Contents

2 Modular Arithmetic in $\mathbb{Z}$

In this chapter, we develop modular arithmetic in $\mathbb{Z}$ and construct the ring $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo m. Then we study the multiplicative structure of the elements with a focus in particular on the units and zero divisors. Next, we analyze systems of modular congruences in one variable and prove the celebrated Chinese Remainder Theorem establishing when a solution to a system of simultaneous congruences will exist.

We then use these results to study the behavior of powers of elements in $\mathbb{Z}/m\mathbb{Z}$, and to prove Fermat's Little Theorem, Wilson's Theorem, and Euler's generalization of Fermat's Little Theorem, and study the related Euler φ-function. We finish with a brief discussion of some applications of these ideas to repeating decimal expansions, and give a brief discussion of primitive roots and discrete logarithms modulo m and how they can be used to compute roots modulo m.

2.1 Modular Congruences and The Integers Modulo m

- The ideas underlying modular arithmetic are familiar to anyone who can tell time. For example, 3 hours after 11 o'clock, it is 2 o'clock. This is quite natural despite the fact that $3+11$ is 14, not 2: simply put, we identify times that are 12 hours apart as the same time of day.

2.1.1 Modular Congruences

- Modular congruence is simply a formalization of this "clock arithmetic":
- Definition: If m is a positive integer and m divides $b-a$, we say that a and b are congruent modulo m (or equivalent modulo m), and write "$a \equiv b \pmod{m}$".
  - Notation: As shorthand we usually write "$a \equiv b \pmod{m}$", or even just "$a \equiv b$" when the modulus m is clear from the context.
  - The statement $a \equiv b \pmod{m}$ can be thought of as saying "a and b are equal, up to a multiple of m".
  - Observe that if $m|(b-a)$, then $(-m)|(b-a)$ as well, so we do not lose anything by assuming that the modulus m is positive.
  - Example: $3 \equiv 9 \pmod{6}$, since 6 divides $9-3=6$.
  - Example: $-2 \equiv 28 \pmod{5}$, since 5 divides $28-(-2)=30$.
  - Example: $0 \equiv -666 \pmod{3}$, since 3 divides $-666-0=-666$.
  - If m does not divide $b-a$, we say a and b are not congruent mod m, and write $a \not\equiv b \pmod{m}$.
  - Example: $2 \not\equiv 7 \pmod{3}$, because 3 does not divide $7-2=5$.
- Modular congruences share a number of properties with equalities:
- Proposition (Modular Congruences): For any positive integers m, k and any integers a, b, c, d, the following are true:

  1. $a \equiv a \pmod{m}$.
  2. $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$.
  3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
  4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$.
  5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
  6. If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$.
  7. If $d|m$, then $a \equiv b \pmod{m}$ implies $a \equiv b \pmod{d}$.
     - Proof: Each of these follows in a relatively straightforward way from the definition of modular congruence. The trickiest is (5), which follows by observing that if m divides $b-a$ and m divides $d-c$, then m divides $bd-ac = b(d-c)+a(b-a)$.
- The first three properties above demonstrate that congruence modulo m is an equivalence relation. As such, we can think of congruence as a sort of "weakened equality": the statement $a \equiv b \pmod{m}$ says that a and b are equal, up to adding or subtracting a multiple of m.
  - Recall that a binary relation $\sim$ defined on a set S is called an equivalence relation if it obeys the following three axioms:

    [E1] For any $a \in S$, $a \sim a$.
    [E2] For any $a, b \in S$, $a \sim b$ implies $b \sim a$.
    [E3] For any $a, b, c \in S$, $a \sim b$ and $b \sim c$ together imply $a \sim c$.
  - Example: Equality of elements in any set (e.g., equality of real numbers) is an equivalence relation.
  - Example: The relation of having the same birthday (on the set of people) is an equivalence relation.

2.1.2 Residue Classes Modulo m

- We would now like to study "arithmetic modulo m". To do this, we need to define the underlying objects of study:
- Definition: If a is an integer, the residue class of a modulo m, denoted $\overline{a}$, is the collection of all integers congruent to a modulo m. Observe that $\overline{a} = \{a + km,\ k \in \mathbb{Z}\}$.
    - Example: The residue class of 2 modulo 4 is the set $\{\dots, -6, -2, 2, 6, 10, 14, \dots\}$.
    - Example: The residue class of 2 modulo 5 is the set $\{\dots, -8, -3, 2, 7, 12, 17, \dots\}$.
    - Example: The residue class of 11 modulo 19 is the set $\{\dots, -27, -8, 11, 30, 49, 68, \dots\}$.
- To motivate modular arithmetic, let us examine the residue classes modulo 3 more closely:
    - The residue class of 0 is $\overline{0} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$ consisting of all multiples of 3.
    - The residue class of 1 is $\overline{1} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$, while the residue class of 2 is $\overline{2} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$.
    - The residue class of 3 is $\overline{3} = \{\dots, -6, -3, 0, 3, 6, 9, 12, \dots\}$, which is the same set as the residue class $\overline{0}$: thus we have $\overline{3} = \overline{0}$. This should not be surprising, since $3 \equiv 0 \pmod 3$.
    - In the same way, we can see that $\overline{4} = \overline{1}$, which stems from the fact that $4 \equiv 1 \pmod 3$. Likewise, $\overline{5} = \overline{2}$, since $5 \equiv 2 \pmod 3$.
    - If we try writing down other residue classes modulo 3, we can see that they are always equal to one of the three classes $\overline{0}$, $\overline{1}$, and $\overline{2}$ we have already identified.
- The observations made above will extend to residue classes modulo m for every m:
- Proposition (Properties of Residue Classes): Suppose m is a positive integer. Then

1. If a, b are integers with respective residue classes $\overline{a}$, $\overline{b}$ modulo m, then $a \equiv b \pmod m$ if and only if $\overline{a} = \overline{b}$.
    - Proof: If $\overline{a} = \overline{b}$, then by definition b is contained in the residue class $\overline{a}$, meaning that $b = a + km$ for some k. Thus, m divides $b - a$, so $a \equiv b \pmod m$.
    - Conversely, suppose $a \equiv b \pmod m$. If c is any element of the residue class $\overline{a}$, then by definition $c \equiv a \pmod m$, and therefore $c \equiv b \pmod m$.
    - Therefore, c is an element of the residue class $\overline{b}$, but since c was arbitrary, this means that $\overline{a}$ is contained in $\overline{b}$.
    - By the same argument with a and b interchanged, we see $\overline{b}$ is also contained in $\overline{a}$, so $\overline{a} = \overline{b}$.
2. Two residue classes modulo m are either disjoint or identical.
    - Proof: Suppose that $\overline{a}$ and $\overline{b}$ are two residue classes modulo m. If they are disjoint, we are done, so suppose there is some c contained in both.
    - Then $c \equiv a \pmod m$ and $c \equiv b \pmod m$, so $a \equiv b \pmod m$. Then by property (1), we see $\overline{a} = \overline{b}$.
3. There are exactly m distinct residue classes modulo m, given by $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$.
    - Proof: By the division algorithm, for any integer a there exists a unique r with $0 \leq r < m$ such that $a = qm + r$ with $q \in \mathbb{Z}$.
    - Then $a \equiv r \pmod m$, so every integer is congruent modulo m to precisely one of the m integers 0, 1, ... , $m - 1$, which is to say, every integer lies in precisely one of the residue classes $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$.

- Remark: If we apply results (2) and (3) from the proposition above when $m = 2$, we obtain the statement that every integer either leaves a remainder of 0 or 1 when divided by 2.
    - Equivalently, this says every integer is either even or odd, and no integer is both.

2.1.3 Modular Arithmetic

- Definition: The collection of residue classes modulo m is denoted $\mathbb{Z}/m\mathbb{Z}$ (read as "$\mathbb{Z}$ modulo $m\mathbb{Z}$" or "$\mathbb{Z}$ mod $m\mathbb{Z}$").
  - Notation: Many other authors denote this collection of residue classes modulo m as $\mathbb{Z}_m$. We will avoid this notation and exclusively use $\mathbb{Z}/m\mathbb{Z}$ (or its shorthand $\mathbb{Z}/m$), since $\mathbb{Z}_m$ is used elsewhere in algebra and number theory for a different object.
  - By our properties above, $\mathbb{Z}/m\mathbb{Z}$ contains exactly m elements $\overline{0}$, $\overline{1}$, ... , $\overline{m-1}$.
- We can now define "modular arithmetic" using residue classes:
  - The fact that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ imply $a+c \equiv b+d \pmod{m}$ and $ac \equiv bd \pmod{m}$ tell us that if we want to compute $a+c$ modulo m, then no matter which element b in the residue class of a and which element d in the residue class of c we take, the sum $b+d$ will lie in the same residue class as $a+c$, and the product bd will lie in the same residue class as ac.
- Definition: The addition operation in $\mathbb{Z}/m\mathbb{Z}$ is defined as $\overline{a}+\overline{b}=\overline{a+b}$, and the multiplication operation is defined as $\overline{a}\cdot\overline{b}=\overline{ab}$.
  - Here are the addition and multiplication tables for $\mathbb{Z}/5\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

