LECTURE 2
(Monday SEP. 30, 2019)
Numbers.
Set of all integers (possibly negative):
\[ \mathbb{Z} = \{ 0, \pm 1, \pm 2, \pm 3, \ldots \} \]

"zahlen"
-2 -1 0 1 2 \[ \rightarrow \mathbb{Z} \]

has addition & multiplication.

Note: \( \mathbb{Z} \) with \( \times \) is a group.
However, \( \mathbb{Z} \) with \( \circ \) is not a group. Even \( \mathbb{Z} \setminus \{ 0 \} \) is still not a group:
\[ \frac{1}{a} \text{ is not in } \mathbb{Z} \text{ unless } a = \pm 1. \]

Recall:
Definition. Let \( a, b \in \mathbb{Z} \). We say \( a \) divides \( b \) (or that \( b \) is divisible by \( a \)) if there's \( a \) \( q \in \mathbb{Z} \) such that
\[ b = qa. \]

Notation: when this happens we write \( a \mid b \).
Example: For any $a \in \mathbb{Z}$, $1 \mid a$ and $a \mid a$.

We say $a > 1$ is a prime number if $\exists q, a^2$ are the only positive divisors.

Note that $(-1) \mid a$ since $a = (-a)(-1)$.

$2, 3, 5, 7, 11, 13, \ldots$ (as many)

"transitive"

Example: $a \mid b$ and $b \mid c \implies a \mid c$.

$(q, b, c \in \mathbb{Z})$

(sketched: $b = qa$ and $c = q_2 b$)

$
\implies c = q_2 (qa) = (q_2 q_1) a
$

Theorem ("Division with remainder") $\forall a \in \mathbb{Z}$

Given any two $a, b \in \mathbb{Z}$ with $a$ positive, there are uniquely determined $q, r \in \mathbb{Z}$ satisfying the following two conditions simultaneously:

\[
\begin{align*}
(1) \quad & b = qa + r \quad \text{and} \\
(2) \quad & 0 \leq r < a.
\end{align*}
\]

(well-ordering principle...)

\[
\begin{array}{ccccccc}
0 & 1a & 2a & \cdots & qa & b & (q+1)a \\
\end{array}
\]
\[ \text{EX (}a=10, \ b=2019\text{)} \quad 2019 = 201 \cdot 10 + 9 \]

- Compare:
  \[ \quad \begin{array}{c}
  a \text{ too big} \\
  r \text{ too small}
  \end{array} \]

Observe:
\[ d \mid a \text{ and } d \mid b \iff d \mid a \text{ and } d \mid r \]
\( (d \in \mathbb{Z}) \quad \text{can use this to find the } \]
\[ \text{"greatest common divisor"} \]
\[ \text{GCD}(a, b) \].

\[ \text{EX Find GCD}(221, 323). \]

\[ \begin{align*}
323 &= 1 \cdot 221 + 102 \\
221 &= 2 \cdot 102 + 17 \\
102 &= 6 \cdot 17 + 0.
\end{align*} \]

Back-substitution allows us to express GCD\((a, b)\) as a linear combination \(ax + by\) for suitable \(x, y \in \mathbb{Z}\):
\[ 17 = 221 + (-2) \cdot 102 = 221 + (-2)(323 - 221) \]
\[ = (-2) \cdot 323 + 3 \cdot 221 \quad \text{[}x=3, y=-2\text{]} \]
Warning: There are infinitely many solutions \((x, y)\)
where \(GCD(a, b) = ax + by\)

\[ = a(x + tb) + b(y - ta) \]

Geometry:
lattice points on a line.

Definition: We say \(a, b \in \mathbb{Z}\) are coprime
when \(GCD(a, b) = 1\).

(i.e., no common factor \(>1\))

\[ \rightarrow \text{in this case: } 1 = ax + by \text{ for suitable coefficients } x, y \in \mathbb{Z}. \]

Application: \(p = \text{prime number.}\)

Suppose \(p | ab\). Then: \(p | a\) or \(p | b\).

(possibly \(p\) divides both)

\[ \text{Why? Assume } p | a, \text{ show } p | b. \]

\[ GCD(a, p) = 1 = ax + py. \]

(divides \(p\) so \(p = 1\) or \(p\))

Multiply by \(b\) on both sides:

\[ b = (ab)x + p(by) \]

- both terms are \(p\) multiples.

\[ \text{Ex. This fails if } p \text{ not prime: } \]

\[ G \mid 2 \cdot 3, \text{ but } G \not| 2 \text{ and } \]

\[ G \not| 3. \]
"least common multiple":
\[ \text{LCM}(a, b) = \frac{ab}{\text{GCD}(a, b)} \]

**Ex:** \( \text{LCM}(221, 323) = \)
\[
\frac{221 \cdot 323}{17} = 13 \cdot 323 = 4199.
\]

- Recall: Can read off GCD and LCM from prime factorizations of \( a, b \).

**Ex.** \( a = 5^7 \) and \( b = p^8 q^3 \) (\( p \neq q \) primes)

Then:
\[ \text{GCD}(a, b) = p^{\min(7, 8)} q^{\min(3, 3)} = 5^3 \]
\[ \text{LCM}(a, b) = p^{\max(7, 8)} q^{\max(3, 3)} = p^8 q^3. \]