Math 180A - Notes

Neil Donaldson

Winter 2022

1 Introduction

In this section[1] we motivate the study of number theory via some classic problems, and investigate the familiar Pythagorean triples.

While modern number theory has many applications and invokes a wide array of techniques from across mathematics, at its heart it is concerned with the *integers* and with integer solutions to equations: these are called *Diophantine Equations* in honor of Diophantus of Alexandria, a Greek Mathematician of the 3rd century CE, and one of the fathers of number theory. Here are some classic problems and examples; some at least should be familiar to you.

1. Find all the integer points (x, y) on the line $3x - 2y = 1$. The answer is $(x, y) = (1 + 2n, 1 + 3n)$ where $n \in \mathbb{Z}$. Can you *prove* right now that these are *all* the solutions?
2. If n is an odd integer then $n^2 - 1$ is a multiple of 8.
3. Find all *Pythagorean triples*: positive integers x, y, z such that $x^2 + y^2 = z^2$.
4. Prime numbers: if n is prime, what is the next prime? Is there a formula for the nth prime? Is $n^2 + n + 41$ always prime whenever n is an integer?
5. Which integers can be written as the sums of two squares? Three? Four?
6. Fermat's Last Theorem:[2] if $n \geq 3$ is an integer, then there are no positive integers x, y, z such that $x^n + y^n = z^n$.

1.1 Notation & Divisibility

To orient ourselves, we start by standardizing notation for our sets of interest.

Natural Numbers: $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$

Whole Numbers: $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$

Integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Rational Numbers: $\mathbb{Q} = \{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}\}$

The real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ will not play much role in this class.

[1] Corresponds roughly to § 1–3 in the textbook: *A Friendly Introduction to Number Theory*, Joseph H. Silverman, 4th ed.

[2] Historical note: In 1637 Pierre de Fermat left a note in the margin of a copy of Diophantus' *Arithmetica* famously claiming to have proved his 'theorem.' A complete proof took mathematicians another three and a half centuries…

Divisibility in the integers

After years of calculus, restricting oneself to the integers can feel alien. The fundamental difficulty is that division is often impossible: e.g. $7 \div 4 = \frac{7}{4}$ is not an integer! In algebraic language the integers fail to be closed under division and form merely a *ring*, not a *field* like the rational or real numbers. Our first order of business is to identify those pairs of integers for which division is permitted.

Definition 1.1. Let $m, n \in \mathbb{Z}$. We say that m *divides* n, and write $m \,|\, n$, if

$$\exists k \in \mathbb{Z} \text{ such that } n = km$$

We also say that m is a *divisor* or *factor* of n.

A *common divisor/factor* of two integers x, y is any (positive) integer d such that $d \,|\, x$ and $d \,|\, y$. We say that x, y are *relatively prime* or *coprime*[a] if the only positive common factor is 1.

[a] Colloquially, "x, y have no common factors."

Examples 1.2. 1. By taking $k = 3$ in the definition, we see that $4 \,|\, 12$ (that is $12 = 3 \cdot 4$).

2. By contrast, $7 \nmid 9$ since $\nexists k \in \mathbb{Z}$ such that $9 = 7k$.
3. For *every* $m \in \mathbb{Z}$ we have $m \,|\, 0$, since $0 = 0m$ (i.e. $k = 0$ works in the definition!). This includes the counterintuitive fact that $0 \,|\, 0$.
4. The common divisors of $x = 18$ and $y = 12$ are 1, 2, 3 and 6.
5. -16 and 27 are relatively prime.

A few observations and tips are in order concerning the definition.

- For brevity, the word *positive* is usually omitted when discussing (common) divisors. For instance, in Example 4 above, -2 plainly divides both 18 and 12.
- It would be tempting to say that m divides n if and only if $\frac{n}{m}$ is an integer but this is incorrect:
  - Certainly $\frac{n}{m} \in \mathbb{Z} \implies m \,|\, n$ is true (take $k = \frac{n}{m}$).
  - The converse is *false*; $0 \,|\, 0$ is the sole counter-example.

  More philosophically, since divisibility is solely a property of the integers, it is cleaner not to introduce rational numbers into the discussion.
- Keep the line vertical! $m \,|\, n$ is a *proposition* (a statement which is either true or false), whereas $m/n = \frac{m}{n}$ is (usually) a rational *number.* Some version of the following is a very common mistake:

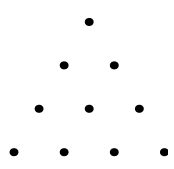
  $$m \,|\, n \nleftrightarrow m/n \nleftrightarrow \frac{m}{n} \in \mathbb{Z}$$

  Not only are we confusing propositions with numbers, but in the context of the previous observation, the resulting fraction is upside-down!

Exercises 1.1 The exercises in this chapter are to be treated informally. Rigorous arguments might require some facts about integers with which you're only somewhat familiar (e.g. prime factorization) but that we'll develop properly in future chapters. The point is to investigate and to *play.*

1. An integer is *triangular* if it is the sum of the first n natural numbers. For example:

   $1 = 1$
   $3 = 1 + 2$
   $6 = 1 + 2 + 3$
   $10 = 1 + 2 + 3 + 4$

   (a) Prove that a number is triangular if and only if it may be written in the form $\frac{1}{2}n(n+1)$ where n is a natural number.

   (b) A number is *square-triangular* if it is both square ($= m^2$) and triangular. Certainly 1 is square-triangular. Find the next square-triangular number.

   (c) Finding all square-triangular numbers m^2 is equivalent to finding all integer solutions (m, n) to the equation

   $$m^2 = \frac{1}{2}n(n+1)$$

   Prove that this is equivalent to finding integers (m, k) such that

   $$m^2 = k(2k+1) \quad \text{or} \quad m^2 = k(2k-1)$$

   (*Hint: n is either even or odd...*)

   (d) Suppose that $d \in \mathbb{N}$ is a divisor/factor of *both* k and $2k+1$. Explain why $d = 1$.

   (e) By part (d), if (m, k) solves $m^2 = k(2k+1)$, then *both* k and $2k+1$ are *perfect squares.* Prove that finding square-triangular numbers is equivalent to finding all integer solutions (x, y) to the equations[a]

   $$x^2 - 2y^2 = \pm 1$$

   (f) Find the first few pairs of solutions (x, y) to these equations and therefore find the first *five* square-triangular numbers.
   (*Hint: This is easier with a spreadsheet or by writing some computer code. Try evaluating $\sqrt{2y^2 \pm 1}$ for $y = 1, 2, 3, 4, \ldots$ and spotting when this is an integer.*)

2. Try summing the first few odd numbers and see if the results satisfy some pattern. Once you find the pattern, express it algebraically. Can you find a *geometric* verification that your formula is correct?
   (*Hint: How can you create a square with $n+1$ dots per side from a square with n dots per side?*)

3. The consecutive odd numbers 3, 5, and 7 are all primes. Are there infinitely many such *prime triplets*? That is, are there infinitely many prime numbers p such that $p+2$ and $p+4$ are also prime?

[a] The equation $x^2 - 2y^2 = 1$ is an example of *Pell's equation,* the solutions of which are related to fun things such as *continued fractions* and rational approximations to $\sqrt{2}$. For example $(99, 70)$ is a solution and $\frac{99}{70} = 1.4142857\ldots \approx \sqrt{2}$.

1.2 Pythagorean Triples

We consider positive integers x, y, z for which $x^2 + y^2 = z^2$. It is easy to find many:

1. Take a known triple, e.g. $(3, 4, 5)$, and multiply by a constant. Thus $(3n)^2 + (4n)^2 = (5n)^2$ for any $n \in \mathbb{N}$. We immediately have infinitely many triples.

2. Use a spreadsheet or computer program: generate pairs (x, y) of integers, take the square-root of $x^2 + y^2$, and test whether this is an integer. The following snippets (loosely C++/Python) do exactly this[3] returning all Pythagorean triples with $x, y \leq 100$.

```
for(int x=1; x<=100; ++x)
    {for(int y=x; y<=100; ++y)
        {real z=sqrt(x^2+y^2);
            if(z-floor(z)==0){write(x,y,z);}
        }
    }
```

```
for x in range (1,101):
    for y in range (x,101):
        z=sqrt(x^2+y^2);
        if z-floor(z)==0:
            print(x,y,z);
```

We need a different approach if we want to describe *all* triples. First we reduce the problem a little.

Definition 1.3. A Pythagorean triple (x, y, z) is *primitive* if no pair of x, y, z has a common factor.

For instance $(3, 4, 5)$ is primitive, while $(6, 8, 10)$ is not. We now state some basic results that help narrow our search:

Lemma 1.4. *Suppose that (x, y, z) is a Pythagorean triple.*

1. *If any pair of x, y, z have a common factor, the third shares this factor.*
2. *All non-primitive triples are a common multiple of a primitive triple.*
3. *If (x, y, z) is primitive, then z is odd.*

Proof. 1. Suppose WLOG that d is a common divisor of x, y. Then $d^2 \,|\, z^2$ and so[4] that $d \,|\, z$.

2. If (x, y, z) is non-primitive, then some pair has a common divisor, which divides all three by part 1. Divide x, y, z by their *greatest common factor* d to obtain the primitive triple $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$.

3. If (x, y, z) is primitive, then at most one of x, y, z can be even. Moreover, they cannot all be odd, since odd + odd $\neq$ odd.

   If $z = 2m$ were even, then $x = 2k + 1$ and $y = 2l + 1$ are both odd. But then

   $$4m^2 = z^2 = x^2 + y^2 = (2k + 1)^2 + (2l + 1)^2 = 4(k^2 + l^2 + k + l) + 2.$$

   The right hand side is not divisible by 4, so we have a contradiction. ∎

[3] This is inefficient but is fine for an initial investigation. If you want to play with it, try entering the C version into the Asymptote Web Application, or the Python into a Sage Cell. A more efficient algorithm might be based on Theorem 1.5.

[4] That $d^2 \,|\, z^2 \implies d \,|\, z$ is not as obvious as it may seem: it requires unique prime factorization (later).

To summarize the Lemma, it is enough for us to find all primitive Pythagorean triples (x, y, z) where x, z are odd and y is even. In such a situation, we start by factorizing:

$$x^2 = z^2 - y^2 = (z + y)(z - y)$$

Suppose that $z + y$ and $z - y$ had a common factor d: plainly d is odd, since both $z \pm y$ are odd. Then $\exists a, b \in \mathbb{Z}$ for which

$$\begin{cases} z + y = ad \\ z - y = bd \end{cases} \implies \begin{cases} 2z = (a + b)d \\ 2y = (a - b)d \end{cases}$$

Since d is odd, it must be a common divisor of both y and z: since (x, y, z) is primitive, $d = 1$.
It now follows[5] that $z + y$ and $z - y$ are both *perfect squares*: write

$$z + y = s^2, \qquad z - y = t^2$$

and solve for y, z and $x = st$. Again, s, t are relatively prime for otherwise y, z would have a common factor. They must also plainly both be odd. Finally, it is worth checking that the expressions we've found really do provide a triple:

$$(st)^2 + \left(\frac{s^2 - t^2}{2}\right)^2 = s^2t^2 + \frac{s^4 + t^4 - 2s^2t^2}{4} = \frac{s^4 + t^4 + 2s^2t^2}{4} = \left(\frac{s^2 + t^2}{2}\right)^2$$

We have therefore proved the main classification result.

Theorem 1.5. *(x, y, z) is a primitive triple with x odd and y even if and only if then there exist odd coprime integers $s > t \geq 1$ such that*

$$x = st, \qquad y = \frac{s^2 - t^2}{2}, \qquad z = \frac{s^2 + t^2}{2}$$

All Pythagorean triples are simply multiples of these or result from switching the order of x, y.

Examples 1.6. 1. Take $s = 9, t = 5$ to obtain the primitive triple $(45, 28, 53)$.

2. The non-primitive triple $(160, 168, 232)$ has common divisor $d = 8$ and is therefore 8 times the primitive triple $(20, 21, 29)$. This has x even and so we compute

   $$s = \sqrt{z + x} = \sqrt{49} = 7, \quad t = \sqrt{z - x} = \sqrt{9} = 3$$

   Putting it together, we obtain the representation

   $$(160, 168, 232) = 8\left(\frac{s^2 - t^2}{2}, st, \frac{s^2 + t^2}{2}\right) = 8\left(\frac{7^2 - 3^2}{2}, 7 \cdot 3, \frac{7^2 + 3^2}{2}\right)$$

Other descriptions of the Pythagorean triples are available: see e.g. Exercise 2.

[5] This again requires unique factorization. If p is a prime factor of x, then $p^2 \mid x^2$. Both factors of p must divide either $z + y$ or $z - y$, since these are coprime. Now repeat with all primes dividing x...

Exercises 1.2 1. (a) We showed that for any primitive Pythagorean triple (x, y, z), either x or y must be even. Use a similar argument to prove that either x or y must be a multiple of 3.

(*Hint: what remainders can squares have after dividing by three?*)

(b) By examining a list of primitive Pythagorean triples, make a guess about when x, y or z is a multiple of 5. Try to show that your guess is correct.

2. Try this alternative approach to finding all primitive Pythagorean triples (x, y, z) where y is even. Let $\hat{y} = \frac{1}{2}y$. Then

$$\hat{y}^2 = \frac{1}{4}y^2 = \frac{1}{4}(z^2 - x^2) = \frac{z-x}{2} \cdot \frac{z+x}{2}$$

The right side is the product of two coprime integers, which must therefore both be perfect squares. Define positive integers u, v by

$$u^2 = \frac{1}{2}(z+x), \qquad v^2 = \frac{1}{2}(z-x)$$

(a) Explain why $\frac{z-x}{2}$ and $\frac{z+x}{2}$ are coprime integers.

(b) Find x, y and z in terms of u and v.

(c) Argue that u and v have no common factor and that precisely one must be even.

(d) Compare with the solution in Theorem 1.5: how do s and t relate to u and v?

3. Let $m \geq 2$ be an integer and write the sum $\frac{1}{m-1} + \frac{1}{m+1}$ as a fraction in lowest terms. For example $\frac{1}{1} + \frac{1}{3} = \frac{4}{3}$, $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$, and $\frac{1}{3} + \frac{1}{5} = \frac{8}{15}$.

(a) Compute the next three examples.

(b) Examine the numerators and denominators of the fractions in (a) and compare them with a table of primitive Pythagorean triples. Formulate a conjecture about such fractions.

(c) Prove that your conjecture is correct.
(*Hint: $m - 1$ and $m + 1$ differ by 2...*)

1.3 Pythagorean Triples and the Unit Circle

The previous discussion of Pythagorean triples was algebraic. Now we introduce a little geometry. If (x, y, z) is a (primitive) Pythagorean triple, observe that

$$x^2 + y^2 = z^2 \implies \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

whence $(\frac{x}{z}, \frac{y}{z})$ is a *rational point* (point with rational co-ordinates) on the unit circle.
Conversely, suppose that α and β are positive rational numbers such that $\alpha^2 + \beta^2 = 1$. Write α, β in lowest terms over the smallest common denominator: i.e.

$$(\alpha, \beta) = \left(\frac{x}{z}, \frac{y}{z}\right)$$

where z is the smallest positive integer for which this is possible. Now observe that

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1 \implies x^2 + y^2 = z^2$$

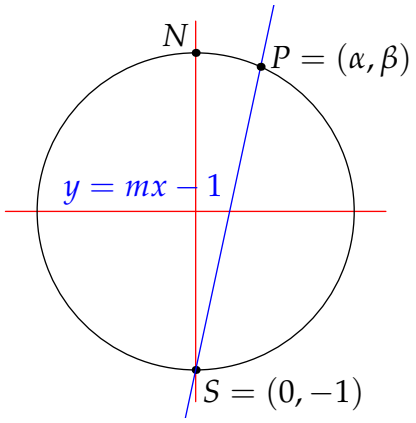
so that (x, y, z) is a Pythagorean triple! More is true, if (x, y, z) were non-primitive, then all three would be divisible by some $d \geq 2$ thus contradicting the minimality of z. To summarize:

Theorem 1.7. 1. *If (x, y, z) is a primitive Pythagorean triple, then $(\frac{x}{z}, \frac{y}{z})$ is a rational point in the first quadrant of the unit circle.*

2. *If (α, β) is a rational point in the first quadrant of the unit circle with α, β in lowest terms, then $\alpha = \frac{x}{z}$ and $\beta = \frac{y}{z}$ where (x, y, z) is a primitive Pythagorean triple.*

We could now use Theorem 1.5, to obtain an expression for the rational points on the circle. Instead, we start with the circle and work geometrically…
Suppose $P = (\alpha, \beta)$ is a point on the unit circle with rational co-ordinates. Provided $\alpha \neq 0$, the line joining P to the south pole $S = (0, -1)$ has *rational gradient*

$$y = mx - 1 \text{ where } m = \frac{\beta + 1}{\alpha} \in \mathbb{Q}$$



By substituting $y = mx - 1$ into the equation for the circle, $x^2 + y^2 = 1$ we obtain a relationship between P and m:

$$\begin{aligned} x^2 + m^2x^2 - 2mx + 1 = 1 &\implies x[(m^2 + 1)x - 2m] = 0 \\ &\implies x = 0, \frac{2m}{m^2 + 1} \end{aligned}$$

Plainly $x = 0$ corresponds to $S = (0, -1)$, while the other solution yields the second intersection P:

$$y = mx - 1 = \frac{2m^2}{m^2 + 1} - 1 \rightsquigarrow P = (\alpha, \beta) = \left(\frac{2m}{m^2 + 1}, \frac{m^2 - 1}{m^2 + 1}\right)$$

The correspondence is in fact tighter: if $m = 0$, we recover $S = (0, -1)$, while[6] $m = \infty$ results in the north pole $N = (0, 1)$. We have therefore proved:

[6] Take limits $\lim_{m \to \infty} (x, y) = (0, 1)$.

Theorem 1.8. *The extended rational numbers $\mathbb{Q} \cup \{\infty\}$ are in bijective correspondence with the rational points (α, β) on the unit circle:*

$$m \mapsto (\alpha, \beta) = \left(\frac{2m}{m^2+1}, \frac{m^2-1}{m^2+1} \right)$$

where m is the gradient of the line joining the south pole $(0,-1)$ with (α, β).

Example 1.9. The above picture shows the line with gradient $m = \frac{14}{3}$, which generates the point $P = \left(\frac{\frac{28}{3}}{\frac{196}{9}+1}, \frac{\frac{196}{9}-1}{\frac{196}{9}+1} \right) = (\frac{84}{205}, \frac{187}{205})$. Note that $(84, 187, 205)$ is a primitive Pythagorean triple.

This method may also be applied to other quadratic curves.

Corollary 1.10. *Suppose $\mathcal{C}$ is a quadratic curve in the plane whose equation has rational coefficients*

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \quad \text{where} \quad a, b, c, d, e, f \in \mathbb{Q}$$

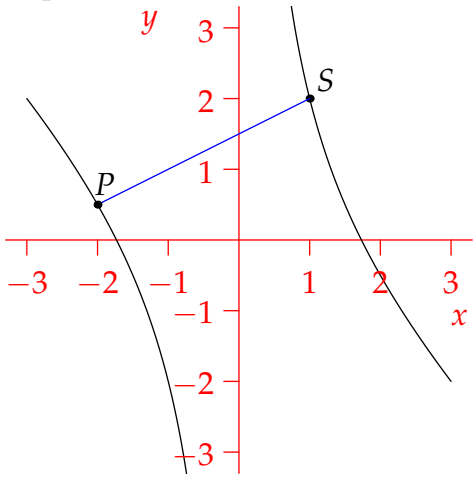
and on which lies a rational point S. Then all rational points on $\mathcal{C}$ may be found by drawing a line through S which is either vertical or has rational gradient and intersecting it with $\mathcal{C}$.

Example 1.11. To find all rational points on the hyperbola $x(y+x) = 3$, we start by choosing the rational point $S = (1, 2)$. The line through S with gradient m has equation

$$y = m(x-1) + 2$$

Substituting into the original curve, we obtain

$$\begin{aligned} &(m+1)x^2 + (2-m)x - 3 = 0 \\ \implies &(x-1)[(m+1)x + 3] = 0 \\ \implies &x = 1, -\frac{3}{m+1} \end{aligned}$$



It follows that all rational points on the hyperbola are given by

$$(x, y) = \left(-\frac{3}{m+1}, \frac{2-2m-m^2}{m+1} \right) : m \in \mathbb{Q} \setminus \{-1\}$$

In this case, $m = -4$ returns the base point S.

The line with gradient $m = -1$ and the vertical line ($m = \infty$) do not yield solutions: this is geometrically clear since they are parallel to the asymptotes of hyperbola. A full discussion of the problem requires an introduction to projective geometry, in which it can be seen that the lines intersect the hyperbola in so-called *ideal points* at infinity. The details are a matter for another course.

Hopefully these introductory discussions convince you of the variety of approaches that may be required in number theory. It is now time to begin a thorough discussion of the integers, of divisibility, and particularly the prime numbers.

Exercises 1.3 1. (a) Use lines through the point $(1,1)$ to describe all points of the circle $x^2+y^2=2$ whose co-ordinates are rational numbers.

(b) (Harder) Repeat part (a) for the conic with equation $x^2-xy-3y^2=-1$ and initial point $(2,1)$.

(*Hint: remember that there's another point with* $x=2\ldots$)

2. Suppose you attempt to apply the same procedure to find all rational points on the circle $x^2+y^2=3$. What goes wrong?

(*Hint: If* x, y *are rational, write both as fractions over the same denominator…*)

3. (a) Consider a general cubic polynomial equation

$$(x-a)(x-b)(x-c)=x^3+p_2x^2+p_1x+p_0=0$$

where a,b,c are the roots. Prove that if the coefficients $p_0,\ldots,p_2$ are rational numbers and that *two* of the roots are rational, then so is the third root.

(b) The curve $y^2=x^3+8$ contains the points $(1,-3)$ and $(-\frac{7}{4},\frac{13}{8})$. The line through these two points intersects the curve in exactly one other point. Use part (a) to help you find it.

The numbers are a little tricky, but persevere: this generalization of the line-intersection method to cubic curves is particularly important with regard to the construction of addition on elliptic curves, a central topic in modern number theory.

2 Divisibility, Primes & Unique Factorization

The main goal of this chapter is to develop the *Fundamental Theorem of Arithmetic*, or *Unique Factorization Theorem*, which states that every integer ≥ 2 can be written uniquely as a product of primes, e.g.,

$$36 = 2^2 \cdot 3^2, \qquad 986 = 2 \cdot 17 \cdot 29, \qquad 10001 = 73 \cdot 137$$

As a precursor, we review some material which you should have encountered in a previous course.

2.1 The Greatest Common Divisor and the Euclidean Algorithm

Our first definition recalls and extends the idea of divisibility seen in the Introduction.

Definition 2.1. Let a, b, d be integers: if $d \mid a$ and $d \mid b$ then d is a *common divisor*[a] of a and b.
If a and b are not both zero, then the *greatest common divisor* of a, b is written $d = \gcd(a, b)$.
We say that a and b are *coprime* or *relatively prime* if $\gcd(a, b) = 1$.

[a] By convention one tends to list only *positive* common divisors.

Since there are finitely many positive common divisors (all satisfy $d \leq \max(|a|, |b|)$) $\gcd(a, b)$ must therefore exist. The definition may be extended to any list of numbers: $\gcd(a_1, \ldots, a_n)$ is the largest divisor of all the numbers $a_1, \ldots, a_n$.

Examples 2.2. $\gcd(0, 9) = 9$, $\gcd(45, 33) = 3$, $\gcd(162, 450) = 18$.

Our first goal is to develop an algorithm to efficiently compute gcd's. This starts with the notion of division in the integers.

Theorem 2.3 (Division algorithm). *If $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, then there exist unique $q, r \in \mathbb{Z}$ (the* quotient *and* remainder*) such that*

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

Example 2.4. The division algorithm should reminder you of elementary school math!

$$\left.\begin{array}{r} 13 \div 4 = 3 \,\mathrm{r}\, 1 \\ b \div a = q \,\mathrm{r}\, r \end{array}\right\} \iff \left\{\begin{array}{r} 13 = 3 \cdot 4 + 1 \\ a = q \cdot b + r \end{array}\right.$$

Proof. Consider the set $S = \mathbb{N}_0 \cap \{a - bz : z \in \mathbb{Z}\}$. This is a non-empty (e.g. take $z = -|a|$) subset of the natural numbers, whence (well-ordering) it has a minimum element $r \in S$.
Certainly $r \in [0, b)$ for otherwise $r - b \in S$ contradicts the minimality of r. Now let $q = \frac{a-r}{b}$ be the corresponding choice of z to establish existence.
For uniqueness, suppose that $a = q_1 b + r_1$ and $a = q_2 b + r_2$ where $0 \leq r_1, r_2 < b$. Then

$$-b < r_1 - r_2 < b \quad \text{and} \quad r_1 - r_2 = (q_2 - q_1)b$$

Thus $r_1 - r_2$ is divisible by b and lies in the interval $(-b, b)$. Clearly $r_2 = r_1$, whence $q_2 = q_1$ and we have uniqueness. ∎

Is it really an *algorithm*? The presentation of Theorem 2.3 doesn't seem very algorithmic: indeed we simply take it as given that we can find q, r by whatever means we wish (messing with a calculator is fine!). To see it more as an algorithm, consider the case where $a > 0$ and follow these instructions:

1. Is $a < b$? If Yes, stop: $r = a$ and $q = 0$.
2. Otherwise, compute $a - b$.
3. Is $a - b < b$? If Yes, stop: $r = a - b$ and $q = 1$.
4. Otherwise, compute $a - 2b$, etc.
5. Repeat until the process terminates.