  - Note that, for example, the statement $\overline{2}+\overline{4}=\overline{1}$ is now perfectly acceptable and correctly stated with the equals sign: it says that if we take any element in the residue class $\overline{2}$ (modulo 5) and add it to any element in the residue class $\overline{4}$ (modulo 5), the result will always lie in the residue class $\overline{1}$ (modulo 5).
  - Here are the addition and multiplication tables for $\mathbb{Z}/4\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

- Arithmetic modulo m is commonly described by ignoring residue classes entirely and only working with the integers 0 through $m-1$, with the result of every computation "reduced modulo m" to obtain a result lying in this range.
  - Thus, for example, to compute $3+10$ modulo 12, we would add to get 13 and then "reduce", yielding 1 modulo 12. Similarly, to find $3 \cdot 10$ modulo 12, we compute $3 \cdot 10 = 30$ and then reduce to obtain a result of 6 modulo 12.
  - However, this is a rather cumbersome and inelegant description. This definition is often used in programming languages, where "a mod m", frequently denoted "$a\%m$", is defined to be a *function* returning the corresponding remainder in the interval $[0, m-1]$.
  - Observe that with this definition, it is not true that $(a+b)\%m = (a\%m)+(b\%m)$, nor is is true that $ab\%m = (a\%m)\cdot(b\%m)$, since the sum and product may each exceed m. Instead, to obtain an actually true statement, one would have to write something like $ab\%m = [(a\%m)\cdot(b\%m)]\%m$.
  - In order to avoid such horrible kinds of statements, the best viewpoint really is to think of the statement $a \equiv b \pmod{m}$ as a congruence that is a "weakened" kind of equality, rather than always reducing each of the terms to its residue in the set $\{0, 1, \ldots, m-1\}$.
  - The other reason we adopt the use of residue classes is that they extend quite well to more general settings (i.e., abstract groups and rings) where we may not have such an obvious set of "representatives".

- Our fundamental result about arithmetic with residue classes is that $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring with 1:
- Theorem ($\mathbb{Z}/m\mathbb{Z}$ is a Ring): The set $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$ of residue classes modulo m, with addition defined by $\overline{a} + \overline{b} = \overline{a+b}$ and multiplication defined by $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, forms a commutative ring with 1. The additive identity is $\overline{0}$, the multiplicative identity is $\overline{1}$, and additive inverses are given by $-\overline{a} = \overline{-a}$.
    - Proof: We first need to show that these operations are well-defined: in other words, we need to check that if we choose different elements $a' \in \bar{a}$ and $b' \in \bar{b}$, the residue class of $a' + b'$ is the same as that of $a + b$, and similarly for the product.
    - These statements follow from our remarks earlier: explicitly, since $a' \in \bar{a}$ there exists k_1 with $a' = a + k_1 m$ and similarly since $b' \in \bar{b}$ there exists k_2 with $b' = b + k_2 m$.
    - Then $a' + b' = (a+b) + m(k_1 + k_2)$, and since these differ by a multiple of m, we see that $\overline{a' + b'} = \overline{a+b}$.
    - Similarly, $a'b' = (a + k_1 m)(b + k_2 m) = ab + m(k_1 b + k_2 a + k_1 k_2 m)$, so $\overline{a'b'} = \overline{ab}$.
    - Hence the operations are well-defined.
    - The ring axioms [R1]-[R8] then follow from their corresponding versions inside $\mathbb{Z}$.
    - For example, for [R1], by definition we have $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b+c} = \overline{a + (b+c)}$ and also $(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c}$.
    - But by the associative property [Z1] in $\mathbb{Z}$, we know that $a + (b+c) = (a+b) + c$, so the associated residue classes are also equal.
    - The other properties follow in a similar way.

2.1.4 Units in $\mathbb{Z}/m\mathbb{Z}$

- We have constructed $\mathbb{Z}/m\mathbb{Z}$ and shown that it has the structure of a commutative ring with 1.
    - For convenience, we will now frequently abuse notation and ignore the distinction between "the residue class of a modulo m" and simply refer to integers modulo m.
    - Observe that the integers modulo m form a *finite* ring, unlike our previous examples of rings like $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Z}[i]$, all of which are infinite.
- A basic question is: what are the units in $\mathbb{Z}/m\mathbb{Z}$? In other words, which residue classes $\overline{a}$ have a multiplicative inverse, meaning that there exists some other residue class $\overline{x}$ with $\overline{x} \cdot \overline{a} = \overline{1} \bmod m$?
    - For example, looking at the multiplication table modulo 6 indicates that $\overline{1}$ and $\overline{5}$ have multiplicative inverses (equal to themselves) while $\overline{0}$, $\overline{2}$, $\overline{3}$, and $\overline{4}$ do not.
    - We can see that 1 and 5 are relatively prime to 6, while 0, 2, 3, and 4 have a common divisor with 6 that is bigger than 1. This is, indeed, what happens in general:
- Proposition (Units in $\mathbb{Z}/m\mathbb{Z}$): A residue class $\overline{a}$ is a unit modulo m if and only a and m are relatively prime.
    - Proof: First suppose $\overline{a}$ is a unit modulo m. Then there exists an integer x with $xa \equiv 1 \pmod m$. By definition, this means there exists an integer y such that $xa - 1 = ym$, so that $xa + ym = 1$. But this implies a and m are relatively prime, as their gcd must divide $xa + ym = 1$ hence must equal 1.
    - Conversely, suppose $\gcd(a, m) = 1$. Then there exist integers x and y such that $xa + ym = 1$. By definition this means $xa \equiv 1 \pmod m$, so $\overline{x} \cdot \overline{a} = \overline{1} \bmod m$.
- Corollary: The residue classes modulo m form a field if and only if m is prime.
    - Proof: If $m = 1$ then the result is trivial. Otherwise, for $m > 1$, then every nonzero integer modulo m is a unit precisely when each of 1, 2, ... , $m - 1$ is relatively prime to m, which is then equivalent to saying that m is prime.
- The above proposition gives a method to compute the inverse of a (presuming it has one): simply apply the Euclidean algorithm to generate x and y with $xa + ym = 1$: then the inverse of $\overline{a}$ modulo m is $\overline{x}$.

- Example: Find the inverse of 7 modulo 52.
  - We apply the Euclidean algorithm:

$$\begin{aligned} 52 &= 7 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \end{aligned}$$

    so the gcd is indeed 1. Solving for the remainders as linear combinations yields $3 = 52 - 7 \cdot 7$ and then $1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (52 - 7 \cdot 7) = 15 \cdot 7 - 2 \cdot 52$.
  - Thus, taking both sides modulo 52 yields $15 \cdot 7 \equiv 1 \pmod{52}$, and therefore $7^{-1} \equiv \boxed{15 \pmod{52}}$.
- Example: Find the inverse of 8537 modulo 44773.
  - By applying the Euclidean algorithm, we can verify that these two numbers are relatively prime.
  - Solving for the remainders as linear combinations yields

$$\begin{array}{rcccc} 2088 &=& & = & 1 \cdot 44773 - 5 \cdot 8537 \\ 185 &=& 8537 - 4 \cdot 2088 & = & -4 \cdot 44773 + 21 \cdot 8537 \\ 53 &=& 2088 - 11 \cdot 185 & = & 45 \cdot 44773 - 236 \cdot 8537 \\ 26 &=& 185 - 3 \cdot 53 & = & -139 \cdot 44773 + 729 \cdot 8537 \\ 1 &=& 53 - 2 \cdot 26 & = & 323 \cdot 44773 - 1694 \cdot 8537 \end{array} .$$

  - Thus, we see that $1 = 323 \cdot 44773 - 1694 \cdot 8537$.
  - Taking both sides modulo 44773 gives $-1694 \cdot 8537 \equiv 1 \pmod{44773}$, so $8537^{-1} \equiv \boxed{-1694 \equiv 43079 \pmod{44773}}$.

2.1.5 Zero Divisors in $\mathbb{Z}/m\mathbb{Z}$

- An important property of arithmetic that we often take for granted is that if x, y are such that $xy = 0$, then $x = 0$ or $y = 0$. However, this property no longer holds for congruences with an arbitrary modulus m.
  - For example, modulo 6 we have $\overline{2} \cdot \overline{3} = \overline{0}$, but $\overline{2} \neq \overline{0}$ and $\overline{3} \neq \overline{0}$.
  - This example also shows that we cannot, in general, perform arbitrary multiplicative cancellations modulo m: notice that $\overline{2} \cdot \overline{3} = \overline{2} \cdot \overline{0}$ modulo 6, but we cannot "cancel $\overline{2}$" because $\overline{3} \neq \overline{0}$ modulo 6.
- Definition: If R is a commutative ring, we say that $x \in R$ is a zero divisor if $x \neq 0$ and there exists a nonzero $y \in R$ such that $xy = 0$. (Note in particular that 0 is *not* a zero divisor!)
  - Example: In $\mathbb{Z}/6\mathbb{Z}$, since $\overline{2} \cdot \overline{3} = \overline{4} \cdot \overline{3} = \overline{0}$, the residue classes represented by 2, 3, and 4 are zero divisors.
- Proposition (Units and Zero Divisors): In a commutative ring with 1, a unit can never be a zero divisor.
  - Proof: If a were both a unit and a zero divisor, then there would exist b, x such that $ab = 1$ and $ax = 0$, with $x \neq 0$.
  - But then we would have $x = (ab)x = b(ax) = 0$, contradicting the assumption that $x \neq 0$.
- We now show that the zero divisors modulo m are simply the nonzero residue classes that are not units:
- Proposition (Zero Divisors in $\mathbb{Z}/m\mathbb{Z}$): An integer a is a zero divisor modulo m if and only if $1 < \gcd(a, m) < m$.
  - Proof: Let $d = \gcd(a, m)$. We break into cases depending on the value of d.
  - If $d = 1$, then a is a unit, and therefore is not a zero divisor.
  - If $d = m$, then $m | a$ meaning that $\overline{a} = \overline{0}$, and 0 is defined not to be a zero divisor.
  - If $1 < d < m$, then $(m/d) \cdot a = m \cdot (a/d) \equiv 0 \pmod{m}$, and m/d is nonzero. Therefore, a is a zero divisor.
- Example: Find the units and zero divisors in $\mathbb{Z}/10\mathbb{Z}$.

