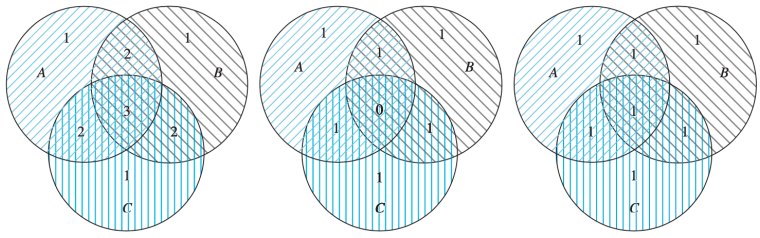
Alison Li

Principle of Inclusion-Exclusion

$|A \cup B| = |A| + |B| - |A \cap B|$.

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.



(a) Count of elements by $|A| + |B| + |C|$

(b) Count of elements by $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$

(c) Count of elements by $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Theorem. Inclusion-Exclusion.

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

($i = 1, 2, \cdots, n$)

proof. omitted.

Problem.

How many integers in $X = \{1, 2, \cdots, 100\}$ are divisible by 2, 3, or 5?

Let $A_2 = \{n \in X : 2 | n\}$

$A_3 = \{n \in X : 3 | n\}$

$A_5 = \{n \in X : 5 | n\}$

Then,

$|A_2| = \lfloor \frac{100}{2} \rfloor = 50$ $\quad |A_2 \cap A_3| = |\{n \in X : 6 | n\}| = \lfloor \frac{100}{6} \rfloor = 16$

$|A_3| = \lfloor \frac{100}{3} \rfloor = 33$ $\quad |A_2 \cap A_5| = |\{n \in X : 10 | n\}| = 10$

$|A_4| = \lfloor \frac{100}{5} \rfloor = 20$ $\quad |A_3 \cap A_5| = |\{n \in X : 15 | n\}| = 6$

$|A_2 \cap A_3 \cap A_5| = |\{n \in X : (2 \cdot 3 \cdot 5) | n\}| = \lfloor \frac{100}{30} \rfloor = 3$

Total by inclusion-exclusion:

$|A_2 \cup A_3 \cup A_5| = |A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|$

$= 50 + 33 + 20 - 16 - 10 - 6 + 3$

Problem.

Let $A = \{1, 2, 3, 4, 5\}$

$B = \{1, 2, 3, 4\}$.

How many $f : A \to B$ are surjective?

Idea: Count not surjective, subtract from the total # of functions.

Let $A_i = \{f : A \to B \mid i \notin \text{range}(f)\}$ for $i = 1, 2, 3, 4$.

Then,

$A_1 = \{f : A \to B \mid 1 \notin \text{range}(f)\}$

$= \{f : A \to \{2, 3, 4\}\}$ (no restrictions).

So, $|A_1| = 3^5$. Similarly $|A_2| = |A_3| = |A_4| = 3^5$.

We also have $|A_1 \cap A_2| = |\{f : A \to \{3, 4\}| = 2^5$.

Similarly,

$|A_i \cap A_j| = 2^5$ $\quad (i \neq j \neq k)$

$|A_i \cap A_j \cap A_k| = 1^5 = 1$.

$|A_1 \cap A_2 \cap A_3 \cap A_4| = |\{f : A \to \emptyset\}| = 0$.

So the number of not surjective functions is:

$|A_1 \cup A_2 \cup A_3 \cup A_4| = \binom{4}{1} \cdot 3^5 + \binom{4}{2} 2^5 - \binom{4}{3} 1^5 + \binom{4}{4} 0$

$= 4 \cdot 3^5 + 6 \cdot 2^5 - 4 \cdot 1^5 + 0$

Total surjective = (all) − (not surjective).

$= 4^5 - 4 \cdot 3^5 + 6 \cdot 2^5 - 4 \cdot 1^5$

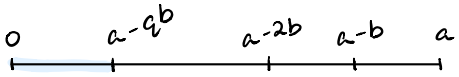
Number Theory

def. $a|b$ if $a \neq 0$ and $b = am$ for some $m \in \mathbb{Z}$ $(a, b \in \mathbb{Z})$.
a divides b.

Theorem. Division "Algorithm."
Let $a, b \in \mathbb{Z}$, $b \neq 0$. There exists $q, r \in \mathbb{Z}$ such that $a = bq + r$, where $0 \leq r < b$.
(q: quotient, r: remainder)

ex. $a = 20$, $b = 3$
then $20 = 3 \cdot 6 + 2$
(6 = "q", 2 = "r")

proof idea.



Subtract multiples of b from a until $a - bq = r$, $0 \leq r < b$.
Formal proof by induction.

def. Let $a, b \in \mathbb{Z}$, not both 0. Then greatest common divisor $\gcd(a, b)$ is the largest $d \in \mathbb{N}$ such that $d|a$ and $d|b$.

