is true for all integers with k distinct prime factors, and suppose n has $k+1$ distinct prime factors, say $n = \prod_{i=1}^{k+1} p_i^{a_i}$. We observe that $\left(\prod_{i=1}^{k} p_i^{a_i}, p_{k+1}^{a_{k+1}}\right) = 1$, and thus by definition of a multiplicative function we know that

$$f\left(\prod_{i=1}^{k+1} p_i^{a_i}\right) = f\left(\prod_{i=1}^{k} p_i^{a_i}\right) f(p_{k+1}^{a_{k+1}}).$$

And by inductive hypothesis we know that

$$f\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} f(p_i^{a_i})$$

and thus we have

$$f\left(\prod_{i=1}^{k+1} p_i^{a_i}\right) = \prod_{i=1}^{k} f(p_i^{a_i}) f(p_{k+1}^{a_{k+1}}) = \prod_{i=1}^{k+1} f(p_i^{a_i}).$$

□

Thus for any multiplicative function, if we can compute its value for prime powers, we can easily compute its value for any number.

5.1 The Euler ϕ-function

For further reading on the material in this subsection, consult **Rosen 7.1, Stein 2.2**.

We want to understand the Euler ϕ-function much better. We will prove that it is a multiplicative function (though, as we observed earlier, it is not completely multiplicative). After that we'll figure out how to compute ϕ of prime powers, which will allow us to easily compute $\phi(n)$ for any positive integer n.

Proposition 5.4. *Let m, n be relative prime natural numbers. Then $\phi(mn) = \phi(m)\phi(n)$. In other words, the function $\phi(n)$ is multiplicative.*

Proof. Write the numbers $\leq mn$ as follows:

$$\begin{array}{ccccccc}
1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
r & m+r & 2m+r & \dots & (n-1)m+r \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
m & 2m & 3m & \dots & nm
\end{array}$$

Note that $(km + r, m) = (r, m)$, thus the first element of a given row is relatively prime to m if and only if *every* element of that row is. Since $(r, m) > 1$ implies that $(r, mn) > 1$, we only need to consider elements in rows r where $(r, m) = 1$. There are, of course, $\phi(m)$ such rows.

Now suppose $(r, m) = 1$ and consider the elements of this row, which are $km + r$ for $0 \leq k \leq n - 1$. We claim this is a complete system of residues modulo n. It's enough to prove that no two elements are congruent to each other, by HW 4 problem 2. But if $im + r \equiv jm + r \mod n$ then $n|m(i - j)$, and since $(n, m) = 1$, by Euclid's lemma this implies $n|i - j$. But $i, j < n$, so $i = j$.

Since this is a complete system of residues, exactly $\phi(n)$ of these integers are relatively prime to n. Since these integers are also relatively prime to m, they are relatively prime to mn.

Thus there are $\phi(m)$ rows that contain any elements relatively prime to mn; each such row contains $\phi(n)$ such elements. Thus there are in total $\phi(m)\phi(n)$ natural numbers relatively prime to mn and $\leq mn$; but this is the definition of $\phi(mn)$. □

Now that we know $\phi(n)$ is a multiplicative function, we know we can compute it purely by computing its value at prime powers. So we turn our attention to computing $\phi(p^k)$. First, recall from homework that $\phi(n) = n - 1$ if and only if n is prime.

Lemma 5.5. *Let p be a prime number, and let k be a positive integer. Then $\phi(p^k) = p^k - p^{k-1}$.*

Proof. An integer is relatively prime to p^k if and only if it is divisible by p. Thus the integers $n \leq p^k$ which are *not* relatively prime to p^k are the integers ℓp for $1 \leq \ell \leq p^{k-1}$. There are of course p^{k-1} such integers, and there are p^k total integers $n \leq p^k$; thus there are $p^k - p^{k-1}$ integers $n \leq p^k$ such that $(n, p^k) = 1$. □

Example 5.6. $\phi(2^{10}) = 2^{10} - 2^9 = 1024 - 512 = 512$.

$\phi(7^3) = 7^3 - 7^2 = 343 - 49 = 298$.

Theorem 5.7. *Let $n = \prod_{i=1}^{k} p_i^{a_i}$ be the prime factorization of a natural number. Then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

Proof. By proposition 5.3, we know that

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{a_i}).$$

But by lemma 5.5 we know that

$$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right).$$

Thus

$$\begin{aligned}\phi(n) &= \prod_{i=1}^{k} \phi(p_i^{a_i}) = \prod_{i=1}^{k} p_i^{a_i}\left(1 - \frac{1}{p_i}\right) \\ &= \left(\prod_{i=1}^{k} p_i^{a_i}\right)\left(\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)\right) \\ &= n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).\end{aligned}$$

□

Example 5.8.

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100(1 - 1/2)(1 - 1/5) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$$

$$\phi(360) = \phi(2^3 \cdot 3^2 \cdot 5) = 360(1 - 1/2)(1 - 1/3)(1 - 1/5) = 360\frac{8}{30} = 96.$$

Corollary 5.9. *If $n > 2$ then $\phi(n)$ is even.*

Proof. Let $n = \prod_{i=1}^{k} p_i^{a_i}$. Then $\phi(n) = \prod_{i=1}^{k} \phi(p_i^{a_i})$.

Suppose n has an odd prime factor p_k. Then since $p_k^{a_k}$ and $p_k^{a_k-1}$ are both odd, $2|p_k^{a_k} - p_k^{a_k-1} = \phi(p_k)|\phi(n)$.

Now suppose n has no odd prime factors. Then $n = 2^r$ and $r > 1$. Then $\phi(n) = 2^r - 2^{r-1} = 2^{r-1}$ is even. □

This opens up an additional question: given an integer m, for what n is $\phi(n) = m$?

Example 5.10. What are the solutions to the equation $\phi(n) = 8$?

Suppose $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Then we have the equation

$$\phi(n) = \prod_{j=1}^{k} p_j^{a_j-1}(p_j - 1)$$

which is just a restatement of theorem 5.7. Then the only primes that can divide n are 2, 3, and 5, since we know that $p_i - 1|n$. Further, if $a_i > 1$ then $p_i|n$, so we know that 3 and 5 can each divide n at most once. Thus we have $n = 2^{a_2}3^{a_3}5^{a_5}$, and a_3, a_5 are either 0 or 1.

Suppose $a_3 = a_5 = 0$ so that $n = 2^{a_2}$. Then $\phi(n) = \phi(2^{a_2}) = 2^{a_2-1}(2-1)$, which impiles that $a_2 = 4, n = 16$.

Suppose $a_3 = 1, a_5 = 0$, so that $n = 2^{a_2} \cdot 3$. Then $\phi(n) = \phi(2^{a_2} \cdot 3) = 2^{a_2-1}(2-1)3^0(3-1) = 2^{a_2}$. This implies that $a_2 = 3, n = 8 \cdot 3 = 24$.

Suppose $a_3 = 0, a_5 = 1$, so that $n = 2^{a_2} \cdot 5$. Then $\phi(n) = \phi(2^{a_2} \cdot 5) = 2^{a_2-1}(2-1)5^0(5-1) = 2^{a_2+1}$. This implies that $a_2 = 2, n = 4 \cdot 5 = 20$.

Suppose $a_3 = 1, a_5 = 1$, so that $n = 2^{a_2} \cdot 3 \cdot 5$. If $a_2 > 0$ then $\phi(n) = \phi(2^{a_2} \cdot 3 \cdot 5) = 2^{a_2-1}(2-1)3^0(3-1)5^0(5-1) = 2^{a_2+2}$. This implies that $a_2 = 1, n = 2 \cdot 3 \cdot 5 = 30$. If $a_2 = 0$ then instead $\phi(n) = \phi(3 \cdot 5) = 2 \cdot 4 = 8$ does in fact work, so $n = 15$.

Thus the possibilities are $n = 15, 16, 20, 24, 30$.

5.2 Summatory functions

For further reading on the material in this subsection, consult **Rosen 7.2, Shoup 2.9**.

In this section we'll discuss another class of multiplicative functions, known as summatory functions. Though these do not look like they should be multiplicative, they often are.

Definition 5.11. If f is an arithmetic function, we define the *summatory function of f* to be

$$F(n) = \sum_{d|n} f(d)$$

where the sum is over all numbers d which divide n.

Definition 5.12. We define the *number of divisors function* $\tau(n)$ to be the number of natural numbers $\leq n$ which divide n. We can write $\tau(n) = \sum_{d|n} 1$ so τ is a summatory function.

We define the *sum of divisors function* $\sigma(n) = \sum_{d|n} d$ to be the sum of the divisors of n. From the definition we see that σ is also a summatory function.

Proposition 5.13. *If f is a multiplicative function, then the summatory function of f, $F(n) = \sum_{d|n} f(d)$, is also multiplicative.*

This result seems quite surprising at first, since addition and multiplication don't always play well together. Our basic strategy is to write each divisor of mn as a divisor of m times a divisor of n–and this is unique since m and n share no common factors. Thus we can split our sum of divisors of mn into a product of sums of divisors of m and sums of divisors of n.

Proof. Suppose $(m, n) = 1$. We wish to prove that $F(mn) = F(m)F(n)$. We know that $F(mn) = \sum_{d|mn} f(d)$.

We can write any factor of mn uniquely as a product of a factor d_1 of m, and a factor d_2 of n, and we have $(d_1, d_2) = 1$. Thus we have

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) = \sum_{d_1|m, d_2|n} f(d_1)f(d_2).$$

But this sum factors, since we can write

$$\begin{aligned}\sum_{d_1|m, d_2|n} f(d_1)f(d_2) &= \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2) = \sum_{d_1|m} \left(f(d_1) \sum_{d_2|n} f(d_2) \right) \\ &= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) = F(m)F(n).\end{aligned}$$

□

Corollary 5.14. *$\sigma(n)$ and $\tau(n)$ are multiplicative functions.*

Lemma 5.15. *Let p be prime and $a \in \mathbb{N}$. Then $\tau(p^a) = a + 1$ and*

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

Proof. The divisors of p^a are $1, p, p^2, \ldots, p^a$. Thus there are $a+1$ and the result for τ follows. The first formula for σ also follows; the second comes from the geometric series formula, or from the difference of $a + 1$st powers formula. □

Corollary 5.16. *Let $n = \prod_{i=1}^{k} p_i^{a_i}$. Then*

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$
$$\tau(n) = \prod_{i=1}^{k} (a_i + 1).$$

Theorem 5.17. *Let n be a positive integer. Then $\sum_{d|n} \phi(d) = n$. That is, the summatory function of the Euler ϕ-function is the identity function.*

Proof. We're going to turn this into a counting/combinatorial argument. We're going to divide the integers $\leq n$ into classes C_d, where each class will contain exactly one number d which divides n, and the class will have $\phi(n/d)$ elements. Thus $\sum_{d|n} \phi(n/d) = \sum_{d|n} \#C_d$, and the latter sum must be n since it sums the sizes of a collection of sets whose union is $\{1, \dots, n\}$.

Say the integer m is in the class C_d if $1 \leq m \leq n$ and $(m, n) = d$. We see that $m|n$ if and only if $(m, n) = m$, so C_d contains exactly one element, d, which divides n.