- From our description, we know that the units are the residue classes relatively prime to 10, while the zero divisors are the nonzero classes that are not relatively prime to 10.
- Thus, the units in $\mathbb{Z}/10\mathbb{Z}$ are $\boxed{\overline{1}, \overline{3}, \overline{7}, \overline{9}}$ while the zero divisors are $\boxed{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}}$.
- Indeed, we can explicitly verify that $\overline{1} \cdot \overline{1} = \overline{3} \cdot \overline{7} = \overline{7} \cdot \overline{3} = \overline{9} \cdot \overline{9} = \overline{1}$ so that the multiplicative inverses of $\overline{1}, \overline{3}, \overline{7}, \overline{9}$ are $\overline{1}, \overline{7}, \overline{3}, \overline{9}$ respectively, and also that $\overline{2} \cdot \overline{5} = \overline{4} \cdot \overline{5} = \overline{6} \cdot \overline{5} = \overline{8} \cdot \overline{5} = \overline{0}$ so that each of $\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}$ is indeed a zero divisor.

- Although the existence of zero divisors causes issues with cancellation, it turns out that we can still essentially perform cancellations (the only difficulty being that the modulus may change):
- Proposition (Modular Cancellation): If $m > 0$ and $d = \gcd(a, m)$, then $ax \equiv ay \pmod{m}$ is equivalent to $x \equiv y \pmod{m/d}$.
  - Proof: First suppose $ax \equiv ay \pmod{m}$. Then there exists an integer k with $a(y - x) = km$, so dividing both sides by d yields $\frac{a}{d}(y - x) = \frac{m}{d}k$.
  - Since $\gcd(a/d, m/d) = \gcd(a, m)/d = 1$, we see that $\frac{m}{d}$ divides $y - x$, meaning that $x \equiv y \pmod{m/d}$.
  - Conversely, suppose that $x \equiv y \pmod{m/d}$, meaning that there exists an integer l with $y - x = \frac{m}{d}l$.
  - Then $a(y - x) = \frac{a}{d}ml$, and since $\frac{a}{d}$ is an integer since d divides a, we see that m divides $a(y - x)$, which is to say, $ax \equiv ay \pmod{m}$.
- Example: Solve the congruence $2x \equiv 0 \pmod{6}$.
  - Since $0 = 2 \cdot 0$, the congruence is equivalent to $2x \equiv 2 \cdot 0 \pmod{6}$.
  - Since $\gcd(2, 6) = 2$ and $6/2 = 3$, then by the proposition on modular cancellation, the solution to the congruence is $\boxed{x \equiv 0 \pmod{3}}$, or equivalently, $\boxed{x \equiv 0, 3 \pmod{6}}$.
- We will further analyze the solutions to linear equations of this type in the next section.

2.2 Linear Equations Modulo m and The Chinese Remainder Theorem

- We now turn our attention to solving linear equations modulo m. Our first task is solving a single equation in a single variable, which (in general) has the form $ax \equiv b \pmod{m}$, where we wish to solve for x.
- Proposition (Linear Equations): The equation $ax \equiv b \pmod{m}$ has a solution for x if and only if $d = \gcd(a, m)$ divides b. If $d|b$, then the set of all such x is given by the residue class $\overline{r}$ modulo m/d, where r is any solution to the equation.
  - Proof: If x is a solution to the congruence $ax \equiv b \pmod{m}$, then there exists an integer k with $ax - mk = b$. Since $d = \gcd(a, m)$ divides the left-hand side, it must divide b.
  - Now suppose $d = \gcd(a, m)$ divides b, and set $a' = a/d$, $b' = b/d$, and $m' = m/d$.
  - Then the original equation becomes $a'dx \equiv b'd \pmod{m'd}$, which is equivalent to $a'x \equiv b' \pmod{m'}$, by one of our properties of congruences.
  - But since a' and m' are relatively prime, a' is a unit modulo m', so we can simply multiply by its inverse to obtain $x \equiv b' \cdot (a')^{-1} \pmod{m'}$. This means that there is a unique solution to the congruence modulo $m' = m/d$, as claimed.
- Now suppose that we wish to solve a collection of simultaneous congruences in the variable x.
  - The above proposition allows us to convert any single equation $cx \equiv d \pmod{m}$ to one of the form $x \equiv a \pmod{m'}$, or to see that such an equation has no solutions (in which case neither does the system!).

- Therefore, to solve general systems, all we must do is characterize those x which satisfy a system of the form

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

- Of course, it is possible for the equations to be inconsistent: for example, the system

$$\begin{aligned} x &\equiv 1 \pmod{4} \\ x &\equiv 2 \pmod{6} \end{aligned}$$

has no solution, because the first equation requires x to be odd and the second requires x to be even.

- The issue in the example above is that 4 and 6 are not relatively prime, and the equations give inconsistent requirements modulo $2 = \gcd(4, 6)$. It turns out that this is the only possible difficulty:

- Theorem (Chinese Remainder Theorem): Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers, and $a_1, a_2, \ldots, a_k$ be arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has an integral solution x. Furthermore, x is unique modulo $m_1 m_2 \cdots m_k$, and any other integer congruent to it modulo $m_1 m_2 \cdots m_k$ is also a solution.

  - Remark: This theorem is so named because it was known to Chinese mathematicians of antiquity. The earliest known statement of the result (as an example without an explicit proof or algorithm) is by the Chinese mathematician Sunzi in the 3rd century CE, and the earliest known algorithm for solving systems of congruences was given by Aryabhata in the 6th century CE.
  - Proof 1 (Semi-Constructive): Since we may repeatedly convert two congruences into a single one until we are done, it suffices to prove the result for two congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}. \end{aligned}$$

  - For existence, the first congruence implies $x = a_1 + km_1$ for some integer k; plugging into the second then yields $a_1 + km_1 \equiv a_2 \pmod{m_2}$. Rearranging yields $km_1 \equiv (a_2 - a_1) \pmod{m_2}$. Since by hypothesis m_1 and m_2 are relatively prime, by our proposition above we see that this congruence has a unique solution for k modulo m_2, and hence a solution for x.
  - For uniqueness, suppose x and y are both solutions. Then $x - y$ is 0 modulo m_1 and 0 modulo m_2, meaning that $m_1 | (x - y)$ and $m_2 | (x - y)$. But since m_1 and m_2 are relatively prime, their product must therefore divide $x - y$, meaning that x is unique modulo $m_1 m_2$. Finally, it is obvious that any other integer congruent to x modulo $m_1 m_2$ also satisfies the system.
  - Proof 2 (Constructive): Let $m = m_1 m_2 \cdots m_k$. Observe that for each i, m/m_i is an integer that is relatively prime to m_i, hence is a unit modulo m_i.
  - Let b_i be an inverse of m/m_i modulo m_i: observe that for $j \neq i$, we have $(m/m_i) b_j \equiv 0 \pmod{m_j}$, since m_j divides m/m_i.
  - Now we claim that $x_0 = \sum_{j=1}^{k} \frac{m}{m_j} b_j a_j$ is a simultaneous solution to all the congruences: modulo m_i, all terms vanish except the ith term of the sum, and there, we obtain $x_0 \equiv \frac{m}{m_i} b_i a_i \equiv a_i \pmod{m_i}$, since b_i and m/m_i are inverses mod m_i.

- The uniqueness follows in the same way as in Proof 1: if x and y are both solutions, then $x-y$ is divisible by each m_i and hence by their product (since they are relatively prime).
- Remark (for those who like ring theory): The Chinese Remainder Theorem has a natural generalization to an arbitrary ring R. In particular, in our setting, it implies that if the prime factorization of m is $m = p_1^{a_1} \cdots p_k^{a_k}$, then $\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})$, where the equivalence is a ring isomorphism.

- In practice, although the second proof gives a completely constructive solution (up to needing to use the Euclidean Algorithm to compute a number of inverses) for any system, by hand it is often easier to apply the method in the first proof.

