Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

A **div** B: quotient

A **mod** B: remainder

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

A **div** B: quotient

A **mod** B: remainder

Simple solution:

```
int q = A/B;   int r = A%B;
```

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

A **div** B: quotient

A **mod** B: remainder

Simple solution:

```
int q = A/B;   int r = A%B;
```

Restriction: we can only use addition and subtraction!

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

Specification: { } { Compute integers q and r } { }

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

Specification: $\{ A > 0 \ \wedge \ B > 0 \}$

Compute integers q and r

$\{$ $\}$

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

Specification: $\{ A > 0 \ \wedge \ B > 0 \}$

Compute integers q and r

$\{ A = q \times B + r \}$

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

Specification:

$$\{ A > 0 \ \wedge \ B > 0 \}$$

Compute integers q and r

$$\{ A = q \times B + r \ \wedge \ 0 \leq r \}$$

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

Specification:

$$\{ A > 0 \ \wedge \ B > 0 \}$$

Compute integers q and r

$$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$$

Integer Division

Write an algorithm that takes two positive numbers A and B and computes A **div** B and A **mod** B.

Specification: $\{ A > 0 \wedge B > 0 \}$

Compute integers q and r

$\{ A = q \times B + r \wedge 0 \leq r \wedge r < B \}$

Example ($A = 5 \wedge B = 2$):

$5 = 2 \times 2 + 1 \wedge 0 \leq 1 \wedge 1 < 2$

Integer Division

Write an algorithm that takes two positive numbers A and B and computes **A div B** and **A mod B**.

Specification: $\{ A>0 \wedge B>0 \}$

Compute integers q and r

$\{ A = q \times B + r \wedge 0 \leq r \wedge r < B \}$

Example $(A=5 \wedge B=2)$:

$5 = 2 \times 2 + 1 \wedge 0 \leq 1 \wedge 1 < 2$

q r

A Programming Technique

Suppose we want to develop an algorithm that establishes $P_1 \wedge P_2$. It can be established as:

A Programming Technique

Suppose we want to develop an algorithm that establishes $P_1 \wedge P_2$. It can be established as:

```
{ Invariant: P1 }
   while ( ... ) { ... }
{ P1 and not the guard }
```

A Programming Technique

Suppose we want to develop an algorithm that establishes $P_1 \wedge P_2$. It can be established as:

```
{ Invariant: P1 }
   while (!P2) { ... }
{ P1 and P2 }
```

A Programming Technique

Suppose we want to develop an algorithm that establishes $P_1 \wedge P_2$. It can be established as:

```
{ Invariant: P1 }
  while (!P2) { ... }
{ P1 ∧ P2 }
```

(provided the loop terminates)

Integer Division

We can use this technique with the problem we have:

$$\{ A > 0 \ \wedge \ B > 0 \}$$

Compute integers q and r

$$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$$

Integer Division

We can use this technique with the problem we have:

$$\{ A > 0 \ \wedge \ B > 0 \}$$

Compute integers q and r

$$\{ \underbrace{A = q \times B + r \ \wedge \ 0 \leq r}_{P_1} \ \wedge \ \underbrace{r < B}_{P_2} \}$$

Integer Division

We can use this technique with the problem we have:

$$\{ A > 0 \ \wedge \ B > 0 \}$$

Compute integers q and r

$$\{ \underbrace{A = q \times B + r \ \wedge \ 0 \leq r}_{P_1} \ \wedge \ \underbrace{r < B}_{P_2} \}$$

Let's choose P_1 as the invariant

Integer Division

We can use this technique with the problem we have:

$\{ A > 0 \wedge B > 0 \}$

Compute integers q and r

$\{ \underbrace{A = q \times B + r \wedge 0 \leq r}_{P_1} \wedge \underbrace{r < B}_{P_2} \}$

Let's choose P_1 as the invariant

Let's choose $!P_2$ as the guard of the loop

Integer Division

$$\{ A > 0 \quad \wedge \quad B > 0 \}$$

Compute integers q and r

$$\{ A = q \times B + r \quad \wedge \quad 0 \leq r \quad \wedge \quad r < B \}$$

Integer Division

$\{ A > 0 \ \wedge \ B > 0 \}$

$\{ \text{Invariant: } A = q \times B + r \ \wedge \ 0 \leq r \}$

```
while (!(r<B)) {
        Compute integers q and r
}
```

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

Integer Division

$\{ A > 0 \ \wedge \ B > 0 \}$

Initialise q and r satisfying invariant

$\{$ **Invariant:** $A = q \times B + r \ \wedge \ 0 \leq r \}$

```
while (!(r<B)) {
        Compute integers q and r
}
```

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

Integer Division

$\{ A > 0 \ \wedge \ B > 0 \}$

$q, r := 0, A \ ;$

$\{ \text{Invariant: } A = q \times B + r \ \wedge \ 0 \leq r \}$

```
while (!(r<B)) {
        Compute integers q and r
}
```

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

Integer Division

$\{ A>0 \ \wedge \ B>0 \}$

$q, r := 0, A ;$ ← the invariant is now valid initially!

