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

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

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:

$$6 \times 9 \equiv 6 \times 5 \pmod 8 \implies 6 \times 9 = 6 \times 5 + 8m \text{ for some}^{1} m \in \mathbb{Z}$$

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

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

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 $2 = \gcd(6, 8)$...

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[2] of Bézout's identity, we see that

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

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

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

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

[2] If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$. 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*.[3] 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!

[3] 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:

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

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

$$\begin{aligned} \mathbf{133} &= 8 \cdot \mathbf{15} + \mathbf{13} \\ \mathbf{15} &= 1 \cdot \mathbf{13} + \mathbf{2} \\ \mathbf{13} &= 6 \cdot \mathbf{2} + \mathbf{1} \end{aligned} \qquad \Longrightarrow d = \gcd(15, 133) = \mathbf{1} \begin{aligned}[t] &= \mathbf{13} - 6 \cdot \mathbf{2} = \mathbf{13} - 6(\mathbf{15} - \mathbf{13}) \\ &= 7 \cdot \mathbf{13} - 6 \cdot \mathbf{15} \\ &= 7(\mathbf{133} - 8 \cdot \mathbf{15}) - 6 \cdot \mathbf{15} \\ &= 7 \cdot \mathbf{133} - 62 \cdot \mathbf{15} \end{aligned}$$

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!

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

We can even factorize in the familiar manner:

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

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,

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

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.[4] 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.

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

Examples 3.20. 1. By testing the values[5] $x \equiv 0, 1, -1 \pmod 7$, 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!

[5] 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[6] 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

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

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

Riffle-shuffling

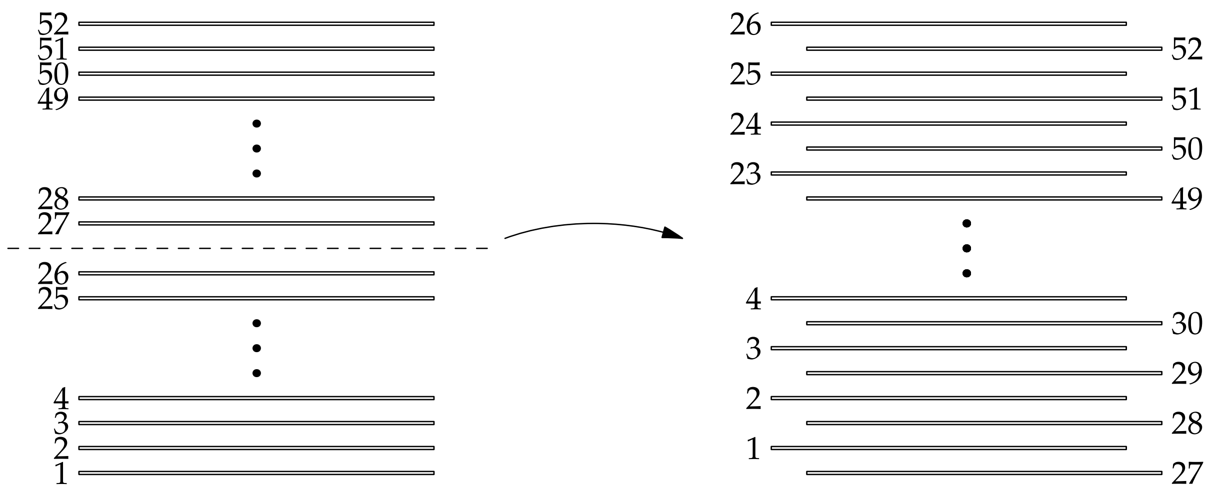
As a fun example of Fermat at work, consider a standard 'riffle' shuffle of a 52-card deck of playing cards. The process is as follows:

- 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?