- math prerequisites
  - Common Divisor
    - defi.
      - y | x — means x % y = 0, x is evenly divisible by y
      - gcd(c, d) — Greatest Common Divisor of c and d
      - gcd(a, b) = 1 — a and b are relatively prime
      - a = b mod m
        - => m | (a - b)
        - => (a - b) % m = 0
        - => b = a mod m
      - Zn
        - set of integers mod n
        - Zn = { 0, 1, 2, ... , n-1 }
      - Z*n
        - set of integers that are relatively prime to n
        - e.g. — Z8 = {0, 1, 2, 3, 4, 5, 6, 7}
Z*8 = {1, 3, 5, 7}
  - Euclid's Algorithm
    - for finding gcd(a, b)
    - content
      - gcd(a, b) = gcd(b, r1) = gcd(r1, r2) = ...

        Proof:

        shows that gcd (a, b) = gcd (b, a - b)

        a = X · gcd (a, b)

        b = Y · gcd (a, b)

        a - b = X · gcd (a, b) - Y · gcd (a, b) = c

        = (X - Y) · gcd (a, b) = c

        gcd (a, b) divides b and c, gcd (a, b) ≤ gcd (b, c)

        gcd (b, c) divides b and c, gcd (b, c) ≤ gcd (a, b) ∴ gcd (a, b) = gcd (b, a - b)

        gcd (a, b) = gcd (b, a - b) = gcd (b, a - 2b) = ... = gcd (b, a - Qb)

        = gcd (b, R) = gcd (b, a mod b).

        where b = aQ + R.
      - a = q1 * b + r1 — r1 = a % b
      - b = q2 * r1 + r2
      - r1 = q3 * r2 + r3
      - ...
      - rn = q_n+2 * r_n-1 + 0
      - r_n+1 = gcd(a, b)
    - implement

      function Euclid(a, b)
      Input: Two integers a and b, where $a \geq b \geq 0$
      Output: gcd(a, b)
      1: **if** $b = 0$:
      2: **return** a
      3: **return** Euclid$(b, a \bmod b)$
    - Extended Euclid's Algorithm
      - efficient way to find inverse — given d, a and b, we can use this algo. to efficiently calculate the coefficient x, y in d = x * a + y * b, and we can verify if d = x * a + y * b is true — where d is supposed to be the gcd(a, b)
      - content
        - r1 = a - q1 * b
        - r2 = b - q2 * r1 — = (-q2) * a + (q1 * q2 + 1) * b
        - ...
        - ri = (...) a + (...) b
      - implement

        function extended-Euclid(a, b)
        Input: Two integers a and b, where $a \geq b \geq 0$
        Output: Integers (x, y, d) such that $d = \gcd(a, b)$ and $ax + by = d$
        1: **if** $b = 0$:
        2: **return** $(1, 0, a)$
        3: $(x', y', d) =$ extended-Euclid$(b, a \bmod b)$
        4: **return** $(y', x' - \lfloor a/b \rfloor y', d)$

        - gcd (b, a mod b) = d = $bx' + (a \bmod b)y'$

          $= bx' + (a - \lfloor \frac{a}{b} \rfloor b)y'$

          $= ay' + b(x' - \lfloor \frac{a}{b} \rfloor y')$

          $= ax + by$

          where $x = y'$, $y = x' - \lfloor \frac{a}{b} \rfloor y'$
        - calculation example:
          - when input a = 25, N = 11
          - 1. On the first call, $a = 25$ and $b = 11$. Since $b \neq 0$, the function will make a recursive call with b and $a \mod b$, which is 11 and 3 respectively.
            2. On the second call, $a = 11$ and $b = 3$. Again, $b \neq 0$, so the function will make another recursive call with b and $a \mod b$, which is 3 and 2 respectively.
            3. On the third call, $a = 3$ and $b = 2$. The function will make yet another recursive call with 2 and 1.
            4. On the fourth call, $a = 2$ and $b = 1$. Now, with another recursive call, the values become $a = 1$ and $b = 0$.
            5. On this fifth call with $b = 0$, the function returns $(1, 0, 1)$ as $\gcd(1, 0) = 1$.
          - From the fourth call:
            $(x', y', d) = (1, 0, 1)$
            Returning:
            $(y', x' - \lfloor \frac{a}{b} \rfloor y') = (0, 1 - \lfloor \frac{2}{1} \rfloor 0) = (0, 1)$

            From the third call:
            $(x', y', d) = (0, 1, 1)$
            Returning:
            $(y', x' - \lfloor \frac{3}{2} \rfloor y') = (1, 0 - 1) = (1, -1)$

            From the second call:
            $(x', y', d) = (1, -1, 1)$
            Returning:
            $(y', x' - \lfloor \frac{11}{3} \rfloor y') = (-1, 1 - (-3)) = (-1, 4$

            From the first call:
            $(x', y', d) = (-1, 4, 1)$
            Returning:
            $(y', x' - \lfloor \frac{25}{11} \rfloor y') = (4, -1 - 2) = (4, -3)$

            So, for $a = 25$ and $b = 11$, the values are:
            $x = 4, y = -3, \text{and} d = \gcd(25, 11) = 1$

            Thus, the result is $x = 4, y = -3$, and $d = 1$.
  - Bazout's theorem
    - exist x, y such that gcd(a, b) = α * a + β * b, where α and β could be negative — β * b = 1 mod a
    - defi. of inverse
      - β is the inverse of b mod a — β * b = 1 mod a
      - α is the inverse of a mod b — α * a = 1 mod b
      - * there is at most 1 inverse x in Zn for x * a = 1 mod n
        - no inverse case — $2x \not\equiv 1 \pmod{4}$ ∀x ......

          a = 2, n = 4
        - when inverse exists?
          - $ax \equiv 1 \pmod{N}$ ⟺ N divide into $(ax - 1)$

            ⟺ $ax - 1 = -yN$ (for $-y$) ⟺ $ax + Ny = 1$ ⟺ $\gcd(N, a) = 1$
          - that is to say, when a and N are co-prime, the inverse exists
  - Euler's Totient Function
    - φ(n)
      - the number of positive integers that are relatively prime to n and less than n
      - = |Z*n| — count of the elements in it
      - e.g. — φ(8) = 4
    - properties
      - p is prime, φ(p) = p-1
      - p, q are distinct primes, n = p * q, |Zpq| = p * q
      - p, q are distinct primes, n = p * q, φ(n) = (p - 1) * (q - 1)
  - Euler's Theorem
    - used to easily reduce large powers modulo
    - content
      - for all a ∈ Z*n, a^{φ(n)} = 1 mod n
      - or, for all a ∈ Z*n and k ≥ 0, a^{k * φ(n) + 1} = a mod n
    - proof — https://en.wikipedia.org/wiki/Euler%27s_theorem — [haven't figure it out yet]
  - generalization
  - RSA Theorem
    - If p, q are distinct primes, n = p • q,
    - for all a ∈ Zn, a ^ φ(n) = 1 mod n
    - or, for all a ∈ Zn, and k ≥ 0, a ^ { k * φ(n) + 1 } = a mod n.