$\{ \text{Invariant: } A = q \times B + r \ \wedge \ 0 \leq r \}$

```
while (!(r<B)) {
        Compute integers q and r
}
```

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

Integer Division

$\{ A>0 \ \wedge \ B>0 \}$

$q, r := 0, A ;$ ← the invariant is now valid initially!

$\{ \text{Invariant: } A = q \times B + r \ \wedge \ 0 \leq r \}$

while $(!(r<B))$ {

Compute integers q and r

}

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

Integer Division

$\{ A>0 \ \wedge \ B>0 \}$

$q, r := 0, A ;$ ← the invariant is now valid initially!

$\{ \text{Invariant: } A = q \times B + r \ \wedge \ 0 \leq r \}$

```
while (!(r<B)) {
    q, r := q + X, r + Y ;
}
```

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

Integer Division

$\{ A>0 \ \wedge \ B>0 \}$

$q, r := 0, A \ ;$ ← the invariant is now valid initially!

$\{ \text{Invariant:} \quad A = q \times B + r \ \wedge \ 0 \leq r \}$

```
while (!(r<B)) {
    q, r := q + X, r + Y ;
}
```

the goal is to calculate X and Y

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

Integer Division

Calculate X and Y such that:

$$\{ A = q \times B + r \quad \wedge \quad 0 \leq r \}$$

$$q, r := q + X, r + Y ;$$

$$\{ A = q \times B + r \quad \wedge \quad 0 \leq r \}$$

Integer Division

$\{P\}\ x := E\ \{Q\} \Leftrightarrow P \Rightarrow Q[x := E]$

Calculate X and Y such that:

$$\{ A = q \times B + r \ \wedge \ 0 \leq r \}$$

$$q, r := q + X, r + Y ;$$

$$\{ A = q \times B + r \ \wedge \ 0 \leq r \}$$

Integer Division

$\{P\}\ x := E\ \{Q\} \Leftrightarrow P \Rightarrow Q[x := E]$

Calculate X and Y such that:

$$\{\ A = q \times B + r \ \wedge\ 0 \leq r\ \}$$

$$q, r := q + X, r + Y\ ;$$

$$\{\ A = q \times B + r \ \wedge\ 0 \leq r\ \}$$

$\Leftarrow$

$$A = q \times B + r \ \wedge\ 0 \leq r \ \Longrightarrow$$

$$A = (q + X) \times B + (r + Y) \ \wedge\ 0 \leq r + Y$$

Integer Division

$\{P\}\ x := E\ \{Q\} \Leftrightarrow P \Rightarrow Q[x := E]$

Calculate X and Y such that:

$$\{\ A = q \times B + r \ \wedge\ 0 \leq r\ \}$$

$$q, r := q + X,\ r + Y\ ;$$

$$\{\ A = q \times B + r \ \wedge\ 0 \leq r\ \}$$

$\Leftarrow$

$$A = q \times B + r \ \wedge\ 0 \leq r \Longrightarrow$$

$$A = (q + X) \times B + (r + Y) \ \wedge\ 0 \leq r + Y$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \implies$$
$$A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

Integer Division

$$A = q \times B + r \quad \wedge \quad 0 \leq r \quad \Longrightarrow$$

$$A = (q+X) \times B + (r+Y) \quad \wedge \quad 0 \leq r+Y$$

$$A = (q+X) \times B + (r+Y)$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

$$A = (q+X) \times B + (r+Y)$$

$(=)$ { arithmetic }

$$A = q \times B + X \times B + r + Y$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

$$A = (q+X) \times B + (r+Y)$$

$\Leftarrow$ { arithmetic }

$$A = q \times B + X \times B + r + Y$$

$\Leftarrow$ { assumption: $A = q \times B + r$ }

$$q \times B + r = q \times B + X \times B + r + Y$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