Further, we see that $m \in C_d$ if and only if $(m, n) = d$, which happens if and only if $(m/d, n/d) = 1$. Thus the number of integers in C_d is the number of integers $\leq n/d$ which are relatively prime to n/d–that is, the size of C_d is $\phi(n/d)$. And this proves what we wanted. □

5.3 Perfect Numbers and Mersenne Primes

For further reading on the material in this subsection, consult **Rosen 7.3, Wikipedia**.

Definition 5.18. We say a positive integer n is a *perfect number* if $\sigma(n) = 2n$.

Example 5.19. Famously 6 is perfect, since $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

28 is perfect since $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$.

Theorem 5.20. *The positive even integer n is perfect if and only if $n = 2^{m-1}(2^m - 1)$ where $m \geq 2$ and $2^m - 1$ is prime.*

Proof. First we show that if $2^m - 1$ is prime then $n = 2^{m-1}(2^m - 1)$ is perfect. Because σ is multiplicative and we have a formula for it, we have

$$\begin{aligned}\sigma(n) &= \sigma(2^{m-1}(2^m - 1)) = \sigma(2^{m-1})\sigma(2^m - 1) \\ &= \frac{2^m - 1}{2 - 1} \cdot (1 + 2^m - 1) = (2^m - 1)2^m = 2n.\end{aligned}$$

Now we want to show that if $\sigma(n) = 2n$ and n is even, then $n = 2^{m-1}(2^m - 1)$ for some m. So write $n = 2^s t$ where t is odd. Then

$$\sigma(n) = \sigma(2^s)\sigma(t) = \frac{2^{s+1} - 1}{2 - 1} \cdot \sigma(t) = (2^{s+1} - 1)\sigma(t).$$

But since n is perfect, we know $\sigma(n) = 2n = 2^{s+1}t$ and thus we have

$$2^{s+1}t = (2^{s+1} - 1)\sigma(t)$$

and thus 2^{s+1} divides $(2^{s+1} - 1)\sigma(t)$.

But we can see that $(2^{s+1}, 2^{s+1} - 1) = 1$, so by Euclid's Lemma $2^{s+1}|\sigma(t)$. So let $\sigma(t) = 2^{s+1}q$ for some integer q, and we have

$$\begin{aligned} 2^{s+1}t &= (2^{s+1} - 1)2^{s+1}q \\ t &= (2^{s+1} - 1)q = 2^{s+1}q - q. \end{aligned}$$

Thus $q|t$ and $q \neq t$.

Adding q to both sides gives $t + q = 2^{s+1}q = \sigma(t)$. But if $q > 1$ then, since $q|t$ and $q \neq t$, we have (at least) three distinct positive divisors of t: $1, q$, and t. Thus $1 + q + t \leq \sigma(t) = q + t$ which is a contradiction. Thus $q = 1$, and $\sigma(t) = t + 1$. But if $\sigma(t) = t + 1$ this implies the only positive factors of t are 1 and t, and thus by definition t is prime. Further $t = (2^{s+1} - 1)q = 2^{s+1} - 1$. □

Thus to find all (even) perfect numbers, we just need to find primes of the form $2^m - 1$. This brings us to a famous old category of primes, called the Mersenne primes.

Definition 5.21. If $m \in \mathbb{N}$, then $M_m = 2^m - 1$ is called the *mth Mersenne number*. If M_m is prime, it is called a Mersenne prime.

Proposition 5.22. *If $m \in \mathbb{N}$ and $M_m = 2^m - 1$ is prime, then m is prime.*

Suppose $m = ab$ for $1 < a, b < m$. Then

$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-2)a} + 2^{(b-1)a}).$$

Since $a, b > 1$, both of these factors are > 1, so $2^m - 1$ is not prime, which is a contradiction.

Remark 5.23. Note that it is *not* true that if p is prime, then M_p is as well. The smallest "pernicious Mersenne number"–that is, M_p where p is prime but M_p is not– is $M_{11} = 2^{11} - 1 = 2047$, which we have discussed in class before.

Mersenne primes provide a relatively easy way to find large primes; the largest known prime is $2^{74,207,281} - 1$, which is a Mersenne prime. The GIMPS (Great Internet Mersenne Prime Search) is a large distributed computing project to test larger candidate Mersenne primes.

It was for a long time inaccurately believed that M_{67} was prime (after Marin Mersenne wrongly included it on his list of Mersenne primes in the 17th century; he also wrongly included M_{257} and excluded M_{61}, M_{89}, and M_{107}. Edouard Lucas showed in 1876 that M_{67} was composite, but did not find a factor.

In 1903, Frank Nelson Cole gave a completely silent "talk" in which he computed $2^{67} - 1$ and $193,707,721 \times 761,838,257,287$ on the blackboard and got the same number both ways (a result which he said took him "three years of Sundays" to find). He returned to his seat without speaking, to applause from the audience.

Though M_p is not always prime for p prime, we have a number of theorems that will help us decide of M_p is in fact prime.

Theorem 5.24. *If p is an odd prime, then any divisor of $M_p = 2^p - 1$ is of the form $2kp+1$ where $k \in \mathbb{N}$.*

Proof. Let q be a prime dividing $M_p = 2^p - 1$. By Fermat's little theorem we know that $2^{q-1} \equiv 1 \mod q$ and thus $q|2^{q-1} - 1$. We can compute that $(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1$. But since $q|2^p - 1, 2^{q-1} - 1$, we know that $q|2^{(p,q-1)} - 1$ and thus $(p, q-1) > 1$. But p is prime, so $(p, q-1) = p$.

Thus $p|q-1$ so there is a natural number m such that $mp = q - 1$. Since q, p are odd, we know that m is even, so write $m = 2k$ for $k \in \mathbb{N}$. Thus $q = 2kp + 1$, and any prime divisor of M_p has the form $2kp + 1$. But the product of two numbers of this form is still a number of this form, and any divisor of M_p is the product of prime divisors, so any divisor has the form $2kp + 1$. □

Corollary 5.25. *There are infinitely many primes.*

Proof. Suppose there are finitely many primes, and let p be the largest. Then $M_p > p$ is not prime, and it has some prime factor. But by theorem 5.24, the prime factor must have the form $2kp + 1 > p$, which is a contradiction. □

Example 5.26. Let us decide whether $M_{13} = 2^{13} - 1 = 8191$ is prime. We only need to check for factors less than $\sqrt{8191} \approx 90$. Further, any factor must have the form $2 \cdot k \cdot 13 + = 26k + 1$,

so we just have to check $27, 53, 79$. 27 isn't prime so we just need to check 53 and 79. But $8191/53 = 154.547$ and $8191/79 = 103.684$. Thus M_{13} must be prime.

Now let's decide if $M_{23} = 2^{23} - 1 = 8,388,607$ is prime. We only need to check primes of the form $46k + 1$. The first of these is 47, and we see $8,388,607/47 = 178,481$. Thus M_{23} is not prime.

Remark 5.27. There is a more efficient test to determine whether a Mersenne number is prime, called the *Lucas-Lehmer Test*. This could make a good paper topic for someone familiar with group theory.

Two last comments on this topic: first, all our work on Mersenne primes was specific to the base 2. We can't actually extend this work to other bases. Or rather, we can, but it's very brief.

Exercise 5.28. *Suppose $a^p - 1$ is prime. Then either $a \leq 2$ or $p = 1$.*

Second, we've only addressed even perfect numbers. It's actually an open question whether odd perfect numbers exist, and commonly conjectured that they do not. We do know a large number of conditions that odd perfet numbers must satisfy:

Fact 5.29. *Suppose N is an odd perfect number. Then*

- *N is not divisible by 105*
- *N satisfies one of $N \equiv 1 \mod 12$, $N \equiv 117 \mod 468$, or $N \equiv 81 \mod 324$*
- *$N = q^a p_1^{2e_1} \dots p_k^{2e_k}$ where*
  - *$q, p_1, \dots, p_k$ are distinct primes*
  - *$q \equiv a \equiv 1 \mod 4$*
  - *The smallest prime factor of N is less than $(2k + 8)/3$*
  - *Either $q^a > 10^{62}$, or $p_j^{2e_j} > 10^{62}$ for some j*
  - *$N < 2^{4^{k+1}}$*
- *The largest prime factor of N is greater than 10^8, the second largest prime factor is greater than 10^4, and the third largest is greater than 100*
- *N has at least 101 prime factors and at least 10 distinct prime factors, and if $3 \nmid N$ then N has at least 12 distincct prime factors.*

- $N > 10^{1500}$

This list of restrictions is sufficiently long that James Joseph Sylvester commented in 1888 that: "...a prolonged meditation on the subject has satisfied me that the existence of any one such [odd perfect number]—its escape, so to say, from the complex web of conditions which hem it in on all sides—would be little short of a miracle."

5.4 Mobius Inversion

For further reading on the material in this subsection, consult **Rosen 7.4**.

We earlier discussed summatory functions, where we write $F(n) = \sum_{d|n} f(n)$ for some function f; we proved that if f is multiplicative, then so is F. In this section we'd like to reverse the summatory function process. That is, if we have $F(n)$ can we use that to compute $f(n)$?

Well, we'll start by exploring. We notice that

$$\begin{aligned}
F(1) &= f(1) \\
F(2) &= f(1) + f(2) \\
F(3) &= f(1) + f(3) \\
F(4) &= f(1) + f(2) + f(4) \\
F(5) &= f(1) + f(5) \\
F(6) &= f(1) + f(2) + f(3) + f(6)
\end{aligned}$$

and thus

$$\begin{aligned}
f(1) &= F(1) \\
f(2) &= F(2) - f(1) = F(2) - F(1) \\
f(3) &= F(3) - f(1) = F(3) - F(1) \\
f(4) &= F(4) - f(2) - f(1) = F(4) - (F(2) - F(1)) - F(1) \\
&= F(4) - F(2) \\
f(5) &= F(5) - f(1) = F(5) - F(1) \\
f(6) &= F(6) - f(3) - f(2) - f(1) = F(6) - (F(3) - F(1)) - (F(2) - F(1)) - F(1) \\
&= F(6) - F(3) - F(2) + F(1).
\end{aligned}$$

We might notice that we seem to always be able to write $f(n)$ as a sum of $\pm F(n/d)$ for $d|n$.

So we might hope we can find an arithmetic function μ that gives a formula

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

Let's figure out what this function would have to look like. $f(1) = F(1)$ so $\mu(1) = 1$. If p is a prime, then $F(p) = f(1) + f(p)$ so $f(p) = F(p) - F(1)$. Thus we must have $\mu(p) = -1$. (Recall that we have $\mu(d)F(n/d)$ so $\mu(p)$ is the coefficient of $F(1)$).

By the same logic, we see that $F(p^2) = f(1) + f(p) + f(p^2)$ so $f(p^2) = F(p^2) - F(p)$. Thus if $\mu(1) = 1$ and $\mu(p) = -1$, we have $\mu(p^2) = 0$. We can follow the same argument to show that $\mu(p^k) = 0$ for every $k > 1$.

If we assume that μ is multiplicative, this completely nails down the values of μ at every number, since we can "compute" it at any prime power. This leads us to the following definition:

Definition 5.30. We define the *Möbius function* $\mu(n)$ by

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^r & n = p_1 p_2 \dots p_r \text{ are distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

In particular, if $p^2 | n$ for any prime p then $\mu(n) = 0$. $\mu(n) \neq 0$ if and only if n is *square-free*.

