1 Greatest Common Divisor (30 marks)

(a) For the definition of gcd (greatest common divisor/denominator) from the lecture:

```
gcd x 0                =  x
gcd 0 y                =  y
gcd (Suc x) (Suc y)    =  (if x < y then gcd (Suc x) (y - x)
                           else gcd (x - y) (Suc y))
```

prove that the gcd divides both its arguments:

```
gcd a b dvd b ∧ gcd a b dvd a
```

Use the theorem finder in Isabelle to find definition and rules for `dvd`. Occasionally useful rules are `mod_if`, `dvd_mod_iff`, and `algebra_simps`.

(b) For the standard Euclidean algorithm

```
gcd2 x 0  =  x
gcd2 x y  =  gcd2 y (x mod y)
```

prove that it is equivalent to the other algorithm and that it returns the greatest divisor:

```
gcd2 a b = gcd a b
[| z dvd a; z dvd b |] ==> z dvd (gcd a b)
```

(c) Calculate the gcd of 9 and 12 in Isabelle.

(d) Calculate the gcd of 139328 and 1262968 in Isabelle.