Simple code

```
int a=240; int b=7;
int q=0; int r=a;
while(r>=b){r=r-b; q=q+1;}
write(q,r);
```

The simple program computes $q = 34$ and $r = 2$ from $a = 240$ and $b = 7$ by repeatedly subtracting 7 from 240 until it can no longer do so. You can check that $240 = 34 \cdot 7 + 2$. If you like, you can paste and edit the code here.

The Euclidean Algorithm For us, the beauty of the division algorithm is that it transfers the gcd of one pair of numbers to another. For instance, dividing $57 \div 12$ we see that

$$57 = 4 \cdot 12 + 9 \quad \text{and} \quad \gcd(57, 12) = 3 = \gcd(12, 9)$$

More generally, suppose $a = bq + r$. Plainly, a and b are both divisible by $\gcd(b, r)$. Since any common divisor of a, b can be no larger than the greatest such;

$$\gcd(b, r) \leq \gcd(a, b)$$

By symmetry $r = a - bq \implies \gcd(a, b) \leq \gcd(b, r)$, and we conclude:

Lemma 2.5. *If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.*

If $a, b > 0$, we may therefore compute $\gcd(a, b)$ by repeatedly invoking the division algorithm until we obtain a remainder $r_{k+1} = 0$: this process is the *Euclidean algorithm.*

$$\begin{array}{lll}
(\text{Line } 1) & a = q_1 b + r_1 & 0 \leq r_1 < b \\
(\text{Line } 2) & b = q_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\
(\text{Line } 3) & r_1 = q_3 r_2 + r_3 & 0 \leq r_3 < r_2 \\
& \vdots & \\
(\text{Line } k) & r_{k-2} = q_k r_{k-1} + r_k & 0 \leq r_k < r_{k-1} \\
(\text{Line } k+1) & r_{k-1} = q_{k+1} r_k + 0 &
\end{array}$$

Theorem 2.6. *The Euclidean algorithm terminates with final non-zero remainder $r_k = \gcd(a, b)$.*

Proof. A *decreasing sequence of positive integers* $b > r_1 > r_2 > r_3 > \cdots > 0$ takes *at most* b steps to reach 0 (in practice far fewer), whence the algorithm terminates in at most b steps.

Finally, by Lemma 2.5,

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(r_k q_{k+1}, r_k) = r_k$$

■

If a or b are negative, simply apply the algorithm to the pair $|a|, |b|$.

Example 2.7. We use the algorithm[a] to compute $\gcd(161, 140)$

$$\left.\begin{aligned} \mathbf{161} &= 1 \cdot \mathbf{140} + \mathbf{21} \\ \mathbf{140} &= 6 \cdot \mathbf{21} + \mathbf{14} \\ \mathbf{21} &= 1 \cdot \mathbf{14} + \mathbf{7} \\ \mathbf{14} &= 2 \cdot \mathbf{7} \end{aligned}\right\} \implies \gcd(161, 140) = 7$$

We could instead have evaluated $\gcd(161, 140)$ by listing the positive divisors of 140 (namely 1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 70, 140) and checking which of these is also a divisor of 161. For larger a, b, finding all the divisors is prohibitively time-consuming, whereas the Euclidean algorithm will always do the job in a (relatively) efficient manner.

To motivate the next result, we now reverse the algorithm to express the gcd as a linear combination of the original pair $(161, 140)$:

$$\begin{aligned} \mathbf{7} &= \mathbf{21} - 1 \cdot \mathbf{14} && \text{(rearrange line 3)} \\ &= \mathbf{21} - (\mathbf{140} - 6 \cdot \mathbf{21}) && \text{(substitute for } \mathbf{r}_2 = \mathbf{14} \text{ using line 2)} \\ &= -\mathbf{140} + 7 \cdot \mathbf{21} \\ &= -\mathbf{140} + 7 \cdot (\mathbf{161} - \mathbf{140}) && \text{(substitute for } \mathbf{r}_1 = \mathbf{21} \text{ using line 1)} \\ &= 7 \cdot \mathbf{161} - 8 \cdot \mathbf{140} \end{aligned}$$

[a] Remainders are in boldface for clarity. We also do this in the next proof. Consider underlining when writing by hand to help avoid mistakes. Observe how one can trace the same remainder diagonally ↙.

The reversal of the algorithm seen in the example is hugely important and can be done in general.

Theorem 2.8 (Extended Euclidean Algorithm/Bézout's Identity). *Suppose that $a, b \in \mathbb{Z}$ are not both zero. Then there exist integers x, y such that*

$$\gcd(a, b) = ax + by$$

There are a great many existence theorems in Mathematics, but few of them tell you explicitly how to construct the desired objects.

Proof. Suppose $a, b > 0$ and that we've applied the Euclidean algorithm to obtain $r_k = \gcd(a, b)$. Rearrange the penultimate line and repeatedly move up the algorithm using each line to substitute for the smallest remainder:

$$\begin{aligned} \mathbf{r}_k &= \mathbf{r}_{k-2} - q_k \mathbf{r}_{k-1} && \text{(line } k\text{)} \\ &= \mathbf{r}_{k-2} - q_k(\mathbf{r}_{k-3} - q_{k-1}\mathbf{r}_{k-2}) = (1 + q_{k-1}q_k)\mathbf{r}_{k-2} - q_k \mathbf{r}_{k-3} && \text{(line } k-1\text{)} \\ &= (1 + q_{k-1}q_k)(\mathbf{r}_{k-4} - q_{k-2}\mathbf{r}_{k-3}) - q_k \mathbf{r}_{k-3} = (\cdots)\mathbf{r}_{k-3} + (\cdots)\mathbf{r}_{k-4} && \text{(line } k-2\text{)} \\ &\ \ \vdots \\ &= (\cdots)\mathbf{b} + (\cdots)\mathbf{r}_1 && \text{(line 2)} \\ &= (\cdots)\mathbf{a} + (\cdots)\mathbf{b} && \text{(line 1)} \end{aligned}$$

Each omitted term $(\cdots)$ is plainly an integer, obtained by adding and multiplying the quotients q_j. If either a or b is negative, compute with $|a|, |b|$ and adjust $\pm$-signs accordingly. ∎

Example 2.9. Find $d = \gcd(1132, 490)$ and integers x, y such that $d = 1132x + 490y$.
Simply apply the algorithm:

$$\left.\begin{aligned} \mathbf{1132} &= 2 \cdot \mathbf{490} + \mathbf{152} \\ \mathbf{490} &= 3 \cdot \mathbf{152} + \mathbf{34} \\ \mathbf{152} &= 4 \cdot \mathbf{34} + \mathbf{16} \\ \mathbf{34} &= 2 \cdot \mathbf{16} + \mathbf{2} \\ \mathbf{16} &= 8 \cdot \mathbf{2} \end{aligned}\right\} \implies \gcd(1132, 490) = 2$$

Now reverse the steps:

$$\begin{aligned} \mathbf{2} &= \mathbf{34} - 2 \cdot \mathbf{16} && \text{(line 4)} \\ &= \mathbf{34} - 2 \cdot (\mathbf{152} - 4 \cdot \mathbf{34}) = 9 \cdot \mathbf{34} - 2 \cdot \mathbf{152} && \text{(line 3)} \\ &= 9 \cdot (\mathbf{490} - 3 \cdot \mathbf{152}) - 2 \cdot \mathbf{152} = 9 \cdot \mathbf{490} - 29 \cdot \mathbf{152} && \text{(line 2)} \\ &= 9 \cdot \mathbf{490} - 29 \cdot (\mathbf{1132} - 2 \cdot \mathbf{490}) = 67 \cdot \mathbf{490} - 29 \cdot \mathbf{1132} && \text{(line 1)} \end{aligned}$$

Hence $(x, y) = (-29, 67)$ is a solution to $d = 1132x + 490y$.

As an example of the immediate theoretical power of Theorem 2.8 we prove the following:

Corollary 2.10. *If a, b are coprime and $a \mid bc$, then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$, $\exists x, y \in \mathbb{Z}$ such that

$$1 = ax + by \implies c = acx + bcy$$

This last is divisible by a by assumption. ∎

Now we apply Bézout to obtain an important visualization of $\gcd(a, b)$.

Corollary 2.11. *Suppose $a, b \in \mathbb{Z}$ are not both zero and $d = \gcd(a, b)$. Then*

$$\{ax + by : x, y \in \mathbb{Z}\} = \{md : m \in \mathbb{Z}\}$$

Plainly d is the least positive member of this set.

Proof. Write $D = \{ax + by : x, y \in \mathbb{Z}\}$ and $M = \{md : m \in \mathbb{Z}\}$.
($D \subseteq M$) Certainly $d \mid ax + by$ for all $x, y \in \mathbb{Z}$, whence every element of D is a multiple of d.
($M \subseteq D$) By Bézout's identity, $d = aX + bY$ for some $X, Y \in \mathbb{Z}$, and so $d \in D$. It follows that

$$md = a(mX) + b(mY) \in D$$

∎

In more advanced treatments involving rings other than the integers, Corollary 2.11 is often used as the *definition* of $\gcd(a, b)$. This has the advantage of permitting one to define the gcd without first requiring a Euclidean algorithm: many more rings have a gcd than have a Euclidean algorithm!

Linear Diophantine Equations

As a simple application, we consider integer solutions x, y to equations $ax + by = c$ where $a, b, c \in \mathbb{Z}$ are given. Bézout's identity tells us how to find a solution whenever $c = \gcd(a, b)$. With the help of Corollary 2.11, this is essentially all we need.

Corollary 2.12. *The Diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b) \mid c$.*

Proof. A solution exists $\iff c \in \{ax + by : x, y \in \mathbb{Z}\} \iff c$ is a multiple of $\gcd(a, b)$. ∎

Example 2.13. Show that $147x - 45y = 2$ has no solutions in integers.

$$\left.\begin{aligned} \mathbf{147} &= 3 \cdot \mathbf{45} + \mathbf{12} \\ \mathbf{45} &= 3 \cdot \mathbf{12} + \mathbf{9} \\ \mathbf{12} &= 1 \cdot \mathbf{9} + \mathbf{3} \\ \mathbf{9} &= 3 \cdot \mathbf{3} \end{aligned}\right\} \implies \gcd(147, 45) = 3 \nmid 2$$

Now let $d = \gcd(a, b)$ and suppose that $d \mid c$ so that we have a solution (x_0, y_0) to $ax + by = c$. Consider $(x, y) = (x_0 + x_h, y_0 + y_h)$ and observe that[7]

$$\begin{aligned} ax + by = c &\iff c = a(x_0 + x_h) + b(y_0 + y_h) = c + ax_h + by_h \\ &\iff ax_h + by_h = 0 \iff \frac{b}{d} y_h = -\frac{a}{d} x_h \end{aligned}$$

Since $\frac{a}{d}, \frac{b}{d}$ are *coprime integers,* Corollary 2.10 shows that $\frac{b}{d}$ divides x_h. This is enough to prove:

Corollary 2.14. *Let $d = \gcd(a, b)$ and suppose (x_0, y_0) is a solution to the Diophantine equation $ax + by = c$. Then all solutions may be found via*

$$(x, y) = \left(x_0 + \frac{b}{d} t, y_0 - \frac{a}{d} t\right) \quad \text{where} \quad t \in \mathbb{Z}$$

Examples 2.15. 1. Find all the solutions to the Diophantine equation $161x + 140y = -14$.

By Example 2.7 we have $d = \gcd(161, 140) = 7$ and a solution $(7, -8)$ to $161x + 140y = 7$. Multiply by -2 to obtain a suitable (x_0, y_0) and apply the Theorem

$$(x, y) = \left(-14 + \frac{140}{7} t, 16 - \frac{161}{7} t\right) = (-14 + 20t, 16 - 23t) : t \in \mathbb{Z}$$

2. Find all solutions in integers to the equation $490x - 1132y = 4$.

By Example 2.9, we know that $d = \gcd(1132, 490) = 2$ and that $(-29, 67)$ is a solution to $1132x + 490y = 2$. Rearranging and taking $\pm$-signs into account, we see that $(x_0, y_0) = (134, 58)$ is a solution to the equation of interest. The general solution is therefore

$$(x, y) = \left(134 + \frac{1132}{2} t,\ 58 + \frac{490}{2} t,\right) = (134 + 566t,\ 58 + 245t) : t \in \mathbb{Z}$$

[7] We use (x_h, y_h) since this solves the associated *homogeneous* equation $ax_h + by_h = 0$. The method of solution is analogous to solving non-homogeneous linear ordinary differential equations and linear algebra problems $A\mathbf{x} = \mathbf{b}$.

Exercises 2.1 1. Verify the following elementary properties of divisibility, where a, b, c are integers.

(a) $a \mid 0$, $a \mid a$ and $\pm 1 \mid a$.

(b) If $a \mid b$ and $b \mid c$, then $a \mid c$ (divides is *transitive*).

(c) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.

2. Use the Euclidean Algorithm to compute the following (*use a calculator!*)

(a) $\gcd(121, 105)$ (b) $\gcd(12345, 67890)$ (c) $\gcd(54321, 9876)$

3. Evaluate $\gcd(4655, 12075)$ in the form $12075x + 4655y$ where $x, y \in \mathbb{Z}$.

4. Find all the integer solutions (if any exist) to the following equations.

(a) $4x - y = 7$ (b) $12x + 4y = 10$ (c) $105x - 121y = 1$

(d) $2072x + 1813y = 2849$ (e) $12345x - 67890y = \gcd(12345, 67890)$

(f) $\begin{cases} 7x + 2y = 21 \\ 3x - 7z = 2 \end{cases}$ (use the method several times)

5. Find all solutions of $19x + 20y = 1909$ with $x > 0$ and $y > 0$.

6. Let $r_0, r_1, r_2, \ldots$ be the successive remainders in the Euclidean Algorithm applied to $a > b > 0$ (take $b = r_0$). Show that every two steps reduces the remainder by at least one half: i.e.,

$$r_{i+2} < \frac{1}{2} r_i \quad \forall i = 0, 1, 2, 3 \ldots$$

Conclude that the Euclidean algorithm terminates in at most $2 \log_2 b$ steps. In particular, show that the number of steps is at most seven times the number of digits in b.

7. The *Fibonacci numbers* $(F_n)_{n=1}^{\infty} = (1, 1, 2, 3, 5, 8, 13, \ldots)$ are defined by the recurrence relation

$$\begin{cases} F_{n+2} = F_{n+1} + F_n, \ \forall n \in \mathbb{N}, \\ F_1 = F_2 = 1 \end{cases}$$

(a) Prove that no two successive Fibonacci numbers have a common divisor $a > 1$.

(b) Use the Euclidean algorithm to verify $\gcd(F_7, F_6) = \gcd(13, 8) = 1$. Repeat for $\gcd(F_8, F_7)$.

(c) Make a hypothesis about how many steps are necessary in order to compute $\gcd(F_{n+1}, F_n)$.

(d) Compute $2 \log_2 F_n$ for $n = 4, 5, 6, 7, 8$. Considering question 6, why might we say that the Euclidean algorithm is very *slow* when applied to successive Fibonacci numbers?

8. Let a, b, r, s be given constants. Prove that the arithmetic progressions

$$\{ax + r : x \in \mathbb{Z}\} \quad \text{and} \quad \{by + s : y \in \mathbb{Z}\}$$

intersect if and only if $\gcd(a, b) \mid (s - r)$.

9. Show that if $ad - bc = \pm 1$, then the fraction $\frac{a+b}{c+d}$ is in reduced form (i.e. $\gcd(a + b, c + d) = 1$).

10. Show that if $\gcd(a, b) = 1$, then $\gcd(a - b, a + b) = 1$ or 2. Exactly when is the value 2?

2.2 Primes and Unique Factorization

Now we turn to the building blocks of the integers, the prime numbers. The very idea that the primes are 'building blocks' is a colloquial expression of a famous result, examples of which are on page 10.

Theorem 2.16 (Fundamental Theorem of Arithmetic/Unique Prime Factorization).
Every integer z is either zero, ± 1, or may be uniquely factored in the form

$$z = up_1^{\mu_1} \cdots p_n^{\mu_n}$$

where $u = \pm 1$, $p_1 < \cdots < p_n$ are primes and each $\mu_i \in \mathbb{N}$.

The first question is obvious: *what is a prime*? You should have previously encountered two suitable notions, though algebraically they present quite differently.

Definition 2.17. An integer $z \geq 2$ is said to be:[a]

Prime if whenever it divides a product, it divides one of the factors: $z \,|\, ab \implies z \,|\, a$ or $z \,|\, b$

Irreducible if its only positive divisors are 1 and itself: $\forall k \in \mathbb{N},\ k \,|\, z \implies k = 1$ or z.

Composite if it is not irreducible: $\exists a, b \in \mathbb{N}$ such that $z = ab$ and $2 \leq a, b < z$.

[a] A note for algebraists who might have seen these definitions elsewhere. We follow the convention in the integers that primes, irreducibles and composites must be *positive*. A more formal algebraic definition allows, say -5 to be prime/irreducible. More properly, if z is prime/irreducible in a ring, so is uz where u is a *unit*: the only units in the ring of integers are ± 1.

Examples 2.18. 1. The integer $z = 5$ is prime/irreducible:

Prime: for example $5 \,|\, (15 \cdot 11)$ and $5 \,|\, 15$.

Irreducible: its only positive divisors are 1 and 5.

2. The integer $z = 4$ is not prime & composite:

Not prime: for example $4 \,|\, (6 \cdot 10)$ but $4 \nmid 6$ and $4 \nmid 10$.

Composite: the positive divisors are 1, 2 and 4.

The distinction between primes and irreducibles is partly artificial: the uniqueness proof of the Fundamental Theorem will be seen to hinge on the fact that *primes and irreducibles are identical*! After this section, *prime* will refer to any positive integer satisfying both of the prime/irreducible conditions in Definition 2.17. In abstract algebra however, the distinction is far more important: there exist many rings where primes and irreducibles are genuinely *different* objects.[8]

[8] In a later class, our approach in this section will be seen to generalize to other rings in which primes and irreducibles are identical; in such cases an analogue of the unique factorization theorem can often be produced. This isn't a universal, for in some rings the concepts are distinct and there might exist non-unique factorizations. For those with some experience: all four of $2, 3, \sqrt{10} \pm 2$ are irreducible in the ring $\mathbb{Z}[\sqrt{10}]$, and we have a non-unique irreducible factorization

$$6 = 2 \cdot 3 = (\sqrt{10} - 2)(\sqrt{10} + 2)$$

In this ring, 2 is irreducible but *not* prime: good luck showing this at the moment!

Existence: Irreducibiles and Composites

The first stage of proving the Fundamental Theorem is to factor every positive integer by irreducibles.

Lemma 2.19. *Every composite is divisible by an irreducible.*

Proof. Suppose $z \geq 2$ is composite but has no irreducible factors. Then:

- $z = a_1 b_1$ where $a_1, b_1 \geq 2$ are not irreducible: plainly a_1, b_1 are composites.
- If a_1 had an irreducible factor then this would be an irreducible factor of z. Hence a_1 is composite and may be written $a_1 = a_2 b_2$ for $a_2, b_2 \geq 2$ composite.
- Repeat the process *ad infinitum*:

  $$z = a_1 b_1 = a_2 b_2 b_1 = a_3 b_3 b_2 b_1 = \cdots$$

  Since each $b_n \geq 2$ we see that $(a_1, a_2, a_3, a_4, \ldots)$ is a decreasing sequence of positive integers: contradiction.

■

We can now prove a famous result dating at least back to Euclid (300 BC).

Theorem 2.20. *There are infinitely many irreducibles.*

Proof. Suppose that $p_1, \ldots, p_n$ constitutes all irreducibles and consider $P := p_1 \cdots p_n + 1$. By Lemma 2.19, P has an irreducible factor p which, by assumption, is one of our irreducibles p_i. But then

$$p \,|\, P \quad \text{and} \quad p \,|\, p_1 \cdots p_n \implies p \,|\, 1$$

which contradicts the fact that $p \geq 2$.

■

We also quickly obtain the existence part of the Fundamental Theorem.

Theorem 2.21. *Every integer $z \geq 2$ is a product of irreducibles.*

Proof. This is merely an iteration of Lemma 2.19.

- If z is irreducible, we are done.
- Otherwise, $z = p_1 a_1$ where p_1 is irreducible and $a_1 \in \mathbb{N}$. If a_1 is irreducible, we are done.
- Otherwise, $z = p_1 p_2 a_2$ where p_2 is irreducible and $a_2 \in \mathbb{N}$. If a_2 is irreducible, we are done.
- Continue until the process terminates and we obtain the factorization $z = p_1 p_2 \cdots p_n$.

If the process never terminated, then $(z, a_1, a_2, \ldots)$ would be a sequence of decreasing positive integers; a contradiction.

■

Nothing in the Theorem assists us in *computing* a suitable factorization. The best approach for small integers is simply to hack at it. For large numbers, factorization is a very hard (i.e. slow) problem.

Uniqueness: Primes and Irreducibles are Identical

The existence part of the Fundamental Theorem is really a claim about *irreducibles.* We've said nothing yet about primes.

Lemma 2.22. *In the integers, primes and irreducibles are identical.*

Proof. 1. (Every prime is irreducible) Suppose p is prime and that $p = kl$ where $k, l \in \mathbb{N}$: our goal is to prove that $\{k, l\} = \{1, p\}$.

Since p is prime, we have $p \mid k$ or $p \mid l$. WLOG suppose the former: $k = p\alpha$ for some $\alpha \in \mathbb{Z}$. But then

$$p = p\alpha l \implies \alpha l = 1$$

Since we are working in the integers and $l > 0$, it follows that $kl = \alpha = 1$ and $k = p$.

2. (Every irreducible is prime) Suppose z is irreducible and that $z \mid ab$ where $a, b \in \mathbb{Z}$: our goal is to prove that $z \mid a$ or $z \mid b$.

Let $d = \gcd(a, z)$. Since z is irreducible, there are only two possibilities:

- $d = 1$: in this case $\gcd(a, z) = 1$ and $z \mid ab$ implies (Corollary 2.10) that $z \mid b$.
- $d = z$: in this case $z \mid a$.

■

The first argument used much less technology than the second, which depended crucially on Bézout's identity and the Euclidean algorithm.[9]

The equivalence of irreducibles and primes yields the uniqueness part of the Fundamental Theorem.

Proof of Theorem 2.16. We can factor z into irreducibles by Theorem 2.21. Now suppose we have two distinct such factorizations

$$z = p_1^{\mu_1} \cdots p_n^{\mu_n} = q_1^{\nu_1} \cdots q_m^{\nu_m}$$

Since the factorizations are distinct, at least some terms remain after dividing both sides by all common irreducible factors:

$$p_{n_1}^{\alpha_1} \cdots p_{n_k}^{\alpha_t} = q_{m_1}^{\beta_1} \cdots q_{m_l}^{\beta_l}$$

where $\{p_{n_1}, \ldots, p_{n_k}\}$ and $\{q_{m_1}, \ldots, q_{m_l}\}$ are distinct sets of irreducibles and all $\alpha_i, \beta_j \in \mathbb{N}$.

Plainly the *irreducible* p_{n_1} divides the *right hand side.* Since p_{n_1} is also *prime* (Lemma 2.22) we see that it divides at least one of the irreducibles $q_{m_1}, \ldots, q_{m_l}$. This is a contradiction. ■

[9] For algebra experts, part 1 really only requires that we're working in an *integral domain*:

$$p = p\alpha l \implies p(1 - \alpha l) = 0 \implies \alpha l = 1$$

since an integral domain has no *zero divisors.* The fact that every prime is irreducible is thus highly generalizable. By contrast, the existence of a Bézout-type identity or a Euclidean algorithm is very *rare* in a general ring. The fact that every irreducible is prime is special to the integers and to relatively few other rings.

Simple Consequences of the Fundamental Theorem

Now that we have unique factorization, several 'obvious' things are seen to be true.

Corollary 2.23. *Suppose* $a = p_1^{\mu_1} \cdots p_n^{\mu_n}$ *and* $b = p_1^{\nu_1} \cdots p_n^{\nu_n}$ *are written in terms of their unique factorizations.*[a] *Then:*

1. $b \mid a \iff \nu_i \leq \mu_i$ *for all* i. *Essentially, all primes in* b *must also be in* a.
2. $\gcd(a,b) = p_1^{\min(\mu_1,\lambda_1)} \cdots p_n^{\min(\mu_n,\lambda_n)}$.
3. a *is a perfect square if and only if every* μ_i *is even (consider* $a = b^2$ *then* $\mu_i = 2\nu_i$*).*
4. $a^2 \mid b^2 \implies a \mid b$.
5. *If* ab *is a perfect square and* $\gcd(a,b) = 1$*, then both* a *and* b *are perfect squares.*

[a] Some exponents may need to be zero in order to have the same lists of primes.

The last two statements were used in our discussion of Pythagorean triples.

Definition 2.24. The *least common multiple* $\operatorname{lcm}(a,b)$ of two positive integers a, b is the smallest positive integer divisible by both a and b.

Following the notation in the Corollary,

$$\left.\begin{aligned} a &= p_1^{\mu_1} \cdots p_n^{\mu_n} \\ b &= p_1^{\nu_1} \cdots p_n^{\nu_n} \end{aligned}\right\} \implies \operatorname{lcm}(a,b) = p_1^{\max(\mu_1,\nu_1)} \cdots p_n^{\max(\mu_n,\nu_n)}$$

$$\implies \operatorname{lcm}(a,b) \cdot \gcd(a,b) = ab$$

This last follows since $\max(\mu_i,\lambda_i) + \min(\mu_i,\lambda_i) = \mu_i + \lambda_i$

Warning: this formula *does not hold* for gcd's or lcm's of three or more integers.