- Example: Find all integers n such that $n \equiv 1 \pmod 7$ and $n \equiv 3 \pmod 8$.
  - The Chinese Remainder Theorem says we only need to compute one solution, and that all others are congruent modulo $7 \cdot 8$.
  - The first congruence implies that $n = 3 + 8k$ for some integer k.
  - Plugging into the second congruence yields $3 + 8k \equiv 1 \pmod 7$, which reduces to $k \equiv -2 \pmod 7$.
  - Taking $k = -2$ yields $n = 3 + 8k = -13$. The set of all solutions are the integers of the form $\boxed{-13 + 56d}$ for $d \in \mathbb{Z}$.

- Although the Chinese Remainder Theorem is only stated for relatively prime moduli, it is easy to deal with the case where the moduli have common divisors.
  - The Theorem implies that if $d|m$ and $\gcd(d, m/d) = 1$, the single equation $x \equiv a \pmod m$ is equivalent to the two equations $x \equiv a \pmod d$ and $x \equiv a \pmod{m/d}$.
  - Thus, if the moduli have common divisors, we need only compute the common divisors (rapidly, using the Euclidean Algorithm), and then split the congruences apart so as to have no common divisors.
  - If we can factor the moduli, we could also just split them all into prime powers. (However, we can still split the moduli into relatively prime pieces in the manner described above, even if we cannot factor them.)
  - Alternatively, we could simply use the method of Proof 1: solve each congruence plug it into the next one, and eliminate coefficients. This also works, though it requires a bit more care in dealing with the case where the coefficients and modulus have a common divisor. (It will also be less obvious precisely where a contradiction between the congruences occurs.)

- Example: Find all solutions to the congruences $n \equiv 34 \pmod{36}$, $n \equiv 7 \pmod{15}$, and $n \equiv 2 \pmod{40}$.
  - Method 1: First observe that 36 and 15 have a common divisor of 3. Since 3^2 divides 36, we split the first congruence into two congruences modulo 4 and 9, and the second into congruences modulo 3 and 5.
    - This yields $n \equiv 34 \pmod 4$, $n \equiv 34 \pmod 9$, $n \equiv 7 \pmod 3$, and $n \equiv 7 \pmod 5$.
    - These congruences' moduli have common divisors with the last congruence, which we split modulo 5 and modulo 8 to obtain $n \equiv 2 \pmod 5$ and $n \equiv 2 \pmod 8$.
    - We then have $n \equiv 34 \equiv 2 \pmod 4$, $n \equiv 34 \equiv 7 \pmod 9$, $n \equiv 7 \equiv 1 \pmod 3$, $n \equiv 7 \equiv 2 \pmod 5$, $n \equiv 2 \pmod 5$, and $n \equiv 2 \pmod 8$.
    - Removing duplicates yields no contradictions, and we get $n \equiv 7 \pmod 9$, $n \equiv 2 \pmod 5$, and $n \equiv 2 \pmod 8$, whose moduli are now relatively prime.
    - The second two congruences visibly have the common solution $n \equiv 2 \pmod{40}$, giving $n = 2 + 40k$ for some k.
    - Plugging into the only remaining congruence yields $2 + 40k \equiv 7 \pmod 9$, whence $4k \equiv 5 \pmod 9$. The inverse of 4 modulo 9 is easily computed as -2. Multiplying by it yields $k \equiv -10 \equiv -1 \pmod 9$.
    - Hence the congruences have a solution $x = 2 + 40k = -38$, and the set of all solutions is $x = \boxed{-38 + 360d}$ for $d \in \mathbb{Z}$.
  - Method 2: Solving the first congruence gives $n = 34 + 36k$ for some integer k.

* Plugging into the second congruence yields $34 + 36k \equiv 7 \pmod{15}$, which reduces to $6k \equiv 3 \pmod{15}$. We cancel the common factor of 3 from all terms, yielding $2k \equiv 1 \pmod{5}$, which has solution $k \equiv 3 \pmod{5}$.
* Thus, $k = 3 + 5l$ for some integer l, so $n = 142 + 180l$ for some integer l.
* Plugging into the third congruence yields $142 + 180l \equiv 2 \pmod{40}$, which reduces to $20l \equiv 20 \pmod{40}$. Cancelling the common factor of 20 from all terms yields $l \equiv 1 \pmod{2}$, so $l = 1 + 2m$ for some integer m.
* Substituting back gives the general solution $n = \boxed{322 + 360m}$ for some $m \in \mathbb{Z}$.

- We can also use the Chinese Remainder Theorem as a tool to solve polynomial equations of higher degree, by reducing the question to one where the modulus is a prime power.
- Example: Find all solutions to the equation $x^2 + 4x \equiv 12 \pmod{52}$.
  - Since $52 = 4 \cdot 13$, the Chinese Remainder Theorem says that solving the first system is equivalent to solving $x^2 + 4x \equiv 12 \pmod{4}$ and $x^2 + 4x \equiv 12 \pmod{13}$.
  - The first equation reduces to $x^2 \equiv 0 \pmod{4}$, which visibly has the two solutions $x \equiv 0, 2 \pmod{4}$. The second equation remains $x^2 + 4x \equiv 12 \pmod{13}$: there is no obvious factorization, so we simply try all of the residues modulo 13 to see that there are two solutions $x \equiv 2$ and $x \equiv 7$.
  - Hence the solutions to the original congruence are those integers satisfying $x \equiv 0, 2 \pmod{4}$ and $x \equiv 2, 7 \pmod{13}$. Using the Chinese Remainder Theorem we can solve for the four possible x modulo 52, obtaining $x \equiv \boxed{2, 20, 28, 46 \pmod{52}}$.
  - Remark: We will later discuss more general methods for solving quadratic equations modulo m.

2.3 Powers Modulo m: Orders, Fermat's Little Theorem, Wilson's Theorem, Euler's Theorem

- We now study powers of elements modulo m.
- As an example to motivate the discussion in the rest of this section, suppose we want to find the remainder when we divide 2^{516} by 61.
  - One way we could do this is simply by computing the actual integer 2^{516} (which has 156 digits in base 10), and then dividing it by 61. This is certainly feasible with a computer, but would be very unpleasant by hand.
  - A faster way would be to compute successive powers of 2 and reduce modulo 61 at each stage: 2, 4, 8, 16, 32, $64 \equiv 3$, 6, 12, 24, 48, $96 \equiv 35$, $70 \equiv 9$, 18, 36, ... This is certainly faster and feasible to do by hand (in the sense of not requiring the computation of a 156-digit integer), but it would still require over 100 multiplications.
  - We can speed up the process significantly if we instead only compute the powers 2^1, 2^2, 2^4, 2^8, 2^{16}, ... , 2^{512} and so forth (modulo 61) by successively squaring the previous values and reducing. Then we can compute $2^{516} = 2^{512} \cdot 2^4$.
  - Explicitly, we obtain the following:

$$\begin{array}{ccc} 2^2 = 4 & 2^{16} \equiv 12^2 = 144 \equiv 22 & 2^{128} \equiv 16^2 \equiv 12 \\ 2^4 = 16 & 2^{32} \equiv 22^2 = 484 \equiv -4 & 2^{256} \equiv 12^2 \equiv 22 \\ 2^8 = 16^2 \equiv 256 \equiv 12 & 2^{64} \equiv (-4)^2 = 16 & 2^{512} \equiv 22^2 \equiv -4 \end{array}$$

  - Therefore we see that $2^{516} = 2^{512} \cdot 2^4 \equiv (-4) \cdot 16 = -64 \equiv \boxed{58}$ modulo 61.
- For posterity, we record this technique of successive squaring:
- Algorithm (Successive Squaring): To compute a^k modulo m, first find the binary expansion of $k = \underline{b_d b_{d-1} \cdots b_0}$. Then compute the powers a^2, a^4, $\cdots$, a^{2^d} by squaring the previous entry in the sequence and reducing modulo m. Finally, compute $a^k \equiv \prod_{\substack{0 \le i \le d \\ b_i = 1}} a^{2^{b_i}}$ modulo m.

- Remark: Observe that the total number of multiplications and reductions mod m required is roughly $2\log_2(k)$, which is a vast improvement over the k multiplications and reductions required to compute a^k directly.

- We can also observe that, in the computations we performed, the later entries started repeating earlier ones. This will in fact always be the case, as we will see imminently.

2.3.1 Orders of Elements Modulo m

- We would like to study the behavior of powers of units modulo m.
  - As we have already observed, if u is a unit then so is u^k is also a unit for any integer k, since its inverse is $(u^{-1})^k$.
  - In particular, since there are only finitely many residue classes in $\mathbb{Z}/m\mathbb{Z}$, then the values of the powers of u must eventually repeat.
  - But if $u^a = u^b$ with $a < b$, multiplying both sides by u^{-a} shows that $u^{b-a} = 1$, meaning that some power of u is equal to 1. We give this situation a name:

- Definition: If u is a unit modulo m, the smallest $k > 0$ such that $u^k \equiv 1 \pmod{m}$ is called the order of u.
  - Notation: The classical number-theoretic terminology for "u has order k modulo m" is "u belongs to the exponent k modulo m".
  - Remark (for those who like group theory): Our use of the word "order" here agrees with the use of the word "order" in group theory, since the set of units in any ring (in particular, in $\mathbb{Z}/m\mathbb{Z}$) forms a group under multiplication.
  - Example: The powers of 2 in $\mathbb{Z}/11\mathbb{Z}$ are as follows:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	$\cdots$
2	4	8	5	10	9	7	3	6	1	2	4	$\cdots$

    Thus, 2 has order 10 in $\mathbb{Z}/11\mathbb{Z}$.
  - Example: The powers of 5 in $\mathbb{Z}/13\mathbb{Z}$ are as follows:

5^1	5^2	5^3	5^4	5^5	5^6	5^7	5^8	$\cdots$
5	12	8	1	5	12	8	1	$\cdots$

    Thus, 5 has order 4 in $\mathbb{Z}/13\mathbb{Z}$.

