Modular arithmetic

\( n \geq 2 \). We say \( a \equiv b \pmod{n} \) if \( a, b \) have same remainder when divided by \( n \). In other words, \( a \equiv b \pmod{n} \) iff \( a - b \) is divisible by \( n \).

**Example:** \( 99 \equiv 6 \pmod{31} \)
\[
2 \equiv 6 \equiv -2 \pmod{4}
\]

We showed last time that if \( a_1 \equiv b_1 \pmod{n} \), \( a_2 \equiv b_2 \pmod{n} \), then
\[
a_1 + a_2 \equiv b_1 + b_2 \pmod{n} \\
a_1 - a_2 \equiv b_1 - b_2 \pmod{n} \\
a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}
\]

\( \mathbb{Z}_n = \{0, 1, \ldots, n-1\} \) = integers \( \pmod{n} \).

Can perform +, -, \( \times \) "quickly" in \( \mathbb{Z}_n \).
Example:

\[ 521^{1000} + 1023^{500} \cdot 723^y \equiv 1^{1000} + (-1)^{500} \cdot (2)^y \equiv 1 + 1 \cdot 16 \equiv 17 \equiv 2 \pmod{5} \]

Remark: If \( d \equiv e \pmod{n} \), we cannot conclude that \( a^d \equiv a^e \pmod{n} \). For example,

\[ 1 \equiv 4 \pmod{3} \text{ but } 2^1 \equiv 2 \not\equiv 2^4 \pmod{3}. \]

The Euclidean algorithm

Used to compute the greatest common divisor of two integers \( \gcd(a, b) \), where \( (a, b) \neq (0, 0) \). May assume \( a \geq b > 0 \). Otherwise replace \( a, b \) by \( |a|, |b| \).
Last time we proved

**Lemma:** If \( q \) is an integer, then \( \gcd(a, b) = \gcd(a-qb, b) \).

The Euclidean algorithm applies this lemma recursively. Each time we divide \( a \) by \( b \) with remainder:

\[
a = qb + r, \text{ where } a \geq b, 0 \leq r < b.
\]

\( \gcd(a, b) = \gcd(b, r) \)

Now replace \((a, b)\) by \((b, r)\) and proceed recursively. Stop when \( r = 0 \).
**Example 1:** $a = 154$, $b = 35$. Euclidean algorithm:

$154 = 4 \cdot 35 + 14 \quad (154, 35)$

$35 = 2 \cdot 14 + 7 \quad (35, 14)$

$14 = 2 \cdot 7 + 0 \quad (14, 7) \rightarrow (7, 0)$

Conclusion: $\gcd(154, 35) = 7$

---

**Example 2:** $a = 553$, $b = 327$. Euclidean algorithm:

$553 = 1 \cdot 327 + 226 \quad (553, 226)$

$327 = 1 \cdot 226 + 101 \quad (327, 226)$

$226 = 2 \cdot 101 + 24 \quad (326, 101)$

$101 = 4 \cdot 24 + 5 \quad (226, 101)$

$24 = 4 \cdot 5 + 4 \quad (101, 24)$

$5 = 1 \cdot 4 + 1 \quad (24, 5)$

$4 = 1 \cdot 4 + 0 \quad (5, 4)$

Conclusion: $\gcd(553, 327) = 1$. 
Bezout’s Theorem

We will now use the Euclidean algorithm to “quickly” find an integer solution to the equation \( ax + by = \gcd(a, b) \) for any given pair of integers \( a \geq b > 0 \).

In particular, we will see that this equation always has a solution.