Examples 2.25. 1. To find $\operatorname{lcm}(110, 154)$, there are three obvious approaches:

(a) Brute force: list several small multiples of each and look for the smallest. This is no fun.

(b) Prime factorizations: if we know that $110 = 2 \cdot 5 \cdot 11$ and $154 = 2 \cdot 7 \cdot 11$, then

$$\operatorname{lcm}(110, 154) = 2 \cdot 5 \cdot 7 \cdot 11 = 770$$

(c) Use the Euclidean algorithm:

$$\left.\begin{aligned} \mathbf{154} &= 1 \cdot \mathbf{110} + \mathbf{44} \\ \mathbf{110} &= 2 \cdot \mathbf{44} + \mathbf{22} \\ \mathbf{44} &= 2 \cdot \mathbf{22} \end{aligned}\right\} \implies \gcd(110, 154) = 22$$

$$\implies \operatorname{lcm}(110, 154) = \frac{110 \cdot 154}{22} = 770$$

2. To find $\operatorname{lcm}(4, 6, 10)$, we use the prime factorizations:

$$\operatorname{lcm}(4, 6, 10) = \operatorname{lcm}(2^2, 2 \cdot 3, 2 \cdot 5) = 2^2 \cdot 3 \cdot 5 = 60$$

Note that

$$60 = \operatorname{lcm}(4, 6, 10) \neq \frac{4 \cdot 6 \cdot 10}{\gcd(4, 6, 10)} = \frac{240}{2} = 120$$

Exercises 2.2 1. Evaluate the following by finding unique prime factorizations: *use a calculator!*

(a) $\operatorname{lcm}(845, 8788)$

(b) $\operatorname{lcm}(825, 495)$

(c) $\operatorname{lcm}(2310, 1870)$

(d) $\operatorname{lcm}(198061, 231896)$

2. Suppose that $\gcd(a, b) = 1$ and let c be an integer.

   (a) Use the prime factorizations of a, b and c to prove the following.

      i. $a \mid bc \implies a \mid c$ (*this is a cheat, since we used it to prove prime factorization!*)

      ii. If $a \mid c$ and $b \mid c$, then $ab \mid c$

      iii. $\gcd(ab, c) = \gcd(a, c)\gcd(b, c)$

      (*It follows that* $\gcd(ab, c) = 1 \iff \gcd(a, c) = 1 = \gcd(b, c)$ *whenever* a, b *are coprime*)

   (b) We proved part (a)(i) in Corollary 2.10 using Bézout's identity. Can you prove (ii) and (iii) similarly; i.e. *without* using unique factorization? (*Warning: (iii) is especially difficult!*)

3. Use Exercise 2 part (a)(iii) to prove that, for all $x, y \in \mathbb{Z}$ we have

   $$\gcd(ab, ay + bx) = \gcd(a, x)\gcd(b, y)$$

4. Suppose a, b, c are all non-zero. Prove or disprove:

   (a) $\gcd(a, b) = \gcd(a, c) \implies \gcd(a^2, b^2) = \gcd(a^2, c^2)$

   (b) $\gcd(a, b) = \gcd(a, c) \implies \gcd(a, b) = \gcd(a, b, c)$

   (c) If $p \mid (a^2 + b^2)$ and $p \mid (b^2 + c^2)$, then $p \mid (a^2 + c^2)$.

5. The square-free numbers are those integers k which are not divisible by the square of any prime (e.g. $1, 2, 3, 5, 6, 7, 10, 11, 13, \ldots$). Prove that every integer ≥ 2 is uniquely the product of a square and a square-free number.

6. Recall that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ for positive integers a, b.

   (a) In Example 2.25 we saw that the same formula *does not* necessarily hold when applied to *three* integers a, b, c. Find another such counter-example.

   (b) Is it ever true that $\gcd(a, b, c) \cdot \operatorname{lcm}(a, b, c) = abc$ for positive integers a, b, c? In general is the LHS less than or greater than abc? Make a hypothesis and try to prove it.

7. Suppose that g, m are positive integers. Prove that $g \mid m$ if and only if there exist integers a, b such that $\gcd(a, b) = g$ and $\operatorname{lcm}(a, b) = m$.

3 Congruences and Congruence Equations

A great many problems in number theory rely only on *remainders* when dividing by an integer. Recall the division algorithm: given $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qn + r, \qquad 0 \leq r < n \tag{$*$}$$

It is to the *remainder* r that we now turn our attention.

3.1 Congruences and $\mathbb{Z}_n$

Definition 3.1. For each $n \in \mathbb{N}$, the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ comprises the *residues modulo n*. Integers a, b are said to be *congruent modulo n* if they have the same residue: we write $a \equiv b \pmod{n}$.

The division algorithm says that every integer $a \in \mathbb{Z}$ has a unique *residue* $r \in \mathbb{Z}_n$.

Example 3.2. We may write $7 \equiv -3 \pmod{5}$, since applying the division algorithm yields

$$7 = 5 \times 1 + 2 \quad \text{and} \quad -3 = 5 \times (-1) + 2$$

Indeed both 7 and 12 have residue 2 modulo 5.

As another example, we prove a very simple result.

Lemma 3.3. *All squares of integers have remainders 0 or 1 upon dividing by 3.*

Proof. Since every integer x has remainder 0, 1 or 2 upon division by 3, we have three mutually exclusive cases to check:

- $x \equiv 0 \pmod{3}$ Write $x = 3y$ for some integer y. But then
$$x^2 = 9y^2 = 3(3y^2) \equiv 0 \pmod{3}$$
- $x \equiv 1 \pmod{3}$ This time $x = 3y + 1$ for some integer y, and
$$x^2 = 9y^2 + 6y + 1 = 3(3y^2 + 2y) + 1 \equiv 1 \pmod{3}$$
- $x \equiv 2 \pmod{3}$ Finally $x = 3y + 2$ yields
$$x^2 = 9y^2 + 12y + 4 = 3(3y^2 + 4y + 1) + 1 \equiv 1 \pmod{3}$$

A perfect square therefore never has remainder 2. ∎

This is very tedious notation. We'd far prefer to compute directly with remainders. Once we've developed such, we'll return to the Lemma to see how the proof improves. To start this process, we observe that there is an easier way to check whether two integers are congruent modulo n.

Theorem 3.4. $a \equiv b \pmod{n} \iff n \mid (a-b)$

Proof. Suppose that $a = q_1 n + r_1$ and $b = q_2 n + r_2$ are the results of applying the division algorithm to a, b modulo n. Plainly $a \equiv b \pmod{n} \iff r_1 = r_2$. We prove each direction separately:

($\Rightarrow$) This is almost immediate:

$$r_1 = r_2 \implies a - nq_1 = b - nq_2 \implies a - b = n(q_2 - q_1)$$

Since $q_2 - q_1$ is an integer, $a - b$ is a multiple of n.

($\Leftarrow$) Conversely, suppose that $a - b = kn$ is a multiple of n. Then

$$r_1 - r_2 = (a - nq_1) - (b - nq_2) = (a - b) + n(q_2 - q_1) = n(k + q_2 - q_2)$$

This says that $r_1 - r_2$ is an integer multiple of n. Recalling the proof of the division algorithm, $-n < r_1 - r_2 < n$ forces $r_1 - r_2 = 0$. ∎

The Theorem says that we can compare remainders *without computing quotients.* In case the advantage isn't clear, we recall our earlier example.

Example (3.2 revisited). $7 \equiv -3 \pmod{5}$ follows since $7 - (-3) = 10$ is divisible by 5. There is no need for us to express 7 and -3 using the division algorithm.

Our next goal is to define an *arithmetic* with remainders, again *without* calculating quotients.

Example 3.5. If $x \equiv 3$ and $y \equiv 5 \pmod{7}$, then there exist integers k, l such that $x = 7k + 3$ and $y = 7l + 5$. But then

$$xy = 7(7kl + 5k + 3l) + 15 = 7(7kl + 5k + 3l + 2) + 1 \implies xy \equiv 1 \pmod{7}$$

It would be so much simpler if we could write

$$x \equiv 3,\ y \equiv 5 \implies xy \equiv 3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$$

Thankfully the next result justifies the crucial step.

Theorem 3.6 (Modular Arithmetic). *Suppose that $x \equiv a$ and $y \equiv b \pmod{n}$. Then*

1. $x \pm y \equiv a \pm b \pmod{n}$
2. $xy \equiv ab \pmod{n}$
3. *For any $m \in \mathbb{N}$, $x^m \equiv a^m \pmod{n}$*

Proof. We just prove 2: part 1 is similar, and part 3 is by induction using part 2 as the induction step. By Theorem 3.4, there exist integers k, l such that $x = kn + a$ and $y = ln + b$. But then

$$xy = (kn + a)(ln + b) = n(kln + al + bk) + ab \implies xy \equiv ab \pmod{n}$$

∎

Examples 3.7. We can now easily compute remainders of complex arithmetic objects.

1. What is the remainder when 17^{113} is divided by 3?

   Don't bother asking your calculator: 17^{113} is 139 digits long! Instead we use modular arithmetic:

   $$\begin{aligned} 17 \equiv -1 \pmod 3 \implies 17^{113} &\equiv (-1)^{113} && \text{(Theorem 3.6, part 3.)} \\ &\equiv -1 \pmod 3 && \text{(since 113 is odd)} \end{aligned}$$

   Since $-1 \equiv 2$, we conclude that 17^{113} has remainder 2 when divided by 3.

2. Similarly, calculating remainders modulo 10 yields

   $$219^{45} - 43^{12} \equiv (-1)^{45} - 3^{12} \equiv -1 - 9^6 \equiv -1 - (-1)^6 \equiv -1 - 1 \equiv -2 \equiv 8 \pmod{10}$$

3. We find the remainder when 4^{49} is divided by 67. Even with the assistance of a powerful calculator, evaluating

   $$4^{49} = 316,912,650,057,057,350,374,175,801,344$$

   doesn't help us! Instead we first search for a power of 4 which is *small* modulo 67: the obvious choice is $4^3 = 64$.

   $$4^{49} \equiv 4 \cdot (4^3)^{16} \equiv 4 \cdot (-3)^{16} \equiv 4 \cdot 3^{16} \pmod{67}$$

   Next we search for a power of 3 which is small: since $3^4 = 81 \equiv 14 \pmod{67}$ we obtain

   $$4^{49} \equiv 4 \cdot (3^4)^4 \equiv 4 \cdot 14^4 \pmod{67}$$

   Now observe that $14^2 = 196 \equiv -5 \pmod{67}$ and we are almost finished:

   $$4^{49} \equiv 4 \cdot (-5)^2 \equiv 4 \cdot 25 \equiv 100 \equiv 33 \pmod{67}$$

Now that we have some better notation, here is a much faster proof of Lemma 3.3.

Proof. Modulo 3 we have:

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 4 \equiv 1$$

Hence squares can only have remainders 0 or 1 modulo 3. ∎

As an application, we can easily show that in a primitive Pythagorean triple (a, b, c) exactly one of a or b is a multiple of three. Just think about the remainders modulo 3:

$$a^2 + b^2 \equiv c^2 \pmod 3$$

The only possibilities are $0 + 0 \equiv 0$, $0 + 1 \equiv 1$ and $1 + 0 \equiv 1$, however the first says that all three of a, b, c are divisible by three which results in a non-primitive triple.

Similar games can be played with other primes.

Congruence and Division By Theorem 3.6, we may add, subtract, multiply and take positive integer powers of remainders without issue. Division is another matter entirely: it simply does not work in the usual sense.

Example 3.8. Since $54 - 30 = 24$ is divisible by 8, we see that $54 \equiv 30 \pmod 8$. We'd like to divide both sides this congruence by 6, however

$$6 \times 9 \equiv 6 \times 5 \pmod 8 \not\Longrightarrow 9 \equiv 5 \pmod 8$$

since the right hand side is *false.* What can we try instead? Instead we follow the definition:

$$6 \times 9 \equiv 6 \times 5 \pmod 8 \implies 6 \times 9 = 6 \times 5 + 8m \text{ for some}^{10} m \in \mathbb{Z}$$

We can't automatically divide this by 6, but we can certainly divide through by 2:

$$3 \times 9 = 3 \times 5 + 4m \implies 3 \,|\, 4m \implies 3 \,|\, m \implies m = 3l \text{ for some } l \in \mathbb{Z}$$

We may now divide by 3 to correctly conclude

$$9 = 5 + 4l \implies 9 \equiv 5 \pmod 4$$

It appears that we were able to divide our original congruence by 6, but at the cost of *dividing the modulus* by 2: it just so happens that $2 = \gcd(6, 8)\ldots$

Theorem 3.9. *If $k \neq 0$ and $\gcd(k, n) = d$, then*

$$ka \equiv kb \pmod n \implies a \equiv b \pmod{\tfrac{n}{d}}$$

Proof. $\gcd(k, n) = d \implies \gcd\left(\frac{k}{d}, \frac{n}{d}\right) = 1$ so that $\frac{n}{d}$ and $\frac{k}{d}$ are *coprime integers.* Appealing to a corollary[11] of Bézout's identity, we see that

$$ka \equiv kb \implies n \,|\, (ka - kb) \implies \frac{n}{d} \,\Big|\, \frac{k}{d}(a - b) \implies \frac{n}{d} \,\Big|\, (a - b)$$

Otherwise said $a \equiv b \pmod{\frac{n}{d}}$. ∎

Examples 3.10.

1. We divide by 4 in the congruence $12 \equiv 28 \pmod 8$. Since $\gcd(4, 8) = 4$ we also divide the modulus by 4 to obtain

$$12 \equiv 28 \pmod 8 \implies 3 \equiv 7 \pmod 2$$

2. We divide by 12 in the congruence $12 \equiv 72 \pmod{30}$. Since $\gcd(12, 30) = 6$, we conclude that

$$12 \equiv 72 \pmod{30} \implies 1 \equiv 6 \pmod 5$$

[10] It is obvious that $m = 3$ but leaving this unsaid makes it easier to see a proof of the following theorem.

[11] If $\gcd(a, b) = 1$ and $a \,|\, bc$, then $a \,|\, c$. This is the crucial step in the calculation, corresponding to the $\implies$ arrows in both the proof and the previous example.

Division in the ring $\mathbb{Z}_n$ The development of modular arithmetic (Theorem 3.6) shows that the set of residues $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ modulo n has the algebraic structure of a *ring*.[12] The interesting question for us is when one can *divide.*

Recall in the real numbers that to divide by x means that we *multiply* by some element x^{-1} satisfying $xx^{-1} = 1$: plainly this is possible provided $x \neq 0$. The same idea holds in $\mathbb{Z}_n$.

Definition 3.11. Let $x \in \mathbb{Z}_n$. We say that $y \in \mathbb{Z}_n$ is the *inverse* of x if $xy \equiv yx \equiv 1 \pmod{n}$.
An element x is a *unit* if it has an inverse. A ring is a *field* if every non-zero element is a unit.

Example 3.12. By considering the multiplication tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$, we can easily identify the units and their inverses:

$\mathbb{Z}_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

There are plainly only *two* units in $\mathbb{Z}_6$, namely 1 and 5. Moreover, each is its own inverse

$$1 \cdot 1 \equiv 1, \quad 5 \cdot 5 \equiv 1 \pmod{6}$$

Modulo 5, however, every non-zero residue is a unit:

$$1 \cdot 1 \equiv 1, \quad 2 \cdot 3 \equiv 3 \cdot 2 \equiv 1, \quad 4 \cdot 4 \equiv 1 \pmod{5}$$

In the example, the units have a simple property in common.

Theorem 3.13. *$x \in \mathbb{Z}_n$ is a unit $\iff \gcd(x, n) = 1$.*
Moreover, every non-zero $x \in \mathbb{Z}_n$ is a unit (thus $\mathbb{Z}_n$ is a field*) if and only if $n = p$ is* prime.

Proof. ($\Rightarrow$) If $xy \equiv 1 \pmod{n}$, then $xy - \lambda n = 1$ for some $\lambda \in \mathbb{Z}$. Plainly any common factor of x and n divides 1, whence $\gcd(x, n) = 1$.

($\Leftarrow$) By Bézout's identity, $\exists \lambda, y \in \mathbb{Z}$ such that

$$xy + n\lambda = 1 \implies xy \equiv 1 \pmod{n}$$

Plainly every non-zero x is a unit if and only if $\gcd(x, n) = 1$ for all $x \in \{1, \ldots, n-1\}$. This is if and only if n has no divisors except itself and 1: i.e. n is prime. ∎

This result gels with Theorem 3.9: we can divide a congruence by k *while remaining in* $\mathbb{Z}_n$ precisely when $d = \gcd(k, n) = 1$. Moreover, the proof tells us how to compute inverses: use Bézout!

[12] More formally, it inherits this structure from the integers as a factor ring: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ is a set of equivalence classes where $x \sim y \iff x \equiv y \pmod{n}$. For this course, familiarity with this construction is unimportant.

Example 3.14. Find the inverse of $15 \in \mathbb{Z}_{26}$.

First observe that $\gcd(15,26) = 1$, so an inverse exists. Now apply the Euclidean algorithm and Bézout's identity:

$$\begin{array}{lll} \mathbf{26} = 1\cdot\mathbf{15}+\mathbf{11} & \implies \gcd(26,15) = \mathbf{1} = \mathbf{4}-\mathbf{3} = \mathbf{4}-(\mathbf{11}-2\cdot\mathbf{4}) \\ \mathbf{15} = 1\cdot\mathbf{11}+\mathbf{4} & & = 3\cdot\mathbf{4}-\mathbf{11} = 3(\mathbf{15}-\mathbf{11})-\mathbf{11} \\ \mathbf{11} = 2\cdot\mathbf{4}+\mathbf{3} & & = 3\cdot\mathbf{15}-4\cdot\mathbf{11} = 3\cdot\mathbf{15}-4(\mathbf{26}-\mathbf{15}) \\ \mathbf{4} = 1\cdot\mathbf{3}+\mathbf{1} & & = 7\cdot\mathbf{15}-4\cdot\mathbf{26} \end{array}$$

from which we see that $15\cdot 7 \equiv 1 \pmod{26}$: the inverse of 15 is therefore 7.

Exercises 3.1 1. Find the residues (remainders) of the following expressions:

(a) $6^4 - 38\cdot 48 \pmod 5$

(b) $117^{32} + 118^{31} \pmod 7$

(c) $3510^{1340} - 2709^{4444} \pmod{24}$

2. Suppose that $d \mid m$. Show that if $a \equiv b \pmod{\frac{m}{d}}$, then

$$a \equiv b, \quad \text{or} \quad b+\frac{m}{d}, \quad \text{or} \quad \cdots, \quad \text{or} \quad b+(d-1)\frac{m}{d} \pmod m$$

3. Show that a positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3.
(*Hint: for example* $471 = 4\cdot 100 + 7\cdot 10 + 1\ldots$)

4. Suppose $z \in \mathbb{N}$ and that $z \equiv 3 \pmod 4$. Prove that at least one of the primes p dividing z must be congruent to 3 modulo 4.

5. (a) State the units in the ring $\mathbb{Z}_{48}$.
(b) Find the inverse of 11 modulo 48.
(c) If $11x \equiv 2 \pmod{48}$ for some $x \in \mathbb{Z}_{48}$, find x.

6. Prove that inverses are unique: if y, z are inverses of $x \in \mathbb{Z}_n$, then $y \equiv z \pmod n$.

7. A non-zero element $x \in \mathbb{Z}_n$ is a *zero divisor* if $\exists y \in \mathbb{Z}_n$ such that $xy \equiv 0 \pmod n$. Prove that $\mathbb{Z}_n$ has zero divisors if and only if n is composite.

8. Suppose p is prime and $a \not\equiv 0$. Prove that the remainders $0, a, 2a, 3a, \ldots, (p-1)a$ are *distinct* modulo p, and thus constitute all of $\mathbb{Z}_p$.

9. Suppose r and s are odd. Prove the following:

(a) $\dfrac{rs-1}{2} \equiv \dfrac{r-1}{2} + \dfrac{s-1}{2} \pmod 2$

(b) $r^2 \equiv s^2 \equiv 1 \pmod 8$

(c) $\dfrac{(rs)^2-1}{8} \equiv \dfrac{r^2-1}{8} + \dfrac{s^2-1}{8} \pmod 8$

10. Prove that (k^k) is periodic modulo 3 and find its period.
(*Hint: First try to spot a pattern...*)

3.2 Congruence Equations and Lagrange's Theorem

In this section we consider polynomial congruence equations $p(x) \equiv 0 \pmod{m}$. The simplest type are *linear*: in fact we know how to solve these already.

$$\exists x \in \mathbb{Z} \text{ s.t. } ax \equiv c \pmod{m} \iff \exists x, y \in \mathbb{Z} \text{ s.t. } ax + my = c$$

This last is a linear Diophantine equation; we need only rephrase our work from earlier.

Theorem 3.15. *Let $d = \gcd(a, m)$. The equation $ax \equiv c \pmod{m}$ has a solution iff $d \mid c$. If x_0 is a solution, then all solutions are given by*

$$x = x_0 + k\frac{m}{d} : k \in \mathbb{Z}$$

Moreover, modulo m, there are exactly d solutions, namely

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

Examples 3.16. 1. We solve the congruence equation $15x = 4 \pmod{133}$.

By the Euclidean algorithm/Bézout, we see that

$$\begin{array}{l} \mathbf{133} = 8 \cdot \mathbf{15} + \mathbf{13} \\ \mathbf{15} = 1 \cdot \mathbf{13} + \mathbf{2} \\ \mathbf{13} = 6 \cdot \mathbf{2} + \mathbf{1} \end{array} \implies d = \gcd(15, 133) = \mathbf{1} \begin{array}{l} = \mathbf{13} - 6 \cdot \mathbf{2} = \mathbf{13} - 6(\mathbf{15} - \mathbf{13}) \\ = 7 \cdot \mathbf{13} - 6 \cdot \mathbf{15} \\ = 7(\mathbf{133} - 8 \cdot \mathbf{15}) - 6 \cdot \mathbf{15} \\ = 7 \cdot \mathbf{133} - 62 \cdot \mathbf{15} \end{array}$$

Since $d = 1$ and $d \mid 4$, there is exactly one solution. Moreover, modulo 133, we see that

$$15 \cdot (-62) \equiv 1 \implies 15 \cdot (-248) \equiv 15 \cdot 18 \equiv 4 \pmod{133}$$

whence $x_0 = 18$ is the unique solution.[a]

2. We solve the linear congruence $1288x \equiv 21 \pmod{1575}$.

Assume we have applied the Euclidean algorithm and Bézout's identity to obtain

$$d = \gcd(1575, 1288) = 7 = 1575 \cdot 9 - 1288 \cdot 11$$

Since $7 \mid 21$, there are precisely *seven* solutions. Indeed

$$7 \equiv 1288(-11) \pmod{1575} \implies x = -33 \equiv 1542 \pmod{1575}$$

Moreover, $\frac{m}{d} = \frac{1575}{7} = 225$, whence all solutions are

$$\{x \equiv -33 + 225k : k = 0, \ldots, 6\} = \{192, 417, 642, 867, 1092, 1317, 1542\}$$

[a] Because $\gcd(15, 133) = 1$, we see that 15 is a unit modulo 133. Indeed the Bézout calculation says that its inverse is $15^{-1} \equiv -62 \equiv 71 \in \mathbb{Z}_{133}$. Since $133 = 7 \cdot 19$, the units are precisely those elements which are divisible by neither 7 nor 19.

Higher degree congruences While we were able to give a complete description of the solutions to a linear congruence, for higher order polynomials, things quickly become very messy. We start with a simple example of a quadratic congruence which can easily be solved by inspection.

Example 3.17. Consider the quadratic equation $x^2 + 3x \equiv 0 \pmod{10}$. One can easily check by plugging in the remainders $0, \ldots, 9$ that the solutions to this equation are

$$x \equiv 0, 2, 5, 7 \pmod{10}$$

This is perhaps surprising, since we are used to quadratic equations having at most *two* solutions.

Now consider the same equation modulo the prime divisors of 10. Since $10 \mid d \iff 2 \mid d$ and $5 \mid d$, we see that

$$x^2 + 3x \equiv 0 \pmod{10} \iff \begin{cases} x^2 + 3x \equiv 0 \pmod{2} \\ x^2 + 3x \equiv 0 \pmod{5} \end{cases}$$

By substituting values for x, we easily check that sanity is restored: each congruence now has two solutions!

$$x^2 + 3x \equiv 0 \pmod{2} \iff x \equiv 0, 1 \pmod{2}$$
$$x^2 + 3x \equiv 0 \pmod{5} \iff x \equiv 0, 2 \pmod{5}$$

We can even factorize in the familiar manner:

$$x^2 + 3x \equiv x^2 - x \equiv x(x-1) \pmod{2}$$
$$x^2 + 3x \equiv x^2 - 2x \equiv x(x-2) \pmod{5}$$

Modulo 10, however, we have two distinct factorizations:

$$x^2 + 3x \equiv x(x-7) \equiv (x-2)(x-5) \pmod{10}$$

For general polynomial congruences, the same sort of thing is true. The number of solutions and types of factorizations are more predictable when the modulus is *prime.*

Theorem 3.18 (Lagrange). *Let p be prime and $f(x)$ a polynomial with integer coefficients and degree n modulo p. Then $f(x) \equiv 0 \pmod{p}$ has at most n distinct roots.*

Lagrange's Theorem is useless for congruences such as $x^{39} + 25x^2 + 1 \equiv 0 \pmod{17}$: since there are only 17 distinct values of x to try, the congruence has a maximum of 17 solutions, not 39.

Before proving Lagrange's Theorem, we need one additional ingredient.

