Brief Article

The Author

Definition 1 (div) $div\,a\,b := \exists\,c,\ b\ =\ a*\ c.$

Notation 1 ("a) $"a\,|\,b"\ :=\ (div\,a\,b)(at\,level\,0).$

Definition 2 (even) $even\,a\ :=\ \exists\,c,\ a\ =\ 2*\ c.$

Definition 3 (odd) $odd\,a\ :=\ \exists\,c,\ a\ =\ 2*\ c+1.$

Lemma 1 (nt0) $nt0:\ even\,12.$

Proof: Using the definition even, our conclusion becomes

$$\exists c : nat, 12 = 2 * c.$$

We shall prove $\exists c : nat, 12 = 2 * c$ by showing

$$12 = 2 * 6.$$

This follows immediately from arithmetic.This is done

$$12 = 2 * 6$$

means that $\exists c : nat, 12 = 2 * c$.

Therefore we have showed

$$\exists c : nat, 12 = 2 * c$$

and so $even 12$.

Lemma 2 (nt1) $nt1\,(a\,b\,c : nat) :\ a\,|\,b\ \wedge b\,|\,c\ \Rightarrow\ a\,|\,c.$

Proof: We will assume

$$Hyp : (a|b) \wedge (b|c)$$

and show

$$a|c.$$

Using the definition of div,

$$Hyp$$

becomes

$$Hyp : (\exists c : nat, b = a * c) \wedge (\exists c0 : nat, c = b * c0)$$

Using the definition div, our conclusion becomes

$$\exists c0 : nat, c = a * c0.$$

Since we know $Hyp : (\exists c : nat, b = a * c) \wedge (\exists c0 : nat, c = b * c0)$ we also know

$$Hyp0 : \exists c : nat, b = a * c$$

$$Hyp1 : \exists c0 : nat, c = b * c0.$$

We choose a variable

$$x$$

in

$$Hyp0$$

to obtain

$$a, b, c, x : nat$$

$$Hyp0 : b = a * x.$$

We choose a variable

$$y$$

in

$$Hyp1$$

to obtain

$$y : nat$$

$$Hyp1 : c = b * y.$$

We rewrite the goal using

$$Hyp1$$

to obtain

$$\exists c0 : nat, b * y = a * c0.$$

We rewrite the goal using

$$Hyp0$$

to obtain

$$\exists c0 : nat, a * (x * y) = a * c0.$$

We shall prove $\exists c0 : nat, a * (x * y) = a * c0$ by showing

$$a * (x * y) = a * (x * y).$$

This follows immediately from arithmetic.This is done

$$a * (x * y) = a * (x * y)$$

means that $\exists c0 : nat, a * (x * y) = a * c0$.

We have proved

$$\exists c0 : nat, a * (x * y) = a * c0$$

and so $\exists c0 : nat, b * y = a * c0$ follows.

We have proved

$$\exists c0 : nat, b * y = a * c0$$

and so $\exists c0 : nat, c = a * c0$ follows.

and so we have proved $\exists c0 : nat, c = a * c0$.

and so we have proved $\exists c0 : nat, c = a * c0$.

We are done with $\exists c0 : nat, c = a * c0$

Therefore we have showed

$$\exists c0 : nat, c = a * c0$$

and so $a|c$.

We have showed that if

$$Hyp : (a|b) \wedge (b|c)$$

then

$$a|c$$

a proof of $((a|b) \wedge (b|c)) \Rightarrow (a|c)$.

Lemma 3 (nt2) $nt2\,(a\,b\,c\,d\ :\ nat) :\ (a\,|\,c)\ \wedge (b\,|\,d)\ \Rightarrow\ ((a * b)\,|\,(c * d))$.

