Euclidean Algorithm:

\[ a = bq_1 + r_1 \quad 0 < r_1 < b \]
\[ b = r_1q_2 + r_2 \quad 0 < r_2 < r_1 \]
\[ r_1 = r_2q_3 + r_3 \quad 0 < r_3 < r_2 \]

Line k-1: \( r_{k-1} = r_{k-2}q_k + r_k \quad 0 < r_k < r_{k-2} \)

Line k: \( r_k = r_{k-1}q_k + r_{k-2} \quad 0 < r_k < r_{k-1} \)

Line k+1: \( r_{k+1} = r_kq_{k+1} + r_{k-1} \quad 0 < r_{k+1} < r_k \)

N.T.P: two things to prove: \( D = \gcd(a, b) \)

1. \( r_k \mid a \) and \( r_k \mid b \)
2. If \( r_k \mid a \) and \( r_k \mid b \), then \( r_k \mid D \)

Proof:

1. Line \( k+1 \Rightarrow r_k \mid r_{k+1} \)
   
   Then since \( r_{k+1} = r_kq_{k+1} + r_{k-1} \)
   
   \( r_k \) also divides \( r_{k-1} \)
   
   Then line \( k-1 \Rightarrow r_k \mid r_{k-1} \)
   
   Continuing the process we get \( r_k \mid b \)
   
2. Suppose \( r_k \mid a \) and \( r_k \mid b \).
   
   Then \( r_k \mid r_1 \) because line \( 1 \Rightarrow r_1 = a - bq_1 \)
   
   Then similarly \( b/c \) \( r_k \mid r_2 \) and \( r_k \mid r_1 \) we get \( r_k \mid r_2 \)
   
   (because line \( k \Rightarrow r_2 = b - r_1q_k \))
   
   Continuing this process we get that \( r_k \mid D \)
   
   So \( r_k \mid D \)

by 1 \& 2, \( D = \gcd(a, b) \).

Euclid's Lemma:

Suppose \( p \mid ab \) and \( p \nmid a \).

Then, \( p \mid b \).

Proof:

Suppose \( p \mid ab \) and \( p \nmid a \).

Need to show: \( p \mid b \).

If \( p \mid a \), Euclid's Lemma either \( p \mid b \) or \( p \mid c \).

If \( p \mid b \), since \( p \mid a \), we get \( p \mid c \).

If \( p \mid c \), since \( p \mid a \), we get \( c \mid b \).

So, we can't have \( ab \mid c \).

Hence, \( ab \mid c \).

**Ch 0 #16**

\[ 126 = 3 \times 4 + 24 \]
\[ 34 = 1 \times 24 + 10 \]
\[ 24 = 2 \times 10 + 4 \]
\[ 10 = 2 \times 4 + 2 \]
\[ 4 = 2 \times 2 + 0 \]

\[ 2 = 10 - 2 \times 4 \]
\[ = 10 - 2 \times (24 - 2 \times 10) = 5 \times 10 - 2 \times 24 \]
\[ = 5 \times (34 - 24) - 2 \times 24 = 5 \times 34 - 7 \times 24 \]
\[ = 5 \times 34 - 7 \times (126 - 3 \times 34) \]
\[ 2 = 26 \times 34 - 7 \times 126 \]
**CHO # 21**
A set with \( n \) elements has \( 2^n \) subsets for every \( n \in \mathbb{Z}^+ \).

Proof by Induction:

Initial case: \( n = 1 \).

Subsets of a set, with a single element are \( \emptyset \) and the set itself, so

For: \( n = 1 \), \# subsets = \( 2^1 = 2 \).

Inductive hypothesis:

Assume a set with \( n \) elements has \( 2^n \) subsets.

Suppose \( A \) has \( n+1 \) elements, say \( A = \{a_1, a_2, ..., a_n, a_{n+1}\} \).

Consider \( B = \{a_1, ..., a_n\} \), any.

By the inductive assumption \( B \) has \( 2^n \) subsets.

Subsets of \( B \) are obviously subsets of \( A \). \( A \) will have additional subsets which are obtained by including \( a_{n+1} \) to each of the subsets of \( B \).

So number of additional subsets will be \( 2^n \) as well.

Total number of subsets of \( A \) is then \( 2^n + 2^n = 2 \cdot 2^n = 2^{n+1} \).

(We used the first principle of induction.)

**CHO # 28**
fn: with Fibonacci number

\[ f_1 = f_2 = 1 \]

\[ f_n = f_{n-1} + f_{n-2} \text{ for } n > 3 \]

Show that \( f_n < 2^n \) for all \( n \geq 3 \).

Proof by Induction:

Initial case: \( n = 3 \).

\[ f_3 = f_2 + f_1 = 1 + 1 = 2 = 2^1 \leq 2^3 \]

Inductive hypothesis:

Assume \( f_k < 2^k \) for all \( k \leq n \).

Prove that \( f_{n+1} < 2^{n+1} \).

\[ f_{n+1} = f_n + f_{n-1} < 2^n + 2^{n-1} \]

\[ = 2^n + 2^{n-1} \]

\[ < 2^n + 2^n = 2^{n+1} \]

By inductive assumption:

\( f_n < 2^n \) and \( f_{n-1} < 2^{n-1} \).

So, \( f_{n+1} < 2^n + 2^{n-1} \leq 2^n + 2^n = 2^{n+1} \).

**CHO # 41**
ISBN for our book: <0 6 1 8 5 1 4 1 6>

dot product with \( \langle 10, 01, 8, 7, 6, 5, 4, 3, 2, 1 \rangle \)

\( \langle 1, 54 + 8 + 56 + 30 + 5 + 16 + 21 + 2 + 6 \mod 11 \rangle - 1 + 8 + 2 + 7 + 5 + 5 + (-9) + 2 + 6 = 0 \)

\( S = \mathbb{Z}, \text{ a R b iff } 5 | a-b \).

i) reflexivity: Is \( a \RA a \in S \)?

Yes does \( 5 | a-a \in \mathbb{Z} \)?

ii) symmetry: If \( a \RA b \) then is \( b \RA a \in S \)?

\[ a \RA b \iff 5 | a-b \iff 5 | -(b-a) \iff 5 | b-a \iff b \RA a \]

iii) transitivity: If \( a \RA b \) and \( b \RA c \) then is \( a \RA c \in S \)?

\[ a \RA b \text{ and } b \RA c \iff 5 | a-b \text{ and } 5 | b-c \iff 5 | a-b+c = 5 | a-c \iff a \RA c \]

Equivalence classes:

\[ \bar{0} = \{ 2 \cdot 5 | a, 2 \cdot 5 | a-1, \ldots, 2 \cdot 5 | a-24 \} \]

\[ \bar{1} = \{ 2 \cdot 5 | a, 2 \cdot 5 | a-1, \ldots, 2 \cdot 5 | a-24 \} \]

\[ \bar{2} = \{ 2 \cdot 5 | a, 2 \cdot 5 | a-1, \ldots, 2 \cdot 5 | a-24 \} \]

\[ \bar{3} = \{ 2 \cdot 5 | a, 2 \cdot 5 | a-1, \ldots, 2 \cdot 5 | a-24 \} \]

\[ \bar{4} = \{ 2 \cdot 5 | a, 2 \cdot 5 | a-1, \ldots, 2 \cdot 5 | a-24 \} \]

Similar for \( 3 \) and \( 4 \).