Set

\[
\begin{align*}
    r_{-1} &= q_1, \quad r_0 = b \\
    r_{-1} &= r_0 q_0 + r_1, \quad 0 \leq r_1 < r_0 \\
    r_0 &= r_1 q_1 + r_2, \quad 0 \leq r_2 < r_1 \\
    r_1 &= r_2 q_2 + r_3, \quad 0 \leq r_3 < r_2 \\
    &\vdots \\
    r_{i-1} &= r_i q_i + r_{i+1}, \quad 0 \leq r_{i+1} < r_i \\
    &\vdots \\
    r_{j-2} &= r_{j-1} q_{j-1} + r_j, \quad 0 \leq r_j < r_{j-1} \\
    r_{j-1} &= r_j q_j \\
\end{align*}
\]

Here \( \gcd(a, b) = r_j \). First we express it as a linear combination of \( r_{j-1} \) and \( r_{j-2} \) with integer coefficients, using the second to last equation,

\[ \gcd(a, b) = r_j = r_{j-2} - q_{j-1} r_{j-1} . \]

Now we use the next equation, \( r_{j-3} = q_{j-2} r_{j-2} + r_{j-1} \) to eliminate \( r_{j-1} \) and express \( \gcd(a, b) \) as a linear combination of \( r_{j-3} \) and \( r_{j-2} \). Continue until \( \gcd(a, b) \) is expressed as an integer linear combination of \( r_{-1} = a \) and \( r_0 = b \).
**Back to Example 1:** Solve $154x + 35y = 7$.

Euclidean algorithm:

$154 = 4 \cdot 35 + 14$

$35 = 2 \cdot 14 + 7$

$14 = 2 \cdot 7 + 0$.

Back substitution:

$7 = 35 - 2 \cdot 14 = 35 - 2 \cdot (154 - 4 \cdot 35) = 35 - 2 \cdot 154 + 8 \cdot 35 = (-2) \cdot 154 + 9 \cdot 35$.

Integer solution to $154x + 35y = 7$: $x = -2, y = 9$.

**Back to Example 2:** $a = 553, b = 327$. Euclidean algorithm:

$553 = 1 \cdot 327 + 226$

$327 = 1 \cdot 226 + 101$

$226 = 2 \cdot 101 + 24$

$101 = 4 \cdot 24 + 5$

$24 = 4 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

$4 = 1 \cdot 4 + 0$.

Solve $553x + 327y = 1$ by back substitution:

$1 = (1 \cdot 5) + (-1 \cdot 4) = (-1 \cdot 24) + (5 \cdot 5)$

$= (5 \cdot 101) + (-21 \cdot 24) = (-21 \cdot 226) + (47 \cdot 101)$

$= (47 \cdot 327) + (-68 \cdot 226) = (-68 \cdot 553) + (115 \cdot 327)$

Solution: $x = -68, y = 115$. 
Bezout's Theorem

Let \( a, b, c \) be integers, \((a, b) \neq (0, 0)\).

The equation \( ax + by = c \) has an integer solution \((x, y)\) if and only if \( c \) is divisible by \( \gcd(a, b) \).

Proof: Suppose \( c \) is divisible by \( d = \gcd(a, b) \), say, \( c = kd \) for some integer \( k \). Using the Euclidean algorithm, we can find integers \( x_0, y_0 \) such that \( ax_0 + by_0 = d \).

Now set \( x = kx_0, y = ky_0 \). Then
\[
ax + by = a(kx_0) + b(ky_0) = k(ax_0 + by_0) = kd = c.
\]

Thus \( ax + by = c \), we have found an integer solution.

Conversely, \( ax + by \) is divisible by \( d = \gcd(a, b) \) for any integers \( x, y \). If \( d \mid c \), then \( ax + by = c \) has no solutions. D.F.D.
Corollary: (1) An integer $a$ has a multiplicative inverse \((\text{mod } n)\) if and only if $\gcd(a, n) = 1$.

(2) $\mathbb{Z}_n$ is a field if and only if $n$ is a prime integer.

Proof: (1) $a$ has a multiplicative inverse \((\text{mod } n)\) if $ax \equiv 1 \pmod{n}$ for some integer $x$. This means $ax - 1$ is divisible by $n$ or $ax - 1 = ny$ for some integer $y$.