Remark 5.31. If we think of 1 as the empty product, then we don't need to define $\mu(1)$ separately, since $1 = \prod_{k=1}^{0} p_i$ and then $\mu(1) = (-1)^0$.

Example 5.32.

$$\begin{aligned} \mu(1) &= 1 & \mu(4) &= 0 \\ \mu(2) &= -1 & \mu(5) &= -1 \\ \mu(3) &= -1 & \mu(6) &= 1. \end{aligned}$$

We can compute that

$$\begin{aligned} \mu(330) &= \mu(2 \cdot 3 \cdot 5 \cdot 11) = (-1)^4 = 1 \\ \mu(660) &= \mu(2^2 \cdot 3 \cdot 5 \cdot 11) = 0 \\ \mu(2310) &= \mu(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = (-1)^5 = -1. \end{aligned}$$

Lemma 5.33. *The Möbius function $\mu(n)$ is multiplicative.*

Proof. Suppose m, n are relatively prime positive integers. We want to show that $\mu(mn) = \mu(m)\mu(n)$. We need to check this case-by-case.

If $m = 1$ then $\mu(m) = 1$, so $\mu(mn) = \mu(n) = \mu(m)\mu(n)$. Similarly if $n = 1$ then $\mu(mn) = \mu(m) = \mu(m)\mu(n)$.

If m is divisible by a square of a prime, then so is mn, so $\mu(mn) = 0 = 0 \cdot \mu(n) = \mu(m)\mu(n)$. Similarly, if n is divisible by a square of a prime, then so is mn, so $\mu(mn) = 0 = \mu(m) \cdot 0 = \mu(m)\mu(n)$.

Finally, suppose $m, n \neq 1$ and neither is divisible by a square of a prime. Then we we can write $m = p_1 \dots p_k$ and $n = q_1, \dots, q_\ell$ where the p_i and the q_i are all distinct. Then we have $\mu(m) = (-1)^k, \mu(n) = (-1)^\ell$. We also have $mn = p_1 \dots p_k q_1 \dots q_\ell$ all distinct factors, so $\mu(mn) = (-1)^{k+\ell} = (-1)^k(-1)^\ell = \mu(m)\mu(n)$. □

Remark 5.34. The Möbius function is not completely multiplicative, since $\mu(2) = -1$ but $\mu(4) = 0$.

Since we have a multiplicative function, the next step is to study its summatory function. Fortunately, the Möbius function has a particularly simple summatory function:

Lemma 5.35. *The summatory function of the Möbius function satisfies the formula*

$$F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1. \end{cases}$$

Proof. When $n = 1$, we have $F(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$.

Now suppose $n > 1$. We know that F is multiplicative, so we just need to evaluate it at prime powers. But

$$\begin{aligned} F(p^k) &= \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \dots + \mu(p^k) \\ &= 1 - 1 + 0 + 0 + \dots + 0 = 0 \end{aligned}$$

as long as $k > 0$.

Suppose $n = p_1^{a_1} \dots p_k^{a_k}$. Then

$$F(n) = \prod_{i=1}^{k} F(p_i^{a_i}) = \prod_{i=1}^{k} 0 = 0.$$

□

So far we've studied some properties of our Möbius function, but we haven't actually proven that it does the thing we want it to do. Recall we were hoping to find an "inversion formula" that allows us to recapture a function from its summative function. If such a function exists and is multiplicative, it must be the Möbius function; but now we're ready to prove that the Möbius function does in fact have this property.

Theorem 5.36 (Möbius Invrsion Formula)**.** *Suppose f is an arithmetic function (which need not be multiplicative!), and F is the summatory function of f, given by*

$$F(n) = \sum_{d|n} f(d).$$

Then, for any natural number n, we have

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

Proof. The proof of this is a fairly straightforward exercise in manipulation of sums, but we must be careful of our indices.

Fix an integer n. We have

$$\begin{aligned}\sum_{d|n} \mu(d)F(n/d) &= \sum_{d|n} \left(\mu(d) \sum_{e|(n/d)} f(e) \right) \\ &= \sum_{d|n} \sum_{e|(n/d)} \mu(d) f(e).\end{aligned}$$

Now we think about the indices. We're summing over all pairs of integers d, e such that $d|n$ and $e|n/d$. But this is the same as summing over all pairs of integers d, e such that $e|n$ and $d|(n/e)$. (Suppose $d|n$ and $em = n/d$. Then $emd = n$ so $e|n$, and $md = n/e$ so $d|n/e$. We can do the same argument in the opposite direction). Thus we have

$$\begin{aligned}\sum_{d|n} \sum_{e|(n/d)} \mu(d) f(e) &= \sum_{e|n} \sum_{d|(n/e)} \mu(d) f(e) \\ &= \sum_{e|n} f(e) \left(\sum_{d|(n/e)} \mu(d) \right).\end{aligned}$$

But recall that $\sum_{d|(n/e)} \mu(d) = 0$ unless $n/e = 1$, which happens precisely when $e = n$, and in this case the sum is equal to 1. So every term of this sum is 0 except the term corresponding to $e = n$, which gives us

$$\sum_{e|n} f(e) \sum_{d|(n/e)} \mu(d) = f(e) \cdot 1 = f(e).$$

□

This is all an example of a process called *Dirichlet convolution*, which you will see more about on the homework.

Corollary 5.37. *If n is a natural number, we have*

$$n = \sum_{d|n} \mu(d)\sigma(n/d) = \sum_{d|n} \mu(n/d)\sigma(d)$$
$$1 = \sum_{d|n} \mu(d)\tau(n/d) = \sum_{d|n} \mu(n/d)\tau(d).$$

Corollary 5.38. *Let f be an arithmetic function and $F(n) = \sum_{d|n} f(n)$ be the summatory function of f. If F is multiplicative, then so is f.*

Remark 5.39. Notice this is the converse of proposition 5.13, which said that if f is multiplicative, then so is its summatory function.

Proof. Suppose m, n are relatively prime natural numbers. We want to show that $f(mn) = f(m)f(n)$. First recall that if $d|mn$ then we can uniquely write $d = d_1d_2$ with $d_1|m, d_2|n$ (since m, n share no factors in common), and $(d_1, d_2) = 1$. Then

$$\begin{aligned}
f(mn) &= \sum_{d|mn} \mu(d)F\left(\frac{mn}{d}\right) \\
&= \sum_{d_1|m,d_2|n} \mu(d_1d_2)F\left(\frac{mn}{d_1d_2}\right) \\
&= \sum_{d_1|m,d_2|n} \mu(d_1)\mu(d_2)F\left(\frac{m}{d_1}\right)\left(\frac{n}{d_2}\right) \\
&= \left(\sum_{d_1|m} \mu(d_1)F(m/d_1)\right)\left(\sum_{d_2|n} \mu(d_2)F(n/d_2)\right) \\
&= f(m)f(n).
\end{aligned}$$

□

6 Primitive Roots and the Discrete Logarithm

For further reading on the material in this subsection, consult **Rosen 9.1**.

In section 3.2 we studied the problem of extending division to modular arithmetic. We noted that trying to find b/a is equivalent to solving the equation $ax = b$, and so we worked on the congruence $ax \equiv b \mod m$.

In this section we will be applying a similar analysis to the logarithm. The real number logarithm $\log_a(b)$ is the solution to the equation $a^x = b$; we wish to study the congruence equation $a^x \equiv b \mod m$.

6.1 The order of an integer

We're going to start with the very simplest case: computing the logarithm of 1. In particular we want to consider the equation $a^x \equiv 1 \mod n$ and see if it has any solutions at all, and if so, how many.

It is of course true that $x = 0$ solves this congruence. But we can find more solutions! Recall that Euler's theorem tells us that if n is a natural number and $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$. Thus $x = \phi(n)$ is also a solution to this congruence. That means there is at least one *positive* solution, and so (by the well-ordering principle) we can ask for the *least* positive solution.

Definition 6.1. Let a, n be relatively prime integers with $a \neq 0$ and n positive. Then the least positive integer x such that $a^x \equiv 1 \mod n$ is called the *order of a modulo n*, written $\operatorname{ord}_n a$.

Example 6.2. Let's compute the orders of 2 and 3 modulo 7. We see

$$2^1 \equiv 2 \mod 7 \qquad 3^1 \equiv 3 \mod 7$$
$$2^2 \equiv 4 \mod 7 \qquad 3^2 \equiv 9 \equiv 2 \mod 7$$
$$2^3 \equiv 1 \mod 7 \qquad 3^3 \equiv 27 \equiv 6 \mod 7$$
$$3^4 \equiv 81 \equiv 4 \mod 7$$
$$3^5 \equiv 4 \cdot 3 \equiv 12 \equiv 5 \mod 7$$
$$3^6 \equiv 5 \cdot 3 \equiv 15 \equiv 1 \mod 7.$$

Thus $\operatorname{ord}_7 2 = 3$ and $\operatorname{ord}_7 3 = 6$.

Lemma 6.3. *If a, n are relatively prime integers with $a \neq 0$ and $n > 0$, then a positive integer x is a solution to the congruence $a^x \equiv 1 \mod n$ if and ony if $\operatorname{ord}_n a | x$.*

Proof. First suppose $\operatorname{ord}_n a | x$. Then we can write $x = m \cdot \operatorname{ord}_n a$ for some integer m, and we have

$$a^x \equiv a^{m \cdot \operatorname{ord}_n a} \equiv \left(a^{\operatorname{ord}_n a}\right)^m \equiv 1^m \equiv 1 \mod n.$$

Conversely, suppose $a^x \equiv 1 \mod n$, we can use the division algorithm divide x by $\operatorname{ord}_n a$ and write

$$x = q \cdot \operatorname{ord}_n a + r, \qquad 0 \rightrightarrows r < \operatorname{ord}_n a.$$

Then we compute

$$1 \equiv a^x \equiv a^{q \cdot \operatorname{ord}_n a + r} \equiv a^{q \cdot \operatorname{ord}_n a} \cdot a^r \equiv a^r \mod n$$

so we have $a^r \equiv 1 \mod n$ but $0 \leq r < \operatorname{ord}_n a$. But $\operatorname{ord}_n a$ is by definition the least positive integer with this property, so r cannot be positive and must be 0. Thus $x = q \cdot \operatorname{ord}_n a$ as desired. □

Remark 6.4. This should remind you of the proof that since (a, b) is the least linear combination of a and b, we know that m is a linear combination of a and b if and only if $(a, b) | m$.

Example 6.5. Let's see if 10, 20, or 30 are solutions to $3^x \equiv 1 \mod 7$. We saw that $\operatorname{ord}_7 3 = 6$, so $3^{30} \equiv 1 \mod 7$ since $6|30$. But $3^{20} \not\equiv 1 \mod 7$ and $3^{10} \not\equiv 1 \mod 7$ since $6 \not| 10, 20$.

Corollary 6.6. *If* $(a, n) = 1$ *with* $n > 0$*, then* $\operatorname{ord}_n a | \phi(n)$.

Proof. Since $(a, n) = 1$ we know that $a^{\phi(n)} \equiv 1 \mod n$, thus $\operatorname{ord}_n a | \phi(n)$. □

We can use this to make it easier to compute orders: we only need to check numbers that divide $\phi(n)$.

