Outline

Recall: Euclidean algorithm for
   Efficiently finding gcd’s
   Efficiently finding multiplicative inverses

Equality mod $m$, integers mod $m$

Sun-Ze’s theorem

Fermat’s Little Theorem

Definition of order

Primitive roots
Equality modulo $m$

To understand the interaction of reduction modulo $m$ with addition and multiplication:

Gauss was the first to notice that divisibility properties can be recast as a kind of equality, thereby making use of our prior experience with manipulation of equalities.

Recall that $x \equiv m$ is an operation which takes ordinary integers as inputs and produces integer outputs.

Equality modulo $m$ is a relation defined by

$$x = y \mod m \text{ if and only if } m | (x - y)$$

Sometimes this is written with *three* lines instead of two, as in

$$x \equiv y \mod m$$

and called a congruence, but it is simply a modified form of equality. Think of mod $m$ as an adverb modifying the verb equals.
For example,

\[ 2 \equiv 7 \mod 5 \text{ because } 5|(2 - 7) \]
\[ 12 \equiv 7 \mod 5 \text{ because } 5|(12 - 7) \]
\[ 127 \equiv 7 \mod 5 \text{ because } 5|(127 - 7) \]
\[ -123 \equiv 127 \mod 5 \text{ because } 5|(-123 - 127) \]

Although the definition does not explicitly compare equality modulo \( m \) with reduction modulo \( m \), there is a simple connection:

**Lemma:** \( x \equiv y \mod m \) if and only if \( x \% m = y \% m \).

**Proof:** If \( m|(x - y) \) and \( x = qm + r \) and \( y = q'm + r' \) with \( 0 \leq r < |m| \) and \( 0 \leq r' < |m| \), then \( m|(qm + r - q'm - r') \) and thus \( m|(r - r') \). Since \( r \) and \( r' \) are non-negative and smaller than \( m \), it must be that \( r = r' \). Thus \( x \% m = y \% m \). On the other hand, if \( x \% m = y \% m \) then \( m|(r - r') \) and \( m|(qm + r - q'm - r') \), so \( m|x - y \). \( /// \)
Equivalence relations, equivalence classes

For fixed modulus $m$, $x = y \mod m$ is an equivalence relation in the sense that

$x = x \mod m$ (Reflexivity)

$x = y \mod m$ implies $y = x \mod m$ (Symmetry)

$x = y \mod m$ and $y = z \mod m$ implies

$x = z \mod m$ (Transitivity)

The equivalence class of congruence class or residue class of $x$ modulo $m$ is the set of all integers $x'$ equal to $x$ modulo $m$. It is often denoted $\bar{x}$ without explicit reference to the modulus. And $x \mod m$ (now using $\text{mod } m$ as an adjective, rather than adverb) may refer to this set. Thus,

$$x \mod m = \bar{x} = \{x' \in \mathbb{Z} : x' = x \mod m\}$$

$$= \{\ldots, x - 2m, x - m, x, x + m, x + 2m, \ldots\}$$

There is no explicit reference to reduction modulo $m$ in this.
For example,

\[
\begin{align*}
2 \mod 5 &= \{\ldots, -8, -3, 2, 7, 12, \ldots \} \\
-1 \mod 5 &= \{\ldots, -6, -1, 4, 9, 14, \ldots \} \\
4 \mod 5 &= \{\ldots, -6, -1, 4, 9, 14, \ldots \} \\
9 \mod 5 &= \{\ldots, -6, -1, 4, 9, 14, \ldots \} \\
5 \mod 5 &= \{\ldots, -10, -5, 0, 5, 10, \ldots \} \\
0 \mod 5 &= \{\ldots, -10, -5, 0, 5, 10, \ldots \}
\end{align*}
\]

But the mental picture of one of these equivalence classes should be as a single entity, not an infinite set.

