Fund Theorem Arith

Every pos int can be uniquely prime factorized

Prime: int divisible by only 1 and itself

\[ 36 = 4 \times 9 = 2^2 \times 3^2 \]

\[ n = \prod_{p \in \text{prime}} p_0^q \]

\[ = 2^2 \times 3^1 \times 5^0 \times 7^0 \times \ldots \]

How to prime factorize: trial division

If a \( n \) is composite, then it has at least 1 divisor \( \leq \sqrt{n} \)

Assume opposite \( a \times b = n \) and \( a \geq \sqrt{n} \) and \( b \geq \sqrt{n} \)

\[ a \times b > \sqrt{n} \times \sqrt{n} = n \]

Write a function to print factorize a number upto \( 10^{12} \).
Fermat’s Thm

If \( \gcd(a, p) = 1 \) and \( p \) is prime, then
\[ a^{p-1} \equiv 1 \pmod{p} \]

\[ p = 101, \ a = 68, \ 68^{100} \equiv 1 \pmod{101} \]

\[ S = \{ 1, 2, 3, \ldots, p-2 \} \]

All non-zero remainders when dividing by \( p \)
\[ \gcd(i, p) = 1 \]
for all \( 1 \leq i \leq p-1 \).

\[ T = \{ a, 2a, 3a, 4a, \ldots, a(p-1) \} \]

Prove that the elements of \( T \) taken \( \mod p \)
are the same set as \( S \).

\( p = 7, \ a = 4 \)

\[ S = \{ 1, 2, 3, 4, 5, 6 \} \]

\[ T = \{ 4, 8, 12, 16, 20, 24 \pmod{7} \} \]

\[ \gcd(4, 7) = 1 \]

4 1 5 2 6 3
Assume the opposite $S \neq T$ (elements $\mod p$)

None of the elements of $T \equiv 0 \pmod{p}$
all must be $\equiv x \pmod{p} \times \equiv 0$.
If all elements unique the $S = T$,
$T$ has a repeat element.

\[ a_i \equiv a_j \pmod{p} \quad 1 \leq i < j \leq n-1 \]

\[ a_i - a_j \equiv 0 \pmod{p} \]
\[ a(i-j) \equiv 0 \pmod{p} \]

\[ \Rightarrow p | a(i-j) \]

\[ \Rightarrow p | a \vee p | (i-j) \]

\[ \times \quad 0 < |i-j| < p-1 \]

Wrong \[ \times \]

Wrong

CONTRACTION!

Conclude that our initial assumption was wrong! It follows that $S = T$ as desired.
\[ S = \{1, 2, \ldots, p-1\} \]
\[ \mathcal{T} = \{a, 2a, 3a, \ldots, a(p-1)\} \]

\[ \prod_{x \in \mathcal{T}} x \equiv \prod_{y \in S} y \pmod{p} \]
\[ \prod_{i=1}^{p-1} a_i \equiv \prod_{i=1}^{p-1} i \pmod{p} \]
\[ a^{p-1} \prod_{i=1}^{p-1} i - \prod_{i=1}^{p-1} i \equiv 0 \pmod{p} \]
\[ \left( \prod_{i=1}^{p-1} i \right) \left( a^{p-1} - 1 \right) \equiv 0 \pmod{p} \]

\[ \Rightarrow p \mid \prod_{i=1}^{p-1} i \quad \lor \quad p \mid \left( a^{p-1} - 1 \right) \]

\[ \times \]
\[ \text{not true} \]

If you take any base any exponent, \( a \), mod \( p \), you'll a looping/cyclic pattern of size \( k \) where \( k \mid (p-1) \).
Generators or primitive roots

Euler Phi Function

\[ \phi(n) = \text{the number of ints from 1 to } n \text{ that are relatively prime with } n. \]

\[ \phi(6) = 2 \quad \{1, 5\} \]

\[ \phi(15) = 8 \quad \{1, 2, 4, 5, 7, 8, 11, 13\} \]

(1) possible keys offline w/ alphabet size \( n \)

\[ \# \text{choices} = n \cdot \phi(n) \]

\[ \# \text{choices} = 6 \cdot 2 = 12 \]

Pub b

Pub G
Euler's Thm

If \( \gcd(a, n) = 1 \), then \( a^\phi(n) \equiv 1 \pmod{n} \)

\[ S = \{1, 2, 4, 7, 8, 11, 13, 14, 15\} \quad S = \{1 \text{ to } n \text{ relative to } n\} \\
S = \{1, 4, 9, 14\} \quad S = \{p^\phi(p)\} \]

\[ T = \{4, 8, 16, 28, 32, 44, 52, 56\} \]

\[ n \equiv 4 \]

Proof: \( S = T \).

Either \( S = T \) or \( T \) has \( s \) repeat!

\[ a \cdot a_i \equiv a \cdot a_j \pmod{n} \quad a_i \neq a_j \]

\[ a_i - a_j \equiv 0 \pmod{n} \]

\[ a \mid (a_i - a_j) \]

\[ \Rightarrow n \mid (a \cdot (a_i - a_j)) \]

Adjusted rule:
if \( \gcd(n, a) = 1 \) and \( n \mid ab \), then \( n \mid b \).

We know \( \gcd(n, a) = 1 \) so

\[ \Rightarrow n \mid (a_i - a_j) \]

\[ 0 < |a_i - a_j| < \phi(n) - 1 \]

Contradiction
\[
\prod_{i=1}^{\phi(n)} a a_i \equiv \prod_{i=1}^{\phi(n)} a_i \pmod{n}
\]

\[
\prod_{i=1}^{\phi(n)} a a_i - \prod_{i=1}^{\phi(n)} a_i \equiv 0 \pmod{n}
\]

\[
\left( \prod_{i=1}^{\phi(n)} a_i \right) \left( a^{\phi(n)} - 1 \right) \equiv 0 \pmod{n}
\]

\[
\rightarrow n \mid \left( \prod_{i=1}^{\phi(n)} a_i \right) \left( a^{\phi(n)} - 1 \right), \text{ but}
\]

\[
gcd\left(n, \prod_{i=1}^{\phi(n)} a_i\right) = 1, \text{ so it follows that}
\]

\[
n \mid \left( a^{\phi(n)} - 1 \right)
\]

\[
\rightarrow a^{\phi(n)} - 1 \equiv 0 \pmod{n}
\]

\[
a^{\phi(n)} \equiv 1 \pmod{n}
\]