Example 6.7. Let's find the order of 7 modulo 9. We can compute that $\phi(9) = 3(3-1) = 6$, so we just need to check 1, 2, 3, 6. We see

$$7^1 \equiv 7 \not\equiv 1 \mod 9$$
$$7^2 \equiv 49 \equiv 4 \not\equiv 1 \mod 9$$
$$7^3 \equiv 4 \cdot 7 \equiv 28 \equiv 1 \mod 9$$

We don't need to check 6.

Example 6.8. Let's find $\operatorname{ord}_{11} 3$. We know that $\phi(11) = 10$ so we just need to check $1, 2, 5, 10$. We have

$$\begin{aligned} 3^1 &\equiv 3 \not\equiv 1 \mod 11 \\ 3^2 &\equiv 9 \not\equiv 1 \mod 11 \\ 3^5 &\equiv 243 = 11(22) + 1 \equiv 1 \mod 11 \end{aligned}$$

so $\operatorname{ord}_{11} 3 = 5$. This saves us from checking 3 or 4 since we know they can't be the answer.

Remark 6.9. Note that sometimes $\operatorname{ord}_n a = \phi(n)$. For instance, you can check that $\operatorname{ord}_{11} 2 = 10$.

Lemma 6.10. *If $(a, n) = 1$, then $a^i \equiv a^j \mod n$ if and only if $i \equiv j \mod \operatorname{ord}_n a$.*

Proof. First, let's suppose $i \equiv j \mod \operatorname{ord}_n a$, and assume that $i \geq j$. Then there is some k such that $i = j + k \cdot \operatorname{ord}_n a$, and we have

$$\begin{aligned} a^i &\equiv a^{j + k \cdot \operatorname{ord}_n a} \equiv a^j \cdot a^{k \cdot \operatorname{ord}_n a} \\ &\equiv a^j \cdot (a^{\operatorname{ord}_n a})^k \equiv a^j \cdot 1^k \equiv a^j \mod n. \end{aligned}$$

Conversely, suppose $a^i \equiv a^j \mod n$, and again without loss of generality assume $i \geq j$. Then we have

$$\begin{aligned} a^i &\equiv a^j \mod n \\ a^j \cdot a^{i-j} &\equiv a^j \mod n \\ a^{i-j} &\equiv 1 \mod n \end{aligned}$$

since $(a, n) = 1$ and thus $(a^j, n) = 1$ so we can use the cancellation lemma. But if $a^{i-j} \equiv 1 \mod n$ then by lemma 6.3 we know that $\operatorname{ord}_n a | i - j$, and so by defnition $i \equiv j \mod \operatorname{ord}_n a$. □

6.2 Primitive Roots

For further reading on the material in this subsection, consult **Rosen 9.1**.

We've shown that the order of any integer modulo n will divide $\phi(n)$. In this subsection we're interested in elements whose order is exactly $\phi(n)$.

Definition 6.11. If $(a, n) = 1$, and $\operatorname{ord}_n a = \phi(n)$, we say that a is a *primitive root* modulo n, and we say that n has a primitive root.

Example 6.12. We showed that $\operatorname{ord}_7 3 = 6 = \phi(7)$ so 3 is a primitive root modulo 7. However, $\operatorname{ord}_7 2 = 3 \neq \phi(7)$, so 2 is not a primitive root modulo 7.

Example 6.13. The number 8 does not have a primitive root. The integers relatively prime to 8 are 1,3,5,7. We can compute $\operatorname{ord}_8 1 = 1$ and $\operatorname{ord}_8 3 = \operatorname{ord}_8 5 = \operatorname{ord}_8 7 = 2$, but $\phi(8) = 4$.

Every prime number has a primitive root; we will prove this in subsection 6.3. Not every composite number has a primitive root, but some, like 6 and 10, do.

Theorem 6.14. *If $(r, n) = 1$ and $n > 0$, and r is a primitive root modulo n, then the set $\{r^1, r^2, \ldots, r^{\phi(n)}\}$ is a reduced residue system modulo n.*

Proof. This set clearly has the correct size, so we need to prove that these numbers are all relatively prime to n and that no two are congruent modulo n.

Because $(r, n) = 1$ we know that $(r^k, n) = 1$ for any natural number k. This satisfies the first requirement.

Suppose $r^i \equiv r^j \mod n$. Then by lemma 6.10 we know that $i \equiv j \mod \operatorname{ord}_n r$. But r is a primitive root, which means that $\operatorname{ord}_n r = \phi(n)$. Thus $\phi(n) | i - j$ but $1 \leq i, j \leq \phi(n)$ and thus $i = j$. □

Example 6.15. We showed that $\operatorname{ord}_7 3 = 6$ so 3 is a primitive root modulo 7. Thus the set

$$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3, 9, 27, 81, 243, 729\}$$

is a reduced residue system modulo 7.

We can check that $\operatorname{ord}_9 2 = 6 = \phi(9)$. Thus the set

$$\{2, 2^2, 2^3, 2^4, 2^5, 2^6\} = \{2, 4, 8, 16, 32, 64\}$$

is a reduced residue system modulo 9.

We already noted that not every integer has a primitive root. But if an integer has a primitive root it usually has several more. We will spend the rest of this subsection making that statement more precise.

Lemma 6.16. *Let n be a natural number, and $(a, n) = 1$, and set $\operatorname{ord}_n a = t$. Then for any $u \in \mathbb{N}$ we have*

$$\operatorname{ord}_n a^u = \frac{t}{(u, t)}.$$

Proof. First set $t_1 = t/(u,t)$ and $u_1 = u/(u,t)$, and set $s = \operatorname{ord}_n a^u$. We know that $(t_1, u_1) = 1$. Now we want to show that $s = t_1$.

First we want to show that $(a^u)^{t_1} \equiv 1 \mod n$. But

$$(a^u)^{t_1} = a^{ut_1} = a^{ut/(u,t)} = (a^t)^{u_1} \equiv 1^{u_1} \equiv 1 \mod n.$$

Thus we know that $s = \operatorname{ord}_n a^u | t_1$ by lemma 6.3.

Conversely, we know that $(a^u)^s \equiv 1 \mod n$, and thus $a^{us} \equiv 1 \mod n$, which implies that $t|us$, again by lemma 6.3. Dividing on both sides by (u,t) gives $t_1|u_1 s$, but $(t_1, u_1) = 1$, so by Euclid's lemma this gives us $t_1|s$.

Since $t_1|s$ and $s|t_1$, we know that $s = t_1$, which gives us $\operatorname{ord}_n(a^u) = \frac{\operatorname{ord}_n a}{(\operatorname{ord}_n a, u)}$, or $s = t/(u,t)$, as desired. □

Corollary 6.17. *Let r be a primitive root modulo n. Then r^u is a primitive root modulo n if and only if $(u, \phi(n)) = 1$.*

Proof. We know that

$$\operatorname{ord}_n r^u = \frac{\operatorname{ord}_n r}{(u, \operatorname{ord}_n r)} = \frac{\phi(n)}{(u, \phi(n))}.$$

Thus r^u is a primitive root if and only if $\operatorname{ord}_n r^u = \phi(n)$ if and only if $(u, \phi(n)) = 1$. □

So if a number n has a primitive root, how many does it have? It must have one for every exponent that's relatively prime to $\phi(n)$.

Corollary 6.18. *If a positive integer n has a primitive root, it has exactly $\phi(\phi(n))$ primitive roots.*

Proof. Let r be a primitive root modulo n. Then r^u is a primitive root if and only if $(u, \phi(n)) = 1$; there are $\phi(\phi(n))$ numbers relatively prime to $\phi(n)$.

(Every primitive root must have the form r^u for some u, since these are all the numbers relatively prime to n). □

Example 6.19. We claimed earlier that $\operatorname{ord}_{11} 2 = 10$, and thus 2 is a primitive root modulo 11. This tells us that 11 has $\phi(\phi(11)) = \phi(10) = 4$ incongruent primitive roots. In particular, these roots are $2, 2^3 = 8, 2^7 = 128 \equiv 7, 2^9 = 512 \equiv 6$. Thus $\{2, 6, 7, 8\}$ is a complete set of incongruent primitive roots modulo 11.

This result does have one weakness: it tells us what happens if there are *any* primitive roots modulo n, but doesn't tell us which integers n have any primitive roots at all.

6.3 Primitive Roots for Primes

In this section we'd like to prove that every prime number has a primitive root. The basic idea is that for a fixed prime p, there are a lot of numbers relatively prime to p. In fact, there are so many that we run out of "room" for non-primitive roots, so some of them have to be primitive roots.

In order to do this, we have to return to looking at polynomial congruences.

Definition 6.20. Let $f(x)$ be a polynomial with integer coefficients. We say c is a *root of f modulo m* if $f(c) \equiv 0 \mod m$. (This is the same idea as a root in the integers, except we're thinking about everything as belonging to the integers modulo m).

Example 6.21. The polynomial $f(x) = x^2 + 1$ has no roots in the integers, but it has two roots modulo 5: $f(2) = 5 \equiv 0 \mod 5$, and $f(3) = 10 \equiv 0 \mod 5$.

Example 6.22. Let $f(x) = x^{p-1} - 1$ for a fixed prime p. Then by Fermat's little theorem, f has $p-1$ incongruent roots modulo p: $1, 2, 3, \ldots, p-1$.

It's a famous result in the real numbers that a polynomial of degree n has at most n distinct roots. A similar result holds modulo p.

Theorem 6.23 (Lagrange's Theorem)**.** *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, and $p \not| a_n$. Then $f(x)$ has at most n incongruent roots modulo p.*

Proof. We prove this by induction. (Yay!) When $n = 1$, we have $f(x) = a_1 x + a_0$ with $p \not| a_1$. By our results on linear congruences, we know that $a_1 x \equiv -a_0 \mod p$ has exactly one solution modulo p, since $(a_1, p) = 1$. Thus f has exactly one root, and thus at most one root.

Suppose the theorem is true for $n-1$, that is, *any* polynomial of degree $n-1$ has at most $n-1$ incongruent solutions. Now let $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Suppose $f(x)$ has $n+1$ incongruent solutions modulo p, which we can call $c_0, c_1, \ldots, c_n$. Then $f(c_i) \equiv 0 \mod p$ for $0 \leq i \leq n$. Then

$$f(x) - f(c_0) = a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0).$$

We see that we can factor $(x - c_0)$ out of each term, so we can write

$$f(x) - f(c_0) = (x - c_0)g(x)$$

for some polynomial $g(x)$ with degree $\leq n - 1$.

We claim that $g(c_i) \equiv 0 \mod p$ for any $1 \leq i \leq n$. For we have

$$(c_i - c_0)g(c_i) = f(c_i) - f(c_0) \equiv 0 - 0 \equiv 0 \mod p.$$

Thus since p is prime, either $p|g(c_i)$ or $p|(c_i - c_0)$. But by hypothesis we know that $c_i \neq c_0 \mod p$ so $p \not| c_i - c_0$, and thus we have $p|g(c_i)$ and $g(c_i) \equiv 0 \mod p$. Thus c_i is a root of g modulo p for $1 \leq i \leq n$.

Thus g is a polynomial of degree $\leq n-1$ with n incongruent solutions, which contradicts the inductive hypothesis. □

Remark 6.24. This theorem does *not* hold for composite moduli. For instance, if we take $g(x) = x^2 - 3x + 2$, then modulo 6 we see that $g(1) = 0 \equiv 0 \mod 6$, and $g(2) = 0 \equiv 0 \mod 6$, and $g(4) = 6 \equiv 0 \mod 6$.