Lemma 3.19 (Factor Theorem in $\mathbb{Z}[x]$). *Suppose $f(x)$ is a polynomial with integer coefficients and that $c \in \mathbb{Z}$. Then there exists a unique polynomial $q(x)$, also with integer coefficients, such that*

$$f(x) = (x - c)q(x) + f(c)$$

Moreover, $f(c) = 0$ if and only if $(x - c)$ is a factor of $f(x)$. This is also true modulo any *n.*

Proof. Suppose $f(x) = a_n x^n + \cdots + a_0$ is given. Since $x - c$ is linear, we require $\deg q = n - 1$. Write $q(x) = q_{n-1}x^{n-1} + \cdots + q_0$, let r be constant, and consider

$$\begin{aligned} a_n x^n + \cdots + a_0 &= (x-c)(q_{n-1}x^{n-1} + \cdots + q_1 x + q_0) + r \\ &= q_{n-1}x^n + (q_{n-2} - cq_{n-1})x^{n-1} + \cdots + (q_0 - cq_1)x + r - cq_0 \end{aligned}$$

Equating the coefficients of $1, x, x^2, \ldots, x^n$ yields the $(n+1) \times (n+1)$ linear algebra problem

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} 1 & -c & 0 & & 0 & 0 \\ 0 & 1 & -c & & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ & & & \ddots & \ddots & \\ 0 & 0 & 0 & & 1 & -c \\ 0 & 0 & 0 & & 0 & 1 \end{pmatrix} \begin{pmatrix} r \\ q_0 \\ q_1 \\ \vdots \\ q_{n-2} \\ q_{n-1} \end{pmatrix} \implies \begin{pmatrix} r \\ q_0 \\ q_1 \\ \vdots \\ q_{n-2} \\ q_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & c & c^2 & & c^{n-2} & c^{n-1} \\ 0 & 1 & c & & c^{n-3} & c^{n-2} \\ 0 & 0 & 1 & & c^{n-4} & c^{n-3} \\ & & & \ddots & \ddots & \\ 0 & 0 & 0 & & 1 & c \\ 0 & 0 & 0 & & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix}$$

Since the inverse matrix has integer coefficients, it follows that each q_j and r are uniquely defined integers. Finally, since $f(x) = (x-c)q(x) + r$, evaluation at $x = c$ yields $r = f(c)$. ∎

We are now ready to prove Lagrange: let us first reiterate the crucial observation from the Factor Theorem: for any n,

$$f(c) \equiv 0 \pmod{n} \iff \exists q(x) \text{ such that } f(x) \equiv (x-c)q(x) \pmod{n}$$

Proof of Lagrange. Suppose $f(x) = a_n x^n + \cdots$ is a polynomial with integer coefficients and degree n modulo p: that is, $p \nmid a_n$. Moreover, assume that $f(c_1) \equiv 0 \pmod{p}$. By the factor theorem, there exists a unique polynomial $q_1(x)$ with integer coefficients, such that

$$f(x) = (x - c_1)q_1(x) + f(c_1) \equiv (x - c_1)q_1(x) \pmod{p}$$

Plainly $q_1(x) = a_n x^{n-1} + \cdots$ has degree $n - 1$ modulo p. If $c_2 \not\equiv c_1$ is another root modulo p, then

$$0 \equiv f(c_2) \equiv (c_2 - c_1)q_1(c_2) \implies q_1(c_2) \equiv 0 \pmod{p}$$

The last step is where we need p to be prime.[13] We may therefore factor out $(x - c_2)$ from $q_1(x)$ modulo p, and thus from $f(x)$. Repeating the process, if there are n distinct roots, then $f(x)$ factorizes as

$$f(x) \equiv (x - c_1) \cdots (x - c_n)q_n(x) \pmod{p}$$

where $q_n(x)$ has degree $n - n = 0$: it is necessarily the constant a_n. Finally, if $\xi \not\equiv c_i$ for any i, then

$$f(\xi) \equiv a_n(\xi - c_1) \cdots (\xi - c_n) \not\equiv 0 \pmod{p}$$

since there are no zero divisors in $\mathbb{Z}_p$. We conclude that $f(x) \equiv 0$ has no further roots modulo p. ∎

In fact the ring of polynomials with coefficients in $\mathbb{Z}_p$ has a Euclidean algorithm which can be used to prove a unique factorization theorem: there is only one way to factorize a polynomial modulo p. We won't prove it, but you are welcome to use the fact nonetheless.

[13] $p \mid (c_2 - c_1)q_1(c_2)$ and $\gcd(c_2 - c_1, p) = 1$, whence $p \mid q_1(c_2)$.

Examples 3.20. 1. By testing the values[14] $x \equiv 0, 1, -1 \pmod 7$, we see that

$$f(x) \equiv x^3 - x \pmod 7$$

has these distinct solutions. By Lagrange, it has no other solutions. Indeed this example factorizes very easily

$$f(x) \equiv x(x-1)(x+1)$$

2. Lagrange only says that there are *at most* n solutions modulo p. It is straightforward to check (let $x = 0, 1 \ldots$) that the polynomial $f(x) \equiv x^2 + x + 1 \pmod 2$ has *no solutions.*

3. Factorize $f(x) = x^3 + 2x^2 + 4x + 3$ over $\mathbb{Z}_5$.

   By inspection we see that $x \equiv \pm 1, -2$ are solutions. By Lagrange's Theorem these are the *only* solutions and we can factorize

   $$f(x) \equiv (x-1)(x+1)(x+2) \pmod 5$$

   We know that the factorization is unique and there are no other solutions, but it is worth seeing it played out in stages.

$$\begin{aligned} f(x) &\equiv x^3 + 2x^2 + 4x + 3 \equiv (x-1)(x^2 + 3x + 7) && \text{(spot } x \equiv 1 \text{ and factorize)} \\ &\equiv (x-1)(x^2 + 3x + 2) && \text{(simplify)} \\ &\equiv (x-1)(x+1)(x+2) && \text{(spot } x \equiv -1 \text{ and factorize)} \end{aligned}$$

Aside: How to factorize? If you have trouble factorizing the previous example, here is a simple algorithm. Since $f(1) \equiv 0$, we know that $f(x) \equiv (x-1)q(x)$ for some quadratic $q(x)$.

1. Since we need an x^3 term, the first coefficient of $q(x)$ is plainly x^2:

   $$x^3 + 2x^2 + 4x + 3 \equiv (x-1)(x^2 + \cdots)$$

2. We now have $-x^2$ on the right hand side, but we want $2x^2$. We therefore need to add $3x^2$ by inserting a linear term into $q(x)$:

   $$x^3 + 2x^2 + 4x + 3 \equiv (x-1)(x^2 + 3x + \cdots)$$

3. We now have $-3x$ on the right hand side, but we want $4x$. We therefore add $7x$ by inserting a constant term into $q(x)$:

   $$x^3 + 2x^2 + 4x + 3 \equiv (x-1)(x^2 + 3x + 7)$$

4. Verify that the factorization is correct by multiplying the constants:

   $$x^3 + 2x^2 + 4x + 3 \equiv (x-1)(x^2 + 3x + 7)$$

   Indeed $3 \equiv -7 \pmod 5$ so we're done.

This approach works for any linear division and has the advantage of being able to write down the answer in one line. Of course, you're welcome to write it out using long division!

[14] Plainly $-1 \equiv 2 \pmod 3$: it is simply easier to use 'smaller' representatives when calculating.

Examples 3.21. 1. Find all roots of $f(x) \equiv x^4 + 2x^3 + 2x - 1 \pmod 7$ and factorize.

We start by trying values: plainly $f(0) \equiv -1$ and $f(1) \equiv 4$ are non-zero. However

$$f(2) \equiv 16 + 16 + 4 - 1 \equiv 2 + 2 + 4 - 1 \equiv 0 \pmod 7$$

so we factor out $x - 2$:

$$f(x) \equiv (x-2)(x^3 + 4x^2 + 8x + 18) \equiv (x-2)(x^3 - 3x^2 + x - 3) \pmod 7$$

$x \equiv 3$ is a root of the cubic, so we factor out $x - 3$:

$$f(x) \equiv (x-2)(x-3)(x^2+1) \pmod 7$$

It is easily checked that $x^2 + 1 \equiv 0 \pmod 7$ has no solutions, so we're done.

2. Compare with Example 3.17. Modulo 6 we have a non-unique factorization:

$$f(x) \equiv x^2 - 5x \equiv x(x-5) \equiv (x-2)(x-3) \pmod 6$$

Re-read the proof of Lagrange's Theorem and make sure you understand where the argument fails!

3. Wind all solutions to $x^2 + 14x - 3 \equiv 0 \pmod{18}$. Rather than try all remainders $0, 1, \ldots, 17$, here is a more systematic approach.

If x is a solution, then both

$$\begin{cases} x^2 + 14x - 3 \equiv x^2 - 1 \equiv 0 \pmod 2 \implies x \text{ odd, and,} \\ x^2 + 14x - 3 \equiv x^2 + 5x - 3 \equiv 0 \pmod 9 \implies x^2 + 2x \equiv 0 \pmod 3 \end{cases}$$

Plainly $x \equiv 0, 1 \pmod 3$ (since 3 is prime, this is in line with Lagrange). We therefore try $x \equiv 0, 1, 3, 4, 6, 7 \pmod 9$ and observe that only $x \equiv 6, 7 \pmod 9$ work. We therefore have to solve two different sets of equations:

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 6 \pmod 9 \end{cases} \quad \text{or} \quad \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 7 \pmod 9 \end{cases}$$

We have two sets of simultaneous equations. In general, the Chinese Remainder Theorem (later) can deal with these, but these are so simple that there is no need. For instance

$$x \equiv 6 \pmod 9 \implies x \equiv 6, 15 \pmod{18}$$

Since x must also be odd (and 18 is even), only $x \equiv 15 \pmod{18}$ will do. Similarly, the second simultaneous congruence has solution $x \equiv 7 \pmod{18}$.

4. Find all solutions to $x^3 - 2x + 1 \equiv 0 \pmod{12}$.

We easily spot that $x \equiv 1 \pmod{12}$ is a solution. Are there others? Considering the primes dividing 12 we see that any solution must satisfy

$$x^3 - 2x + 1 \equiv (x-1)(x^2 + x - 1) \equiv 0 \pmod 2 \quad \text{and} \quad \pmod 3.$$

It is clear by inspection that the *only* solutions modulo 2 and 3 are $x \equiv 1$. It follows that any solution must satisfy $x \equiv 1 \pmod 6$. Stepping this up to modulo 12, we should try $x \equiv 1$ and $x \equiv 7 \pmod{12}$. The first is certainly a solution. As for the latter,

$$7^3 - 2 \cdot 7 + 1 \equiv 7 \cdot 49 - 14 + 1 \equiv 7 - 2 + 1 \equiv 6 \pmod{12}$$

It follows that the only solution is $x \equiv 1 \pmod{12}$.

Exercises 3.2 1. Solve the following equations for x, or show that there is no solution:

(a) $3x - 4 \equiv 7 \pmod{11}$

(b) $12x + 5 \equiv 7 \pmod{16}$

(c) $7x - 9 \equiv 5 \pmod{21}$

2. Solve the following polynomial congruence equations modulo a prime.

(a) $x^2 + 4x + 3 \equiv 0 \pmod{11}$

(b) $x^3 - 4x \equiv 0 \pmod{17}$

(c) $x^2 + 4x + 1 \equiv 0 \pmod{13}$

(d) $x^4 + 4x + 2 \equiv 0 \pmod{7}$

(e) $x^3 + x^2 - 2 \equiv 0 \pmod{13}$

(f) $x^3 - 100x \equiv 0 \pmod{997}$

You can solve these by trial and error, but can you do them systematically?

3. Solve the following polynomial congruence equations modulo a composite.

(a) $x^2 + 4x + 5 \equiv 0 \pmod{10}$

(b) $x^2 + 4x + 3 \equiv 0 \pmod{15}$

(c) $x^3 + x^2 - 2 \equiv 0 \pmod{39}$

4. Suppose that $\gcd(a, b) = 1$. Prove that

$$x \equiv 0 \pmod{ab} \iff \begin{cases} x \equiv 0 \pmod{a} \\ x \equiv 0 \pmod{b} \end{cases}$$

What goes wrong when a, b are not coprime?

5. Informally explain why a quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{15}$ has *at most four* distinct solutions.

3.3 Powers and Fermat's Little Theorem

Fermat's Little[15] Theorem provides a useful trick for simplifying large powers in congruences.

Theorem 3.22 (Fermat's Little Theorem). *If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$*

Proof. Recall Exercise 3.2.8, where we saw that the remainders $a, 2a, \ldots, a(p-1)$ are distinct and non-zero: they are simply $1, 2, \ldots, p-1$ in a different order. Multiply these lists together to obtain

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

Since p is prime and $\gcd\big((p-1)!, p\big) = 1$, we divide by $(p-1)!$ for the result. ∎

Examples 3.23. The power of Fermat's Little Theorem to simplify calculations is considerable. Imagine how tedious the following would be without it!

1. Since 239 is not divisible by the prime 137, we instantly see that

$$239^{136} \equiv 1 \pmod{137}$$

2. We compute the remainder when 66^{98} is divided by the prime 97.

$$\begin{aligned} 66^{98} &\equiv 66^{97-1} \cdot 66^2 \equiv 66^2 \pmod{97} \\ &\equiv (-31)^2 \equiv 961 \equiv -9 \\ &\equiv 88 \pmod{97} \end{aligned}$$

3. We solve the high-degree congruence $x^{74} \equiv 12 \pmod{37}$.

   First note that 37 is prime and that if there is a solution x, then it is non-zero. The theorem therefore applies, and we see that

$$x^{37-1} \equiv x^{36} \equiv 1 \pmod{37}$$

   Since $74 = 36 \times 2 + 2$ we conclude that

$$12 \equiv x^{74} \equiv (x^{36})^2 \cdot x^2 \equiv x^2 \pmod{37}$$

   We have therefore reduced the congruence to something much more manageable.

   This new equation can be solved by brute force: by considering numbers congruent to 12 modulo 37, we don't have far to look before we find a perfect square!

$$12,\ 49, \ldots$$

   Thus $x \equiv 7$ is a solution, which says that $x \equiv -7 \equiv 30$ is another. By Lagrange's Theorem, there are at most two solutions to this congruence: we conclude

$$x^{74} \equiv 12 \iff x \equiv 7, 30 \pmod{37}$$

[15] To distinguish it from his famous Last Theorem. The *little* theorem is often abbreviated FℓT, and the *last* FLT.

Riffle-shuffling

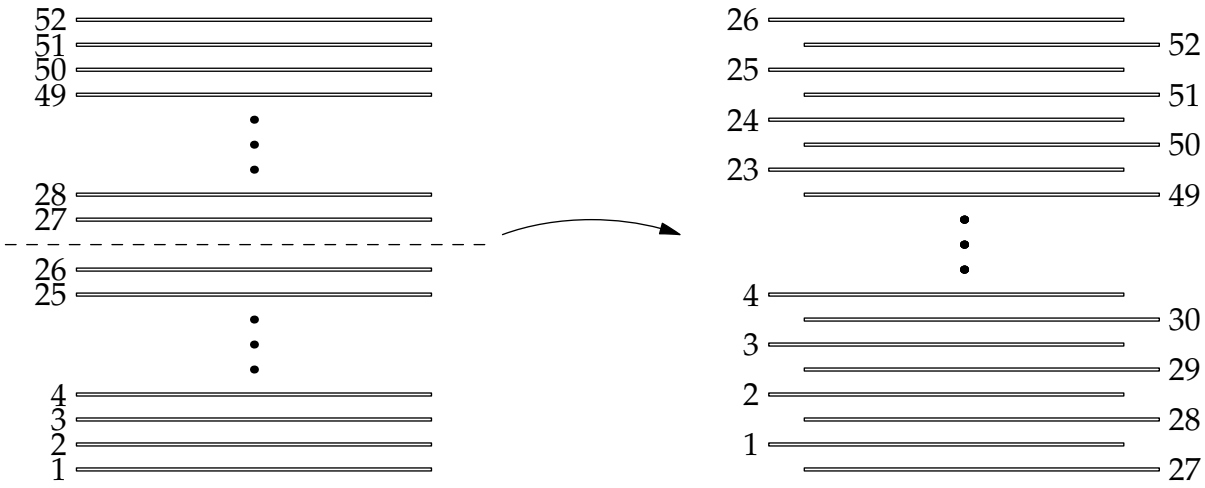
As a fun example of Fermat at work, consider a standard 'riffle' shuffle of a 52-card deck of playing cards. The process is as follows:

- Label the cards $1, 2, 3, \ldots 52$ from bottom to top.
- Cut the deck into two stacks of 26 cards.
- Alternate cards from the bottom of each stack: position x moves to position $s(x)$, where

x	1	2	3	$\cdots$	25	26	27	28	$\cdots$	50	51	52
$s(x)$	2	4	6	$\cdots$	50	52	1	3	$\cdots$	47	49	51

  It is not hard to give a formula to this function:

$$s : \{1, 2, \ldots, 52\} \to \{1, 2, \ldots, 52\} : x \mapsto 2x \pmod{53}$$



We can now ask some simple questions:

1. If we keep perfectly shuffling the pack, will it eventually end up in the starting arrangement and how long with it take?
2. Of all possible arrangements of a deck, how many can be achieved just by shuffling?

Fermat's Little Theorem makes these questions easy to answer:

1. Shuffling n times produces the function

$$s_n : x \mapsto 2^n x \pmod{53}$$

   Since 53 is prime, $s_{52}(x) \equiv 2^{52}x \equiv x \pmod{53}$, whence every card ends up in its starting position after 52 riffle shuffles. It is tedious to check, but in fact this is the *minimum* number of shuffles required.

2. Even though there are $52! \approx 10^{68}$ potential arrangements of 52 cards in a deck, perfect shuffling of a new pack can only result in a comparatively tiny 52 distinct arrangements. Thankfully shuffling is rarely perfect, even when performed by a pro!

You should be able to think up several modifications of this problem, and we'll return to it later…

We finish with another nice result tying together Lagrange and Fermat.

Corollary 3.24 (Wilson's Theorem). *If p is prime then* $(p-1)! \equiv -1 \pmod{p}$

Proof. Consider the polynomial congruence

$$g(x) \equiv (x^{p-1} - 1) - (x-1)(x-2)\cdots\big(x-(p-1)\big) \equiv 0 \pmod{p}$$

- Multiply out and cancel the leading x^{p-1} terms to see that g has degree *at most* $p-2$. Lagrange says that $g(x) \equiv 0$ has *at most* $p-2$ distinct roots.
- Fermat says that $g(x) \equiv 0$ has *at least* $p-1$ distinct roots, namely $x \equiv 1, 2, \ldots, p-1$.

The only way to make sense of this is if $g(x)$ is not really a polynomial! It must be *identically zero* modulo p. It follows that

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots\big(x-(p-1)\big) \pmod{p}$$

Finally, evaluate at $x \equiv 0$ for the result. ∎

If you're having trouble understanding the proof, try an example! When $p = 3$ we have

$$g(x) \equiv x^2 - 1 - (x-1)(x-2) \equiv x^2 - 1 - x^2 + 3x - 2 \equiv 3x - 3 \equiv 0 \pmod{3}$$

The point is that while $g(x)$ might look like it has degree ≤ 1, it is in fact the *zero polynomial*.

Exercises 3.3 1. Solve the following congruences with the assistance of Fermat's Little Theorem.

(a) $x^{86} \equiv 6 \pmod{29}$ (b) $x^{39} \equiv 8 \pmod{13}$ (c) $x^{502} \equiv 16 \pmod{101}$

2. Let p be prime. By describing the *distinct* roots of $x^{p-1} - 1 \equiv 0$ and factorizing, prove that

$$x^{p-1} - 1 \equiv a(x-1)(x-2)\cdots\big(x-(p-1)\big) \pmod{p}$$

for some non-zero $a \in \mathbb{Z}_p$. Hence provide an alternative proof of Wilson's Theorem.

3. Recall the *binomial theorem*: $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$, where $\binom{p}{r} = \frac{p!}{r!(p-r)!}$ (this is an integer[a]).

(a) If p is prime and $1 \leq r \leq p-1$, prove that $p \mid \binom{p}{r}$. Hence prove that

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

(b) For any integers $x_1, \ldots, x_n$, prove that $(x_1 + \cdots + x_n)^p \equiv x_1^p + \cdots + x_n^p \pmod{p}$.

(c) Prove that $a^p \equiv a \pmod{p}$ for all integers a. Hence give an alternative proof of Fermat.

4. (a) Suppose a deck has 30 cards. Argue that riffle shuffling will eventually reset the deck.

(b) How many shuffles do you *really* need when there are 30 cards? *It is a lot less than 30...*

(c) Suppose that a deck has $2m$ cards. What *might* go wrong with the argument?

[a] Can you convince yourself of this? How many ways can you choose r objects from p?

4 Euler's Totient Function

4.1 Euler's Function and Euler's Theorem

Recall Fermat's little theorem:

$$p \text{ prime and } p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$$

Our immediate goal is to think about extending this to *composite* moduli. First let's search for patterns in the powers a^k modulo 6, 7 and 8:

modulo 6

k	1	2	3	4	5
$a=1$	1	1	1	1	1
2	2	4	2	4	2
3	3	3	3	3	3
4	4	4	4	4	4
5	5	1	5	1	5

modulo 7

k	1	2	3	4	5	6
$a=1$	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

modulo 8

k	1	2	3	4	5	6	7
$a=1$	1	1	1	1	1	1	1
2	2	4	0	0	0	0	0
3	3	1	3	1	3	1	3
4	4	0	0	0	0	0	0
5	5	1	5	1	5	1	5
6	6	4	0	0	0	0	0
7	7	1	7	1	7	1	7

The column in red (modulo 7) represents Fermat's little theorem. Unfortunately there don't seem to be many 1's in the other tables: indeed the tables should suggest the following.

Lemma 4.1. *If $k \geq 1$ is such that $a^k \equiv 1 \pmod{n}$, then $\gcd(a,n) = 1$ (a is a unit modulo n).*

The proof is a (hopefully) straightforward exercise.
We turn now to the converse: if $\gcd(a,n) = 1$, can we find k such that $a^k \equiv 1 \pmod{n}$? Again, let's consider the tables and look for patterns:

Modulo 6 The units are $a \equiv 1, 5$. For such a we see that $a^2 \equiv 1 \pmod{6}$.

Modulo 7 Every non-zero remainder is a unit, and $a^6 \equiv 1 \pmod{7}$.

Modulo 8 The units are $a \equiv 1, 3, 5, 7$. For such a we see that $a^2 \equiv 1 \pmod{8}$.

In each case, observe that $a^k \equiv 1$ whenever k is the *number of units*[16] *modulo n.* Given all this, we make a definition and a hypothesis:

Definition 4.2. *Euler's totient function* $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by[17]

$$\varphi(n) = \left|\{0 < a \leq n : \gcd(a,n) = 1\}\right|$$

Theorem 4.3 (Euler's Theorem). *If $\gcd(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

[16] Certainly $a^4 \equiv 1 \pmod{8}$ satisfies this pattern, even though a lower power $k = 2$ does also.

[17] Whenever $n \geq 2$, Euler's function returns the number of units modulo n. The definition is constructed so as to include $\varphi(1) = 1$. In what follows, the $n = 1$ case is always trivial and uninteresting; to avoid tedium we'll assume that $n \geq 2$.

Here are the first few values of Euler's function; we also list the units.

$$\begin{aligned}
\varphi(1) &= 1 = |\{1\}| & \varphi(7) &= 6 = |\{1,2,3,4,5,6\}| \\
\varphi(2) &= 1 = |\{1\}| & \varphi(8) &= 4 = |\{1,3,5,7\}| \\
\varphi(3) &= 2 = |\{1,2\}| & \varphi(9) &= 6 = |\{1,2,4,5,7,8\}| \\
\varphi(4) &= 2 = |\{1,3\}| & \varphi(10) &= 4 = |\{1,3,7,9\}| \\
\varphi(5) &= 4 = |\{1,2,3,4\}| & \varphi(11) &= 10 = |\{1,2,3,4,5,6,7,8,9,10\}| \\
\varphi(6) &= 2 = |\{1,5\}| & \varphi(12) &= 4 = |\{1,5,7,11\}|
\end{aligned}$$

Whenever p is prime, we clearly have $\varphi(p) = p - 1$, from which we see that Fermat's little theorem is merely a special case of Euler's. You should mentally check that the main result holds for several of the values listed above with composite moduli: e.g.

$$4^{\varphi(9)} \equiv 4^6 \equiv 16^3 \equiv (-2)^3 \equiv -8 \equiv 1 \pmod 9$$

Perhaps unsurprisingly, we can prove Euler's theorem analogously to how we proved Fermat's.

