# Quiz 1

- Start time: 9:00am
- End time: 9:20am

# GCD

- Recall that $gcd(a, b)$ is the greatest common divisor of $a$ and $b$

- For any non-zero integer $n$, $gcd(n, 0) = n$
  $gcd(0, 0)$ is undefined

- If $a \in \mathbf{Z}$, $b \in \mathbf{Z}^+$ and $a = bq + \mathrm{r}$ then $gcd(a, b) = gcd(r, b)$
  **Proof**: Suppose $gcd(a, b) = k$
  Then $\exists n \in \mathbf{Z}$, $a = kn$ and $\exists m \in \mathbf{Z}$, $b = km$
  So $kn = (km)q + r$ and hence $r = k(n - mq)$
  Thus $k$ is a common divisor of $b$ and $r$

  Suppose $gcd(b, r) = t > k$
  Since $t \mid b$ and $t \mid r$ then $t \mid (bq + r)$
  So $t$ is a common divisor of $a$ and $b$, a contradiction (since $t > k$)

- See 1pm lecture notes for a different proof

# Euclidean algorithm for GCD

- **Corollary**: For positive integers $a$ and $b$, $gcd(a, b) = gcd(b, a \bmod b)$

- A 2,300 year old algorithm (pseudocode):

```
procedure gcd(a, b: positive integers)
  x := a
  y := b
  while y ≠ 0
    r := x mod y
    x := y
    y := r
  return x
```

| $x$ | $y$ | $r = x \bmod y$ |
|---|---|---|
| 105 | 252 | 105 |
| 252 | 105 | 42 |
| 105 | 42 | 21 |
| 42 | 21 | 0 |
| 21 | 0 | |

- *Example*: $gcd(105, 252) = 21$

# Recursive algorithm for GCD

- Recursion is a technique for reducing a big problem into one or more similar, *smaller*, problems
  - with a *base case* to handle the simplest problems

```
procedure gcd(a, b: positive integers)
  r := a mod b
  if (r = 0) return b
  else return gcd(b, r)
```

| ***a*** | ***b*** | ***r* = *a* mod *b*** |
|---|---|---|
| 105 | 252 | 105 |
| 252 | 105 | 42 |
| 105 | 42 | 21 |
| 42 | 21 | 0 |
| 21 | 0 | |

- *Example*: *gcd*(105, 252) = 21