In other words, $a$ has a multiplicative inverse \((\text{mod } n)\) if and only if the equation $ax - ny = 1$ has an integer solution \((x, y)\). By Bezout's theorem, this happens if and only if $\gcd(a, n) = 1$. 
Proof of (2): If \( n \) is a prime, then \( \gcd(a, n) = 1 \) for any \( a = 1, 2, \ldots, n-1 \). Thus every non-zero \( a \) in \( \mathbb{Z}_n \) has a mult. inverse. Last time we saw that \( \mathbb{Z}_n \) is a ring for any \( n \geq 2 \). Thus if \( n \) is a prime, then \( \mathbb{Z}_n \) is a field.

Conversely, if \( n \) is not a prime, say \( n = ab \), where \( 2 \leq a, b \leq n-1 \), then \( \gcd(a, n) = a > 1 \), so by (1), \( a \) does not have a mult. inverse in \( \mathbb{Z}_n \), so \( \mathbb{Z}_n \) is not a field.

Q.E.D.
Example: What is $\frac{11}{21}$ in $\mathbb{Z}_{41}$.

First, let us compute $21^{-1} \pmod{41}$.

Need to find integer solution to

$$21x + 41y = 1$$

Apply Euclidean algorithm to compute $\gcd(21, 41)$.

$$41 = 1 \cdot 21 + 20$$

$$21 = 1 \cdot 20 + 1$$

$$20 = 20 \cdot 1 + 0$$

Back substitution:

$$1 = 1 \cdot 21 - 1 \cdot 20 = 1 \cdot 21 - (41 - 21)$$

$$= 2 \cdot 21 - 1 \cdot 41$$

$$\times x \quad \div y$$

Thus $21 \cdot 2 \equiv 1 \pmod{41}$, so $21^{-1} \equiv 2 \pmod{41}$. 

\[
\frac{11}{21} \equiv 11 \cdot 21^{-1} \equiv 11 \cdot 2 \equiv 22 \pmod{41}.
\]

Back to coding theory.

**Proposition:** \( A_q(n,2) = q^{n-1} \), for any \( q \geq 2 \).

Recall: By Singleton,
\( A_q(n,2) \leq q^{n-1} \). In the case where \( q = 2 \), we showed that equality holds by using the idea of "parity check".

We will now use a similar construction with \( F_q = \mathbb{Z}_q \). Our goal is to show that \( A_q(n,2) \geq q^{n-1} \), i.e., to construct a \( q \)-ary \((n,2)\)-code \( C \) of size \( q^{n-1} \).
To construct $C$, start with $\mathbb{F}_q^{n-1} = \{\text{all } q\text{-ary words of length } n-1\}$. To each word, append one digit $a_n$ in position $n$.

$$(a_1, \ldots, a_{n-1}) \mapsto (a_1, \ldots, a_{n-1}, a_n)$$

where $a_n \equiv -a_1 - a_2 - \cdots - a_{n-1} \pmod{q}$.

The resulting code $C$ has length $n$, size $q^{n-1}$. It remains to show that $d(C) = 2$. To see that $d(C) \leq 2$, start with

$a = (0, \ldots, 0) \mapsto a' = (0, 0, \ldots, 0, 0)$
$b = (1, 0, \ldots, 0) \mapsto b' = (1, 0, \ldots, 0, q-1)$

$d(a', b') = 2$. Thus $d(C) \leq 2$. 

It remains to show that \( d(C) \geq 2 \).

Suppose there exist \( x, y \) in \( C \) at distance 1. In other words, \( x = (x_1, \ldots, x_n) \) and \( y = (y_1, \ldots, y_n) \) differ in exactly one position, say in position \( k \). Then by construction

\[
\begin{align*}
  x_1 + \cdots + x_n &\equiv 0 \pmod{q} \\
  y_1 + \cdots + y_n &\equiv 0
\end{align*}
\]

Subtract second equation from first:

\[
  x_k - y_k \equiv 0 \pmod{q}
\]

This means \( x_k \equiv y_k \pmod{q} \), so \( x, y \) are same in every position, contradicting \( d(x, y) = 1 \).

\[\text{Q.E.D.}\]