- We collect a few useful results about orders.

- Proposition (Properties of Orders): Suppose m is a positive integer and u is a unit modulo m.

1. If $u^n \equiv 1 \pmod{m}$ for some $n > 0$, then the order of u divides n.
   - Proof: Clearly, if $u^n \equiv 1 \pmod{m}$ for some $n > 0$, then $u^k \equiv 1 \pmod{m}$ for some minimal positive integer k by the well-ordering axiom.
   - Now let k be the order of u and apply the division algorithm to write $n = qk + r$ with $0 \leq r < k$: then we have $u^r = u^{n-qk} = u^n(u^k)^{-q} \equiv 1 \cdot 1^{-q} = 1 \pmod{m}$.
   - If r were not zero, then we would have $u^r \equiv 1 \pmod{m}$ with $0 < r < k$, which contradicts the definition of order. Thus $r = 0$, meaning that k divides n.
2. If u has order k, then u^n has order $k/\gcd(n,k)$. In particular, if n and k are relatively prime, then u^n also has order k.
   - Proof: Let $d = \gcd(n,k)$: then $(u^n)^{k/d} = (u^k)^{n/d} \equiv 1^{n/d} = 1 \pmod{m}$, so the order of u^n cannot be larger than k/d.
   - Furthermore, if $1 \equiv (u^n)^a \equiv u^{na} \pmod{m}$, (1) above implies that k divides na, so that k/d divides $(n/d)a$.

- But since k/d and n/d are relatively prime, this implies k/d divides a, and so $a \geq k/d$.
- Thus, the order of u^n is equal to k/d as claimed. The second statement is simply the case $d = 1$.

3. If $u^n \equiv 1 \pmod{m}$ and $u^{n/p} \not\equiv 1 \pmod{m}$ for any prime divisor p of n, then u has order n.
   - Proof: Suppose u has order k: then by the above, k must divide n.
   - If $k < n$, then there must be some prime p in the prime factorization of n that appears to a strictly lower power in the factorization of k: then k divides n/p.
   - But then $u^{n/p}$ would be an integral power of $u^k \equiv 1 \pmod{m}$, so that $u^{n/p} \equiv 1 \pmod{m}$, which is a contradiction. Thus, $r = n$.
4. If u has order k and w has order l, where k and l are relatively prime, then uw has order kl.
   - Proof: First observe that $(uw)^{kl} = (u^k)^l(w^l)^k \equiv 1 \pmod{m}$, uw has some finite order $d \leq kl$.
   - Since $(uw)^d \equiv 1 \pmod{m}$, raising to the kth power yields $1 \equiv (uw)^{dk} \equiv w^{dk} \pmod{m}$, so l divides dk.
   - Then since l and k are relatively prime, this implies l divides d. By a symmetric argument, k divides d. Since l and k are relatively prime, we see kl divides d, and so the only possibility is $d = kl$.
   - Remark: A weaker result also holds when the orders k and l are not relatively prime: in general, the argument above shows that the order of uw is a multiple of $kl/\gcd(k,l)^2$, and divides $kl/\gcd(k,l) = \operatorname{lcm}(k,l)$. (We cannot hope to sharpen these results in general, as the case with $u = w^{-1}$ indicates.)

- Part (3) of the proposition above gives us a method for verifying that a unit u modulo m has a particular order, in a way that is more efficient than computing all of the lower powers of u.
- Example: Show that 5 has order 20 modulo 41.
  - We compute $5^2 \equiv 25$, $5^4 \equiv 25^2 \equiv 10$, $5^8 \equiv 10^2 \equiv 18$, and $5^{16} \equiv 18^2 \equiv -4 \bmod 41$ using successive squaring.
  - Then $5^{20} = 5^{16} \cdot 5^4 \equiv (-4) \cdot (10) \equiv 1 \pmod{41}$, so the order of 5 divides 20.
  - Also, since the prime divisors of 20 are 2 and 5, we must also compute $5^{20/2} = 5^{10}$ and $5^{20/5} = 5^4$ modulo 41.
  - Since $5^{10} = 5^8 \cdot 5^2 \equiv 18 \cdot 25 \equiv 40 \pmod{41}$, and $5^4 \equiv 10 \pmod{41}$, the order of 5 cannot divide 10 or 4, and therefore the order must be $\boxed{20}$ as claimed.

2.3.2 Fermat's Little Theorem, Wilson's Theorem

- From the examples above, we can see that $2^{11} \equiv 2 \pmod{11}$, and also that $5^{13} \equiv 5 \pmod{13}$. The presence of these exponents is not an accident:
- Theorem (Fermat's Little Theorem): If p is a prime, then $a^p \equiv a \pmod{p}$.
  - Remark: If $p \nmid a$, we can multiply by a^{-1} to get the equivalent formulation $a^{p-1} \equiv 1 \pmod{p}$. Since the result is immediate if $p|a$, Fermat's Little Theorem is often also stated as "$a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$".
  - We will give three different proofs of this result.
  - Proof 1: We will show that p divides $a^p - a$ by induction on a. It is clearly enough to show the result for $0 \leq a \leq p$. The base case $a = 0$ is immediate.
  - For the inductive step, suppose that p divides $a^p - a$. We want to show that p divides

$$(a+1)^p - (a+1) = \sum_{k=0}^{p} \left[\binom{p}{k} a^k - a - 1 \right] = [a^p - a] + \sum_{k=1}^{p-1} \binom{p}{k} a^k.$$

  - By the inductive hypothesis, we know that p divides $a^p - a$, so it is enough to show that for each integer $0 < k < p$, that the binomial coefficient $\binom{p}{k}$ is divisible by p.
  - By definition, we have $\binom{p}{k} = \dfrac{p!}{k! \cdot (p-k)!}$, which is an integer. Observe that the numerator is divisible by p, while the denominator is not (because p is prime and both k and $p - k$ are less than p, neither factorial contains any multiple of p): therefore, the integer $\binom{p}{k}$ is divisible by p, as claimed.

- Proof 2: Consider the problem of counting the number of distinct circular necklaces with p beads, each of which is colored one of a colors. Clearly, there are a^p such necklaces.
- Observe that an assignment of colors to the p beads is the same as assigning colors to $f(\overline{0})$, $f(\overline{1})$, ... , $f(\overline{p-1})$. (Thus, the necklace red-red-blue would have $f(\overline{0}) =$ red, $f(\overline{1}) =$ red, $f(\overline{2}) =$ blue.)
- Suppose a necklace has the same bead colorings in the same positions as one of its rotations: say, the rotation forward by b beads. This is equivalent to having $f(\overline{x}) = f(\overline{x+b})$ for each x.
- Iterating this relation yields $f(\overline{0}) = f(\overline{b}) = f(\overline{2b}) = \cdots = f(\overline{(p-1)b})$. Since b is a unit modulo p, these values are all distinct (since $bx \equiv by \pmod{p}$ implies $x \equiv y \pmod{p}$): hence we conclude that all beads on the necklace must be the same color.
- Hence there are two types of necklaces: the a necklaces all of whose beads are the same color, and the $a^p - a$ necklaces each of which has p distinct possible rotations.
- We now declare two necklaces to be "equivalent" if one can be rotated into the other. From the above analysis, we see that the total number of inequivalent necklaces is $a + \dfrac{a^p - a}{p}$. In particular, since this is an integer, so must be $\dfrac{a^p - a}{p}$.
- Proof 3: We will show that $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$.
- By assumption, a is a unit. Consider the $p-1$ elements a, $2a$, $3a$, ... , $(p-1)a$ of multiples of a modulo p: these elements are all distinct: if $xa \equiv ya \pmod{p}$, then since a is a unit, multiplying both sides by a^{-1} yields $x \equiv y \pmod{p}$, whence $x = y$.
- Then since there are $p-1$ elements listed and they are all nonzero and distinct modulo p, they must represent all of the the nonzero residue classes modulo p.
- Therefore the two products $\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \cdots \cdot \overline{p-1}$ and $\overline{a} \cdot \overline{2a} \cdot \overline{3a} \cdot \cdots \cdot \overline{(p-1)a}$ consist of the same terms, merely rearranged, and so they are equal.
- By factoring out the a from each term in the second product, we obtain $(p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod{p}$, and so since $(p-1)!$ is a unit modulo p, cancelling it yields the desired statement $a^{p-1} \equiv 1 \pmod{p}$.