$$A = (q+X) \times B + (r+Y)$$

$\Leftarrow$ { arithmetic }

$$A = q \times B + X \times B + r + Y$$

$\Leftarrow$ { assumption: $A = q \times B + r$ }

$$q \times B + r = q \times B + X \times B + r + Y$$

$\Leftarrow$ { arithmetic }

$$0 = X \times B + Y$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

$$A = (q+X) \times B + (r+Y)$$

$\Leftarrow$ { arithmetic }

$$A = q \times B + X \times B + r + Y$$

$\Leftarrow$ { assumption: $A = q \times B + r$ }

$$q \times B + r = q \times B + X \times B + r + Y$$

$\Leftarrow$ { arithmetic }

$$0 = X \times B + Y$$

$\Leftarrow$

$$X = 1 \;\wedge\; Y = -B$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \implies A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

Conclusion: part of the invariant satisfied when

$$X = 1 \;\wedge\; Y = -B$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

Conclusion: part of the invariant satisfied when

$$X = 1 \quad \wedge \quad Y = -B$$

$$\{\, A = q \times B + r \;\wedge\; 0 \leq r \,\}$$

$$q, r := q + X, r + Y ;$$

$$\{\, A = q \times B + r \;\wedge\; 0 \leq r \,\}$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

Conclusion: part of the invariant satisfied when

$$X = 1 \quad \wedge \quad Y = -B$$

$$\{\, A = q \times B + r \;\wedge\; 0 \leq r \,\}$$

$$q, r := q + X, r + Y;$$

$$\{\, A = q \times B + r \;\wedge\; 0 \leq r \,\}$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

Conclusion: part of the invariant satisfied when

$$X = 1 \;\wedge\; Y = -B$$

$$\{\, A = q \times B + r \;\wedge\; 0 \leq r \,\}$$

$$q, r := q + 1 \;,\; r - B \;;$$

$$\{\, A = q \times B + r \;\wedge\; 0 \leq r \,\}$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \implies A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

Conclusion: part of the invariant satisfied when

$$X = 1 \;\wedge\; Y = -B$$

$$\{\, A = q \times B + r \;\wedge\; 0 \leq r \,\}$$

$$q, r := q + 1, r - B;$$

$$\{\, A = q \times B + r \;\wedge\; 0 \leq r \,\}$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

Conclusion: part of the invariant satisfied when

$$X = 1 \;\wedge\; Y = -B$$

$$\{\, A = q \times B + r \;\wedge\; \boxed{0 \leq r} \,\}$$

$$q, r := q + 1 \;,\; r - B \;;$$

$$\{\, A = q \times B + r \;\wedge\; \boxed{0 \leq r} \,\}$$

Integer Division

$$A = q \times B + r \;\wedge\; 0 \leq r \;\Longrightarrow\; A = (q+X) \times B + (r+Y) \;\wedge\; 0 \leq r+Y$$

Conclusion: part of the invariant satisfied when

$$X = 1 \;\wedge\; Y = -B$$

$$\{\, A = q \times B + r \;\wedge\; \boxed{0 \leq r} \,\}$$

$$q, r := q + 1, r - B;$$

$$\{\, A = q \times B + r \;\wedge\; \boxed{0 \leq r} \,\}$$

This is also an invariant; we can use the guard of the loop to prove it.

Integer Division

Final algorithm:

$\{ A>0 \ \wedge \ B>0 \}$

$q, r := 0, A \ ;$

$\{ \text{Invariant: } A = q \times B + r \ \wedge \ 0 \leq r \}$

while $(!(r<B))$ {

$q, r := q+1, r-B \ ;$

}

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r<B \}$

Integer Division

Final algorithm:

$\{ A>0 \ \wedge \ B>0 \}$

$q, r := 0, A \ ;$

$\{ \text{Invariant: } A = q \times B + r \ \wedge \ 0 \leq r \}$

while $(r \geq B)$ {

$q, r := q + 1, r - B \ ;$

}

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

Integer Division

Final algorithm:

$\{ A>0 \ \wedge \ B>0 \}$

$q, r := 0, A ;$

$\{ \text{Invariant:} \quad A = q \times B + r \ \wedge \ 0 \leq r \}$

while $(r \geq B)$ {

$q, r := q + 1, r - B ;$

}

$\{ A = q \times B + r \ \wedge \ 0 \leq r \ \wedge \ r < B \}$

No need to verify the algorithm: it is **correct by construction!**