The set of equivalence classes of integers mod \( m \) is denoted

\[
\mathbb{Z}/m
\]

This is the set of integers modulo \( m \)
Well-definedness of arithmetic mod $m$

To prove that reduction modulo $m$ interacts well with addition and multiplication, we really prove, instead, that addition and multiplication (and subtraction) are well-defined modulo $m$.

Well-definedness is not a concept that one meets in more elementary mathematics. The point is that something that appears to be a reasonable definition as output of an operation may fail by secretly specifying more than one output. One way that this frequently occurs is where objects have many different names, by specifying the output in terms of one name, but getting different outputs depending on which name of the same object is used.

We want the outcome to depend on the object, not on a name for it.
In the case at hand, we want to prove that
If $x = x' \mod m$ and $y = y' \mod m$, then

- $x + y = x' + y' \mod m$
- $x \cdot y = x' \cdot y' \mod m$

In other words, we claim that if $x, y, x', y'$ are integers with $\overline{x} = \overline{x'}$ and $\overline{y} = \overline{y'}$ then

- $\overline{x + y} = \overline{x' + y'}$
- $\overline{x \cdot y} = \overline{x' \cdot y'}$

That is, the equivalence class of a sum or product does not depend on the name we use for equivalence classes, but only upon the equivalence classes themselves.
Proof: Let \( x' = x + am \) and \( y' = y + bm \). Then
\[
x' + y' = (x + am) + (y + bm) \\
= x + y + m \cdot (a + b)
\]
so
\[
(x' + y') - (x + y) = m \cdot (a + b)
\]
which fits into the definition, giving
\[
x' + y' = x + y \mod m
\]
Similarly,
\[
x' \cdot y' = (x + am) \cdot (y + bm) \\
= x \cdot y + m \cdot (ay + xb + abm)
\]
so
\[
(x' \cdot y') - (x \cdot y) = m \cdot (ay + xb + abm)
\]
which fits into the definition, giving
\[
x' \cdot y' = x \cdot y \mod m
\]
Thus, we have an addition and multiplication of equivalence classes \( \mod m \).
This well-definedness is what implies that reduction modulo $m$ interacts well with addition and multiplication. To show that

$$((x \% m) + (y \% m)) \% m = (x + y) \% m$$

note that $z \% m = z \mod m$ for any $z \in \mathbb{Z}$. With $z = (x \% m) + (y \% m)$ gives

$$((x \% m) + (y \% m)) \% m$$

$$= (x \% m) + (y \% m) \mod m$$

With $z = x \% m$ and $z = y \% m$, using well-definedness of addition modulo $m$, this becomes

$$= x + y \mod m$$

Similarly, using the principle with $z = x + y$, the right-hand side is

$$(x + y) \% m = x + y \mod m$$

Thus, the two things are equal modulo $m$, which by an earlier observation implies that their reductions modulo $m$ are the same.
Composite moduli, Sun-Ze’s theorem

(Also called Chinese remainder theorem)

**Theorem:** Let $m$ and $n$ be relatively prime integers. Given $a$ and $b$, there is an integer $x$ such that both

\[
\begin{align*}
    x &= a \mod m \\
    x &= b \mod n
\end{align*}
\]

This $x$ is unique $\mod mn$ in the sense that any other solution $x'$ to that system satisfies

\[x' = x \mod mn\]

In particular, let $r, s$ be integers such that

\[rm + sn = 1 \quad (= \gcd(m, n))\]

Then

\[x = rm \cdot b + sn \cdot a \mod mn\]

is the solution $\mod mn$. 
Proof: If \( x \) and \( x' \) are two solutions to the system, then \( x - x' = 0 \) mod \( m \) and \( x - x' = 0 \) mod \( n \), so \( m|(x - x') \) and \( n|(x - x') \). Since \( m \) and \( n \) are relatively prime, \( mn|(x - x') \) (as we showed a week or two ago in class). Thus, \( x = x' \mod mn \), which is the asserted uniqueness.

