xgcd (extended Euclidean Algorithm)

Problem: compute $d = \gcd(a,b)$

<u>and</u> $u, v \in \mathbb{Z}$ s.t. $d = ua + vb$.

```
int xgcd(int a, int b, int& u, int& v) {
    if (b == 0) {
        u = 1;   // gcd(a,b) = a = 1·a + 0b
        v = 0;
        return a;
    }
    int ū, v̄;
    int d = xgcd(b, a%b, ū, v̄);
    // d = bū + (a%b)v̄ and d = gcd(a,b).
#if 0
    a = qb + r, (q = a/b, r = a%b in C++)
                      ↖ integer division!!!
                        (So (a/b)*b might not be == a.)
    r = a - qb.
  So, d = bū + rv̄
        = bū + (a-qb)v̄
        = av̄ + b(ū - qv̄)
#endif
    u = v̄;
    v = ū - (a/b)v̄;
    return d;
}
```

Power set: Compute all subsets of a set.

Say $S = \{0, 1, 2\}$

$$\mathcal{P}(S) = \{\{\}, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$$

How might recursion help??

Note: $H \subseteq S \Rightarrow \underline{\mathcal{P}(H)} \subseteq \mathcal{P}(S)$