

$$\text{gcd}(a, b) = \text{gcd}(b, a \% b)$$

trace: $\text{gcd}(9, 12)$

$$\downarrow$$

$$\text{gcd}(12, 9)$$

$$\downarrow$$

$$\text{gcd}(9, 3) = 3 \quad (\text{base case: } 5|a).$$

Extended GCD:

Recall that $\text{gcd}(a, b) = ua + bv$
 some $u, v \in \mathbb{Z}$

(in fact, $\text{gcd}(a, b) = \min_{u, v \in \mathbb{Z}} \{ua + bv\}$)

Sketch: add by reference parameters for u, v

```
int gcd(int a, int b, int& u, int& v) {
```

```
    // base case
```

```
    if (a % b == 0) {
```

```
        u = 0;
```

```
        v = 1;
```

```
        return b; // =  $\overset{u}{0}a + \overset{v}{1}b$ 
```

```
    }
```

```
    // Now assume gcd works for smaller input:
```

```
    int a', v';
```

```
    int d = gcd(b, a % b, u', v');
```

```
    // Now we know  $u' \cdot b + v' \cdot (a \% b) = d$ .
```

```
    // Note:  $a \% b = a - (v_b) \cdot b$ 
```

```
    // multiply, gather a, b terms... set u, v...
```

```
    return d;
```

```
}
```

Back to Subsets:

Write a function that computes $\mathcal{P}(S)$,
the set of all subsets.

We'll work with vectors.

input: $[1, 2, 3]$

output: $[\ [], [1], [2], [3],$
 $[1, 2], [1, 3], [2, 3], [1, 2, 3]]$

if $V.size() = n$, then $|\mathcal{P}(V)| = 2^n$.

$v[0], v[1], v[2]$

1	0	0	$[1]$
0	1	0	$[2]$
0	0	1	$[3]$
1	1	0	$[1, 2]$
1	0	1	$[1, 3]$
0	1	1	$[2, 3]$
1	1	1	$[1, 2, 3]$
0	0	0	$[\]$

Now for the algorithm:

input: $[1, 2, 3]$.

if we call on $[1, 2]$, we get
 $[\ [], [1], [2], [1, 2]]$

These all work, but we're missing all
the subsets that had 3.

Answer: $\mathcal{P}(V \setminus \{3\}) \cup$ " $\mathcal{P}(V \setminus \{3\})$
with 3 added
to each element "