Next, claim that with \( r, s \) such that \( rm + sn = 1 \) the integer

\[
x = rm \cdot b + sn \cdot a
\]

satisfies \( x = a \mod m \) and \( x = b \mod n \). From \( rm + sn = 1 \) we get \( rm = 1 \mod n \). Thus mod \( n \)

\[
x = rm \cdot b + sn \cdot a = 1 \cdot b + 0 \cdot a = b \mod n
\]

Symmetrically, \( sn = 1 \mod m \) and

\[
x = rm \cdot b + sn \cdot a = 0 \cdot b + 1 \cdot a = a \mod m
\]

as desired. ///
For example, find $x$ such that

\[
\begin{align*}
x & = 1 \pmod{5} \\
x & = 2 \pmod{7}
\end{align*}
\]

The extended Euclidean algorithm yields

\[
3 \cdot 5 + (-2) \cdot 7 = 1
\]

Thus, the formula gives

\[
x = (3 \cdot 5) \cdot 2 + ((-2) \cdot 7) \cdot 1 = 30 - 14 = 16
\]

We can check that indeed

\[
\begin{align*}
16 & = 1 \pmod{5} \\
16 & = 2 \pmod{7}
\end{align*}
\]
For example, find $x$ such that

$$\begin{cases} x & = & 5 \mod 101 \\ x & = & 7 \mod 157 \end{cases}$$

The extended Euclidean algorithm yields

$$
\begin{align*}
157 & - 1 \cdot 101 = 56 \\
101 & - 1 \cdot 56 = 45 \\
56 & - 1 \cdot 45 = 11 \\
45 & - 4 \cdot 11 = 1 \\
1 & = (1)45 + (-4)11 \\
& = (1)45 + (-4)(56 - 1 \cdot 45) \\
& = (-4)56 + (5)45 \\
& = (-4)56 + (5)(101 - 1 \cdot 56) \\
& = (5)101 + (-9)56 \\
& = (5)101 + (-9)(157 - 1 \cdot 101) \\
& = (-9)157 + (14)101
\end{align*}
$$
So

\[ 1 = (14)_{101} + (-9)_{157} \]

Thus, the formula gives

\[ x = (14 \cdot 101) \cdot 7 + ((-9) \cdot 157) \cdot 5 \]

\[ = 9898 - 7065 = \boxed{2833} \mod 101 \cdot 157 \]

We can check that indeed

\[
\begin{cases}
2833 = 2833 \mod 101 &= 5 \mod 101 \\
2833 = 2833 \mod 157 &= 7 \mod 157
\end{cases}
\]
Fermat’s Little Theorem

A fundamental and non-obvious fact.

**Theorem:** (Fermat’s Little Theorem) For $p$ prime for any integer $b$

\[ b^p = b \mod p \]

**Theorem:** (Variant) For $p$ prime for an integer $b$ not divisible by $p$

\[ b^{p-1} = 1 \mod p \]

**Remark:** This is very different from the naive expectation: $\mod p$ an exponent of $p$ cannot be replaced by 0, despite the fact that $p = 0 \mod p$. That is, generally

\[ b^p \neq b^0 \mod p \]

Instead, the variant version asserts that, for $b$ prime to $p$,

\[ b^{p-1} = 1 = b^0 \mod p \]
Proof: Proven by induction on \( b \), using

\[(b + 1)^p = b^p + \binom{p}{1} b^{p-1} + \ldots + \binom{p}{p-1} b + 1\]

Those binomial coefficients are \textit{integers} since they are the inner coefficients in

\[(x + y)^p = x^p + \ldots + y^p\]

On the other hand all these binomial coefficients are are divisible by \( p \) since

\[\binom{p}{i} = \frac{p!}{i! (p - i)!}\]

and the denominator has no factor of \( p \). (\textit{Unique Factorization}!) Thus, we have

\[(b + 1)^p = b^p + 1 = b + 1 \mod p\]

by induction. ///
The notion of order

The order of $b \mod m$ (with $\gcd(b, m) = 1$) is the smallest positive integer $\ell$ such that

$$b^\ell = 1 \mod m$$

**Corollary:** (of Fermat’s Little Theorem) For prime $p$ and for $b$ not divisible by $p$, the order of $b$ modulo $p$ is a divisor of $p - 1$.