Proof. Let a be a unit and let $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n : \gcd(x,n) = 1\}$ be the set of units modulo n. Define $f_a(x) = ax \pmod n$. We claim that $f_a : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ is *bijection* (invertible). This requires two checks:

1. If $x \in \mathbb{Z}_n^\times$, then $f_a(x) = ax$ is also a unit: if neither a nor x have any common divisors with n, then neither does the product ax.
2. Since a is a unit, it has an inverse b. But then $f_a^{-1} = f_b$ as is readily checked: for any x,

$$(f_a \circ f_b)(x) \equiv f_a\big(f_b(x)\big) \equiv a(bx) \equiv (ab)x \equiv x \pmod n$$

Since $f_a : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ is bijective, we may list the units in two ways:

$$\mathbb{Z}_n^\times = \{x_1, x_2, \ldots, x_{\varphi(n)}\} = \{ax_1, ax_2, \ldots, ax_{\varphi(n)}\}$$

Multiply these together to obtain

$$x_1 x_2 \cdots x_{\varphi(n)} \equiv ax_1 ax_2 \cdots ax_{\varphi(n)} \equiv a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \pmod n$$

Since the x_i are all relatively prime to n, we may divide out, thus obtaining the result. ∎

Example 4.4. It should be clear that $\gcd(a,35) = 1 \iff \gcd(a,5) = 1$ and $\gcd(a,7) = 1$, whence the set of units modulo 35 is

$$\mathbb{Z}_{35}^\times = \mathbb{Z}_{35} \setminus \{0,5,10,15,20,25,30,7,14,21,28\} \implies \varphi(35) = 35 - 11 = 24$$

We may now employ this to simplify congruences as we did with Fermat. For instance, suppose you wanted to solve the congruence equation

$$x^{49} \equiv 12 \pmod{35}$$

First observe that if x is a solution and $\gcd(x,35) = d$, then $d \mid 12$ and $d \mid 35$, whence $d = 1$: it follows that x is a unit and we may apply Euler's theorem.

$$x^{24} \equiv 1 \implies x^{49} \equiv x \equiv 12 \pmod{35}$$

Computing Euler's Function

Rather than a laborious direct computation, we follow the classic number-theory approach: worry about primes first, then powers of primes, then glue everything together.

$\varphi(p)$ where p is prime: Since $\mathbb{Z}_p^\times = \{1, \dots, p-1\}$, we plainly have $\varphi(p) = p - 1$.

$\varphi(p^2)$: We want to count the remainders in the set $\{1, 2, 3, \dots, p^2\}$ which are coprime to p^2: this means *deleting the multiples of* p:

$$\varphi(p^2) = \mathbb{Z}_{p^2}^\times = \left|\{1, 2, \dots, p^2\} \setminus \{p, 2p, 3p, \dots, (p-1)p, p^2\}\right| = p^2 - p$$

$\varphi(p^k)$: We again delete the multiples of p:

$$\left|\{1, \dots, p^k\} \setminus \{ap : 1 \le a \le p^{k-1}\}\right| = p^k - p^{k-1} \implies \boxed{\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)}$$

It remains to investigate moduli n which are divisible by more than one prime. Start by looking for patterns in the table of small values on page 37 and observe that

$$\varphi(6) = \varphi(2)\varphi(3), \qquad \varphi(10) = \varphi(2)\varphi(5), \qquad \varphi(12) = \varphi(3)\varphi(4)$$

Moreover, recalling Example 4.4, we see that $\varphi(35) = 24 = 4 \cdot 6 = \varphi(5)\varphi(7)$ also satisfies the pattern! We therefore have a hypothesis.

Theorem 4.5. *Euler's function φ is* multiplicative:

$$\gcd(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$$

There are many simpler examples of multiplicative functions, for instance

$$f(x) = 1, \qquad f(x) = x, \qquad f(x) = x^2$$

though these satisfy the product formula even if m, n are not coprime. The Euler function is more exotic; it really requires the coprime restriction!

Using the unique prime decomposition, the theorem quickly tells us that

$$\varphi(n) = \varphi(p_1^{\mu_1} \cdots p_k^{\mu_k}) = \varphi(p_i^{\mu_1}) \cdots \varphi(p_n^{\mu_k}) = p_1^{\mu_1}(1 - p_1^{-1}) \cdots p_k^{\mu_k}(1 - p_k^{-1})$$

from which we conclude:

Corollary 4.6. $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \frac{p-1}{p}$

We don't need the entire decomposition, only the list of distinct primes dividing n.

Example 4.7.
1. $\varphi(72) = \varphi(8 \cdot 9) = \varphi(2^3 \cdot 3^2) = 72 \cdot \frac{1}{2} \cdot \frac{2}{3} = 24$.
2. $\varphi(1000000) = 1000000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400000$

Proving the multiplicative property is a little awkward. To help follow along, consider listing all the remainders modulo $36 = 9 \times 4$ in a rectangle:

0	1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26
27	28	29	30	31	32	33	34	35

The units (coprime to 36) are distributed in six columns containing two each. By rewriting the table modulo 9 and 4 we can now make an argument for why $\varphi(36) = 12 = 6 \times 2 = \varphi(9)\varphi(4)$:

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

0	1	2	3	0	1	2	3	0
1	2	3	0	1	2	3	0	1
2	3	0	1	2	3	0	1	2
3	0	1	2	3	0	1	2	3

1. The columns being distinct modulo 9, all elements coprime to 9 lie in one of $\varphi(9) = 6$ columns.
2. Each column contains a complete set of remainders modulo 4; exactly $\varphi(4) = 2$ entries in each column are therefore coprime to 4.
3. A remainder is coprime to 36 if and only if it is coprime to both 9 and 4: such must be one of the $\varphi(4)$ entries in one of the $\varphi(9)$ columns of interest. We conclude that $\varphi(36) = \varphi(9)\varphi(4)$.

The proof of the multiplicative property is merely an abstraction of this example.

Proof of Theorem 4.5. If either of m, n are equal to 1, then $\varphi(mn) = \varphi(m)\varphi(n)$ is trivial. We therefore suppose that $\gcd(m, n) = 1$ where $m, n > 1$ and list all the elements of $\mathbb{Z}_{mn}$ in an $n \times m$ table:

$$\begin{array}{cccccc} 0 & 1 & 2 & \cdots & m-1 \\ m & m+1 & m+2 & \cdots & m+(m-1) \\ 2m & 2m+1 & 2m+2 & \cdots & 2m+(m-1) \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)m & (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+(m-1) \end{array}$$

We count the $\varphi(mn)$ entries coprime to mn in a different way, by first observing that

$$\gcd(x, mn) = 1 \iff \gcd(x, m) = 1 = \gcd(x, n)$$

In the first row of the table there are $\varphi(m)$ entries coprime to m. Since each column is congruent modulo m, the entries coprime to m consist precisely of everything in these $\varphi(m)$ columns.

Now consider the j^{th} column: $j, m+j, 2m+j, \ldots, (n-1)m+j$. Since $\gcd(m, n) = 1$, no two of these elements are congruent modulo n:

$$km + j \equiv lm + j \implies km \equiv lm \implies k \equiv l \pmod{n}$$

Each column consists of a complete set of remainders modulo n, and so $\varphi(n)$ of the entries in each column are coprime to n.

Putting this together, we have $\varphi(m)$ columns coprime to m, each of which contains $\varphi(n)$ entries coprime to n: thus $\varphi(m)\varphi(n)$ entries in the full table are coprime to both m and n. ∎

Example 4.8. As a nice example of the formula, we find all n such that $\varphi(n) = 6 = 2 \cdot 3$.

Writing $n = p_1^{\mu_1} \cdots p_k^{\mu_k}$, we see that $2 \cdot 3 = p_1^{\mu_1 - 1} \cdots p_k^{\mu_k - 1}(p_1 - 1) \cdots (p_k - 1)$. The divisors of 6 are $1, 2, 3, 6$: if one greater than these is prime, that prime might also be a divisor of n: thus we need also consider *at most* one factor of 7: $n = 2^a 3^b 7^c$ where $a, b \geq 0$ and $c = 0, 1$. Now compute all the possibilities:

$$2 \cdot 3 = \varphi(n) = \binom{2^{a-1}}{1} \cdot \binom{2 \cdot 3^{b-1}}{1} \cdot \binom{6}{1}$$

where we must take one factor from each pair (the bottom row corresponds to $a, b, c = 0$). It is not hard to check that only ways to make 6 are

- $\varphi(n) = 1 \cdot 1 \cdot 6 \implies n = 2^0 3^0 7^1 = 7$
- $\varphi(n) = 2^{1-1} \cdot 1 \cdot 6 \implies n = 2^1 3^0 7^1 = 14$
- $\varphi(n) = 1 \cdot (2 \cdot 3^{2-1}) \cdot 1 \implies n = 2^0 3^2 7^0 = 9$
- $\varphi(n) = 2^{1-1} \cdot (2 \cdot 3^{2-1}) \cdot 1 \implies n = 2^1 3^2 7^0 = 18$

Counting residues Euler's function records how many integers in $\mathbb{Z}_n$ are relatively prime to n. What about counting residues with other gcd's with n? Euler's function does this as well.

Lemma 4.9. *If $d \mid n$, then $\varphi\left(\frac{n}{d}\right)$ residues a satisfy $\gcd(a, n) = d$.*

Proof. Start by observing that $\gcd(a, n) = d \iff \gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$. However, by definition, $\varphi\left(\frac{n}{d}\right)$ of the values $1 \leq \frac{a}{d} \leq \frac{n}{d}$ are coprime to $\frac{n}{d}$. ∎

Example 4.10. There are $\varphi(\frac{136}{4}) = \varphi(34) = 16$ integers $1 \leq a \leq 136$ for which $\gcd(136, a) = 4$. Indeed these are precisely

$$4, 12, 20, 28, 36, 44, 52, 60, 68, 76, 84, 92, 100, 108, 116, 132$$

More surprising perhaps is what happens when you sum the value of Euler's function over all divisors of an integer.

Theorem 4.11. *Summing over all* positive *divisors d of n, we obtain* $\sum_{d \mid n} \varphi(d) = n$

Proof. Partition $\{1, \ldots, n\}$ into subsets according to the gcd of each with n. By Lemma 4.9, this $\gcd(a, n) = d$ for exactly $\varphi\left(\frac{n}{d}\right)$ of the numbers. Hence

$$\sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = n$$

since we've counted the whole set! Since the values $\frac{n}{d}$ are simply the divisors of n listed in the reverse order to d, the sums must be identical: $\sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = \sum_{d \mid n} \varphi(d)$. ∎

Example 4.12. With $n = 28$, we verify that

$$\begin{aligned}\sum_{d|28} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(4) + \varphi(7) + \varphi(14) + \varphi(28) \\ &= 1 + 1 + 2 + 6 + 6 + 12 = 28\end{aligned}$$

Exercises 4.1

1. Find the values of $\varphi(97)$ and $\varphi(8800)$.
2. Prove Lemma 4.1.
3. (a) If $n \geq 3$, explain why $\varphi(n)$ is always even.
   (b) Find all values n for which $\varphi(n)$ is not divisible by 4.
4. Find all n such that $\varphi(n)$ is the indicated value:
   (a) $\varphi(n) = 10$ (b) $\varphi(n) = 12$ (c) $\varphi(n) = 20$ (d) $\varphi(n) = 100$
5. Find all values n that solve each of the following equations. If there are none, explain why.
   (a) $\varphi(n) = \frac{n}{2}$ (b) $\varphi(n) = \frac{n}{3}$ (c) $\varphi(n) = \frac{n}{6}$

   For an extra challenge, find all n for which $\varphi(n) \,|\, n$.
6. Show that if $d \,|\, n$ then $\varphi(d) \,|\, \varphi(n)$.
7. Suppose $\gcd(a, b) = d$. Use prime decompositions to prove that $\varphi(ab) = \dfrac{d\varphi(a)\varphi(b)}{\varphi(d)}$
8. (A challenge!) Show that $\displaystyle\sum_{d|n}(-1)^{n/d}\varphi(d) = \begin{cases} 0 & \text{if } n \text{ even} \\ -n & \text{if } n \text{ odd} \end{cases}$

   (*Hint: write $n = 2^k m$ where m is odd and take the $k = 0, \geq 1$ cases separately*)
9. A unit $x \in \mathbb{Z}_n$ (i.e. $\gcd(x, n) = 1$) is a *primitive root* modulo n if the *smallest* exponent k such that $x^k \equiv 1 \pmod{n}$ is $k = \varphi(n)$.
   (a) Find a primitive root modulo 7. Modulo 14.
   (b) Show that 8 does not have any primitive roots.
   (c) If x is a primitive root modulo n, prove that the set of units in $\mathbb{Z}_n$ is given by $\{x, x^2, \ldots, x^{\varphi(n)}\}$
10. Recall the discussion of riffle-shuffling from the previous chapter.
    (a) Show that repeatedly shuffling a pack of $2m$ cards always eventually returns the pack to its initial position.
    (b) Let $n \geq 1$ be the minimum number of shuffles required to return the deck to its original order.
        i. Compute n when $2m = 4, 6, 8, 10, 12, 14$.
        ii. Prove that $n \,|\, \varphi(2m + 1)$.
        (*Hint: apply the division algorithm to $\varphi(2m + 1)$ and n*)
    (c) Investigate what happens if you try to shuffle an odd number of cards. Or if you shuffle so that the bottom card (labelled 1) starts on the bottom?

4.2 The Chinese Remainder Theorem

In this section we see how to solve *simultaneous* congruence equations. This is straightforward to see with a small example.

Example 4.13. Solve the simultaneous congruences

$$\begin{cases} x \equiv 4 \pmod{50} \\ x \equiv 15 \pmod{33} \end{cases}$$

Any solution x simultaneously satisfies $x = 4 + 50k = 15 + 33l$ for some integers k, l. Applying the Euclidean algorithm (or invoking divine intervention), we see that

$$(k, l) = (22, -33) \quad \text{satisfies} \quad 50k + 33l = 11$$

whence $x = 4 + 50 \cdot 22 = 1104$ solves the congruences.

We can say a little more, since we know that all suitable k satisfy $k = 22 + 33t$ for some $t \in \mathbb{Z}$, and so all solutions x have the form

$$x = 4 + 50(22 + 33t) = 1104 + 50 \cdot 33t \equiv 1104 \pmod{1650}$$

We therefore have a *unique* solution modulo the product of the original moduli.

This pattern holds in general, *provided the moduli are coprime.*

- Suppose $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. Otherwise said,

$$\exists k, l \in \mathbb{Z} \text{ such that } x = a + km = b + ln \implies km - ln = b - a$$

- Since $\gcd(m, n) = 1$, we can find suitable k, l using Bézout's identity: if $\kappa m + \lambda n = 1$, then

$$\begin{aligned} & (b-a)\kappa m + (b-a)\lambda n = b - a \\ \implies & k = (b-a)\kappa + nt : t \in \mathbb{Z} \\ \implies & x = a + ((b-a)\kappa + nt)m \equiv a + (b-a)\kappa m \pmod{mn} \\ & \equiv a(1 - \kappa m) + b\kappa m \equiv a\lambda n + b\kappa m \pmod{mn} \end{aligned} \tag{$*$}$$

Not only do we see that the simultaneous congruence has a unique solution modulo mn, but we have a nice formula for evaluating it. Before seeing the full result, note that our abstract expression $(*)$ for x really does satisfy both congruences:

$$\begin{cases} a\lambda n + b\kappa m \equiv a\lambda n \equiv a \pmod{m} \\ a\lambda n + b\kappa m \equiv b\kappa m \equiv b \pmod{n} \end{cases}$$

The observation is that $\lambda n \equiv 1 \pmod{m}$ and $\kappa m \equiv 1 \pmod{n}$; that is, we have *inverses* for m and n *modulo each other.*

Theorem 4.14 (Chinese Remainder Theorem). *Suppose that moduli $n_1, \ldots, n_k$ are* pairwise coprime[a]*. Then the simultaneous congruences*

$$x \equiv b_1 \pmod{n_1}, \quad x \equiv b_2 \pmod{n_2}, \quad \ldots \quad x \equiv b_k \pmod{n_k} \tag{†}$$

have a unique solution modulo $N := n_1 \cdots n_k$. Specifically, for each i, define $N_i = \frac{N}{n_i}$ and compute its inverse $\lambda_i N_i \equiv 1 \pmod{n_i}$, then

$$x \equiv b_1\lambda_1 N_1 + b_2\lambda_2 N_2 + \cdots + b_k\lambda_k N_k \pmod{N}$$

[a] $\gcd(n_i, n_j) = 1$ whenever $i \neq j$

Proof. Plainly $\gcd(N_i, n_i) = 1$ since $N_i = \frac{N}{n_i}$ is the product of all coprime moduli $n_1 \cdots n_k$ *except* n_i. Bézout's identity says N_i has an inverse λ_i modulo n_i. Moreover, since $j \neq i \implies n_j \mid N_i$, we have

$$\lambda_i N_i \equiv \begin{cases} 0 \pmod{n_j} & \text{if } i \neq j \\ 1 \pmod{n_i} \end{cases}$$

It is now immediate that the advertised x solves all the congruences (†).

Finally suppose that y also solves the congruences. Then $x - y \equiv 0 \pmod{n_i}$ for all i which, since the n_i are pairwise coprime, forces $x \equiv y \pmod{N}$. ∎

Examples 4.15. 1. First we revisit Example 4.13 in this language.

$$x \equiv 4 \pmod{50}, \qquad x \equiv 15 \pmod{33}$$

The moduli 50 and 33 are pairwise coprime so the theorem applies. We compute

$$N = 50 \cdot 33 = 1650, \qquad N_1 = 33, \qquad N_2 = 50 \qquad (N_1 = \tfrac{mn}{m} = n \text{ and } N_2 = m \text{ in } (*))$$

We must therefore solve:

$$\begin{cases} 33\lambda_1 \equiv 1 \pmod{50} \implies \lambda_1 \equiv -3 \\ 50\lambda_2 \equiv 1 \pmod{33} \implies \lambda_2 \equiv 2 \end{cases} \qquad (\lambda_1 = \lambda \text{ and } \lambda_2 = \kappa \text{ in } (*))$$

Finally,

$$x \equiv b_1\lambda_1 N_1 + b_2\lambda_2 N_2 \equiv 4 \cdot (-3) \cdot 33 + 15 \cdot 2 \cdot 50 \equiv 1500 - 396 \equiv 1104 \pmod{1650}$$

2. Find all solutions $x \in \mathbb{Z}$ to the simultaneous congruences

$$x \equiv 3 \pmod{5}, \quad x \equiv 5 \pmod{7}, \quad x \equiv 2 \pmod{8}$$

Since the moduli 5, 7 and 8 are pairwise coprime the theorem applies and we compute:

$$N = 5 \cdot 7 \cdot 8 = 280, \qquad N_1 = 56, \qquad N_2 = 40, \qquad N_3 = 35$$

$$\implies \begin{cases} 56\lambda_1 \equiv 1 \pmod{5} \implies \lambda_1 \equiv 1 \\ 40\lambda_2 \equiv 1 \pmod{7} \implies \lambda_2 \equiv 3 \\ 35\lambda_3 \equiv 1 \pmod{8} \implies \lambda_3 \equiv 3 \end{cases}$$

$$\implies x \equiv 3 \cdot 1 \cdot 56 + 5 \cdot 3 \cdot 40 + 2 \cdot 3 \cdot 35 \equiv 978 \equiv 138 \pmod{280}$$

Non-coprime moduli?

We state without proof the following generalization of the Chinese Remainder Theorem.

Corollary 4.16. *A system of congruences* (†) *may be solved if and only if* $\gcd(n_i, n_j) \mid (b_i - b_j)$ *for all* $i \neq j$. *In such a case, all solutions are congruent modulo* $\operatorname{lcm}(n_1, \ldots, n_k)$.

The method is essentially to remove superfluous congruences so that we can apply the Chinese Remainder Theorem.

Example 4.17. The corollary applies to the simultaneous congruences

$$x \equiv 1 \pmod 3, \qquad x \equiv 2 \pmod 4, \qquad x \equiv 8 \pmod{10}$$

the only divisor property we need to check being $\gcd(4, 10) \mid (2 - 8)$.
The final congruence holds if and only if $x \equiv 0 \pmod 2$ and $x \equiv 3 \pmod 5$. The first condition is unnecessary since it follows from $x \equiv 2 \pmod 4$. We therefore solve the congruence system

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \end{cases} \implies x \equiv 58 \pmod{60} \qquad (\ddagger)$$

using the standard Chinese remainder theorem. Note that the modulus is $60 = \operatorname{lcm}(3, 4, 10)$.

Exercises 4.2

1. Find the solutions to the following simultaneous congruences using the Chinese remainder theorem.
   (a) $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 9$
   (b) $x \equiv 1 \pmod 4$, $x \equiv 4 \pmod{15}$
2. (a) Do the calculations to solve the simultaneous triple congruence (‡) in Example 4.17.
   (b) Solve the triple congruence
   $$x \equiv 3 \pmod 4, \quad x \equiv 5 \pmod{21}, \quad x \equiv 7 \pmod{25}$$
   (c) Solve the triple congruence (*be careful!*)
   $$3x \equiv 9 \pmod{12}, \quad 4x \equiv 5 \pmod{35}, \quad 6x \equiv 2 \pmod{11}$$
3. Give x explicitly in terms of $b_1, \ldots, b_4$ if
   $$x \equiv b_1 \pmod 2, \qquad x \equiv b_2 \pmod 3, \qquad x \equiv b_3 \pmod 5, \qquad x \equiv b_4 \pmod 7$$
4. Find the solutions: note the generalized Corollary 4.16.
   (a) $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 7 \pmod{10}$
   (b) $x \equiv 1 \pmod{12}$, $x \equiv 4 \pmod{21}$, $x \equiv 18 \pmod{35}$
5. Solve $x^3 - x + 15 \equiv 0 \pmod{63}$.
   (*Don't just list solutions! Consider modulo 7 and 9 then use the Chinese remainder theorem*)
6. Prove the ($\Rightarrow$) direction of Corollary 4.16: if the system has a solution, then $\gcd(n_i, n_j) \mid (b_i - b_j)$.

5 Primes

5.1 The Distribution of the Set of Primes

Given the usefulness of primes as the 'building blocks' of the integers, we naturally want to investigate how they are distributed: we'd like answers to questions such as the following.

1. How many primes are there?
2. How many primes are there with a certain property? (e.g. congruent to 3 modulo 4)
3. If we have discovered the first n primes, how much larger is the next?
4. Can we write every even integer ≥ 4 as a sum of two primes?
5. Are there infinitely many primes p such that $p+2$ is also prime?
6. Does there exist at least one prime between any consecutive squares?
7. Are there infinitely many primes of the form N^2+1?

The first three questions can, more or less, be answered, whereas the remaining four are famous conjectures (the Goldbach, Twin Prime, Legendre's and N^2+1 conjectures respectively) that have remained unsolved for over a century.[18]

The first question has the oldest answer: we earlier saw Euclid's Theorem stating that there are infinitely many primes. We can extend his approach to other situations. For example, it is clear that any prime $p \geq 3$ cannot be even and must therefore be congruent to 1 or 3 modulo 4. Consider the following table of the primes p such that $3 \leq p \leq 120$, arranged by remainder modulo 4:

$p \equiv 1 \pmod 4$	5	13	17	29	37	41	53	61	73	89	97	101	109	113	$\cdots$	
$p \equiv 3 \pmod 4$	3	7	11	19	23	31	43	47	59	67	71	79	83	103	107	$\cdots$

It appears that the primes are fairly evenly distributed between the two classes, and we might reasonably conjecture that there are infinitely many primes of each type. This is indeed the case.

Theorem 5.1. *Infinitely many primes are congruent each to 1 and 3 modulo 4.*

Proof of half the Theorem. We modify Euclid's proof. Suppose that there are finitely many primes congruent to 3 modulo 4: list them as $3, p_1, \ldots, p_n$ and define

$$\Pi := 4p_1p_2p_3 \cdots p_n + 3$$

Certainly $\Pi \equiv 3 \pmod 4$ and therefore odd, so all primes dividing it are odd. Note that

$$x, y \equiv 1 \pmod 4 \implies xy \equiv 1 \pmod 4 \qquad (*)$$

hence, if all primes dividing Π were congruent to 1, so also would be Π. Plainly Π is divisible by some prime $p \equiv 3 \pmod 4$. By assumption we have all of these, and there are two possibilities:

1. $p = 3$ from which $3 \mid 4p_1p_2p_3 \cdots p_n \implies 3 \mid p_i \implies p_i = 3$ for some i; a contradiction.
2. $p = p_i$ for some i, in which case $p \mid 3 \implies p = 3$; again a contradiction.

■

[18] Several results which are very close to these have been proved recently, for example the weak Goldbach conjecture states that every odd integer ≥ 9 is the sum of three odd primes was proved in 2013.

Before moving on, consider why the proof cannot be modified to show that infinitely many primes are congruent to 1 modulo 4. One issue is that the corresponding proposition to $(*)$ is false: in fact

$$x, y \equiv 3 \pmod 4 \implies xy \equiv 1 \pmod 4!$$

and we cannot therefore claim that any $\Pi \equiv 1$ (or $\equiv 3$) is divisible by a prime congruent to 1. Indeed:

- $\Pi := 21 = 3 \cdot 7 \equiv 1 \pmod 4$ is not divisible by any primes congruent to 1.
- $\Pi := 3 \cdot 7 \cdot 11 = 231 \equiv 3 \pmod 4$ is not divisible by any primes congruent to 1.

A simple proof of the $\equiv 1$ part of the Theorem will be given later using quadratic residues.
In fact a much harder and more general result is available.

Theorem 5.2 (Dirichlet). *If* $\gcd(a, m) = 1$, *then infinitely many primes* p *satisfy* $p \equiv a \pmod m$.

Counting Primes Now we turn to the third in our list of questions. To think about this, we introduce the concept of a *counting function*: a function $f : \mathbb{N} \to \mathbb{N}_0$ for which $f(x)$ is the number of positive integers less or equal to x satisfying some property. Euler's totient function φ is an example:

$$\varphi(x) = |\{n \in \mathbb{N}_{\leq x} : \gcd(x, n) = 1\}|$$

Here is another.