We want to use Lagrange's Theorem to put limits on how many elements can have a given order modulo p.

Proposition 6.25. *Let p be a prime and let d be a divisor of $p-1$. Then the polynomial $f(x) = x^d - 1$ has exactly d incongruent roots modulo p.*

Proof. We know that $d|p-1$, so by the difference of nth powers formula we have $(x^d - 1)|x^{p-1} - 1$. In particular

$$x^{p-1} - 1 = (x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{p-1-d}).$$

Set $g(x) = 1 + x^d + \cdots + x^{p-1-d}$; this is a polynomial of degree $p - 1 - d$.

By Fermat's Little Theorem, we know that $x^{p-1} - 1$ has exactly $p-1$ incongruent roots. We can see that every root of $x^{p-1} - 1$ that is not a root of g must be a root of $x^d - 1$ (since if $p|x^{p-1} - 1$ then either $p|g(x)$ or $p|x^d - 1$).

But by Lagrange's theorem we know that g has at most $p - 1 - d$ incongruent roots, so $x^d - 1$ must have at least $p - 1 - (p - 1 - d) = d$ incongruent roots. But again we know that $x^d - 1$ has at most d incongruent roots, so it has exactly d incongruent roots. □

Lemma 6.26. *Let p be a prime and let $d|p-1$. Then there are fewer than $\phi(d)$ positive integers less than p that have order d modulo p.*

Proof. Let $F(d)$ be the number of positive integers of order d modulo p that are less than p. We wish to prove that $F(d) \leq \phi(d)$.

If there are no roots of order d modulo p then it's clear that $F(d) = 0 \leq \phi(d)$. So suppose there is an integer a of order d modulo p. Then the integers $a, a^2, \ldots, a^d$ are all incongruent modulo p.

Further, we see that for any $k \in \mathbb{N}$, we compute that $(a^k)^d = (a^d)^k \equiv 1^k \equiv 1 \mod p$, so a^k is a root of $x^d - 1$ modulo p for any k. Thus we have d incongruent roots of $x^d - 1$ on this list. Since we know $x^d - 1$ has exactly d incongruent roots modulo p, we know that the set of roots is exactly the set $a, a^2, \dots, a^d$.

By lemma 6.16, we see that $\operatorname{ord}_p a^k = \frac{\operatorname{ord}_p a}{(k, \operatorname{ord}_p a)} = \frac{d}{(k,d)}$, and thus a^k has order d if and only if $(k, d) = 1$. There are exactly $\phi(d)$ such integers k with $1 \leq k \leq d$, and thus if there is one element of order d modulo p, there are exactly $\phi(d)$ positive integers less than p of order d modulo p. Thus $F(d) \leq \phi(d)$. □

Remark 6.27. This theorem proves that for a given $d|p-1$, either there are $\phi(d)$ elements of order d or there are 0. But we didn't state it that way because we are about to leverage it into an even better result.

Theorem 6.28. *Let p be a prime, and let d be a positive divisor of $p-1$. Then the number of incongruent ingeters of order d modulo p is exactly $\phi(d)$.*

Proof. This is essentially a counting argument. For any $d|p-1$, let $F(d)$ be the number of positive integers of order d modulo p that are less than p. Because every integer from 1 to $p-1$ has an order dividing $p-1$, we see that

$$p - 1 = \sum_{d|p-1} F(d).$$

But we also know that

$$p - 1 = \sum_{d|p-1} \phi(d),$$

so

$$\sum_{d|p-1} F(d) = \sum_{d|p-1} \phi(d).$$

From lemma 6.26 we know that $F(d) \leq \phi(d)$, but their sums are equal; the only way this is possible is if $F(d) = \phi(d)$ for each $d|p-1$. Thus there are exactly $\phi(d)$ incongruent integers of order d modulo p. □

Corollary 6.29. *Every prime has a primitive root.*

Proof. Let p be a prime. Then there are exactly $\phi(p-1)$ incongruent integers of order $p-1$ modulo p by theorem 6.28. But these are all primitive roots by definition. Since $\phi(p-1) \geq 1$, this completes the proof. □

This proves that every prime has a primitive root, but doesn't give us a way to find them. In fact locating primitive roots is not trivial; on the other hand, 2 appears to be a primitive root quite often. But we don't know whether it is a primitive root infinitely often.

Conjecture 6.30 (Artin)**.** *Any integer a such that $a \neq \pm 1$ and a is not a perfect square is a primitive root of infinitely many primes.*

Proposition 6.31 (Hooley 1967)**.** *The Generalized Riemann Hypothesis implies Artin's conjecture.*

Proposition 6.32 (Heath-Brown 1985)**.** *There are at most three positive square-free integers a such that a is a primitive root of only finitely many primes. Thus at least one of 2, 3, 5 is a primitive root for infinitely many primes.*

6.4 Primitive Roots for Composites

We now understand exactly when a prime number has a primitive root (always), and how many it has ($\phi(p-1)$). What about composite numbers?

We start with the simplest kind of composite numbers: the prime powers.

Lemma 6.33. *Let p be an odd prime, with primitieve root r. Then either r or $r+p$ is a primitive root modulo p^2.*

Remark 6.34. This means that there is some integer that is a primitive root modulo p and also modulo p^2, since $p+r$ is a primitive root modulo p.

Proof. We know that $\operatorname{ord}_p r = \phi(p) = p-1$. Let $n = \operatorname{ord}_{p^2} r$. By definition $r^n \equiv 1 \mod p^2$, and thus $r^n \equiv 1 \mod p$. This implies that $p-1 = \operatorname{ord}_p r | n$.

But we know that $\operatorname{ord}_{p^2} r | \phi(p^2) = p(p-1)$, so we have $p-1 | n | p(p-1)$. Thus either $n = p-1$ or $n = p(p-1)$. If $n = p(p-1)$ then r is a primitive root modulo p^2; so suppose $n = p-1$.

Let $s = r+p$. Then since s is also a primitive root modulo p, by the same logic we know that $\operatorname{ord}_{p^2} s$ is either $p-1$ or $p(p-1)$. We wish to show that $\operatorname{ord}_{p^2} s \neq p-1$.

By the binomial theorem, we compute

$$\begin{aligned} s^{p-1} = (r+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} p^i r^{p-1-i} \\ &= r^{p-1} + (p-1)pr^{p-2} + \cdots + (p-1)p^{p-2}r + p^{p-1} \\ &\equiv r^{p-1} + (p-1)pr^{p-2} \mod p^2 \\ &\equiv 1 + (p-1)pr^{p-2} \mod p^2. \end{aligned}$$

But since $p \not| r$ we see that $(p-1)pr^{p-2} \not\equiv 0 \mod p^2$ so $s^{p-1} \not\equiv 1 \mod p^2$ as desired.

Thus $\text{ord}_{p^2} s \neq p-1$, and the only remaining possibility is that $\text{ord}_{p^2} s = p(p-1) = \phi(p^2)$. □

Example 6.35. We have seen that 2 is a primitive root modulo 11. But $2^{10} = 1024 \equiv 56 \mod 121$ so $\text{ord}_{121} 2 \neq 10$. Thus we must have $\text{ord}_{121} 2 = 110 = \phi(121)$ so 2 is a primitive root modulo 121.

We hve seen that 3 is a primitive root modulo 7. But $3^6 = 729 \equiv 43 \not\equiv 1 \mod 49$. Thus $\text{ord}_{49} 3 \neq 6$ so $\text{ord}_{49} 3 = 42 = \phi(49)$ and 3 is a primitive root modulo 49.

Example 6.36. Let $p = 487$ be prime, and we compute that $\text{ord}_{487} 10 = 486$. (We do not do this by hand). But $10^{486} \equiv 1 \mod 487^2$ so 10 is not a primitive root modulo 487^2. Thus we know that $497 = 10 + 487$ is a primitive root modulo 487^2.

Lemma 6.37. *Let p be an odd prime. Then p^k has a primitive root for any $k \in \mathbb{N}$. Moreover, if r is a primitive root modulo p^2, then r is a primitive root modulo p^k for any $k \in \mathbb{N}$.*

Proof. By lemma 6.33 we know that p has a primitive root r that is also a primitive root modulo p^2, and thus $r^{p-1} \not\equiv 1 \mod p^2$.

First we will prove by induction that $r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k$ for any $k \geq 2$. The base case when $k = 2$ follows from Lemma 6.33. Suppose the assertion is true for k, and we will prove it for $k+1$.

By inductive hypothesis, we know that

$$r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k.$$

But also $(r, p) = 1$ since r is a primitive root, and thus $(r, p^{k-1}) = 1$. Thus $\phi(p^{k-1}) = p^{k-2}(p-1)$ and thus

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \mod p^{k-1}.$$

Thus we can find some integer such that

$$r^{p^{k-2}(p-1)} = 1 + dp^{k-1}$$

where $p \not| d$ since otherwise the congruence would hold moduldo p^k. We can raise both sides

of this to the pth power, which gives

$$\begin{aligned} r^{p^{k-2}(p-1)(p)} &= \sum_{i=0}^{p} \binom{p}{i} (dp)^{(k-1)i} \\ r^{p^{k-1}(p-1)} &= 1 + dp^k + p^{k+1} \text{ (stuff)} \\ r^{p^{k-1}(p-1)} &\equiv 1 + dp^k \mod p^{k+1} \\ &\not\equiv 1 \mod p^{k+1} \end{aligned}$$

since $p \not| d$. Thus by induction, for any $k \geq 2$ we have

$$r^{p^{k-1}(p-1)} \not\equiv 1 \mod p^{k+1}.$$

Now we wish to show that r is a primtiive root modulo p^k. Let $n = \text{ord}_{p^k} r$. We know that $n|\phi(p^k) = p^{k-1}(p-1)$. Further, we know that $\text{ord}_p r = p-1$ so we must have $p-1|n$. So $n = p^t(p-1)$ for some $0 \leq t \leq k-1$.

But we know that

$$r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k,$$

so we must have $t < k-2$. Thus $t = k-1$ and so $\text{ord}_r = p^{k-1}(p-1) = \phi(p^k)$, and r is a primitive root modulo p^k. □

Example 6.38. We saw that 2 is a primitive root modulo 11 and also modulo 121. Thus 2 is a primitive root modulo 11^k for any $k \in \mathbb{N}$.

Now we turn our attention to powers of even primes.

Lemma 6.39. *If a is an odd integer and k is an integer with $k \geq 3$, then*

$$a^{\phi(2^k)/2} = a^{2^{k-2}} \equiv 1 \mod 2^k.$$

Thus there are no primitive roots modulo 2^k for $k \geq 3$.

Proof. We prove this by induction, again.

Our base case is $k = 3$, which you checked for homework: we saw that $\phi(2^3) = \phi(8) = 4$, but $a^2 \equiv 1 \mod 8$ for any odd a.

Now suppose $a^{2^{k-2}} \equiv 2^k$. Then there is an integer d with $a^{2^{k-2}} = 1 + d2^k$. Squaring both sides gives

$$\begin{aligned} a^{2^{k-2} \cdot 2} &= (1 + d2^k)^2 \\ a^{2^{k-1}} &= 1 + 2^{k+1}d + d^2 2^{2k} \\ a^{2^{k-1}} &\equiv 1 \mod 2^{k+1} \end{aligned}$$

as desried.