Note:
(1) $1 \mid$ anything so $\gcd(a, b) \geq 1$.
(2) $\gcd(a, 0) = |a|$ (everything divides 0, i.e. $n|0$ since $0 = n \cdot 0$).
(3) $\gcd(\pm a, \pm b) = \gcd(a, b)$.
(4) $a|b$ and $b \neq 0 \Rightarrow |a| \leq |b|$.
(5) $a|b$ and $b|a \Leftrightarrow a = \pm b$.

proof of (5).
$a|b$ so $b = ax$ some $x \in \mathbb{Z}$ $(a \neq 0)$.
$b|a$ so $a = by$ some $y \in \mathbb{Z}$ $(b \neq 0)$.
So,
$b = (by)x$.
Since $b \neq 0$, $1 = xy$.
So $x = \pm 1$, $y = \pm 1$. So $a = \pm b$. □

Lemma.
Let $a, b \in \mathbb{Z}$. $b > 0$. If $a = bq + r$, $0 \leq r < b$, then $\gcd(a,b) = \gcd(b,r)$.

proof.
Let $X = \{d \in \mathbb{Z} \mid d|a \wedge d|b\}$
$Y = \{d \in \mathbb{Z} \mid d|b \wedge d|r\}$

We show:

(i) Let $d \in X$ i.e. $d|a$, $d|b$. So $a = ds$, $b = dt$, for some $s, t \in \mathbb{Z}$.
Then $a = bq + r$ so $ds = dtq + r$. So $r = d(\underbrace{s - tq}_{\in \mathbb{Z}})$, hence $d|r$.

Know $d|b$ so $d \in Y$.

(ii) Let $d \in Y$. So $d|b$ and $d|r$. So $b = dt$, $r = du$, for some $t, u \in \mathbb{Z}$.
Then $a = bq + r = dtq + du = d(tq + tu)$.
So $d|a$. Know $d|b$ so $d \in X$.

Thus, common divisor of a, b same as b, r. Hence, greatest common divisor also same. □

Euclidean Algorithm.
Let $a, b \in \mathbb{N}$, not both 0. To find $\gcd(a,b)$:

(1) If $b = 0$, $\gcd(a,b) = a$.
Return a.

(2) If $b \neq 0$, write $a = bq + r$, $0 \leq r \leq b$.
Then $\gcd(a,b) = \gcd(b,r)$.
So compute and return $\gcd(b,r)$.

proof.
Two things to prove:

(1) Algorithm gives correct answer.
True by lemma $\gcd(a,b) = \gcd(b,r)$.

(2) Algorithm terminates.
The second number decreases each time since $r < b$, so case 1. Stop. □

Corollary. Bézout's Theorem.
Let $a, b \in \mathbb{Z}$, not both 0. Then there exists $s, t \in \mathbb{Z}$ such that $\gcd(a,b) = as + bt$.
i.e $\gcd(a,b)$ can be written as "integer linear combination" of a, b.
To find s, t : run Euclidian algorithm, then "substitute backwards."

ex. Find $d = \gcd(30, 112)$ and s, t such that $d = 30s + 112t$.

$\gcd(30,112)$: $30 = 0(112) + 30$
$\gcd(112,30)$: $112 = 3(30) + 22$ ↑
$\gcd(30,22)$: $30 = 1(22) + 8$ |
$\gcd(22,8)$: $22 = 2(8) + 6$ |
$\gcd(8,6)$: $8 = 1(6) + 2$ ← start backwards from here.
$\gcd(6,2)$: $6 = 3(2) + 0$
$\gcd(2,0)$: $2 = \gcd(30,112)$ ✓

"substitution back" to find s, t for $2 = 30s + 112t$.

$$
\begin{aligned}
2 &= 8 - 1(6) \\
&= 8 + 6(-1) && \text{sub } 6 = 22 - 2(8) \\
&= 8 + (22 + 8(-2))(-1) \\
&= 8 + 22(-1) + 8(2) \\
&= 8(3) + 22(-1) && \text{sub } 8 = 30 - 1(22) \\
&= (30 + 22(-1))(3) + 22(-1) \\
&= 30(3) + 22(-3) + 22(-1) \\
&= 30(3) + 22(-4) && \text{sub } 22 = 112 - 3(30) \\
&= 30(3) + (112 + 30(-3))(-4) \\
&= 30(3) + 112(-4) + 30(12) \\
&= 30(15) + 112(-4) \\
&\quad\ \ s \qquad\quad\ \ t
\end{aligned}
$$

Note: In $\gcd(a,b) = sa + bt$, the s, t are not unique.

proof of Bezout's Theorem.
Use induction. Write out this "substitution back" procedure formally.
(Do not try! Not necessary for exercise.)