Example 5.3. Consider the counting function

$$f(x) = |\{n \in \mathbb{N}_{\leq x} : n \equiv 4 \pmod 7\}|$$

To get a feel for f, compute the first few values:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$f(x)$	0	0	0	1	1	1	1	1	1	1	2	2	2	2	2	2	2	3	3	3

It seems reasonable to claim that, for large x, $f(x)$ is approximately a seventh of x. More precisely,

$$\frac{x-3}{7} \leq f(x) < \frac{x+4}{7} \implies \frac{x-3}{7x} \leq \frac{f(x)}{x} < \frac{x+4}{7x} \overset{\text{Squeeze}}{\underset{\text{Thm}}{\Longrightarrow}} \lim_{x\to\infty} \frac{f(x)}{x} = \frac{1}{7}$$

There is terminology for this: '$f(x)$ is *asymptotic to* $\frac{1}{7}x$,' and we write

$$f(x) \sim \frac{1}{7}x$$

Intuitively, $f(x)$ *grows like* $\frac{1}{7}x$. This is one way of giving precision to the statement, 'one seventh of the integers are congruent to 4 modulo 7.'

Armed with our new notation, we consider the asymptotic behavior of the primes.

Definition 5.4. $\pi(x) := |\{p : p \leq x\}|$ is the number of primes less than x.

Theorem 5.5 (Prime number theorem). $\pi(x) \sim \frac{x}{\ln x}$. *Otherwise said,* $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$.

A proof is too involved for this course; interpreting the result is tough enough! One approach involves probability: the chance of a random integer in the interval $[1, x]$ being prime is

$$\mathbb{P}\big(y \in [1,x] \text{ prime}\big) = \frac{\pi(x)}{x} \approx \frac{1}{\ln x}$$

While the expression $\frac{x}{\ln x}$ estimates the function $\pi(x)$, it is, in fact, always an under-estimate. A more accurate estimate involves an integral, albeit one that needs its own estimation!

$$\pi(x) \sim \int_2^x \frac{1}{\ln t}\mathrm{d}t$$

Example 5.6. To check the veracity of these claims: consider the 1000^{th} prime $p_{1000} = 7919$:

$$\pi(7919) = 1000, \qquad \frac{7919}{\ln 7919} \approx 882, \qquad \int_2^{7919} \frac{1}{\ln t}\mathrm{d}t \approx 1016$$

A little extra algebra tells us that the n^{th} prime should be located around $p_n \approx n \ln n$. Indeed $1000 \ln 1000 \approx 6908$, which is a 13% under-estimate.

Exercises 5.1 1. (a) Verify that every even number between 70 and 80 is a sum of two primes.

(b) How many different ways can 70 be written as a sum of two primes $70 = p + q$ with $p \leq q$? Repeat the question for 80.

2. (a) Show that if $p \geq 5$ is prime, then $p \equiv \pm 1 \pmod 6$.

(b) Mimic the half-proof of Theorem 5.1 to show that there are infinitely many primes congruent to 5 modulo 6.
(*Hint: let* $\Pi := 6p_1p_2\cdots p_n + 5$ *where* $p_1, \ldots, p_n \equiv 5 \pmod 6$)

3. (a) Explain the statement "one-fifth of all numbers are congruent to 2 modulo 5" by using the counting function

$$F(x) = |\{\text{positive numbers } n \leq x \text{ satisfying } n \equiv 2 \pmod 5\}|$$

(b) Explain the statement "most numbers are not squares" by using the counting function

$$S(x) = |\{\text{square numbers less than } x\}|$$

4. Let n be large. By computing $\frac{x}{\ln x}$ when $x = n \ln n$, argue that $p_n \approx n \ln n$ is a reasonable estimate for the value of the n^{th} prime. Use this expression to argue that, for large n,

$$p_{n+1} - p_n \approx 1 + \ln(n+1)$$

Comment on the values of p_{1000} and p_{1001}.

5. (Hard) Let p be an odd prime and consider the quantity

$$\frac{A_p}{B_p} := 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{p-1} \quad \text{where} \quad \gcd(A_p, B_p) = 1$$

(a) Find the value of $A_p \pmod p$ and prove that your answer is correct.

(b) (Even harder - also proves part (a)) Make a conjecture for $A_p \pmod{p^2}$ and prove it.
(*Hint: try adding* $\frac{1}{k} + \frac{1}{p-k}$ *in pairs*)

5.2 Mersenne Primes and Perfect Numbers

While Euclid assures us that the set of primes is infinite, this hasn't prevented a semi-formal competition to find the *largest known prime.* Prior to the advent of computers and mechanical calculators, the largest verified prime had 39 digits. As of early 2022, the largest known prime is $2^{82,589,933} - 1$ with 24,862,048 digits! Such primes have a special name.

Definition 5.7. A *Mersenne prime* is a prime of the form $M_p = 2^p - 1$ where p is itself prime.

These are named for Marin Mersenne, a 17th century French music theorist, mathematician and priest.

Examples 5.8. $M_2 = 2^2 - 1 = 3$, $M_3 = 2^3 - 1 = 7$, $M_5 = 2^5 - 1 = 31$, $M_7 = 2^7 - 1 = 127$. Not all Mersenne numbers are prime, for instance

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$$

In fact most Mersenne numbers are not prime; the current largest known prime is only the 51st Mersenne prime to be discovered! It is merely conjectured that there are infinitely many of them.

Whenever the 'world's largest prime' is announced, it is usually a Mersenne prime.[19] There are several reasons for this: a simple motivator is the fact that exponentiation quickly provides large candidates. A related reason is that similar-looking numbers with other bases are never prime:

Theorem 5.9. *If $P = a^n - 1$ is prime for some $a, n \geq 2$, then $a = 2$ and n is prime: that is, P is a Mersenne prime.*

Proof. If $a \geq 3$, then

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$$

is composite. By a similar factorization, if $n = mk$ is composite, so also is $2^n - 1$:

$$2^n - 1 = (2^m)^k - 1 = (2^m - 1)((2^m)^{k-1} + (2^m)^{k-2} + \cdots + 1)$$

■

There are many known results about Mersenne primes; look them up if you are interested. We now turn our attention to an old problem which turns out to be related to Mersenne primes, using it partly as an excuse to introduce another commonly-used function.

Definition 5.10. Let $n \in \mathbb{N}$. Define $\sigma(n) = \sum_{d|n} d$ to be the sum of the (positive) divisors of n.

We say that n is *perfect* if it equals the sum of its proper (positive) divisors: that is

$$\sigma(n) = 2n \quad (= \text{proper divisors} + n)$$

Examples 5.11. $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$ are both perfect.

[19] The Great Internet Mersenne Prime Search is an ongoing collaborative project hunting for such: anyone with a computer can sign up. If you're the first to find a prime with 100 million digits, $100,000 could be yours!

We can compute $\sigma(n)$ similarly to how we evaluated Euler's function. First observe a simple fact following from unique prime factorization:

If $\gcd(m,n)=1$ and $d \mid mn$, then $d = d_1 d_2$ is *uniquely* a product of divisors $d_1 \mid m$ and $d_2 \mid n$

(prime factorization!). When m, n are coprime, it is now immediate that

$$\sigma(mn) = \sum_{d \mid mn} d = \sum_{d_1 \mid m,\, d_2 \mid n} d_1 d_2 = \sum_{d_1 \mid m} d_1 \cdot \sum_{d_2 \mid n} d_2 = \sigma(m)\sigma(n)$$

Moreover, the geometric series formula allows us to easily compute σ applied to a prime power:

$$\sigma(p^\mu) = \sum_{j=0}^{\mu} p^j = \frac{p^{\mu+1}-1}{p-1}$$

and we've now proved the main result:

Theorem 5.12. *σ is multiplicative. Moreover, if $n = p_1^{\mu_1} \cdots p_k^{\mu_k}$ is the prime decomposition of n, then*

$$\sigma(n) = \prod_{j=1}^{k} \frac{p_j^{\mu_j+1}-1}{p_j-1}$$

Examples 5.13. The sum of the positive divisors of $260 = 2^2 \cdot 5 \cdot 13$ is

$$\sigma(260) = \frac{2^3-1}{1} \cdot \frac{5^2-1}{4} \cdot \frac{13^2-1}{12} = 588$$

This can tediously be checked since 260 has divisors 1, 2, 4, 5, 10, 13, 20, 26, 52, 65, 130, 260.
Repeating with $n = 1000 = 2^3 \cdot 5^3$, we see that

$$\sigma(1000) = \frac{2^4-1}{2-1} \cdot \frac{5^4-1}{5-1} = 2340$$

There is an intimate relation between perfect numbers and Mersenne primes: half of it indeed appears in Euclid's *Elements*.

Theorem 5.14. *If $2^p - 1$ is a Mersenne prime, then $2^{p-1}(2^p-1)$ is perfect.*

Proof. Suppose that $M_p = 2^p - 1$ is a Mersenne prime. Since $2^p - 1$ is prime,

$$\sigma(M_p) = \sigma(2^{p-1})\sigma(2^p-1) = \frac{2^p-1}{2-1} \cdot (2^p - 1 + 1) = 2 \cdot 2^{p-1}(2^p-1) = 2M_p$$

■

For small values of p we have the following table: the numbers increase very quickly!

p	$2^p - 1$	$n = 2^{p-1}(2^p - 1)$
2	3	$6 = 1 + 2 + 3$
3	7	$28 = 1 + 2 + 4 + 7 + 14$
5	31	$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$
7	127	$8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064$
13	8191	33,550,336
17	131,072	8,589,869,056

It was conjectured in the middle ages and proved in the 1700's that all *even* perfect numbers have this form.

Theorem 5.15 (Euler). *Every even perfect number has the form $2^{p-1}(2^p - 1)$ for some Mersenne prime $M_p = 2^p - 1$.*

Proof. Suppose that $n = 2^k m$ is an even perfect number, where $k \geq 1$ and m is odd. Our goal is to prove that *m is prime;* we will do this by showing that $\sigma(m) = m + 1$.

Since n is perfect and $\gcd(2^k, m) = 1$, we have two expressions for $\sigma(n)$:

$$\sigma(n) = \begin{cases} 2n = 2^{k+1}m \\ \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m) \end{cases} \implies (2^{k+1} - 1)\sigma(m) = 2^{k+1}m$$

Since $2^{k+1} - 1$ is odd, we see that $2^{k+1} \mid \sigma(m)$ so that $\sigma(m) = 2^{k+1}\alpha$ for some $\alpha \in \mathbb{N}$. We now have

$$(2^{k+1} - 1)\alpha = m$$

If we can show that $\alpha = 1$ then we are finished: in such a case

$$\sigma(m) = 2^{k+1} = (2^{k+1} - 1) + 1 = m + 1$$

whence m is prime.

To obtain a contradiction, assume that $\alpha > 1$. Then m is divisible by the distinct divisors $1, \alpha, m$. But then

$$2^{k+1}\alpha = \sigma(m) \geq 1 + \alpha + m = 1 + \alpha + (2^{k+1} - 1)\alpha = 1 + 2^{k+1}\alpha$$

Contradiction!

We conclude that $m = 2^{k+1} - 1$ is prime. By Theorem 5.9 we see that $k + 1 = p$ must also be prime, whence $m = M_p$ is a *Mersenne prime.* ∎

Since only fifty-one Mersenne primes have thus far been discovered, only fifty-one perfect numbers are known to exist, with the currently known largest having 49,724,095 digits! Of course the conjectured infinity of Mersenne primes would also imply the existence of infinitely many even perfect numbers. It remains unknown whether there are any *odd* perfect numbers.

Exercises 5.2 1. Prove that p is prime if and only if $\sigma(p) = p + 1$.

2. Suppose that $M_p = 2^p - 1$ is a Mersenne prime. List all the divisors of $2^{p-1}(2^p - 1)$ and use the geometric sequence formula to explicitly sum them. Hence provide a more explicit proof of Theorem 5.14.

3. Define $\tau(n)$ to be the number of positive divisors of n. Prove that τ is multiplicative and find a formula for $\tau(n)$ in terms of the prime decomposition of $n = p_1^{\mu_1} \cdots p_k^{\mu_k}$. Hence or otherwise, find the number of positive divisors of 1,000,000.

4. If $a^n + 1$ is prime for some integers $a \geq 2$ and $n \geq 1$, show that n must be a power of 2.

   (*Hints: if n is odd, show that $(a+1) \mid (a^n + 1)$ similarly to the proof of Theorem 5.14. Then write $n = 2m$, $a^2 = b$ and repeat...*)

5. Primes of the form $F_k = 2^{2^k} + 1$ are called *Fermat primes*.[20] For instance

   $$F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

   (a) If $k \geq 2$, prove that the final digit of F_k is 7.
   (*Hint: Think modulo 2 and 5. What is the period of 2^m modulo 5?*)

   (b) Show that if $k \neq m$, then F_k and F_m are coprime.
   (*Hint: if $k > m$, show that F_m divides $F_k - 2$*)

6. Suppose $n \mid M_p$ where p is an odd prime. Prove that $n = 2kp + 1$ for some integer k.

   (*Hint: if q is a prime divisor of $2^p - 1$, think about why p should divide $q - 1$*)

   The remaining questions consider the potential impossibility of odd perfect numbers.

7. (a) Show that a power of 3 can never be a perfect number.
   (b) More generally, if p is an odd prime, show that p^k is not perfect.

8. (a) Show that a number of the form $3^i 5^j$ can never be perfect.
   (b) More generally, if $p \geq 5$ is an odd prime, show that the product $3^i p^j$ can never be perfect.
   (c) Even more generally, show that if p and q are distinct odd primes, then a number of the form $q^i p^j$ can never be perfect.

9. (Hard) Show that $3^i 5^j 7^k$ is never perfect.

   (*Hint: consider $\sigma(n)$ and sums $1 + 3 + 3^2 + \cdots$, etc. modulo 4, then think modulo 5*)

[20] Fermat thought that all the F_k might be prime, however Euler (1732) and Clausen/Landry (1855/1880) successively showed that F_5 and F_6 are composite with prime factorizations:

$$F_5 = 4{,}294{,}967{,}297 = 641 \cdot 6700417, \qquad F_6 = 18{,}446{,}744{,}073{,}709{,}551{,}617 = 274{,}177 \cdot 67{,}280{,}421{,}310{,}721$$

These were incredible achievements for the time. As of 2022, no other Fermat primes have been discovered, and only up to F_{11} has been completely factored! A distributed computing project similar to GIMPS continues the search...

6 Powers and Roots in $\mathbb{Z}_n$

6.1 Successive Squaring and k^{th} Roots

In this chapter, we flesh out two contrasting ideas: Powers are *easy*, roots (and factorization) are *hard.*

Example 6.1. To compute $14^{217} \pmod{67}$, we currently have a couple of options:

1. Reduce the problem via Euler/Fermat $14^{217} \equiv 14^{3\cdot 66+19} \equiv 14^{19} \pmod{67}$.
2. Hunt for a small power of 14 which has small remainder modulo 67. This could take a while!

For large moduli, these options become markedly less attractive! Instead we try a more systematic approach where we repeatedly compute squares:

$$\begin{aligned} 14^2 \equiv 196 \equiv -5 &\implies 14^4 \equiv (-5)^2 \equiv 25 \\ &\implies 14^8 \equiv 25^2 \equiv 625 \equiv 22 \\ &\implies 14^{16} \equiv 22^2 \equiv 484 \equiv 15 \pmod{67} \end{aligned}$$

Each squaring was easy, and by considering the binary decomposition $19 = 16+2+1 = 2^4+2^1+2^0$ of the exponent, we now have enough information to compute the answer:

$$14^{19} \equiv 14^{16+2+1} \equiv 15 \cdot (-5) \cdot 14 \equiv 22 \pmod{67}$$

Successive Squaring Algorithm to compute $a^k \pmod{m}$

1. Take the binary decomposition $k = 2^r + 2^{r-1}\mu_{r-1} + \cdots + 2\mu_1 + \mu_0$ where each $\mu_j = 0, 1$.
2. Repeatedly square modulo m: compute $A_j \equiv a^{2^j} \equiv A_{j-1}^2 \pmod{m}$
3. Compute $a^k \equiv A_r A_{r-1}^{\mu_{r-1}} \cdots A_0^{\mu_0} \cdots \pmod{m}$.

Example 6.2. We compute $6^{73} \pmod{25}$ using the successive squaring algorithm:

1. $73 = 64+8+1 = 2^6+2^3+2^0$.
2. Starting with $A_0 = a = 6$ we square:

$$\begin{aligned} A_1 \equiv 6^2 \equiv 35 \equiv 11 &\implies A_2 \equiv 11^2 \equiv 121 \equiv -4 \\ &\implies A_3 \equiv (-4)^2 \equiv 16 \equiv -9 \\ &\implies A_4 \equiv 16^2 \equiv 256 \equiv 6 \equiv A_0 \\ &\implies A_5 \equiv A_1 \equiv 11, \qquad A_6 \equiv A_1 \equiv -4 \end{aligned}$$

   Notice how the pattern repeats once we reach $A_4 \equiv A_0$.

3. $6^{73} \equiv A_6 A_3 A_0 \equiv (-4)\cdot(-9)\cdot 6 \equiv 16 \pmod{25}$.

For more speed, we could have started with Euler's Theorem: $\varphi(25) = 5 \cdot 4 = 20$, whence

$$6^{73} \equiv (6^{20})^3 \cdot 6^{13} \equiv 6^{2^3+2^2+2^0} \equiv A_3 A_2 A_0 \equiv (-9)\cdot(-4)\cdot 6 \equiv 16 \pmod{25}$$

However, considering how the original list started repeating, this didn't save us much time.

Efficiency While tedious to perform by hand, the algorithm is very efficient for a computer: this is what we mean by *powers are easy.*

- The binary expansion of $k = \mu_0 + 2\mu_1 + 2^2\mu_2 + \cdots + 2^r$ has $r+1$ terms if and only if

  $$2^r \leq k < 2^{r+1} \iff r \leq \log_2 k < r+1$$

  This is likely the form in which the computer stores k already!

- Squaring and computing each A_j and the product $A_0^{\mu_0} \cdots A_r$ requires $r+1$ *take the remainder* calculations.

- The algorithm therefore requires approximately $\log_2 k$ remainder steps to complete; roughly 3.3 times number of digits of k.

- There are many algorithms available for taking the remainder: these are roughly about as efficient as multiplying, so the full algorithm is very efficient indeed!

Slightly faster algorithms even than this are available; even when x, k, m are 100's of digits long, a modern computer can evaluate $x^k \pmod b$ in *micro*seconds. To really stress a computer, we need much larger exponents! Here are a few benchmarking times[21] where $x = 13^{89} + 1$ and $m = 17^{81} + 3$ are 100-digit numbers.

27 μs:	$x^{10^{100}}$	$\equiv$ 28113683767197032635280630918465515590312537596688739582642477241267257395851838126566833044467214 16
17 ms:	$x^{10^{100,000}}$	$\equiv$ 44889754565483688038590522070459199098021165912257209775760917725606936177245912447375884572850873 56
174 ms:	$x^{10^{1,000,000}}$	$\equiv$ 89261598289061966598061053487449354749455681755372018207341719404714255041408715452144882822741567 6
1.78 s:	$x^{10^{10,000,000}}$	$\equiv$ 22254149320737417349787502030037838676985736003885099039953870206232390405470812862628463932110453 16
17.7 s:	$x^{10^{100,000,000}}$	$\equiv$ 33498692500814836763572589952952787478860450253806454138049887207140161051051454458304895427823668 76

Note how the computing time is roughly proportional to the number of digits in the exponent: each calculation (100000 $\to$ 1 million $\to$ 10 million $\to$ 100 million digits) takes approximately 10 times as long as the previous.

Computing k^{th} roots modulo m

The contrasting problem of finding k^{th} roots is much *harder,* in that computers cannot do it efficiently. Again we motivate via an example.

Example 6.3. Solve the congruence $x^5 \equiv 7 \pmod{26}$: that is, find the 5^{th} roots of 7 modulo 26.

- First note that $\gcd(7, 26) = 1$ and that any solution x must therefore be a unit:

  $$d \mid x \text{ and } d \mid 26 \implies d \mid 7 \implies d = 1 \implies \gcd(x, 26) = 1$$

- By Euler's Theorem: $x^{\varphi(26)} \equiv x^{12} \equiv 1 \pmod{26}$.

- Now hunt for a multiple of 5 which is congruent to 1 modulo $\varphi(m) = 12$. In this case

  $$5^2 = 25 = 2\varphi(26) + 1 \implies x \equiv x^{1+2\varphi(26)} \equiv x^{25} \equiv 7^5 \equiv 11 \pmod{26}$$

In the last step we may appeal to successive squaring to compute 7^5 or simply hack at it...

[21] These times were obtained running Sage on a single core of an Intel i5-9600K desktop CPU, clocked at 4.4 GHz.

We lucked out in the example: the final step relied on being able to solve the congruence

$$5u \equiv 1 \pmod{12}$$

which we know we can do because $\gcd(5, 12) = 1$. When trying to take k^{th} roots in general, this step may not be possible. At least we have identified the critical ingredient necessary for being able to find a *unique* k^{th} root.

Theorem 6.4. *Suppose that* $\gcd(b, m) = \gcd\big(k, \varphi(m)\big) = 1$. *Then the congruence equation* $x^k \equiv b \pmod{m}$ *has a unique solution, which can be found as follows:*

1. *Compute* $\varphi(m)$.
2. *Find* $u \in \mathbb{N}$ *such that* $ku \equiv 1 \pmod{\varphi(m)}$.
3. *Evaluate* $x \equiv b^u \pmod{m}$.

Proof. First observe that any purported solution x must be a unit ($\gcd(x, m) = 1$): if not, then $b \equiv x^k$ and m would have a common divisor greater than 1, contradicting our assumptions.

Step 2 is possible since $\gcd\big(k, \varphi(m)\big) = 1$; we can therefore write $ku = 1 + \lambda\varphi(m)$ for some $\lambda \in \mathbb{N}$. Since any suitable x is a unit, we can now apply Euler's Theorem

$$b^u \equiv (x^k)^u \equiv x^{1+\lambda\varphi(m)} \equiv x \pmod{m}$$

Uniqueness is clear since we found $x \equiv b^u$ by doing the same thing (raising to the power u) to both sides of the congruence $x^k \equiv b \pmod{m}$. ∎

Example 6.5. Find the unique solution to $x^{283} \equiv 29 \pmod{42}$

We trivially verify that $\gcd(29, 42) = 1$ and $\varphi(42) = 12$. We therefore need to solve

$$283u \equiv 1 \pmod{12}$$

This is straightforward, since $283 \equiv 7 \pmod{12}$, we easily spot that $u \equiv 7$ is a solution.[a] Now compute

$$\begin{aligned} x^{283} \equiv 29 &\implies x^{283\cdot 7} \equiv 29^7 \pmod{42} \\ &\implies x \equiv x^{1+165\varphi(42)} \equiv 29^7 \pmod{42} \end{aligned}$$

It remains to compute the final power: applying the successive squaring algorithm, we have $7 = 2^0 + 2^1 + 2^2$, and

$$A_0 = 29, \qquad A_1 = 29^2 = 169 = 1, \qquad A_2 = 1$$

whence

$$x \equiv 29^7 \equiv 29 \cdot 1 \cdot 1 \equiv 29 \pmod{42}$$

[a] If this makes you nervous, use the Euclidean algorithm to solve $7u = 1 + 12\lambda$, or indeed $283 = 1 + 12\lambda$:

$$\left.\begin{aligned} \mathbf{283} &= \mathbf{12} \cdot 23 + \mathbf{7} \\ \mathbf{12} &= \mathbf{7} \cdot 1 + \mathbf{5} \\ \mathbf{7} &= \mathbf{5} \cdot 1 + \mathbf{2} \\ \mathbf{5} &= \mathbf{2} \cdot 2 + \mathbf{1} \end{aligned}\right\} \implies \gcd(283, 12) = \mathbf{1} = \mathbf{12} \cdot 118 - \mathbf{283} \cdot 5 \implies \mathbf{283} \cdot 7 = \mathbf{1} + \mathbf{12} \cdot 165$$

where we reversed the algorithm to obtain the final result.

Efficiency Even when a unique k^{th} root exists, finding it is typically much slower than computing a k^{th} power. Comparing the steps in Theorem 6.4:

1. Computing $\varphi(m)$ is *very, very* slow; you essentially need to factorize m.
2. The Euclidean algorithm is fast to implement.
3. This can be done using successive squaring; also fast.

When m is large the discrepancy in computing speeds becomes *enormous.*

The same modern desktop considered earlier took 216 seconds to factorize the 100-digit base discussed previously:

$$17^{81}+3 = 2^2\times 5\times 107\times 20381297\times 5040257978377\times 1048716516137182133268555529797 37\times 2011898964764031749438190479000474814228011 71$$

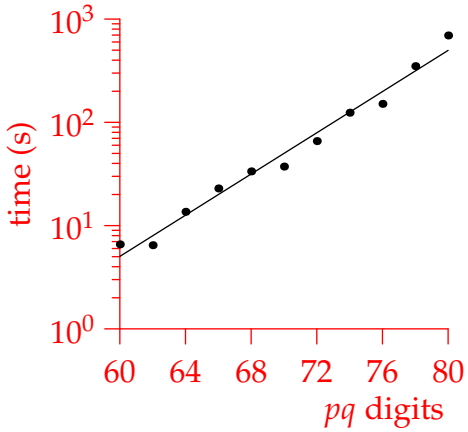
This example isn't ideal since if a large number is lucky enough to be divisible by several small primes, it can often be factorized very quickly. For a more sensible benchmark, here are the times taken by the computer to factorize several *semiprimes* pq, where the primes p, q were of comparable size.

pq digits	60	62	64	66	68	70	72	74	76	78	80
Factorization time (s)	6.58	6.46	13.6	22.9	33.5	37.3	65.8	124	151	350	694

When the factorization time is graphed logarithmically, the data appears linear. The best-fitting straight line therefore represents an *exponential* model:

$$T(n) \approx \exp(0.2297n - 12.1665)$$

By this metric, we might expect that factoring a 100-digit semiprime would require $13\frac{1}{2}$ *hours*, a 150-digit semiprime 150 *years*!