□

This shows that there is never a primitive root modulo 2^k if $k \geq 3$. However, there is always an "almost primitive root"–a number whose order is as big as possible without being a primitive root. In fact, 5 is always such a number. The proof is very similar to the last two proofs we did.

Exercise 6.40. *Let $k \geq 3$ be an integer. Then*

$$\operatorname{ord}_{2^k} 5 = \phi(2^k)/2 = 2^{k-2}.$$

6.4.1 Primitive roots modulo not prime powers

We now have a pretty thorough understanding of when a prime power has a primitive root. What about other composite numbers? *Mostly* they don't have primitive roots.

Lemma 6.41. *If n is a positive integer that is not a prime power or twice a prime power, then n does not have a primitive root.*

Proof. Let $n = p_1^{t_1} \dots p_m^{t_m}$, and suppose r is a primitive root modulo n. Then $(r, n) = 1$ and $\operatorname{ord}_n r = \phi(n)$.

We know that $(r, p^t) = 1$ for any p in the prime factorization of n, and for any $t \in \mathbb{N}$. Thus $r^{p^{t-1}(p-1)} = r^{\phi(p^t)} \equiv 1 \mod p^t$.

Let U be the least common multiple of $\phi(p_i^{t_i})$ i.e.

$$U = \operatorname{lcm}\left(\phi(p_1^{t_1}), \dots, \phi(p_m^{t_m})\right).$$

Then since $\phi(p_i^{t_i}) | U$ we know that $r^U \equiv 1 \mod p_i^{t_i}$ for every i. Thus, by the Chinese Remainder Theorem, $r^U \equiv 1 \mod n$.

Then we must have $\phi(n) = \operatorname{ord}_n r \leq U$. But since ϕ is multiplicative, this must imply that

$$\phi(p_1^{t_i}) \dots \phi(p_m^{t_m}) \leq U = \operatorname{lcm}\left(\phi(p_1^{t_1}), \dots, \phi(p_m^{t_m})\right).$$

But the product of a set of integers is always at least their least common multiple, with equality only when all the numbers are relatively prime. So we must have the $\phi(p_i^{t_i})$ all pairwise relatively prime.

But recall that $\phi(\ell)$ is even unless ℓ is 1 or 2. Thus in order for the $\phi(p_i^{t_i})$ to all be pairwise relatively prime, there can be at most one $p_i^{t_i}$ that is not equal to 2. Thus either $n = p_1^{t_i}$ and is a prime power, or $n = 2p_1^{t_1}$ and is two times a prime power, as desired. □

This lemma limits which numbers can have primitive roots. We've shown that many of the possibilities do in fact have primitive roots: we know that prime powers have primitive roots as long as the prime is not 2. But we haven't checked this case of "twice a prime power," so we do that now.

Lemma 6.42. *If p is an odd prime and t is a positive integer, then $2p^t$ has a primitive root.*

In particular, if r is an odd primitive root modulo p^t then it is also a primitive root modulo $2p^t$. If r is an even primitive root modulo p^t then $r + p^t$ is a primitive root modulo $2p^t$.

Proof. If r is a primitive root modulo p^t, then $\operatorname{ord}_{p^t} r = \phi(p^t) = p^{t-1}(p-1)$. We observe that $\phi(2p^t) = \phi(2)\phi(p^t) = \phi(p^t)$, so $\operatorname{ord}_{p^t} r = \phi(2p^t)$ as well.

If r is odd, then $r \equiv 1 \mod 2$ so $r^{\phi(2p^t)} \equiv 1 \mod 2$. Since $r^{\phi(2p^t)} \equiv 1 \mod p^t$, by the Chinese Remainder Theorem we have $r^{\phi(2p^t)} \equiv 1 \mod 2p^t$. But if $r^n \equiv 1 \mod 2p^t$ then $r^n \equiv 1 \mod p^t$, and we know $\operatorname{ord}_{p^t} r = \phi(2p^t)$ so $n \geq 2p^t$. Thus $\operatorname{ord}_{2p^t} r = \phi(2p^t)$ and thus r is a primitive root modulo $2p^t$.

If r is even, then $r + p^t$ is odd and a primitive root modulo p^t, and by the same argument we see that $r + p^t$ is a primitive root modulo $2p^t$. □

Example 6.43. We showed that 2 is a primitive root modulo 11^k for any $k \in \mathbb{N}$. Since 2 is even, we know that $2 + 11^k$ is a primitive root modulo $2 \cdot 11^k$ for any $k \in \mathbb{N}$.

Combining everything we have shown, we can state the following theorem:

Theorem 6.44. *Let n be a positive integer greater than 1. Then n possesses a primitive root if and only if $n = 2, 4, p^t$, or $2p^t$ for some odd prime p and natural number t.*

6.5 Discrete Logarithms

For further reading on the material in this subsection, consult **Rosen 9.4, Shoup 11.1-11.2**.

Recall from theorem 6.14 that if r is a primitive root modulo m, then $\{r^k : 1 \leq k \leq \phi(m)\}$ is a reduced residue system modulo m. Thus the equation $r^x \equiv a \mod m$ has a solution whenever $(a, m) = 1$, and this solution is unique modulo $\phi(m)$.

Definition 6.45. Let m be a natural number with primitive root r, and let a be a positive integer with $(a, m) = 1$. the unique integer x with $1 \leq x \leq \phi(m)$ and $r^x \equiv a \mod m$ is called the *index* or *discrete logarithm* of a to the base r modulo m, and is denoted $\operatorname{ind}_r a$ or $\log_r a$.

Clearly $r^{\operatorname{ind}_r a} \equiv a \mod m$. Further, by lemma 6.10 we see that $a \equiv b \mod m$ if and only if $\operatorname{ind}_r a \equiv \operatorname{ind}_r b \mod \phi(m)$, indeed if and only if $\operatorname{ind}_r a = \operatorname{ind}_r b$ since the index is always between 1 and $\phi(m)$.

Example 6.46. Earlier we worked out the table

$$3^1 \equiv 3 \mod 7 \qquad 3^2 \equiv 9 \equiv 2 \mod 7$$
$$3^3 \equiv 27 \equiv 6 \mod 7 \qquad 3^4 \equiv 81 \equiv 4 \mod 7$$
$$3^5 \equiv 4 \cdot 3 \equiv 12 \equiv 5 \mod 7 \qquad 3^6 \equiv 5 \cdot 3 \equiv 15 \equiv 1 \mod 7.$$

Thus modulo 7 we have

$$\operatorname{ind}_3 1 = 6 \qquad \operatorname{ind}_3 2 = 2 \qquad \operatorname{ind}_3 3 = 1$$
$$\operatorname{ind}_3 4 = 4 \qquad \operatorname{ind}_3 5 = 5 \qquad \operatorname{ind}_3 6 = 3.$$

If we use a different base we get different indices. For instance, we see that 5 is a primitive root modulo 7, and we have

$$\operatorname{ind}_5 1 = 6 \qquad \operatorname{ind}_5 2 = 4 \qquad \operatorname{ind}_5 3 = 5$$
$$\operatorname{ind}_5 4 = 2 \qquad \operatorname{ind}_5 5 = 1 \qquad \operatorname{ind}_5 6 = 3.$$

We can prove that the "index" operation has most of the properties of logarithms.

Exercise 6.47. *Let m be a natural number with primitive root r, and let a, b be relatively prime to m. Then*

1. $\operatorname{ind}_r 1 \equiv 0 \mod \phi(m)$
2. $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \mod \phi(m)$
3. $\operatorname{ind}_r a^k \equiv k \operatorname{ind}_r a \mod \phi(m)$.

Example 6.48. We know that modulo 7, we have $\operatorname{ind}_5 2 = 4$ and $\operatorname{ind}_5 3 = 5$. We compute that $\operatorname{ind}_5(2 \cdot 3) = \operatorname{ind}_5 2 + \operatorname{ind}_3 = 4 + 5$, and modulo $\phi(7) = 6$ this is indeed equivalent to $\operatorname{ind}_5 6 = 3$.

Example 6.49. We can use this to solve exponential congruences. Suppose we wish to find all solutions of $6x^{12} \equiv 11 \mod 17$. We can compute that 3 is a primitive root modulo 17, and can compute (or look up) a table of indices of integers modulo 17.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Then we have

$$\begin{aligned}
\operatorname{ind}_3(6x^{12}) &\equiv \operatorname{ind}_3(11) \mod \phi(17) \\
\operatorname{ind}_3 6 + \operatorname{ind}_3 x^{12} &\equiv \operatorname{ind}_3 11 \mod 16 \\
\operatorname{ind}_3 6 + 12 \operatorname{ind}_3 x &\equiv \operatorname{ind}_3 11 \mod 16 \\
15 + 12 \operatorname{ind}_3 x &\equiv 7 \mod 16 \\
12 \operatorname{ind}_3 x &\equiv 8 \mod 16 \\
3 \operatorname{ind}_3 x &\equiv 2 \mod 4 \\
\operatorname{ind}_3 x &\equiv 2 \cdot 3 \equiv 2 \mod 4.
\end{aligned}$$

Thus we have $\operatorname{ind}_3 x \in \{2, 6, 10, 14\}$ and thus

$$x \equiv 3^2, 3^6, 3^{10}, 3^{14} \equiv 9, 15, 8, 2 \mod 17.$$

Example 6.50. Find all solutions of $7^x \equiv 6 \mod 17$.

We have

$$\begin{aligned} \operatorname{ind}_3(7^x) &\equiv \operatorname{ind}_3 6 \mod 16 \\ x \cdot \operatorname{ind}_3 7 &\equiv 15 \mod 16 \\ 11x &\equiv 15 \mod 16 \\ x &\equiv 11^{-1} \cdot 15 \equiv 3 \cdot 15 \equiv 13 \mod 16. \end{aligned}$$

Thus $7^x \equiv 6 \mod 17$ if and only if $x \equiv 13 \mod 16$.

Remark 6.51. You might notice that we did a lot of work with the cavalier statement "we can compute a table of indices." In fact, computing indexes or discrete logarithms is quite computationally intensive, and there isn't much of a better way of computing $\operatorname{ind}_3 12$ than just raising 3 to a bunch of powers and seeing which one gives you 12. (Thus if you're computing indices at all you might as well build a table).

The fact that this problem is computationally difficult underlies the security of much cryptography currently in use; it is comparable to the problem of factoring large integers.

Like integer factorization, the discrete logarithm problem can be solved quickly on a quantum computer. We don't currently have useful quantum computers, but researchers are worried that they will be practical in the near-to-medium future, and we are starting to move to "lattice-based" encryption methods that do not depend on the discrete logarithm problem.

7 Quadratic Reciprocity

We are now ready to work towards the major result of this course, Euler's famous law of Quadratic Reciprocity.

7.1 Power residues

For further reading on the material in this subsection, consult **Rosen 9.4, 11.1, PMF 11.1, Stein 4.1, Shoup 2.8**.

Definition 7.1. Let m be a natural number. We say a is a *kth power residue of m* if the congruence $x^k \equiv a \mod n$ has a solution, or in other words if a has a kth root modulo m. Otherwise we say a is a *nonresidue*.

Remark 7.2. Some sources, including Rosen, claim a residue has to be relatively prime to m by definition. This convention makes some theorems more awkward and others less.

