Discrete Log Problem
Typed Notes Added!

\[ 2^5 = 32 \iff \log_2 32 = 5 \]
exp func \rightarrow \text{inv exp}

What power do I raise 2 to, to obtain 32?

\[ 2^x = 32 \quad \text{What is } x? \]
Assuming \( b > 1 \), if \( x < y \), then \( \log_b x < \log_b y \).

Goal: Calc \( \log_2 128 \), and I find out that \( \log_2 32 = 5 \), then I know my ans > 5.

\[ 2^x \equiv 3 \pmod{11} \quad \text{What is } x? \]
\[ \text{ans} = 8 \]

<table>
<thead>
<tr>
<th>exp</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2^\text{mod11})</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

\( \text{NO SIMPLE PATTERN!} \)
\[ 10 \mod 11 \mid 1 \mid 10 \mid 1 \mid 10 \mid 1 \mid 10 \mid \ldots \]

\[ 10^x \equiv 3 \pmod{11} \]

No answer!

Not a good base because many "answers" aren't possible.

For each possible base \((1, 2, 3, \ldots, p-1)\),
we know by Fermat's \( b^{p-1} \equiv 1 \pmod{p} \)
but for some bases \( \exists x \mid x < p-1, x > 0 \)
and \( b^x \equiv 1 \pmod{p} \).

Define term: primitive root/generator is
a value \( b \) such that the minimum
positive integer \( x \) such that \( b^x \equiv 1 \pmod{p} \)
for a prime \( p \) is \( x = p-1 \).

1. Generate program to list each base to
each power for a prime
   \( \rightarrow \) look table pick out primitive roots

2. Assuming 1 primitive root exists,
   we'll count the # of primitive
   roots

3. Write program to generate all De primitive
   roots (or test if a value is a
   primitive)
ord(b) \mod p \text{ is min value of } x \\
s.t. \ b^x \equiv 1 \pmod{p}.

If \ ord(b) = p-1, it's a primitive root

\[ 4^3 = (2^2)^3 = 26 \]

So now for 4 is skipping every other item on the row for 2.

\[ 2^3 = 8, \text{ so } 8^k \text{ will be skipping 2 items.} \]

So modular exponentiation is like running around a tree in \ 2^x

Every running around goes \ k \ notches each second \ 1 \leq k \leq 10. \text{ If } \gcd(k,10) \neq 1, \text{ then we'll never visit all notches.}

\# \text{ of primitive roots = \# ints } 1 \text{ to } p-1 \text{ that are relatively prime to } p-1 = \phi(p-1).
Write

How to test for a primitive root

\[ p = 17 \quad \| \quad p = 37 \]
\[ p - 1 = 16 \quad \| \quad p - 1 = 36 = 2^2 \cdot 3^2 \]
\[ b^{\frac{p-1}{2}} \neq 1 \mod p \]
\[ b^{\frac{p-1}{3}} \neq 1 \mod p \]

Find each unique prime divisor of \( p - 1 \)
\[ q_1, q_2, \ldots, q_k \]

\[ b^{\frac{p-1}{q_i}} \neq 1 \mod p \quad \text{for each} \]
\[ 1 \leq i \leq k, \text{ then } b \text{ is a primitive root.} \]