Non-unique k^{th} roots It is reasonable to ask what can happen in when either or both of the conditions $\gcd(b,m) = 1 = \gcd\left(k, \varphi(m)\right) = 1$ fails. The short answer is that anything is possible; you could have no k^{th} root, a unique root, or several roots. Some of the details are in the exercises.

Example 6.6. Modulo 6, we have $\gcd(\varphi(6), 4) = 2 \neq 1$. By computing fourth powers modulo 6:

x	0	1	2	3	4	5
x^4	0	1	4	3	4	1

we see that the congruence $x^4 \equiv b \pmod 6$ has a unique solution if $b = 0, 3$, two solutions if $b = 1, 4$, and no solutions if $b = 2, 5$.

Exercises 6.1 1. Use the method of successive squaring to compute each of the following:

(a) $5^{13} \pmod{23}$ (b) $12^{260} \pmod{1000}$ (c) $28^{749} \pmod{1147}$

(*Use a calculator*!)

2. For each congruence, verify the hypotheses of the Theorem 6.4 and solve the congruences:

(a) $x^{83} \equiv 15 \pmod{322}$ (b) $x^{329} \equiv 452 \pmod{1147}$

3. We search for k^{th} roots of b modulo m in situations where at least one of the standard conditions fails:

$$\gcd(b, m) \neq 1 \quad \text{or} \quad \gcd\big(k, \varphi(m)\big) \neq 1 \qquad (*)$$

(a) If p is an odd prime, show that 1 has exactly two square-roots modulo p. Which of the conditions $(*)$ fails in this case?

(b) Investigate the cube-roots of b modulo 8 for each remainder b (see, e.g., Example 6.6). How many such b have a cube-root? Are they unique? What do the gcd conditions $(*)$ say in each case? When could we have used the theorem on unique k^{th} roots?

(c) Repeat for the fourth-roots of b modulo 8.

(d) Repeat for the cube-roots of b modulo 10.

6.2 The RSA Cryptosystem

Perhaps the modern-world's most utilised cryptosystem, it is likely that you (indirectly) use some version of RSA[22] every day, when your phone or computer connects securely to another, for instance using https. Here is how the method works.

Encoding 1. Start with distinct primes p, q and build the semiprime $m = pq$.

2. Calculate $\varphi(m) = (p-1)(q-1)$.

3. Choose an integer s such that $1 < s < \varphi(m)$ and $\gcd\big(s, \varphi(m)\big) = 1$.

4. Encode a numerical message by mapping $x \mapsto x^s \pmod{m}$.

Decoding This is based on the following.

Theorem 6.7. *Let $u \in \mathbb{N}$ satisfy $us \equiv 1 \pmod{\varphi(m)}$. Then, for all x, $(x^s)^u \equiv x \pmod{m}$.*

Proof. Since $m = pq$ is a semiprime, we have

$$x^{su} \equiv x \pmod{m} \iff \begin{cases} x^{su} \equiv x \pmod{p}, \text{ and} \\ x^{su} \equiv x \pmod{q} \end{cases}$$

Since $su \equiv 1 \pmod{\varphi(m)}$ we see that $su = 1 + j(p-1)(q-1)$ for some $j \in \mathbb{Z}$. If $x \equiv 0 \pmod{p}$, then Fermat's little theorem tells us that

$$x^{su} \equiv x \cdot (x^{p-1})^{j(q-1)} \equiv x \pmod{p}$$

The result is plainly trivial if $x \equiv 0$, and the calculation is similar for the other modulus q. ∎

The process is very simple: think of s for 'scramble' and u for 'unscramble.'

$$x \overset{\text{encode}}{\longmapsto} x^s \pmod{m} \overset{\text{decode}}{\longmapsto} (x^s)^u \equiv x \pmod{m}$$

As we saw in the previous section, even if m, s, u are 100+ digits long, these calculations are very fast for modern computers.

The values m, s are known as the *public key*: these are all you need to encode messages. Indeed these can be made freely available so that anyone can encode.

To decode messages, one also requires the *private key* u. Provided you keep this number secret, only you can decode messages sent to you.

One implementation involves a group of friends each of whom have different keys. They keep secret their private keys u, but share their public keys s, m with the group. Then all friends can send messages to each other but, once encoded, each can only be decoded by the intended recipient.

[22] The acronym is formed from the initials of Rivest, Shamir and Adleman who discovered the system while working at MIT in 1977. It was in fact first described in 1973 by Clifford Cocks while working for GCHQ, the British equivalent of the US National Security Agency. Cocks' discovery was classified, even though, due to the lack of available computing power, it was deemed to have no practical application.

Examples 6.8. 1. For a very simple example, we start by encoding a message via the obvious substitution $A \mapsto 1$, $B \mapsto 2$, etc.:

I	T	S	A	L	L	G	R	E	E	K	T	O	M	E
9	20	19	1	12	12	7	18	5	5	11	20	15	13	5

If we choose the semiprime $m = 5 \times 7 = 35$, then $\varphi(m) = 4 \times 6 = 24$, and we can choose, say, $s = 5$. We then encode by mapping $x \mapsto x^5 \pmod{35}$:

$$9 \mapsto 9^5 \equiv 81^2 \cdot 9 \equiv 11^2 \cdot 9 \equiv 16 \cdot 9 \equiv 4 \pmod{35}$$

$$20 \mapsto 20^5 \equiv 20 \qquad 19 \mapsto 19^5 \equiv 24, \qquad 1 \mapsto 1^5 \equiv 1, \ldots$$

resulting in the string of numbers

4, 20, 24, 1, 17, 17, 7, 23, 10, 10, 16, 20, 15, 13, 10

We could also translate the encoded message back into letters:

D, T, X, A, Q, Q, G, W, J, J, P, T, O, M, J

To decode, we require u such that $5u \equiv 1 \pmod{24}$; that is $u = 5$ (it doesn't matter for us that this equals s!). Again compute

$$4^5 \equiv 4^3 \cdot 4^2 \equiv 64 \cdot 4^2 \equiv -6 \cdot 4^2 \equiv -24 \cdot 4 \equiv 44 \equiv 9 \pmod{35}$$

$$20^5 \equiv 20, \qquad 24^5 \equiv 19, \ldots$$

to recover the original string of numbers and message ITSALLGREEKTOME.

2. Suppose you intercept the message

59, 4, 57, 2, 82, 4, 86, 43, 4, 43, 57, 4

which you know has been encoded using the public key $s = 11$, $m = 119$. You also know that the message may be read via the translation

$$11 \leftrightarrow A,\ 12 \leftrightarrow B, \ldots,\ 36 \leftrightarrow Z$$

To crack the code, our first job is computing the totient: $m = 7 \times 17 \implies \varphi(m) = 6 \cdot 16 = 96$.

We now need to find the private key, which satisfies $11u \equiv 1 \pmod{96}$. A relatively short application of the Euclidean algorithm says that

$$1 = 11 \cdot 35 - 4 \cdot 96 \implies u = 35$$

We now compute:[a]

$$59 \mapsto 59^{35} \equiv 19 \mod 119$$

etc. The full decode is

19, 29, 19, 30, 25, 24, 30, 18, 15, 30, 15, 29, 30

which you're welcome to translate into letters if you're so inclined...

[a] If you don't want to beg the help of a calculator, use the successive squaring algorithm: the binary decomposition is $35 = 2^5 + 2^1 + 2^0$, which yields

$$A_0 = 59, \quad A_1 = 30, \quad A_2 = -52, \quad A_3 = -33, \quad A_4 = 18, \quad A_5 = -33$$

$$\implies 59^{35} \equiv A_5 A_1 A_0 \equiv -33 \cdot 30 \cdot 59 \equiv 19 \pmod{119}$$

Don't knock it: it's what your computer has to do for *every* element of the code!

Speed and Security of the RSA system

Encoding and decoding (once in possession of the private key) require only the computation of powers modulo m. While our examples used very small moduli, modern applications use semiprimes with 300 or more digits. While unfeasible in 1973, for modern computers such work is trivial.

Now suppose that you are in possession of the public key m, s and want to crack an encoded message. You need to do two things:

1. Find $\varphi(m)$; equivalently factorize $m = pq$. As we saw in the previous section, for moduli in the 300 digit range this is essentially impossible in any reasonable time-frame.[23]
2. Find $u \in \mathbb{N}$ such that $us \equiv 1 \pmod{\varphi(m)}$. Employing the Euclidean algorithm requires no more than $2\log_2 \varphi(m)$ applications of the division algorithm and some back substitution. Even for 300 digit numbers, this can be completed in microseconds *provided* $\varphi(m)$ *is known.*

While resilient against general attack, RSA is not foolproof. Its main drawback is that it is a *table cipher*: if $18 \mapsto 11$ during encoding, then 18 is always mapped to 11. If a decoded message is intercepted, a hacker then knows how to decode any future messages without calculation. Long messages reduce security since common combinations such as 'e' and 'the' might be guessable if they appear frequently. Correctly guessing even a few letters makes decoding a full message much easier. Of course, with very large moduli perhaps the entire message can be transmitted using only one digit! RSA can also easily be combined with other cryptographic methods for greater security.

Exercises 6.2 1. For each message and public key m, s, find the private key u and decode the message, using $1 \mapsto A$, $2 \mapsto B$, etc. to translate back to letters.

   (a) When $m = 35$ and $s = 11$ you receive $28, 4, 18, 18, 10, 2, 4, 14, 28, 28, 4, 2, 1, 6, 6, 10, 24$

   (b) When $m = 143$ and $s = 103$ you receive $63, 1, 63, 63, 12, 113, 27, 123, 63, 1, 63, 141, 141, 27, 72$

2. (a) Let $m = p_1 \cdots p_n$ be a product of *distinct* primes, and assume that $\gcd(k, \varphi(m)) = 1$ so that $\exists u$ with $ku \equiv 1 \pmod{\varphi(m)}$. Prove that $x^k \equiv b \pmod{m}$ has unique solution $x \equiv b^u \pmod{m}$, regardless of whether $\gcd(b, m) = 1$.

   (*Hint: Carefully read the proof of Theorem 6.7*)

   (b) Consider the congruence $x^5 \equiv 6 \pmod{9}$. Show that you can find u satisfying $5u \equiv 1 \pmod{\varphi(9)}$, but that $x \equiv 6^u$ is not a solution to the required congruence. Can you identify where the *distinct prime* condition was needed in part (a)?

   (c) Solve the congruence $x^{49} \equiv 3 \pmod{1155}$

3. In Example 6.8, we saw that the public and private keys s, u were equal (both being 5). Relative to the semiprime modulus $m = 35$, show that this is *always* the case; regardless of which s you choose, you will always have $u = s$.

4. Modern implementations typically replace Euler's totient function $\varphi(m) = (p-1)(q-1)$ with $\Lambda(m) := \operatorname{lcm}(p-1, q-1)$.

   Given a public key m, s where $\gcd(s, \Lambda(m)) = 1$, show that decoding may be accomplished by finding the private key satisfying $us \equiv 1 \pmod{\Lambda(m)}$.

[23] RSA Labs used to offer cash prizes for factoring large semiprimes (the *RSA-numbers*). As of 2020, the largest yet factorized has 250 digits, requiring supercomputer resources equivalent to over 1000 years on a single desktop core.

7 Quadratic Residues

Recall our earlier discussion of k^{th} roots:

> If $\gcd(a,m) = 1 = \gcd\big(k, \varphi(m)\big)$, then $x^k \equiv a \pmod{m}$ has a unique solution.

This result contains an almost glaring omission: (when $m \geq 3$) $\varphi(m)$ is *always even*, so the simplest type of root, *square roots*, never fit the pattern! In this chapter we focus on the equation $x^2 \equiv a \pmod{p}$ where p is an odd prime, and consider the question of when a has a square root modulo p.

7.1 Squares Modulo an Odd Prime

Definition 7.1. Let p be an odd prime. A non-zero residue a is a *quadratic residue* (QR) modulo p if $x^2 \equiv a \pmod{p}$ has a solution. Otherwise it is a quadratic non-residue (QNR, or just NR).

Examples 7.2. Here are all possible equations modulo $p = 3, 5$ and 7, and whether each a is a quadratic residue modulo p.

a	equation	solutions	QR?
1	$x^2 \equiv 1 \pmod 3$	$x \equiv 1, 2$	✓
2	$x^2 \equiv 2 \pmod 3$	none	X

a	equation	solutions	QR?
1	$x^2 \equiv 1 \pmod 5$	$x \equiv 1, 4$	✓
2	$x^2 \equiv 2 \pmod 5$	none	X
3	$x^2 \equiv 3 \pmod 5$	none	X
4	$x^2 \equiv 4 \pmod 5$	$x \equiv 2, 3$	✓

a	equation	solutions	QR?
1	$x^2 \equiv 1 \pmod 7$	$x \equiv 1, 6$	✓
2	$x^2 \equiv 2 \pmod 7$	$x \equiv 3, 4$	✓
3	$x^2 \equiv 3 \pmod 7$	none	X
4	$x^2 \equiv 4 \pmod 7$	$x \equiv 2, 5$	✓
5	$x^2 \equiv 5 \pmod 7$	none	X
6	$x^2 \equiv 6 \pmod 7$	none	X

The first thing you should observe is that precisely half $\frac{p-1}{2}$ of the non-zero remainders are quadratic residues. This follows immediately from a simple calculation.

Lemma 7.3. *If p is an odd prime, then the numbers $0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are distinct modulo p.*

Proof. $x^2 \equiv y^2 \implies (x-y)(x+y) \equiv 0 \pmod{p}$. By unique factorization, we have $x \equiv \pm y$. ∎

Partly in view of the Lemma, it is often useful when discussing quadratic residues to consider remainders as lying in the set of *least residues* $\{0, \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$: i.e. with minimal absolute value.

Note also that the Lemma really requires a prime modulus (from which unique factorization follows). For composite moduli we don't expect distinct values from square: for instance

$$1^2 \equiv 3^2 \pmod 8$$

Indeed, modulo 8, the only equations $x^2 \equiv a$ with solutions are when $a \equiv 0, 1, 4$. Even for non-zero remainders, only two in seven have square roots modulo 8.

A second property that might take a little longer to spot is the *multiplicativity* of quadratic residues: for example 2 and 4 are quadratic residues modulo 7, as is $2 \cdot 4 \equiv 1$. With a proof of this in mind, we make a useful definition.

Definition 7.4. Given an odd prime p and an integer a, define the *Legendre symbol*

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a QR modulo } p \\ -1 & \text{if } a \text{ is a QNR modulo } p \end{cases}$$

Examples 7.5. Look at the above tables: $\left(\frac{1}{3}\right) = \left(\frac{-1}{5}\right) = \left(\frac{2}{7}\right) = 1$ and $\left(\frac{-2}{3}\right) = \left(\frac{-2}{5}\right) = \left(\frac{3}{7}\right) = -1$

Legendre symbols will prove very useful for checking whether we have a quadratic residue. To see how, we develop a little algebra.

Theorem 7.6. *If p is an odd prime and $a, b \in \mathbb{Z}$, then:*

1. $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $p \nmid a \implies \left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$: *otherwise said QR×QR=QR, QR×NR=NR, NR×NR=QR.*

This follows as a corollary of a more complex result later, but for now it is worth a direct proof.

Proof. Parts 1 and 2 are immediate from the definition. In particular, note that

$$a \text{ is a QR} \iff \exists c \in \mathbb{Z}_p^\times \text{ such that } a \equiv c^2 \pmod{p}$$

For part 3, the statement is trivial if either or both $p \mid a$ or $p \mid b$. Otherwise, we treat the three cases separately: suppose throughout that c, d are units (non-zero modulo p).

(a) $c^2 d^2 \equiv (cd)^2$, so the product of QR's is a QR.

(b) By part (a), $c^2 n \equiv d^2 \implies n \equiv (dc^{-1})^2$ is a QR. The contrapositive says that if n is a NR, so also is $c^2 n$.

(c) Let n be a NR. Since $n \not\equiv 0$, we have a bijective map[a]

$$\mu : x \mapsto nx : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times \qquad \text{(the inverse is } \mu^{-1}(x) := n^{-1}x\text{)}$$

For any QR c^2, part (b) says that $\mu(c^2) = nc^2$ is an NR. Since (Lemma 7.3) the sets of QR's and NR's have equal cardinality, it follows that μ maps the QR's bijectively to the NR's and must therefore map NR's back to QR's. In particular, if m is a NR, then $\mu(m) = mn$ is a QR. ∎

[a] If you've done group theory, this argument should remind you of the comparison of even and odd cycles in the symmetric group S_n, where we see that the sets of such have the same cardinality. Indeed we are really proving that the function $f(a) = \left(\frac{a}{p}\right)$ is a homomorphism of multiplicative groups $f : \mathbb{Z}_p^\times \to \{\pm 1\}$.

Example 7.7. To check whether 27 is a QR modulo 61, we compute the Legendre symbol.

$$\left(\frac{27}{61}\right) = \left(\frac{3^2}{61}\right)\left(\frac{3}{61}\right) = \left(\frac{3}{61}\right)$$

We are left to decide whether 3 is a QR modulo 61; equivalently, we want to solve $x^2 \equiv 3 \pmod{61}$. By inspection, $x \equiv 8$ is a solution (as is $x \equiv -8 \equiv 53$), whence 27 is a QR modulo 61.
We can actually go further:

$$8^2 \equiv 3 \implies (3 \cdot 8)^2 \equiv 3^3 \implies 24^2 \equiv 27 \pmod{61}$$

It follows that the solutions to the original congruence are

$$x^2 \equiv 27 \pmod{61} \iff x \equiv \pm 24 \equiv 24,\ 37 \pmod{61}$$

While Legendre symbols were undoubtedly helpful for our example, they weren't quite enough. We still needed to be able to spot that 3 was a quadratic residue, though thankfully this was easy in the example. In general we can't rely on being able to spot a solution; we therefore need some method of computing a Legendre symbol directly.

Example 7.8. Suppose we want to find the value of $\left(\frac{2}{101}\right)$: equivalently we are asking whether $x^2 \equiv 2 \pmod{101}$ has a solution. Simply trying all possible values of x is a bad idea! Instead, suppose that there was a solution x: plainly it would have to be a unit modulo 101 and so we could apply Fermat's little theorem:

$$x^2 \equiv 2 \implies 1 \overset{\text{F}\ell\text{T}}{\equiv} x^{100} \equiv 2^{50} \pmod{101}$$

A short calculation (successive squaring?) should convince you that $2^{50} \equiv -1$, whence 2 is a non-residue and $\left(\frac{2}{101}\right) = -1$.

The approach works in general:

Theorem 7.9 (Euler's Criterion). *If p is an odd prime, then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

Proof. If $p \mid a$, both sides are trivially zero.
If a is a QR, then $a \equiv b^2$ for some $b \in \mathbb{Z}_p^\times$, whence $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem.
Now consider the equation $y^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. By Lagrange, this has *at most* $\frac{p-1}{2}$ solutions. However, all $\frac{p-1}{2}$ quadratic residues (Lemma 7.3) are already solutions! Hence

$$a \text{ is a quadratic residue} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Finally observe that Fermat's little theorem may be factorized (*uniquely* modulo p):

$$0 \equiv a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \pmod{p}$$

We conclude that a is a non-residue $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. ∎

Examples 7.10. 1. 3 is a QR modulo 13 since $3^{\frac{13-1}{2}} \equiv 3^6 \equiv 27^2 \equiv 1^2 \equiv 1 \mod 13$. It is easy to see that the solutions to $x^2 \equiv 3 \mod 13$ are $x \equiv 4, 9$.

2. Returning to Example 7.7 and applying successive squaring,

$$\left(\frac{3}{61}\right) \equiv 3^{\frac{61-1}{2}} \equiv 3^{30} \equiv 3^{2+4+8+16} \equiv 9 \cdot 20 \cdot (-27) \cdot (-3) \equiv 1 \pmod{61}$$

Is -1 a Quadratic Residue? Here is a straightforward application of Euler's criterion where we see for precisely which primes -1 is a quadratic residue.

Theorem 7.11. *If p is an odd prime, then -1 is a QR $\iff$ $p \equiv 1 \pmod 4$. Indeed*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

As a surprising by-product, we obtain a proof of a result promised earlier in the course.

Theorem 7.12. *There are infinitely many primes congruent to 1 modulo 4.*

The idea is to construct an impossible solution to some $x^2 \equiv -1 \pmod q$ where $q \equiv 3 \pmod 4$.

Proof. Suppose that $p_1, \ldots, p_n$ constitute all primes congruent to 1 modulo 4. Define

$$x := 2p_1 \cdots p_n \text{ and } \Pi := x^2 + 1$$

Certainly Π is divisible by some prime q, which is plainly odd and cannot be one of the primes $p_1, \ldots, p_n$. We conclude that $q \equiv 3 \pmod 4$. However, we now have

$$\Pi \equiv 0 \implies x^2 \equiv -1 \pmod q$$

which contradicts Theorem 7.11. ∎

Is 2 a Quadratic Residue? This is harder than dealing with -1, though a nice answer is still available, based on a sneaky trick attributable to Gauss.[24]

Examples 7.13. 1. We multiply the even remainders modulo 23 in two ways:

$$2 \cdot 4 \cdot 6 \cdots 22 \equiv 2^{11} \cdot 11! \pmod{23}$$

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots 22 &\equiv 2 \cdot 4 \cdots 10 \cdot 12 \cdot 14 \cdots 22 \\ &\equiv 2 \cdot 4 \cdots 10 \cdot (-11) \cdot (-9) \cdots (-1) \\ &\equiv (-1)^6 \cdot 11! \pmod{23} \end{aligned}$$

It follows that $2^{11} \equiv 2^{\frac{23-1}{2}} \equiv (-1)^6 \equiv 1 \pmod{23}$, whence 2 is a quadratic residue modulo 23.

[24] Carl Friedrich Gauss (1777–1855) was arguably the most consequential mathematician in history, and a major contributor to number theory, which he considered the *Queen of Mathematics*.

2. Let $p = 37$. This time $\frac{p-1}{2} = 18$ so we we break the even remainders at 18:

$$\begin{aligned} 2^{18} \cdot 18! &\equiv 2 \cdot 4 \cdot 6 \cdots 36 \\ &\equiv 2 \cdot 4 \cdots 18 \cdot 20 \cdot 22 \cdots 36 \\ &\equiv 2 \cdot 4 \cdots 18 \cdot (-17) \cdot (-15) \cdots (-1) \\ &\equiv (-1)^9 \cdot 18! \pmod{37} \\ \implies 2^{\frac{37-1}{2}} &\equiv 2^{18} \equiv (-1)^9 \equiv -1 \pmod{37} \end{aligned}$$

We conclude that 2 is a non-residue modulo 37.

For the main result, we need only do this in the abstract!

Theorem 7.14. *If p is an odd prime, then 2 is a QR $\iff$ $p \equiv 1, 7 \pmod 8$. Otherwise said,*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$$

Proof. Since p is odd, we may define the integer $P = \frac{p-1}{2}$. Multiply together the even remainders modulo p to obtain

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^P \cdot 1 \cdot 2 \cdots P = 2^P P! \tag{$*$}$$

Now consider the same product, split at P:

$$\underbrace{2 \cdot 4 \cdot 6 \cdots}_{\leq P} \underbrace{\cdots (p-5)(p-3)(p-1)}_{> P} \equiv 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (-5) \cdot (-3) \cdot (-1)$$

To finish the proof, we need to make sure that the right side has the form $(-1)^m \cdot P!$ and we need to *count the number of negative signs m*. There are two cases.

$P = 2k$ is even: Plainly $p = 2P + 1 = 4k + 1 \equiv 1 \pmod 4$. There are $P = 2k$ even remainders modulo p, whence the split is as follows:

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots (p-1) &\equiv \underbrace{2 \cdot 4 \cdot 6 \cdots P}_{k \text{ terms} \leq P} \cdot \underbrace{(P+2) \cdots (p-5)(p-3)(p-1)}_{k \text{ terms} > P} \\ &\equiv 2 \cdot 4 \cdots P \cdot \big(-(P-1)\big) \cdots (-3) \cdot (-1) \\ &\equiv (-1)^k \cdot P! \pmod p \end{aligned}$$

where we used the fact that $(P+2) - p = P + 2 - 2P - 1 = -(P-1)$. Combined with $(*)$, we see that

$$2^{\frac{p-1}{2}} \equiv 2^P \equiv (-1)^k \equiv \begin{cases} 1 & \text{if } k \text{ is even} \iff p \equiv 1 \pmod 8 \\ -1 & \text{if } k \text{ is odd} \iff p \equiv 5 \pmod 8 \end{cases}$$

$P = 2k + 1$ is odd: This is similar and we leave it as an exercise. ∎

Example 7.15. To check whether $x^2 \equiv 95 \pmod{127}$ has any solutions, observe that

$$\left(\frac{95}{127}\right) = \left(\frac{-32}{127}\right) = \left(\frac{-1}{127}\right)\left(\frac{4^2}{127}\right)\left(\frac{2}{127}\right) = \left(\frac{-1}{127}\right)\left(\frac{2}{127}\right) = (-1)\cdot 1 = -1$$

where we used that fact that

$$127 = 15\cdot 8 + 7 \implies \begin{cases} 127 \equiv 3 \pmod 4 \\ 127 \equiv 7 \pmod 8 \end{cases}$$

We conclude that 95 is a non-residue modulo 127.

Similar results can be obtained for other values though, as we'll see, such aren't really necessary...