Example 7.3. Under our convention, 0 is a kth power residue modulo m for any $k, m \in \mathbb{N}$. Under either convention, 1 is a kth power residue modulo m for any $k, m \in \mathbb{N}$.

Example 7.4. We can find the kth power residues modulo m simply by raising every element to the kth power. For instance, we can compute

$$0^2 \equiv 0 \mod 7 \qquad 1^2 \equiv 1 \mod 7 \qquad 2^2 \equiv 4 \mod 7 \qquad 3^2 \equiv 2 \mod 7$$
$$4^2 \equiv 2 \mod 7 \qquad 5^2 \equiv 4 \mod 7 \qquad 6^2 \equiv 1 \mod 7$$

thus the second-power residues (or quadratic residues) modulo 7 are 0, 1, 2, 4. The nonresidues are 3, 5, 6,

Similarly, we can compute

$$0^3 \equiv 0 \mod 7 \qquad 1^3 \equiv 1 \mod 7 \qquad 2^3 \equiv 1 \mod 7 \qquad 3^3 \equiv 6 \mod 7$$
$$4^3 \equiv 1 \mod 7 \qquad 5^3 \equiv 6 \mod 7 \qquad 6^3 \equiv 6 \mod 7$$

thus the third-power (or cubic) residues modulo 7 are 0, 1, 6, and the nonresidues are 2, 3, 4, 5.

Notice that it's easier to prove that something is a residue than to prove that it isn't: to prove something is a residue, we just need to provide a root, but to prove something is not a residue, we need to compute a power of every possible base.

This is an awful lot of computation, so we'd like to determine the set of residues more easily.

Lemma 7.5. *Let m be a positive integer with a primitive root, and let a be relatively prime to m. Then a is a kth power residue modulo m if and only if $a^{\phi(m)/d} \equiv 1 \mod m$, where $d = (k, \phi(m))$.*

Furthermore, if a is a kth power residue modulo m, then $x^k \equiv a \mod m$ has exactly d incongruent solutions modulo m.

Proof. Let r be a primitive root modulo m. Then $x^k \equiv a \mod m$ if and only if $k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \mod \phi(m)$.

If we set $y = \operatorname{ind}_r x$ then our congruence is $ky \equiv \operatorname{ind}_r a \mod \phi(m)$, and by our results on linear congruences this has a solution if and only if $d | \operatorname{ind}_r a$, and if $d | \operatorname{ind}_r a$ then there are exactly d incongruent solutions.

But $d | \operatorname{ind}_r a$ if and only if $(\operatorname{ind}_r a)\phi(m)/d \equiv 0 \mod \phi(m)$, which by lemma 6.10 holds if and only if

$$a^{\phi(m)/d} \equiv a^{(\operatorname{ind}_r a)\phi(m)/d} \equiv 1 \mod \phi(m).$$

And this proves the lemma. □

Corollary 7.6. *If p is a prime and $p \nmid a$, then a is a kth power residue modulo p if and only if $a^{(p-1)/d} \equiv 1 \mod p$.*

Example 7.7. Is 5 a sixth-power residue modulo 17?

We see that $(6, 16) = 2$, so we compute

$$5^{16/2} = 5^8 \equiv 25^4 \equiv 8^4 \equiv 64^2 \equiv (-4)^2 \equiv -1 \mod 17.$$

We see that $2 \nmid -1$ and thus 5 is not a sixth-power residue modulo 17.

We'd like an even more precise statement, but making that in the most general case is quite difficult. So we will now focus on one particular special case.

7.2 Quadratic Residues

For further reading on the material in this subsection, consult **Rosen 11.1, PMF 11.2, Stein 4.1, Shoup 12.1**.

Definition 7.8. If m is a positive integer, we say a is a *quadratic residue of m* if the congruence $x^2 \equiv a \mod m$ has a solution. You will notice that this is just the definition of a 2nd-power residue again.

We can get an initial result purely from counting. We recall a result from homework 5:

Lemma 7.9. *Suppose p is an odd prime and a is a positive integer with $(a,p)=1$. Then the congruence $x^2 \equiv a \mod p$ either has no solution, or has exactly two solutions moduo p.*

Using this we can prove:

Lemma 7.10. *If p is an odd prime, then there are exactly $(p+1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues modulo p in the set $\{0,\dots,p-1\}$.*

Proof. First notice that 0 is always a quadratic residue modulo p. So we need to prove that of the $p-1$ integers relatively prime to p, then $(p-1)/2$ of them are residues and $(p-1)/2$ are not.

But each congruence $x^2 \equiv a \mod p$ has either two solutions or zero solutions, and the total set of solutions has size $p-1$, since every number has exactly one square and thus solves exactly one of these congruences.

So it must be the case that $(p-1)/2$ of these congruences have 2 solutions each, and the other $(p-1)/2$ of them have no solutions, proving our lemma. □

We can also use indices and the results of subsection 7.1 to make statements about quadratic residues.

Lemma 7.11. *Let p be a prime and let r be a primitive root of p. If $p \nmid a$, then a is a quadratic residue of p if and only if $\operatorname{ind}_r a$ is even.*

Proof. Suppose $\operatorname{ind}_r a$ is even. Then

$$(r^{\operatorname{ind}_r a/2})^2 = r^{\operatorname{ind}_r a} \equiv a \mod p$$

and thus a is a square and thus a quadratic residue modulo p.

Now suppose a is a quadratic residue modulo p. Then there is an integer x such that $x^2 \equiv a \mod p$. Taking indices to the base r for some primitive root r, we have

$$\begin{aligned} \operatorname{ind}_r x^2 &\equiv \operatorname{ind}_r a \mod \phi(p) \\ 2\operatorname{ind}_r x &\equiv \operatorname{ind}_r a \mod p-1 \end{aligned}$$

and since $2\operatorname{ind}_r x$ and $p-1$ are both even, so is $\operatorname{ind}_r a$. □

Corollary 7.12. *If r is a primitive root modulo an odd prime p. Then r is a quadratic nonresidue modulo p.*

Proof. We know that $\operatorname{ind}_r r = 1$ is not even. □

7.3 Quadratic residues modulo primes

For further reading on the material in this subsection, consult **Rosen 11.1, PMF 11.2, Stein 4.2, Shoup 12.1**.

Since we'll be discussing this a great deal more, it will be useful to introduce some notation for it. We want to attack this question exactly like we attack all our other number theoretic questions: we solve it for primes, then generalize.

Since we'll be talking about this a lot, we introduce some new notation.

Definition 7.13. Let p be an odd prime, and a an integer. Then we define the *Legendre symbol* by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a nonzero quadratic residue modulo } p \\ -1 & a \text{ is a quadratic nonresidue modulo } p \\ 0 & a \equiv 0 \mod p \end{cases}$$

The symbol is named after Legendre, who repeatedly attempted to prove Euler's conjectured reciprocity law, until it was finally proven by Gauss.

Theorem 7.14 (Euler's Criterion)**.** *Let p be an odd prime and a an integer. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

Proof. If $(a,p) \neq 1$ then $p|a$, so both sides are equivalent to 0 modulo p. So we can assume $(a,p) = 1$.

Suppose $\left(\frac{a}{p}\right) = 1$. Then there is some x such that $x^2 \equiv a \mod p$. Then we compute that

$$a^{(p-1)/2} = x^{(p-1)} \equiv 1 \mod p$$

by Euler's theorem.

Now suppose $\left(\frac{a}{p}\right) = -1$. Then the congruence $x^2 \equiv a \mod p$ has no solutions. Now consider the numbers $1, \dots, p-1$. We know that for each $1 \leq i \leq p-1$ there is a unique $1 \leq j \leq p-1$ such that $ij \equiv a \mod p$; and since a is a quadratic nonresidue, each pairing is distinct. (That is, we never have $i^2 \equiv a \mod p$).

Thus the product of all the numbers from 1 to $p-1$ is equivalent to $a^{(p-1)/2}$ modulo p. Thus we have

$$a^{(p-1)/2} \equiv (p-1)! \equiv -1 \mod p$$

by Wilson's theorem. □

Example 7.15. Let $p = 23$ and $a = 5$. We can compute that $5^{11} \equiv -1 \mod 23$, so by Euler's criterion we have $\left(\frac{5}{23}\right) = -1$ and thus 5 is a quadratic residue modulo 23.

Proposition 7.16. *Let p be an odd prime and let a, b be integers. then*

1. *If $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.*
3. *$\left(\frac{a^2}{p}\right) = 1$ if $p \nmid a$.*

Proof. 1.

2. By Euler's criterion, we have

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p \qquad \left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \mod p$$

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \mod p \\ &\equiv a^{(p-1)/2} b^{(p-1)/2} \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p.\end{aligned}$$

   Since the two values are equivalent modulo p and both must be ± 1 we conclude they are equal.

3.

□

Remark 7.17. This tells us that the product of two quadratic residues is a quadratic residue, which is obvious. It tells us that the product of a residue and a non-residue is not a residue, which seems reasonable. And it tells us the product of two non-residues is a residue.

We now want to figure out when any number is a quadratic residue modulo a prime. We start, as usual, with studying the primes, but we need to also check one other case.

Lemma 7.18. *If p is an odd prime then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv -1 \mod 4. \end{cases}$$

Proof. By Euler's criterion we know that

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \mod p.$$

If $p \equiv 1 \mod 4$ then $(p-1)/2$ is even and thus $(-1)^{(p-1)/2} = 1$. But if $p \equiv 3 \mod 4$ then $(p-1)/2 = 2k+1$ is odd, and thus $(-1)^{(p-1)/2} = -1$. □

In order to sort out the other primes, we need one more major tool. It is awkward to state, so we almost never want to use it directly; but it is quite useful in proofs.

Lemma 7.19 (Gauss's lemma)**.** *Let p be an odd prime and let a be an integer with $(a,p) = 1$. If s is the number of least positive residues of the integers $a, 2a, \dots, a(p-1)/2$ that are greater than $p/2$, then $\left(\frac{a}{p}\right) = (-1)^s$.*

Proof. Consider the list of integers $a, 2a, \dots, a(p-1)/2$. Relabel them so that $u_1, \dots, u_s$ are the elements of the list greater than $p/2$, and $v_1, \dots, v_t$ are the elements less than $p/2$. (No element can be equal to $p/2$ since it is not an integer).

First we claim that the set $\{p-u_1, \dots, p-u_s, v_1, \dots, v_t\}$ is equal to the set $\{1, 2, \dots, (p-1)/2\}$. We just need to show that none of the integers are congruent, since it is a list of $(p-1)/2$ elements between 1 and $(p-1)/2$.

So we can check that $u_i \not\equiv u_j$ and $v_i \not\equiv v_j$ if $i \neq j$, since otherwise we'd have $ma \equiv na \mod p$ and thus $m \equiv n \mod p$ and thus $m = n$.

So suppose $p - u_i \equiv v_j \mod p$. Then $ma \equiv p - na \mod p$, so $ma \equiv -na \mod p$ and $m = -n \mod p$. But this can't happen since m and n are both between 1 and $(p-1)/2$. So we have proven that our set is the set of integers from 1 to $(p-1)/2$.