- The third proof above uses only the fact that $(p-1)!$ is a unit modulo p. We can, in fact, compute its exact value mod p:

- Theorem (Wilson's Theorem): If p is a prime, $(p-1)! \equiv -1 \pmod{p}$.
  - Proof: Consider the product $1 \cdot 2 \cdot \cdots \cdot (p-1)$.
  - We would like to match up pairs (a, a^{-1}), whose product is 1 modulo p. (For example, modulo 7, we would pair up 2 and 4, as well as 3 and 5.)
  - As long as $a \not\equiv a^{-1} \pmod{p}$, we will always be able to pair up a with its inverse, and cancel them from the product.
  - Observe that $a \equiv a^{-1} \pmod{p}$ is equivalent to $a^2 \equiv 1 \pmod{p}$, which is in turn equivalent to saying that p divides $(a-1)(a+1)$.
  - But since p is prime, this is equivalent to having $p|(a-1)$ or $p|(a+1)$, which is to say, $a \equiv \pm 1 \pmod{p}$.
  - Therefore, we can pair up all the terms in the product except 1 and $p-1$. Hence $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$, as desired.

- By using Fermat's little theorem, we can reduce the exponents substantially when calculating powers modulo a prime:

- Example: Calculate (as efficiently as possible) the remainder when 2^{3003} is divided by 61.
  - We could use successive squaring to compute this, but we would need to square 12 times (since $2^{12} = 2048$).
  - Since 61 is prime, we can do the computation much more quickly if we use Fermat's Little Theorem, which tells us that $2^{60} \equiv 1 \pmod{61}$.
  - Taking the 50th power of this yields $2^{3000} = (2^{60})^{50} \equiv 1^{50} = 1 \pmod{61}$.
  - Thus, $2^{3003} = 2^3 \cdot 2^{3000} \equiv \boxed{8 \pmod{61}}$.

2.3.3 The Euler φ-Function and Euler's Theorem

- Fermat's little theorem tells us that for any integer a, $a^p \equiv a \pmod{p}$. We would like to find a generalization that covers the case when the modulus is composite by finding an exponent such that $a^{\#\#\#} \equiv a \pmod{m}$, or something similar. For motivation, we first try a few examples:
  - Consider the powers of 2 modulo 24:

$$\begin{array}{cccccccccc} 2^1 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 & \cdots \\ 2 & 4 & 8 & 16 & 8 & 16 & 8 & 16 & \cdots \end{array}$$

  - Here, we see that the powers do eventually start repeating, but they never return to 1 (nor even to 2). This should not be surprising, because 2 is not a unit modulo 24. In particular, we see that there is no exponent bigger than 1 such that $2^{\#\#} \equiv 2 \pmod{24}$.
  - Instead, perhaps we should only consider cases where a is a unit modulo m. Consider the powers of 2 modulo 21:

$$\begin{array}{cccccccccccccc} 2^1 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 & 2^9 & 2^{10} & 2^{11} & 2^{12} & \cdots \\ 2 & 4 & 8 & 16 & 11 & 1 & 2 & 4 & 8 & 16 & 11 & 1 & \cdots \end{array}$$

    so we see that 2 has order 6 modulo 21. We also note that $2^{20} \equiv 4 \not\equiv 1 \pmod{21}$, so the proper exponent is not simply $m-1$, like it is for primes.
  - For another example, consider the powers of 3 modulo 16:

$$\begin{array}{ccccc} 3^1 & 3^2 & 3^3 & 3^4 & \cdots \\ 3 & 9 & 11 & 1 & \cdots \end{array}$$

    so we see that 3 has order 4 modulo 16. Once again, the proper exponent seems very different from $m-1=16$.
  - For another example, consider the powers of 5 modulo 27:

$$\begin{array}{cccccccccccccccccc} 5^1 & 5^2 & 5^3 & 5^4 & 5^5 & 5^6 & 5^7 & 5^8 & 5^9 & 5^{10} & 5^{11} & 5^{12} & 5^{13} & 5^{14} & 5^{15} & 5^{16} & 5^{17} & 5^{18} & \cdots \\ 5 & 25 & 17 & 4 & 20 & 19 & 14 & 16 & 26 & 22 & 2 & 10 & 23 & 7 & 8 & 13 & 11 & 1 & \cdots \end{array}$$

    so we see that 5 has order 18 modulo 27.

- To try to find a pattern to these numbers, notice that we are only interested in the units modulo m, so since powers of units will only be other units, perhaps instead of considering all of the $m-1$ nonzero residue classes, we should only look at the unit residue classes.
  - By making a list, we can count that there are 12 units modulo 21 (the residue classes not divisible by 3 or 7), 8 units modulo 16 (the odd residue classes), and 18 units modulo 27 (the residue classes not divisible by 3).
  - In each case, notice that the order of the element we computed divides the total number of units modulo m.
  - This observation suggests that the correct generalization of Fermat's little theorem might involve the total number of units modulo m.

- Definition: If m is a positive integer, we define the Euler φ-function $\varphi(m)$ (also called Euler's totient function) to be the number of units in $\mathbb{Z}/m\mathbb{Z}$. Equivalently, $\varphi(m)$ is the number of integers between 1 and m inclusive that are relatively prime to m.
  - Example: To compute $\varphi(30)$, we simply list the integers relatively prime to 30 in the proper range. It is not hard to see that 1, 7, 11, 13, 17, 19, 23, and 29 are the only ones, so $\varphi(30) = 8$.
  - Example: It is easy to see that $\varphi(1) = 1$ and that $\varphi(p) = p-1$ if p is a prime.
  - More generally, we can evaluate $\varphi(p^k)$ where p is prime by observing that a has a common divisor with p^k if and only if p divides a.
  - Thus, the integers between 1 and p^k which are *not* relatively prime to p^k are simply the multiples of p, of which there are p^{k-1}.

- Then the remaining $p^k - p^{k-1}$ integers are relatively prime to p, so we see that $\varphi(p^k) = p^k - p^{k-1}$.
- Example: We have $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$.

- A very useful consequence of the Chinese Remainder Theorem is the following convenient fact abouts units modulo mn:

- Proposition (Units Modulo Products): If m and n are relatively prime positive integers, then the residue class $\overline{a}$ is a unit modulo mn if and only if it is a unit modulo m and modulo n. As an immediate consequence[1], if m and n are relatively prime, we have $\varphi(mn) = \varphi(m)\varphi(n)$.

  - Proof: First suppose that a is a unit modulo mn. Then a has a multiplicative inverse b modulo mn, meaning that $ab \equiv 1 \pmod{mn}$. Reducing both sides mod m and n then yields $ab \equiv 1 \pmod{m}$ and $ab \equiv 1 \pmod{n}$, so b is also the multiplicative inverse of a modulo m and modulo n, so a is a unit mod m and mod n.
  - Conversely, suppose that a is a unit modulo m and modulo n, and choose b and c such that $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{n}$.
  - Because m and n are relatively prime, the Chinese Remainder Theorem implies there exists an integer d such that $d \equiv b \pmod{m}$ and $d \equiv c \pmod{n}$.
  - Then $ad \equiv ab \equiv 1 \pmod{m}$ and $ad \equiv ac \equiv 1 \pmod{n}$, and therefore because m and n are relatively prime, we conclude that $ad \equiv 1 \pmod{mn}$, meaning that a is a unit mod mn as claimed.
  - Finally, for the formula $\varphi(mn) = \varphi(m)\varphi(n)$ we simply count the number of units modulo mn: there are $\varphi(mn)$ units modulo mn and there are $\varphi(m)\varphi(n)$ ordered pairs of units modulo m and modulo n. By what we just showed, these two quantities are counting the same thing, so $\varphi(mn) = \varphi(m)\varphi(n)$.

- By breaking an integer apart as a product of prime powers, we can give a formula for the Euler φ-function:

- Corollary (Formula for $\varphi(n)$): If the prime factorization of n is $n = \prod_{i=1}^{k} p_i^{a_i}$, then $\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$.

  - Remark: The formula for $\varphi(n)$ is also often written as $\varphi(n) = n \cdot \prod_{i=1}^{k}(1 - 1/p_i)$. In particular, note the interesting fact that the value of $\varphi(n)/n$ only depends on the primes dividing n.
  - Proof: By a trivial induction applying the relation $\varphi(mn) = \varphi(m)\varphi(n)$ to the factorization of m into prime powers, we can see that $\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{a_i})$. Then applying the evaluation $\varphi(p^k) = p^{k-1}(p - 1)$ for prime powers p^k that we derived above immediately yields the the claimed formula $\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$.

- Example: Find $\varphi(1680)$.

  - First we factor $1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$. Then $\varphi(1680) = \varphi(2^4)\varphi(3)\varphi(5)\varphi(7) = 8 \cdot 2 \cdot 4 \cdot 6 = \boxed{384}$.