Exercises 7.1

1. Use the methods of this section to decide which are quadratic residues:
   (a) $7 \pmod{11}$ (b) $6 \pmod{31}$ (c) $39 \pmod{41}$
2. (a) Suppose that a is a quadratic residue modulo p, where $p \equiv 3 \pmod 4$. Check that the solutions of $x^2 \equiv a \pmod p$ are $x = \pm a^{\frac{p+1}{4}} \pmod p$.
   (b) Find all solutions to the congruence $x^2 \equiv 7 \pmod{31}$.
   (c) Still working with $p \equiv 3 \pmod 4$, if $p \nmid a$ and a is a quadratic non-residue modulo p, what is the value of $\left(a^{\frac{p+1}{4}}\right)^2$?
3. (a) Find the prime decomposition of 924.
   (b) Check that 37 is a quadratic residue modulo each odd prime dividing 924. Also check that $x^2 \equiv 37 \pmod{2^k}$ is solvable where 2^k is the largest power of 2 dividing 924.
   (c) How many solutions has the congruence $x^2 \equiv 37 \pmod{924}$? Why?
4. In the manner of question 3, decide whether the following have solutions and, if so, how many.
   (a) $x^2 \equiv 3 \pmod{143}$
   (b) $x^2 \equiv 2 \pmod{437}$
   (c) $x^2 \equiv 393 \pmod{1564}$
5. Suppose $p \nmid a$. Show that if $p \equiv 1 \pmod 4$, then both or neither of $\pm a$ are quadratic residues modulo p. Similarly, if $p \equiv 3 \pmod 4$, show that exactly one of $\pm a$ are quadratic residues.
6. Compute $2^{2048} \pmod{4097}$. What does this tell you about whether 4097 is prime?
   (*Hint: 4096 is a power of 2...*)
7. Complete the proof of Theorem 7.14 where p is an odd prime and $P = \frac{p-1}{2} = 2k+1$ is odd.
8. Show that if $p \nmid m$, then $\sum_{a=1}^{p-1} \left(\frac{ma}{p}\right) = 0$.
   (*Hint: show first that* $\sum \left(\frac{a}{p}\right) = 0$, *then recall that multiplication by m permutes residue classes...*)
9. Let a be given and suppose that n is a value assumed by the polynomial $f(x,y) = x^2 - ay^2$ where $x, y \in \mathbb{Z}$. Prove that, for every odd prime divisor p of n, either $p \mid x$ or $\left(\frac{a}{p}\right) = 1$.

7.2 Quadratic Reciprocity

For a result which is essentially unknown outside mathematics, the law of quadratic reciprocity has a surprising number of distinct proofs: around 200 are claimed, arguably more than any other result. Gauss himself gave at least *six* in his lifetime, the first when he was only 18, and the law is said to have been his favorite theorem. So why did he like it so much? Have a read and judge for yourself...

Theorem 7.16 (Quadratic Reciprocity). *If $p \neq q$ are prime, then*

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

Otherwise said, $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \iff$ both $p, q \equiv 3 \pmod 4$.

Reciprocity encompasses the idea that if q says something about p, then p says something about q:

> If we know whether (or not) $x^2 \equiv p \pmod q$ has a solution, then we know whether (or not) $x^2 \equiv q \pmod p$ has a solution.

That these equations should have anything to do with each other is surprising to say the least! We'll give a proof of the law later, but for now we start by seeing its utility.

Examples 7.17. 1. Suppose we are asked to decide whether -1500 is a QR modulo 997. We start to compute, using all our knowledge from the previous section:

$$\begin{aligned}
\left(\frac{-1500}{977}\right) &= \left(\frac{-1}{997}\right)\left(\frac{3}{997}\right)\left(\frac{2^2}{997}\right)\left(\frac{5^3}{997}\right) && \text{(Theorem 7.6, part 3)}\\
&= \left(\frac{-1}{997}\right)\left(\frac{3}{997}\right)\left(\frac{5}{997}\right) && \text{(Theorem 7.6, part 2)}\\
&= \left(\frac{3}{997}\right)\left(\frac{5}{997}\right) && \text{(Theorem 7.11, since } 997 \equiv 1 \pmod 4)
\end{aligned}$$

Without reciprocity, we'd be stuck with Euler's criterion (Theorem 7.9) and the nasty evaluation of $3^{498}5^{498} \pmod{997}$. Instead we simply flip the Legendre symbols and continue!

$$\begin{aligned}
\left(\frac{-1500}{977}\right) &= \left(\frac{997}{3}\right)\left(\frac{997}{5}\right) && \text{(reciprocity, since } 997 \equiv 1 \pmod 4)\\
&= \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = -1 && \text{(Theorem 7.14)}
\end{aligned}$$

We conclude that -1500 is a quadratic non-residue modulo 997.

2. We use reciprocity three times: note that $997 \equiv 1$ and $43, 563 \equiv 3 \pmod 4$:

$$\begin{aligned}
\left(\frac{563}{997}\right) = \left(\frac{997}{563}\right) = \left(\frac{-129}{563}\right) &= \left(\frac{-1}{563}\right)\left(\frac{3}{563}\right)\left(\frac{43}{563}\right) && \text{(factorize: Theorem 7.6)}\\
&= (-1)(-1)\left(\frac{563}{3}\right)(-1)\left(\frac{563}{43}\right) = -\left(\frac{2}{3}\right)\left(\frac{4}{43}\right) = 1 && \text{(Theorem 7.14)}
\end{aligned}$$

Note that this calculation doesn't help us solve the congruence $x^2 \equiv 563 \pmod{997}$: it only tells us that solutions[a] exist!

[a] In fact $x \equiv \pm 470 \equiv 470,\ 527 \pmod{997}$

Jacobi Symbols

Legendre symbols have a huge weakness: the reciprocity formula only applies when you have two primes. For large numbers you might need to do a lot of factorizing or perform several computations of the form $a^{\frac{p-1}{2}}$. With a small extension of the definition, however, this problem can be overcome and the computation of Legendre symbols becomes purely algorithmic.

Definition 7.18. Let a be an integer and n an odd positive integer. If $n = p_1^{\lambda_1} \cdots p_k^{\lambda_k}$ is the prime decomposition, then we define the *Jacobi Symbol* $\left(\frac{a}{n}\right)$ in terms of the Legendre symbols $\left(\frac{a}{p_i}\right)$

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\lambda_1} \cdots \left(\frac{a}{p_k}\right)^{\lambda_k}$$

If n is an odd prime, then $\left(\frac{a}{n}\right)$ is plainly a Legendre symbol. Moreover, the basic properties of Legendre symbols *and* the reciprocity results (Theorems 7.6, 7.11, 7.14 & 7.16) translate over almost immediately:

Theorem 7.19. *If $a, b \in \mathbb{Z}$ and m, n are odd positive integers, then;*

1. $a \equiv b \pmod{n} \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\gcd(a, n) = 1 \implies \left(\frac{a^2}{n}\right) = 1$
3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
4. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
5. $\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4} \\ -1 & \text{if } n \equiv 3 \pmod{4} \end{cases}$
6. $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1, 7 \pmod{8} \\ -1 & \text{if } n \equiv 3, 5 \pmod{8} \end{cases}$
7. *If* $\gcd(m, n) = 1$, *then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} = \begin{cases} 1 & \iff m \text{ or } n \equiv 1 \pmod{4} \\ -1 & \iff m \text{ and } n \equiv 3 \pmod{4} \end{cases}$$

The only real disadvantage of working modulo a composite n is that a Jacobi symbol being 1 doesn't correspond to the existence of solutions to a quadratic congruence.

Example 7.20. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, however $x^2 \equiv 2 \pmod{15}$ has no solution!

We won't pursue this further, instead using Jacobi symbols mainly to assist with the computation of Legendre symbols.

Proof. Arguments are barely required for parts 1–4: these follow from the corresponding propertied of Legendre symbols and the Definition. Parts 5 and 6 are exercises.

We content ourselves with a proof of the main reciprocity law (part 7).
Let $m = p_1 \cdots p_k$ and $n = q_1 \cdots q_l$ be the prime decompositions, where there are no primes in common between the lists and repeats are permitted. Then, by decomposing (parts 3, 4) and applying the quadratic reciprocity law,

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \left(\frac{p_1 \cdots p_k}{n}\right)\left(\frac{n}{p_1 \cdots p_k}\right) = \prod_{i=1}^{k}\left(\frac{p_i}{n}\right)\left(\frac{n}{p_i}\right) = \prod_{i=1}^{k}\left(\frac{p_i}{q_1 \cdots q_l}\right)\left(\frac{q_1 \cdots q_l}{p_i}\right) \\ &= \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i,j}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\end{aligned}$$

Since the only way a negative can appear is if *both* $p_i \equiv q_j \equiv 3 \pmod 4$, we count the number of such primes in each of m and n. Suppose there are s and t such primes in m and n respectively, then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{st} = \begin{cases} 1 & \iff s \text{ or } t \text{ even} \iff m \text{ or } n \equiv 1 \pmod 4 \\ -1 & \iff s \text{ and } t \text{ odd} \iff m \text{ and } n \equiv 3 \pmod 4 \end{cases}$$

■

If you're unsure why the final implications hold, revisit the discussion of primes modulo 4 from earlier in the course.

The usefulness of Jacobi symbols is that we can apply the rules *without checking primality!* By combining the rules, we can easily compute the value of any Legendre (or Jacobi) symbol, where the only required factorizations are to divide out negatives and 2's.

Example 7.21. We know that 317 is prime, and we want to check whether 246 is a quadratic residue. We compute, indicating which part of the theorem we're using each time.

$$\begin{aligned}\left(\frac{246}{317}\right) &= \left(\frac{2}{317}\right)\left(\frac{123}{317}\right) = -\left(\frac{123}{317}\right) && \text{(parts 3, 6: since } 317 \equiv 5 \pmod 8\text{)} \\ &= -\left(\frac{317}{123}\right) && \text{(part 7: since } 317 \equiv 1 \pmod 4\text{)} \\ &= -\left(\frac{71}{123}\right) = \left(\frac{123}{71}\right) && \text{(parts 1, 7: since } 71, 123 \equiv 3 \pmod 4\text{)} \\ &= \left(\frac{31}{71}\right) = -\left(\frac{71}{31}\right) && \text{(parts 1, 7: since } 31, 71 \equiv 3 \pmod 4\text{)} \\ &= -\left(\frac{9}{31}\right) = -1 && \text{(parts 1 and 2)}\end{aligned}$$

Therefore 246 is a quadratic non-residue modulo 317.

It is easy to see how to state this algorithmically: to find $\left(\frac{a}{n}\right)$:

1. Reduce a modulo n, factor out any copies of $\left(\frac{-1}{n}\right)$, $\left(\frac{2}{n}\right)$ or $\left(\frac{b^2}{n}\right)$ and evaluate.
2. Apply the main reciprocity formula to each remaining factor.
3. Repeat steps 1 & 2 until all terms in step 1 are evaluated.

Primality Testing

Recall Euler's criterion: if n is an odd prime and $n \nmid a$, then $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$. If we are not sure whether n is prime, we could compute both sides of this for some a...

Definition 7.22 (Solovay–Strassen Primality Test). Let n be an odd positive integer. A *witness* to the compositeness of n is any unit $a \in \mathbb{Z}_n^\times$ for which

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n}$$

If n is composite, any unit a for which $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$ is termed a *liar*, and n a *pseudoprime to base* a.

One witness is all you need to prove that n is composite! Even if n is very large, both sides of the congruence can be found rapidly with a computer. Moreover, if n is composite, *at least half* of the units modulo n can be shown to be witnesses, so you shouldn't have to try for long.

As a test for *primality*, Solovay–Strassen is only *probabilistic*. If you try four values of a and find no witnesses, then you have roughly a $\frac{1}{2^4} = \frac{1}{16}$ chance that n is composite; ten trials without a witness and the probability drops to roughly $\frac{1}{1024}$. Of course this is no good for *proving* that a large number is prime: you would have to try *half* the remainders without finding a witness before this could be your certain conclusion!

Examples 7.23. 1. We test to see if $n = 3599$ is composite by choosing $a = 2$. Use successive squaring to compute

$$2^{\frac{n-1}{2}} \equiv 2^{1799} \equiv 946 \pmod{3599}$$

Plainly this isn't ± 1 and so cannot be the value of a Lagrange/Jacobi symbol: $a = 2$ is therefore a witness and n is composite. For completion, since $8 \mid 200$ we can quickly verify that

$$n \equiv -1 \equiv 7 \pmod{8} \implies \left(\frac{2}{3599}\right) = 1$$

In fact $n = 59 \times 61$, but we did not need this information.

2. Given the 1000-digit number $n = 10^{999} + 7$, we have a computer verify that, modulo n,

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \text{ for each } a \in \{2, 3, 5, 7, 11\}$$

We conclude that n is likely prime with a probability of at least $1 - \frac{1}{2^5} = \frac{2047}{2048} = 99.95\%$ (this took the computer only 200 μs!). In fact n is prime; the smallest 1000-digit prime.

There are many other primality tests of varying degrees of complexity and predictive power. Computer packages are likely to rely on the Miller–Rabin test and its extension, the Baillie-PSW test. While neither test can prove conclusively that a given candidate is prime, no counter-examples (*pseudoprimes*) are known for the latter.

Gauss' Lemma and the Proof of Quadratic Reciprocity

With a view to proving the quadratic reciprocity law, we revisit the idea of least residues (page 60).

Definition 7.24. Let p be an odd prime and define $P = \frac{p-1}{2}$. Given $a \in \mathbb{Z}$, its *least residue modulo* p is the unique value r such that

$$a \equiv r \pmod{p} \text{ and } -P \leq r \leq P$$

If $r < 0$ we say that a has *negative least residue.* Now define a counting function; if $p \nmid a$ let,

$$\mu(a,p) = \left|\{x \in \{a, 2a, 3a, \ldots, Pa\} : x \text{ has negative least residue modulo } p\}\right|$$

Example 7.25. To find $\mu(8,13)$, start with $P = \frac{13-1}{2} = 6$ and compute

$$\{8k : 1 \leq k \leq \tfrac{13-1}{2}\} = \{8, 16, 24, 32, 40, 48\} \equiv \{-5, 3, -2, 6, 1, -4\} \implies \mu(8,13) = 3$$

One purpose of the function μ is to provide a general way of computing Legendre symbols.

Theorem 7.26 (Gauss' Lemma). $\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$

Examples 7.27. 1. Continuing the previous example, we verify that

$$\left(\frac{8}{13}\right) = \left(\frac{2^2}{13}\right)\left(\frac{2}{13}\right) = -1 = (-1)^{\mu(8,13)}$$

2. To compute $\mu(17,11)$, note that $17 \equiv -5 \pmod{11}$ and build the set

$$\{17, \ldots, 5 \cdot 17\} \equiv \{-5, 1, -4, 2, -3\} \pmod{11} \implies \mu(17,11) = 3$$

Similarly, $11 \equiv -6 \pmod{17}$, whence

$$\{11, \ldots, 8 \cdot 11\} \equiv \{-6, 5, -1, -7, 4, -2, -8, 3\} \pmod{17} \implies \mu(11,17) = 5$$

By Gauss' Lemma, neither $x^2 \equiv 17 \pmod{11}$ nor $x^2 \equiv 17 \pmod{11}$ have solutions.

The proof is little more than a generalization of part of Theorem 7.14.

Proof. Since a is invertible modulo p, the (least) residues $a, 2a, 3a, \ldots, Pa$ are distinct. Moreover, for any $x, y \in \{1, \ldots, P\}$, if the least residues of ax, ay were negative each other,

$$ax \equiv -ay \implies x \equiv -y \pmod{p}$$

is a contradiction. We conclude that, modulo p, we have $\{a, 2a, 3a, \ldots, Pa\} = \{(\pm 1), (\pm 2), \ldots, (\pm P)\}$ where precisely one of each $\pm$ remainder appears. Plainly $\mu(a,p)$ is the number of negative signs appearing in the second representation. To finish, simply multiply together the remainders, cancel $P!$, and recall Euler's criterion (Theorem 7.9):

$$a^{\frac{p-1}{2}} P! \equiv a \cdot 2a \cdot 3a \cdot Pa \equiv (-1)^{\mu(a,p)} P! \implies a^{\frac{p-1}{2}} \equiv (-1)^{\mu(a,p)} \pmod{p}$$

■

In view of Gauss' Lemma, the quadratic reciprocity formula may now be rewritten as

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

To complete the proof, it suffices to show that

$$\mu(p,q) + \mu(q,p) \equiv \frac{p-1}{2}\cdot\frac{q-1}{2} \pmod 2$$

We do this somewhat sneakily: given distinct primes p, q construct the hexagon H as shown.

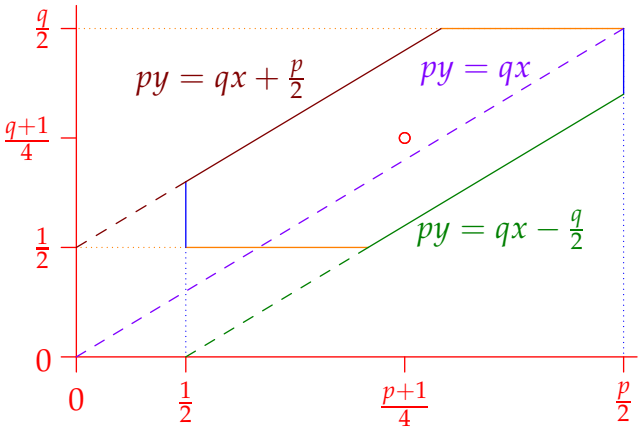
All points inside H satisfy four inequalities

$$\frac{1}{2} < x < \frac{p}{2} \qquad \frac{1}{2} < y < \frac{q}{2}$$

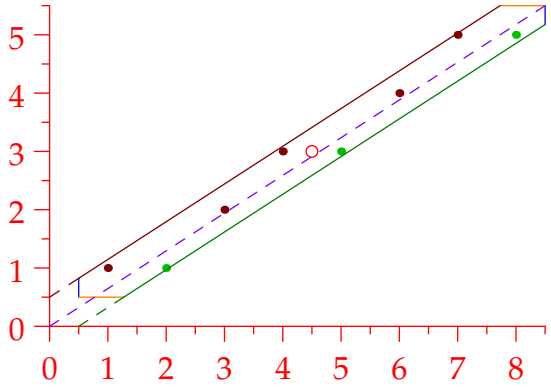
$$-\frac{q}{2} < py - qx < \frac{p}{2}$$

The circled point has co-ordinates $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$

We count the number of points with *integer* co-ordinates inside H in two ways, thereby recovering both sides of the desired congruence.

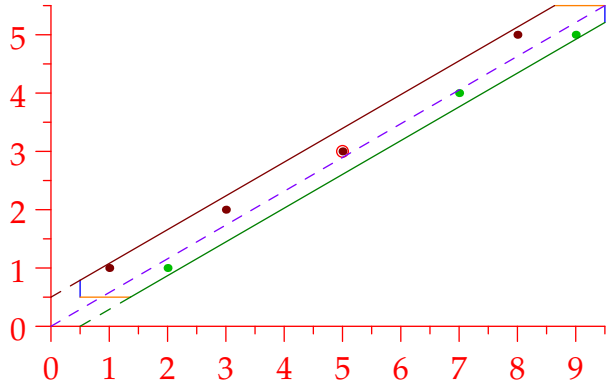


Here are two concrete examples where the integer points are plotted. We color the points differently depending on their location relative to the diagonal. Our goal is to relate the numbers of these points to values of Gauss' μ-function.



$p = 17,\ q = 11$

$\mu(p,q) + \mu(q,p) = 3 + 5$ is *even*



$p = 19,\ q = 11$

$\mu(p,q) + \mu(q,p) = 3 + 4$ is *odd*

The main result follows by observing some simple properties regarding the distribution of the integer points: see if you can make the relevant hypotheses *before* turning the page!

Lemma 7.28. *The integer points in H satisfy the following:*

1. *Symmetry around the circled point $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$. The number of integer points is odd precisely when the circled point has integer co-ordinates: when $p, q \equiv 3 \pmod 4$.*
2. *(a) No points lie on the boundaries or the diagonal of H.*
   (b) $\mu(p,q)$ points lie below the diagonal.
   (c) $\mu(q,p)$ points lie above the diagonal.

By part 2, the number of integer points in H is $\mu(p,q) + \mu(q,p)$. By part 1, this total is congruent to $\frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2$. The Lemma therefore establishes the required formula and completes the proof of the quadratic reciprocity law (Theorem 7.16).

Proof. 1. The reflection of (x,y) in the circled point is given by[a]

$$\left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$$

Since p, q are *odd*, this has integer co-ordinates if and only if (x,y) does.

It is moreover straightforward to check that the reflection maps opposite edges of H to each other: the circled point is therefore the centroid of H (and of the integer points therein).

2. (a) This is an easy exercise.

(b) Suppose $(x,y) \in H$ is an integer point lying below the diagonal. Since $(x,y) \in H$, we have

$$\frac{1}{2} < x < \frac{p}{2}, \quad \frac{1}{2} < y < \frac{q}{2}$$

To lie below the diagonal means

$$-\frac{q}{2} < py - qx < 0 \iff py \text{ has } \textit{negative least residue} \text{ modulo } q$$

Conversely, suppose y is an integer satisfying $\frac{1}{2} < y < \frac{q}{2}$ and such that py has negative least residue modulo q. Precisely one positive integer $x \left(> \frac{1}{2}\right)$ satisfies the inequality $-\frac{q}{2} < py - qx < 0$. Moreover,

$$qx < py + \frac{q}{2} \implies x < \frac{p}{q}y + \frac{1}{2} < \frac{p}{q} \cdot \frac{q}{2} + \frac{1}{2} = \frac{p+1}{2} \implies x \leq \frac{p-1}{2} < \frac{p}{2}$$

since x is an *integer*. We therefore obtain a point $(x,y) \in H$ lying below the diagonal.
We conclude that there are precisely as many integer points below the diagonal as there are elements with negative least residue modulo q in the set

$$\left\{py : y = 1, \ldots, \tfrac{q-1}{2}\right\} = \left\{p, 2p, 3p, \ldots, \tfrac{q-1}{2}p\right\}$$

Otherwise said, there are $\mu(p,q)$ integer points below the diagonal.

(c) Being almost identical to part (b), we omit the argument. ∎

[a] If you're unsure why, observe that the midpoint of (x,y) and its reflection is $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$. Alternatively, think vector thoughts and compute $(x,y) + 2\left[\left(\frac{p+1}{4}, \frac{q+1}{4}\right) - (x,y)\right]$...

Exercises 7.2 1. Recall Exercise 7.21. Compute the Legendre symbol $\left(\frac{246}{317}\right)$ *without* using Jacobi symbols: i.e. factorize 246 fully, and use reciprocity *only* if both terms are prime.

2. Evaluate the Legendre symbols $\left(\frac{503}{773}\right)$ and $\left(\frac{501}{773}\right)$ using any method you like.

3. (a) Pretend you don't know the prime factorization of 91. Compute $\left(\frac{9}{91}\right)$ and $9^{45} \pmod{91}$. What do you observe? Does this say anything about whether 91 is prime or composite?
   (b) Now compute $\left(\frac{2}{91}\right)$ and $2^{45} \pmod{91}$. What happens this time?

4. (a) Identify the witnesses and liars for the Solovay–Strassen test modulo 15.
   (b) Explain why there are *at least two* liars for every odd composite modulus n.
   (c) Let n be composite and suppose a is a witness and b a liar for n:

$$\gcd(a,n) = 1 = \gcd(b,n), \quad a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \text{ and } b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$$

   By considering ab, prove there are at least as many witnesses as liars.
   (*This explains the $\frac{1}{2^k}$ probability estimation in the Solovay–Strassen test*)

5. A simpler primality test involves checking only that $a^{\frac{n-1}{2}} \equiv \pm 1$. Comment on your answer to question 3b, and compare what happens with the simple test and Solovay–Strassen for $a = 8$ modulo $n = 21$.

6. Compute the value of $\mu(12, 17)$ by finding the least residues of the set $\{12, 24, \ldots, 12 \cdot 8\}$. Confirm that your set of least residues and the value of μ fits with Gauss' Lemma.

7. Revisit Theorems 7.11 and 7.14, where we computed the values of $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$. What are the values of $\mu(-1, p)$ and $\mu(2, p)$?

8. Use the law of quadratic reciprocity to prove that, for any prime $p \geq 5$, we have

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \iff p \equiv 1 \text{ or } 11 \pmod{12} \\ -1 & \iff p \equiv 5 \text{ or } 7 \pmod{12} \end{cases}$$

9. Verify the claim about the opposite sides of H being reflected to each other in the proof of Lemma 7.28. Also prove part 2(a) of the same result.

10. We prove parts 5 and 6 of Theorem 7.19.
    (a) Suppose that $n = p_1 \cdots p_k q_1 \cdots q_l$ is written as a product of primes where each $p_i \equiv 1$ and $q_j \equiv 3 \pmod{4}$. Prove that $n \equiv (-1)^l \pmod{4}$. Hence establish the formula for the Jacobi symbol $\left(\frac{-1}{n}\right)$.
    (b) (Harder) Prove the formula for the Jacobi symbol $\left(\frac{2}{n}\right)$.
    (*Hint: write n as a product of primes congruent to each of 1, 3, 5 and 7 modulo 8 and think about their products modulo 8*)

11. (For a bit of fun to end the term)
    (a) Find all the 2-digit integers x whose squares end in x (i.e. $10 \leq x \leq 99$).
    (b) Show that the only 3-digit integers x whose squares end in x are 376 and 625.
    (c) See how far you can generalize the problem…