Last class:

Main results:

- Division with remainder:
  \( a, b \) integers, \( b > 0 \)
  \( \Rightarrow \exists \) unique \( q \) and \( r \), \( 0 \leq r < b \) s.t.
  \[ a = qb + r \]

- \( a, b \) integers \( \Rightarrow \exists \) integers \( s \) and \( t \) s.t.
  \[ \gcd(a, b) = as + bt \]

Def. \( \text{A integer } a \text{ is called } \text{prime} \text{ if} \)
its only divisors are \( \pm 1 \) and \( \pm a \)

- Two integers \( a \) and \( b \) are \text{relatively prime} if
  \[ \gcd(a, b) = 1 \]
Euclid's Lemma  \(a, b\) integers, \(p\) prime

\[ p \mid ab \implies p \mid a \text{ or } p \mid b \]

Proof. Assume \( p \nmid a \)

\[ \implies \gcd(p, a) = 1 \]

by previous result: \(1 = sa + tp\) for some integers \(s\) and \(t\)

\[ b = b \cdot 1 = b (sa + tp) = abs + btp \]

obv. \( p \mid btp \)

by ass. \( p \mid ab\)

\( p \mid (abs + btp) = b \)
Application:

**Theorem (Uniqueness of Prime Decomposition)**

Any integer \( n \) can be written as a product of primes uniquely up to the order of the primes (e.g., \( 30 = 2 \cdot 3 \cdot 5 = 5 \cdot 3 \cdot 2 \ldots \) )

(proof later as needed)

Proof of uniqueness statement depends on Euclid's Lemma)
Modular Arithmetic

Question: Is 1173 \cdot 2357 odd or even?

Answer: Both numbers are odd.

We know odd \cdot odd = odd.

Let a, n be integers, 

\[ n > 0 \]

We write \[ a \mod n = r \]

if \[ a = qn + r \]

with \[ 0 \leq r < n \]

Examples:

1173 \mod 2 = 1
2357 \mod 2 = 1
27 \mod 12 = 3
Lemma: Let $a, b, n$ be integers, $n > 0$.

\[ a \mod n = b \mod n \iff n \mid (a - b) \]

Proof:

Let $a = q_1 n + r_1$, $0 \leq r_1, r_2 < n$,

\[ b = q_2 n + r_2 \]

"\[ \Rightarrow \]

by assumption $r_1 = r_2$

\[ \Rightarrow \]

$a \mod n = b \mod n$

\[ \Rightarrow \]

$a - b = (q_1 n + r_1) - (q_2 n + r_2)$

\[ = (q_1 - q_2) n + (r_1 - r_2) \]

\[ \Rightarrow \]

$n \mid (a - b)$

\[ \iff \]

(exercise, can reverse steps from "\[ \Rightarrow \]"

\[ \iff \]

(by ass.)
**Theorem**

\[ a, b, n \text{ integers, } n > 0 \]

\[ a \mod n = r_1 \]
\[ b \mod n = r_2 \]

\[ \implies \]

\[ a \times b \mod n = (r_1 + r_2) \mod n \]
\[ a \times b \mod n = r_1 \cdot r_2 \mod n \]

**Proof.**  

(a) enough to show: \( n \mid a \times b - (r_1 + r_2) \) by lemma

\[ a \times b - r_1 \cdot r_2 = (q_1 n + r_1) + (q_2 n + r_2) - r_1 \cdot r_2 \]

\[ = a \]
\[ = b \]

\[ = q_1 n + q_2 n \]

\[ = n(q_1 + q_2) \]

i.e. \( n \mid a \times b - r_1 \cdot r_2 \)  \( \checkmark \)
(b) same strategy

\[ \alpha = q_1 n + r_1 \]
\[ b = q_2 n + r_2 \]

\[ ab - r_1 r_2 = (q_1 n + r_1)(q_2 n + r_2) - r_1 r_2 \]
\[ = q_1 q_2 n^2 + q_1 n r_2 + r_1 q_2 n + r_1 r_2 - r_1 r_2 \]
\[ = n(q_1 q_2 n + q_1 r_2 + r_1 q_2) \]

\[ \Rightarrow n \mid ab - r_1 r_2 \]

Examples: (1) \[ n \text{ odd } \iff n \mod 2 = 1 \]

\[ 1173 \mod 2 = 1 \]
\[ 2357 \mod 2 = 1 \]

\[ \Rightarrow 1173 \cdot 2357 \mod 2 = 1 \cdot 1 \mod 2 = 1 \]

\[ \Rightarrow \text{ product is also odd} \]
(2) Calculate $19^5 \mod 17$

Solution:

$19 \mod 17 = 2$

$19^5 \mod 17 = 2^5 \mod 17$

$= 32 \mod 17$

$= 15$

(3) Calculate the last digit of $3^{403}$

Solution:

We need to calculate $3^{403} \mod 10$

$3^2 \mod 10 = 9 \mod 10 = 9$

$3^3 \mod 10 = 27 \mod 10 = 7$

$3^4 \mod 10 = 81 \mod 10 = 1$
\[ 3^{403} = 3^4 \cdot 100 + 3 \]
\[ = (3^4)^{100} \cdot 3^3 \]

\[ \Rightarrow 3^{403} \mod 10 = (3^4)^{100} \cdot 3^3 \mod 10 \]
\[ = 1^{100} \cdot 7 \mod 10 \]

\[ \text{Theorem} \]
\[ = 7 \]

Remark: Calculating \( a^k \mod n \) for high powers \( k \) is simplified by:
- Determine smallest number \( h \) s.t. \( a^h \equiv 1 \mod n \) (if possible);
- Write \( k = qh + r \) \( \Rightarrow a^k = a^{qh+r} \).
4. Prove that \( x^2 - y^2 = 1002 \) cannot have any integer solutions.

Solution: Consider this equation mod 4

\[
\begin{array}{c|c|c}
 x \mod 4 & x^2 \mod 4 & x^2 \mod 4 \\
 0 & 0 & 0 \text{ or } 1 \\
 1 & 1 & 0 \text{ or } 1 \\
 2 & 0 & 0 \\
 3 & 1 & 1 \\
\end{array}
\]

\( x^2 \mod 4 \) is either 0 or 1.

Same for \( y^2 \mod 4 \).
Consider all possible cases

<table>
<thead>
<tr>
<th>$x^2 \mod 4$</th>
<th>$y^2 \mod 4$</th>
<th>$x^2 - y^2 \mod 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>-1 mod 4 = 3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Result: $x^2 - y^2 \mod 4 \neq 2$

for any choice of integers $x$ and $y$

$\Rightarrow x^2 - y^2 = 1002$ does not have an integer solution.