- With the formula for $\varphi(n)$ in hand, we can now establish Euler's generalization of Fermat's Little Theorem:

- Theorem (Euler's Theorem): If a and m are relatively prime, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

  - The proof is essentially the same as the third proof we gave for Fermat's Little Theorem.
  - Proof: By assumption, a is a unit mod m.
  - Let the set of all units mod m be $u_1, u_2, \ldots, u_{\varphi(m)}$, and consider the elements $a \cdot u_1, a \cdot u_2, \ldots, a \cdot u_{\varphi(m)}$ modulo m: we claim that they are simply the elements $u_1, u_2, \ldots, u_{\varphi(m)}$ again (possibly in a different order).
  - Since there are $\varphi(m)$ elements listed and they are all still units, it is enough to verify that they are all distinct.
  - So suppose $a \cdot u_i \equiv a \cdot u_j \pmod{m}$. Since a is a unit, multiply by a^{-1}: this gives $u_i \equiv u_j \pmod{m}$, but this forces $i = j$.

[1] A function f on positive integers having the property that $f(mn) = f(m)f(n)$ whenever m and n are relatively prime is called a multiplicative function. This terminology is somewhat infelicitous since it would tend to suggest that $f(mn) = f(m)f(n)$ holds for *any* m and n, not just relatively prime ones. (A function that does have this latter property is called completely multiplicative.)

- Hence modulo m, the elements $a \cdot u_1,\ a \cdot u_2, \cdots, a \cdot u_{\varphi(m)}$ are simply u_1, u_2, ... , $u_{\varphi(m)}$ in some order.
- Therefore we have $(a \cdot u_1)(a \cdot u_2) \cdots (a \cdot u_{\varphi(m)}) \equiv u_1 \cdot u_2 \cdots u_{\varphi(m)} \pmod{m}$, and so cancelling $u_1 \cdot u_2 \cdots u_{\varphi(m)}$ from both sides yields $a^{\varphi(m)} \equiv 1 \pmod{m}$ as desired.
- Remark (for those who like group theory): The collection of units modulo m forms a group under multiplication, of size $\varphi(m)$. In this lens, Euler's Theorem is an immediate corollary of Lagrange's Theorem (which says that, in a finite group, the size of any subgroup divides the size of the group): taking the subgroup to be the one generated by the element a immediately implies that the order of a divides the size of the group.

- Like with Fermat's Little Theorem, we can use Euler's Theorem to give quicker calculations of large powers modulo m:
- Example: Find the last two digits of 17^{2020} when written in base 10.
  - Equivalently, we wish to find 17^{2020} modulo 100. Since $100 = 2^2 5^2$ we have $\varphi(100) = \varphi(2^2)\varphi(5^2) = 2 \cdot 20 = 40$.
  - Then Euler's Theorem says that $17^{40} \equiv 1 \pmod{100}$. Hence, taking the 50th power yields $17^{2000} = (17^{40})^{50} \equiv 1^{50} = 1 \pmod{100}$.
  - Then $17^{2020} \equiv 17^{20} \pmod{100}$, and we can compute this by successive squaring:

$$\begin{aligned} 17^2 &= 289 \equiv -11 \pmod{100} \\ 17^4 &\equiv (-11)^2 = 121 \equiv 21 \pmod{100} \\ 17^8 &\equiv 21^2 = 441 \equiv 41 \pmod{100} \\ 17^{16} &\equiv 41^2 = 1681 \equiv 81 \pmod{100} \end{aligned}$$

  Therefore, we see that $17^{2020} \equiv 17^{20} = 17^{16} \cdot 17^4 \equiv 81 \cdot 21 \equiv 1 \pmod{100}$, so the last two digits are $\boxed{01}$.

2.3.4 Primitive Roots and Discrete Logarithms

- Euler's Theorem says that the order of any element modulo m divides $\varphi(m)$. We might wonder: can the order actually equal $\varphi(m)$? The answer is yes, and such elements are quite useful:
- Definition: If u is a unit modulo m and the order of u is $\varphi(m)$, we say that u is a primitive root modulo m.
  - Example: The powers of 2 modulo 5 are 2, 4, 3, and 1, so 2 is a primitive root mod 5 (since it has order 4). Similarly, we can check that 3 is also a primitive root mod 5.
  - Example: The powers of 2 modulo 9 are 2, 4, 8, 7, 5, and 1, so 2 is a primitive root mod 9 (since it has order $6 = \varphi(9)$).
  - Non-Example: There is no primitive root modulo 15: the units are 1 (order 1), 2 (order 4), 4 (order 2), 7 (order 4), 8 (order 4), 11 (order 2), and 14 (order 2), and none of these is a primitive root.
  - Remark (for those who like group theory): The units modulo m form an abelian group of order $\varphi(m)$. The existence of a primitive root u says that the unit group is cyclic and generated by u. The group of units modulo 15 is isomorphic to $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, which is not a cyclic group.

- Proposition (Primitive Roots and Powers): A unit u is a primitive root modulo m if and only if every unit modulo m is congruent to a power of u.
  - We can see this in the examples above: for example, the units modulo 5 are 1, 2, 3, and 4, and they are congruent mod 5 to 2^0, 2^1, 2^3, and 2^2 respectively.
  - Proof: If u is a primitive root modulo m, then by definition each of u^1, u^2, $\cdots$, $u^{\varphi(m)}$ is distinct modulo m. Since there are $\varphi(m)$ elements in this list and they are all units, this means they represent each of the invertible residue classes modulo m.

- For the other direction, if the powers of u exhaust all of the different residue classes modulo m, then the order of u must be at least $\varphi(m)$ (since otherwise there would be fewer than $\varphi(m)$ distinct powers of u modulo m), but since the order of u divides $\varphi(m)$ by Euler's Theorem, we must have equality.

- The above proposition implies, in particular, that if u is a primitive root modulo m, then for any unit a there is a k such that $a \equiv u^k \bmod m$. Furthermore, this exponent k is unique modulo $\varphi(m)$.

- Definition: If u is a primitive root modulo m and a is a unit with $a \equiv u^k \pmod{m}$, we say that k is the discrete logarithm of a modulo m to the base u, and write $k = \log_u(a)$. (Implicitly, the discrete logarithm is considered modulo $\varphi(m)$.)

  - The reason this map is called the discrete logarithm is because its definition is precisely the same as the usual logarithm: $\log_u(a) = k \pmod{\varphi(m)}$ is equivalent to $a \equiv u^k \pmod{m}$.
  - Furthermore, as we would expect, it obeys the standard rules of logarithms: $\log_u(ab) = \log_u(a) + \log_u(b)$, and $\log_u(a^r) = r \log_u(a)$ for $r \in \mathbb{Z}$.

- Having a table of discrete logarithms relative to a primitive root modulo m is very useful for computations.

  - For example, it allows for very rapid multiplication and exponentiation, in the same manner as usual logarithms do. This is not terrifically helpful because there already exist fast algorithms for these procedures.
  - More usefully, having a table of discrete logarithms also allows us to compute nth roots, if they exist.

- Example: Find the discrete logarithms of each unit modulo 11 to the base 2, and use the results to solve the equation $x^4 \equiv 9 \pmod{11}$.

  - Since 2 is a primitive root modulo 11, we can write each unit as a power of 2. The simplest way to do this is simply to compute each of the values 2^0, 2^1, ... , 2^{10} modulo 11; here is a table of the results:

n	1	2	3	4	5	6	7	8	9	10
$\log_2 n$	0	1	8	2	4	9	7	3	6	5

  - Observe, for example, that $3 \cdot 6 \equiv 7 \pmod{11}$, and $\log_2(3) + \log_2(6) \equiv \log_2(7) \pmod{10}$, since 10 is the order of 2 modulo 11. Likewise, $3^3 \equiv 5 \pmod{11}$, and $3\log_2(3) \equiv \log_2(5) \pmod{10}$.
  - To solve the equation $x^4 \equiv 9 \pmod{11}$, we take discrete logarithms to the base 2, yielding $\log_2(x^4) \equiv \log_2(9) \pmod{10}$, or $4\log_2 x \equiv 6 \pmod{10}$.
  - Since $\gcd(4, 10) = 2$ this congruence is equivalent to $2\log_2(x) \equiv 3 \pmod{5}$, which has the solution $\log_2(x) \equiv 4 \pmod{5}$. Modulo 10 there are two solutions: 4 and 9.
  - Exponentiating then yields that there are two solutions to the original congruence: $x \equiv 2^4, 2^9 \bmod 11$, or equivalently $x \equiv \boxed{5, 6} \bmod 11$.

- Example: Solve the congruence $x^4 \equiv 2 \pmod{89}$, given that 3 is a primitive root mod 89 and $2 \equiv 3^{16} \pmod{89}$.

  - The given information says $x^4 \equiv 2 \equiv 3^{16} \pmod{89}$, so taking discrete logarithms to the base 3 yields $4\log_3(x) \equiv 16 \pmod{88}$, since taking discrete logarithms yields a congruence modulo $\varphi(89) = 88$.
  - Reducing the factor of 4 yields $\log_2(x) \equiv 4 \pmod{22}$, which has the four solutions $\log_2 x \equiv 4, 26, 48, 70 \pmod{88}$.
  - Then $x \equiv 3^4, 3^{26}, 3^{48}, 3^{70} \pmod{89}$. Equivalently, these yield $x = \boxed{81, 84, 8, 5} \pmod{89}$.

- Now that we have some applications for primitive roots, we would like to know: when does there actually exist a primitive root modulo m?