So now consider the product of the whoel set. We have

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &\equiv (p-u_1)(p-u_2)\dots(p-u_s)v_1v_2\dots v_t \\
&\equiv (-1)^s u_1u_2\dots u_sv_1v_2\dots v_t \\
&\equiv (-1)^s a(2a)(3a)\dots(a(p-1)/2) \\
&\equiv (-1)^s a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \mod p
\end{aligned}$$

and by cancellation, we have

$$\begin{aligned}
1 &\equiv (-1)^s a^{(p-1)/2} \mod p \\
(-1)^s \equiv a^{(p-1)/2} &\equiv \left(\frac{a}{p}\right) \mod p
\end{aligned}$$

by Euler's criterion. □

We can now use Gauss's lemma to figure out what happens in some additional cases.

Lemma 7.20. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Remark 7.21. We can rephrase this to say that 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 8$.

Proof. By Gauss's lemma 7.19, we just need to determine the number of least positive residues in the set $\{1 \cdot 2, 2 \cdot 2, \dots, 2(p-1)/2\}$ which are greater than $p/2$. But since all of these numbers are between 1 and p, we just need to check the number of set elements that are bigger than $p/2$.

If $1 \leq j \leq (p-1)/2$, then $2j < p/2$ if and only if $j \leq p/4$. Thus the number of integers less than $p/2$ is $\lfloor p/4 \rfloor$, and so we have

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/2 - \lfloor p/4 \rfloor}.$$

So we just want to show that if p is an odd integer, then

$$\frac{p-1}{2} - \lfloor p/4 \rfloor \equiv \frac{p^2-1}{8} \mod 2.$$

We claim that this formula holds for an odd integer n if and only if it holds for $n+8$. For

$$\begin{aligned}\frac{p+8-1}{2} - \lfloor (p+8)/4 \rfloor &= \frac{p-1}{2} + 4 - \lfloor p/4 + 2 \rfloor = \frac{p-1}{2} - \lfloor p/4 \rfloor + 2 \\ &\equiv \frac{p-1}{2} - \lfloor p/4 \rfloor \mod 2 \\ \frac{(p+8)^2-1}{8} &= \frac{p^2-1}{8} + 2p + 8 \equiv \frac{p^2-1}{8} \mod 2.\end{aligned}$$

Thus by induction we only need to check the formula for $p = \pm 1$ and $p = \pm 3$. Checking these by hand, we see the theorem is proved. □

7.4 The Law of Quadratic Reciprocity

For further reading on the material in this subsection, consult **Rosen 11.2, PMF 11.3-4, Stein 4.1,4.3 Shoup 12.1**.

We've figured out when -1 is a quadratic residue, and when 2 is a quadratic residue. Now we want to look at the other prime numbers.

Unfortunately there is not a good formula for telling whether one odd prime is a quadratic residue modulo another. However, we have a very powerful result which is almost as good, known as the Law of Quadratic Reciprocity. A reciprocity law is a law like this that does *not* give a formula, but does relate two unknown things in a way that often gives us information about them.

Theorem 7.22 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

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

We can use this law, combined with the properties of the Legendre symbol, to compute whther most numbers are quadratic residues.

Example 7.23. Let $p = 13$ and $q = 17$. By quadratic reciprocity, we know that

$$\left(\frac{13}{17}\right)\left(\frac{17}{13}\right) = (-1)^{12/2\cdot 16/2} = 1$$

and thus $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$. But we know that

$$\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = 1.$$

Thus we know that $\left(\frac{13}{17}\right) = 1$ and thus 13 is a quadratic residue modulo 17.

Example 7.24. Suppose we want to determine if 7 is a quadratic residue modulo 19. Then quadratic reciprocity tells us that

$$\left(\frac{7}{19}\right)\left(\frac{19}{7}\right) = (-1)^{6/2\cdot 18/2} = (-1)^{27} = -1.$$

Thus

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right).$$

We could check this by hand, but we can also see that

$$\left(\frac{5}{7}\right)\left(\frac{7}{5}\right) = (-1)^{6/2\cdot 4/2} = 1$$

so

$$-\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = -(-1)^{(5^2-1)/8} = -(-1)^3 = 1.$$

Thus 7 is a quadratic residue modulo 19.

If we want to determine whether a composite number is a quadratic residue modulo a prime, we can factor it into primes and use the complete multiplicativity of the Legendre symbol.

Example 7.25. Is 15 a quadratic residue modulo 31?

We compute that $\left(\frac{15}{31}\right) = \left(\frac{5}{31}\right)\left(\frac{3}{31}\right)$. Then quadratic reciprocity tells us that

$$\begin{aligned}\left(\frac{5}{31}\right)\left(\frac{31}{5}\right) &= (-1)^{4/2\cdot 30/2} = 1\\ \left(\frac{5}{31}\right) &= \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1\\ \left(\frac{3}{31}\right)\left(\frac{31}{3}\right) &= (-1)^{2/2\cdot 30/2} = -1\\ \left(\frac{3}{31}\right) &= -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1.\end{aligned}$$

Thus we see that

$$\left(\frac{15}{31}\right) = 1\cdot(-1) = -1$$

so 15 is not a quadratic residue modulo 31.

Now we should prove the law of quadratic reciprocity, which will take a bit of work.

Lemma 7.26 (Eisenstein)**.** *If p is an odd prime and a is an odd integer with $p \nmid a$, then*

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$$

where

$$T(a,p) = \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor .$$

Proof. We reduce this to Gauss's lemma 7.19. As before, consider the set $a, 2a, \ldots, a(p-1)/2$, and let $u_1, \ldots, u_s$ be the elements whose least positive residues are greater than $p/2$, and $v_1, \ldots, v_t$ be those whose least positive residues are less than $p/2$. We know by Gauss's lemma that

$$\left(\frac{a}{p}\right) = (-1)^s$$

so we just need to prove that $s \equiv T(a,p) \mod 2$.

For each ja, we can use the division algorithm to divide by $\lfloor ja/p \rfloor$ to get

$$ja = p\lfloor ja + p \rfloor + r_j$$

where the remainder is one of the u_i or v_i (since it is the least positive residue of ja). If we add these equations together for each $1 \leq j \leq (p-1)/2$, we get

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\lfloor ja/p \rfloor + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j.$$

But as before we have that the integers from 1 to $(p-1)/2$ are the integers $p-u_i, v_j$ in some order, so

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t} v_t = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j.$$

Subtracting the second equation from the first gives

$$\begin{aligned}
\sum_{j=1}^{(p-1)/2} j(a-1) &= \sum_{j=1}^{(p-1)/2} p\lfloor ja/p \rfloor - ps + 2\sum_{j=1}^{s} u_j \\
&= T(a,p) - ps + 2\sum_{j=1}^{s} u_j \\
(a-1)\sum_{j=1}^{(p-1)/2} j &= T(a,p) - ps + 2\sum_{j=1}^{s} u_j \\
0 &\equiv T(a,p) - s \mod 2.
\end{aligned}$$

□

Proof of Quadratic Reciprocity. Let p and q be odd primes. Let S be the set of pairs of integers $\{(x,y) : 1 \leq x \leq (p-1)/2, 1 \leq y \leq (q-1)/2\}$. Notice that S has $(p-1)(q-1)/4$ elements, and that we can draw it as the "lattice points" or integer-valued points in a $(p-1)/2 \times (q-1)/2$ rectangle in the real plane.

We draw a diagonal line $x = (p/q)y$ or $qx = py$ *almost* through the corners of this rectangle, and we count the points above and below it. We first note that no point is on this line, since if $qx = py$ then $q|py$ and thus either $q|p$ (which is not true since both are prime), or $q|y$, which is not true since $1 \leq y \leq (q-1)/2$. So every point is above or below the line.

A point $(x,y) \in S$ is below the line if and only if $py < qx$, if and only if $1 \leq y \leq qx/p$. For a fixed x, the number of points we get this way is $\lfloor qx/p \rfloor$, thus the total number of points below the line is $\sum_{x=1}^{(p-1)/2} \lfloor qj/p \rfloor$. Notice this is exactly $T(q,p)$ from lemma 7.26.

Similarly, the number of points *above* the line is $\sum_{y=1}^{(p-1)/2} \lfloor pj/q \rfloor = T(p,q)$. In particular, the sum of these sums is $(p-1)(q-1)/4$ because every point is counted exactly once, and

thus we have

$$T(q,p) + T(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2}$$
$$(-1)^{T(q,p)}(-1)^{T(p,q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

But from lemma 7.26 we know that $(-1)^{T(q,p)} = \left(\frac{q}{p}\right)$ and $(-1)^{T(p,q)} = \left(\frac{p}{q}\right)$, which completes our proof. □

7.5 Bonus Material: the Jacobi Symbol

For further reading on the material in this subsection, consult **Rosen 11.3, PMF 11.6, Stein 4.3, Shoup 12.2-3**.

So far we've only dealt with determining quadratic residues modulo a prime. We'd like to be able to answer this question about composites as well.

Definition 7.27. Let $n = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ be an odd positive integer. We define the *Jacobi symbol* by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1} \dots \left(\frac{a}{p_k}\right)^{t_k}.$$

If $(a,n) = 1$ then $\left(\frac{a}{n}\right) = \pm 1$. If $(a,n) \neq 1$ then $\left(\frac{a}{n}\right) = 0$. When n is prime then this is just the Legendre symbol.

We can see that if $\left(\frac{a}{n}\right) \neq 1$ then a is not a quadratic residue modulo n. For if a is a residue modulo n it must be a residue modulo p_i for each i, since its square root modulo n will also be a square root modulo p_i.

Unfortunately, the converse is not true; if $\left(\frac{a}{n}\right) = 1$ that does not imply that a is a quadratic residue modulo n. For instance, if $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$ then $\left(\frac{a}{pq}\right) = 1$ but a is not a quadratic residue modulo pq.

We can carry over or reprove many results from our section on primes.

Proposition 7.28 (Facts about the Jacobi Symbol)**.** *Let n be an odd positive integer, and a, b integers. Then*

1. *If $a \equiv b \mod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.*
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
3. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
4. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

Theorem 7.29 (Quadratic Reciprocity for the Jacobi Symbol)**.** *If n and m are relatively prime odd integers greater than 1, then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Our Jacobi symbol computations do make it easier for us to compute Legendre symbols, however. The one difficulty we had using quadratic reciprocity earlier was that to compute $\left(\frac{a}{p}\right)$ when a was composite, we had to factor it into primes–which is in general difficult. But now we can use the same algorithm without ever having to factor.

Example 7.30. Let us determine whether 93 is a quadratic residue modulo 179. Since 179 is prime, we just need to compute $\left(\frac{93}{179}\right)$. By quadratic reciprocity we have

$$\begin{aligned}
\left(\frac{93}{179}\right)\left(\frac{179}{93}\right) &= (-1)^{92/2\cdot 178/2} = 1\\
\left(\frac{93}{179}\right) = \left(\frac{179}{93}\right) &= \left(\frac{-7}{93}\right) = \left(\frac{7}{93}\right)\left(\frac{-1}{93}\right)\\
\left(\frac{-1}{93}\right) &= (-1)^{(93-1)/2} = (-1)^{46} = 1\\
\left(\frac{7}{93}\right)\left(\frac{93}{7}\right) &= (-1)^{6/2\cdot 92/2} = 1\\
\left(\frac{7}{93}\right) = \left(\frac{93}{7}\right) &= \left(\frac{2}{7}\right) = (-1)^{(7^2-1)/8} = (-1)^6 = 1
\end{aligned}$$

and thus $\left(\frac{93}{179}\right) = 1 \cdot 1 = 1$.