**Proof:** Let the order of $b$ be $\ell$. Using the division algorithm, we can write $p - 1 = q \cdot \ell + r$ with $0 \leq r < \ell$. Then, using Fermat’s Little Theorem, all modulo $p$,

$$1 = b^{p-1} = b^{q\ell + r}$$

$$= (b^\ell)^q \cdot b^r = 1^q \cdot b^r = b^r \mod p$$

Thus,

$$b^r = 1 \mod p$$

$\ell$ is the smallest positive integer with this property, so $r = 0$. Thus, $\ell | (p - 1)$. //
A primitive root \( g \) modulo a prime \( p \) is an integer \( g \) relatively prime to \( p \) such that no positive exponent \( \ell \) smaller than \( p - 1 \) will make

\[
g^\ell = 1 \mod p
\]

That is, a primitive root has order \( p - 1 \mod p \). From Fermat’s Little Theorem \( b^{p-1} = 1 \mod p \), and we showed that in any case the actual order of \( b \) is a divisor of \( p - 1 \).

**Theorem:** Primitive roots modulo primes exist.

*This is not easy to prove, and is very important.*
Testing for primitive roots

**Corollary:** An integer $b$ is a primitive root modulo a prime $p$ if and only if, for every prime $q$ dividing $p - 1$,

$$b^{\frac{p-1}{q}} \neq 1 \mod p$$

**Proof:** We already saw the the order $\ell$ of $b$ is a divisor of $p - 1$. If $\ell < p - 1$ then $(p - 1)/\ell > 1$. Then $(p01)/\ell$ would have a prime divisor $q$, and we’d still have

$$\ell | \frac{p - 1}{q}$$

Let $(p - 1)/q = k\ell$ for some integer $k$. Then, mod $p$,

$$b^{(p-1)/q} = b^{k\ell} = (b^\ell)^k = 1^k = 1 \mod p$$

as claimed.  

///
**Example:** Is 2 a primitive root modulo 29?

Applying the criterion above, 2 will be a primitive root mod 29 if and only if for every prime $q$ dividing $29 - 1$ we have

$$2^{(29-1)/q} \not\equiv 1 \mod 29$$

By trial division, the primes $q$ dividing $29 - 1$ are 2 and 7. Then mod 29

$$2^{(29-1)/2} = 2^{14} = 16384 = 28 \not\equiv 1 \mod 29$$

$$2^{(29-1)/7} = 2^4 = 16 \not\equiv 1 \mod 29$$

Thus, 2 is a primitive root modulo 29.

**Remark:** With larger exponents it is obviously necessary to use the fast modular exponentiation algorithm.
**Example:** Is 2 a primitive root modulo 67?

Applying the criterion above, 2 will be a primitive root mod 67 if and only if for every prime $q$ dividing $67 - 1$ we have

$$2^{(67-1)/q} \not\equiv 1 \mod 67$$

By trial division, the primes $q$ dividing $67 - 1$ are 2, 3, 11. Use fast modular exponentiation to compute $2^{(67-1)/2} \mod 67$: the successive states are $(2, 33, 1), (2, 32, 2), (4, 16, 2), (16, 8, 2), (55, 4, 2), (10, 2, 2), (33, 1, 2), (33, 0, 66)$ so

$$2^{(67-1)/2} = 2^{33} = 66 \not\equiv 1 \mod 67$$

To compute $2^{(67-1)/3} \mod 67$, the states are $(2, 22, 1), (4, 11, 1), (4, 10, 4), (16, 5, 4), (16, 4, 64), (55, 2, 64), (10, 1, 64), (10, 0, 37)$ so

$$2^{(67-1)/3} = 2^{22} = 37 \not\equiv 1 \mod 67$$

And

$$2^{(67-1)/11} = 2^{6} = 64 \not\equiv 1 \mod 67$$

Thus, 2 is a primitive root modulo 67.