  - The answer is: there exists a primitive root modulo m if and only if $m = 1, 2, 4$ or m is of the form p^k or $2p^k$ for an odd prime p and some $k \geq 1$.
  - We will return to prove this theorem in a later chapter, after establishing some facts about factorization of polynomials modulo p.

2.4 Repeating Decimals

- Repeating-decimal expansions of rational numbers are likely familiar from elementary school. (We will generally confine our attention to repeating decimals in base 10, but there are only minimal changes necessary to discuss repeating decimals in base b.)
- Some typical examples are

$$\begin{aligned} 1/11 &= 0.090909090909\cdots = 0.\overline{09} \\ 1/7 &= 0.142857142857\cdots = 0.\overline{142857} \\ 22/15 &= 1.466666666666\cdots = 1.4\overline{6}. \end{aligned}$$

  - In general, the division algorithm implies that any rational number p/q has a decimal expansion that eventually repeats or terminates (since there are only finitely many remainders when dividing by q when doing long division). Any terminating decimal expansion also has an infinite repeating expansion consisting of all 9s (e.g., $\frac{1}{2} = 0.5 = 0.4\overline{9}$).
  - The repeated digit sequence is sometimes called the repetend, though it is just as easy to refer to it as the repeating part of the decimal expansion. The length of the repeating part is called the period of the expansion (thus, 1/7 has period 6).
- Given a repeating decimal expansion, we can easily compute its value as a rational number. The most obvious method would be to sum the geometric series, but an easier approach is to multiply by appropriate powers of 10 and then subtract to cancel the decimal part.
  - For example, if we have $x = 0.2\overline{71}$, then $10x = 2.\overline{71}$ and $1000x = 271.\overline{71}$. Subtracting yields $990x = 269$, whence $x = \frac{269}{990}$.
- In general, we would like to know why (for example) the repeating decimal expansion of $\frac{1}{11}$ repeats with period 2, while the repeating decimal expansion of $\frac{1}{7}$ repeats with period 6.
- It turns out that there is a simple way to determine the period of any repeating decimal expansion. We start with decimal expansions that begin repeating immediately after the decimal point, since they are slightly easier to analyze:
- Proposition (Decimal Periods): If $0 < p < q$ and q is relatively prime to p and 10, then the repeating decimal expansion of $\frac{p}{q}$ begins repeating immediately after the decimal point, and the length of the period is the order of 10 modulo q. In particular, the length of the period divides $\varphi(q)$.
  - Proof: If $x = 0.\overline{d_1 d_2 \cdots d_k}$, then $x = \frac{d_1 d_2 \cdots d_k}{10^k - 1}$, either by summing the geometric series or computing $10^k x - x$.
  - From this, we see that $\frac{p}{q}$ has a repeating decimal expansion of length k (starting immediately after the decimal point) if and only if we can write $\frac{p}{q} = \frac{a}{10^k - 1}$ for some integer a.
  - Cross-multiplying yields $p(10^k - 1) = aq$, and since p and q are relatively prime, the existence of such an a is equivalent to saying that q divides $10^k - 1$.
  - By definition, the order of 10 modulo q is the minimal integer k such that q divides $10^k - 1$, but (by the above) this is precisely the same thing as the period k of the decimal expansion.
  - For the last statement, by Euler's Theorem we know that $10^{\varphi(q)} \equiv 1 \pmod{q}$ since 10 is a unit modulo q. From properties of orders, if $u^n \equiv 1 \pmod{m}$ then the order of u divides n: thus, k divides $\varphi(q)$.
- In general, we have the following:

- Proposition (General Decimals): If $0 < p < q$, and $q = 2^a 5^b r$ where r is relatively prime to 10, then the repeating decimal expansion of p/q begins with $m = \max(a, b)$ nonrepeating digits, followed by the repeating-decimal portion of $10^m \dfrac{p}{q} = \dfrac{2^{m-a} 5^{m-b} p}{r}$, which has period equal by the order of 10 modulo r.

  - Proof: Write $10^m \dfrac{p}{q} = \dfrac{2^{m-a} 5^{m-b} p}{r}$, whose repeating decimal expansion is simply that of p/q, shifted by m places. The previous proposition applies to the fractional portion of this rational number, since its denominator is now relatively prime to 10, and yields all of the stated results.

- Example: Find the period of the repeating decimal expansion of $\dfrac{1}{17}$.

  - By the above, we see that the period is the order of 10 modulo 17, which divides $\varphi(17) = 16$ and hence must be a power of 2.
  - By successive squaring we see that $10^2 \equiv (-7)^2 \equiv -2 \pmod{17}$, $10^4 \equiv 4 \pmod{17}$, and $10^8 \equiv -1 \pmod{17}$, so the period must in fact be $\boxed{16}$.
  - The repeating decimal part is then the integer $\dfrac{10^{16} - 1}{17} = 588235294117647$, so we get $\dfrac{1}{17} = 0.\overline{0588235294117647}$ (which is indeed the correct decimal expansion).

- There are quite a few interesting properties of repeating decimal expansions. For example, observe that

$$\begin{aligned} 1/7 &= 0.\overline{142857} \\ 2/7 &= 0.\overline{285714} \\ 3/7 &= 0.\overline{428571} \\ 4/7 &= 0.\overline{571428} \\ 5/7 &= 0.\overline{714285} \\ 6/7 &= 0.\overline{857142} \end{aligned}$$

  and see that each of the expansions for $n/7$ are cyclic shifts of the expansion of $1/7$.

  - We can explain this by observing that shifting the expansion of $\dfrac{1}{7}$ forward 1 decimal place is equivalent to multiplying by 10, and $\dfrac{10}{7} = 1 + \dfrac{3}{7}$. Shifting by 2 decimal places gives the expansion for $\dfrac{100}{7} = 14 + \dfrac{2}{7}$, shifting by 3 decimal places gives the expansion $142 + \dfrac{6}{7}$, and so forth. By shifting forward we can obtain each of the expansions of $n/7$ for $1 \le n \le 6$.
  - Another way of saying this is that the residues of 10^k modulo 7 for $1 \le 6 \le k$ each lie in distinct residue classes modulo 6, and this is simply reflecting the fact that 10 has order 6 modulo 7.

- The analysis above holds in general:

- Proposition (Cyclic Shifts): If p is prime and 10 is a primitive root modulo p, then the repeating decimal expansions for $\dfrac{k}{p}$ with $1 \le k \le p - 1$ are cyclic shifts of one another.

  - Proof: If 10 has order $p - 1$ modulo p, then the integers 10^1, 10^2, ... , 10^{p-1} are all distinct modulo p. Since they are all units, they give representatives for each of the $p - 1$ nonzero residue classes modulo p. Hence the $p - 1$ cyclic shifts of the repeating decimal expansion of $1/p$ yield the repeating decimal expansions for k/p for $1 \le k \le p - 1$ as claimed.

- Here are some other interesting numerological properties of repeating decimals:

- Observe that

$$\begin{aligned} 1/99 &= 0.0101010101\ldots \\ 1/98 &= 0.0102040816\ldots \\ 1/97 &= 0.01030927\ldots \\ 1/96 &= 0.010416\ldots \\ &\vdots \quad \vdots \quad \vdots \\ 1/91 &= 0.0109\ldots \\ 1/90 &= 0.0111\ldots \\ 1/89 &= 0.011235\ldots \end{aligned}$$

  Notice that the decimal expansions for $\frac{1}{99}$ through $\frac{1}{90}$ are geometric series, while the expansion for $\frac{1}{89}$ consists of the Fibonacci numbers.

- The pattern above also holds for larger denominators:

$$\begin{aligned} 1/9998 &= 0.000100020004000800160032\ldots \\ 1/9997 &= 0.000100030009002700810243\ldots \\ &\vdots \quad \vdots \quad \vdots \\ 1/9901 &= 0.00010099\ldots \\ 1/9900 &= 0.000101010101010101010101\ldots \\ 1/9899 &= 0.000101020305081322345 5\ldots \\ 1/9898 &= 0.0001010305112143\ldots \\ 1/9897 &= 0.00010104071940\ldots \end{aligned}$$

  where the terms for the expansion in $\frac{1}{9898}$ are generated by the relation $A_n = A_{n-1} + 2A_{n-2}$, and the terms for the expansion of $\frac{1}{9897}$ are generated by the relation $B_n = B_{n-1} + 3B_{n-2}$, mirroring the Fibonacci relation $F_n = F_{n-1} + F_{n-2}$ appearing in the expansion of $\frac{1}{9899}$.

- Another pattern:

$$\begin{aligned} 1/81 &= 0.\overline{012345679} \\ 2/81 &= 0.\overline{024691358} \\ 4/81 &= 0.\overline{049382716} \\ 5/81 &= 0.\overline{061728395} \\ 7/81 &= 0.\overline{086419853} \\ 8/81 &= 0.\overline{987654320} \end{aligned}$$

  and (besides the patterns of consecutive integers in the digits) these period-9 expansions also have the interesting property that the digits are all distinct and that the "missing digit" for $k/81$ is $9 - k$.

Well, you're at the end of my handout. Hope it was helpful.