Proof: We will assume

$$Hyp : (a|c) \wedge (b|d)$$

and show

$$(a * b)|(c * d).$$

Using the definition of div,

$$Hyp$$

becomes

$$Hyp : (\exists c0 : nat, c = a * c0) \wedge (\exists c : nat, d = b * c)$$

Since we know $Hyp : (\exists c0 : nat, c = a * c0) \wedge (\exists c : nat, d = b * c)$ we also know

$$Hyp0 : \exists c0 : nat, c = a * c0$$

$$Hyp1 : \exists c : nat, d = b * c.$$

We choose a variable

$$x$$

in

$$Hyp0$$

to obtain

$$a, b, c, d, x : nat$$

$$Hyp0 : c = a * x.$$

We choose a variable

$$y$$

in

$$Hyp1$$

to obtain

$$y : nat$$

$$Hyp1 : d = b * y.$$

We rewrite the goal using

$$Hyp0$$

to obtain

$$(a * b)|(a * (x * d)).$$

We rewrite the goal using

$$Hyp1$$

to obtain

$$(a * b)|(a * (x * (b * y))).$$

Using the definition div, our conclusion becomes

$$\exists c0 : nat, a * (x * (b * y)) = a * (b * c0).$$

We shall prove $\exists c0 : nat, a * (x * (b * y)) = a * (b * c0)$ by showing

$$a * (x * (b * y)) = a * (b * (x * y)).$$

This follows immediately from arithmetic.This is done

$$a * (x * (b * y)) = a * (b * (x * y))$$

means that $\exists c0 : nat, a * (x * (b * y)) = a * (b * c0)$.

Therefore we have showed

$$\exists c0 : nat, a * (x * (b * y)) = a * (b * c0)$$

and so $(a * b)|(a * (x * (b * y)))$.

We have proved

$$(a * b)|(a * (x * (b * y)))$$

and so $(a * b)|(a * (x * d))$ follows.

We have proved

$$(a * b)|(a * (x * d))$$

and so $(a * b)|(c * d)$ follows.

and so we have proved $(a * b)|(c * d)$.

and so we have proved $(a * b)|(c * d)$.

We are done with $(a * b)|(c * d)$

We have showed that if

$$Hyp : (a|c) \wedge (b|d)$$

then

$$(a * b)|(c * d)$$

a proof of $((a|c) \wedge (b|d)) \Rightarrow ((a * b)|(c * d))$.

Lemma 4 (nt3) $nt3\,(a\,b\,c : nat) :\ a\,|\,b\ \wedge a\,|\,c\ \Rightarrow\ a\,|(\,b + c)$.

Proof: We will assume

$$Hyp : (a|b) \wedge (a|c)$$

and show

$$a|(b + c).$$

Using the definition of div,

$$Hyp$$

becomes

$$Hyp : (\exists c : nat, b = a * c) \wedge (\exists c0 : nat, c = a * c0)$$

Since we know $Hyp : (\exists c : nat, b = a * c) \wedge (\exists c0 : nat, c = a * c0)$ we also know

$$Hyp0 : \exists c : nat, b = a * c$$

$$Hyp1 : \exists c0 : nat, c = a * c0.$$

We choose a variable

$$x$$

in

$$Hyp0$$

to obtain

$$a, b, c, x : nat$$

$$Hyp0 : b = a * x.$$

We choose a variable

$$y$$

in

$$Hyp1$$

to obtain

$$y : nat$$

$$Hyp1 : c = a * y.$$

We rewrite the goal using

$$Hyp0$$

to obtain

$$a|((a * x) + c).$$

We rewrite the goal using

$$Hyp1$$

to obtain

$$a|((a * x) + (a * y)).$$

Using the definition div, our conclusion becomes

$$\exists c0 : nat, (a * x) + (a * y) = a * c0.$$

We shall prove $\exists c0 : nat, (a * x) + (a * y) = a * c0$ by showing

$$(a * x) + (a * y) = a * (x + y).$$

This follows immediately from arithmetic.This is done

$$(a * x) + (a * y) = a * (x + y)$$

means that $\exists c0 : nat, (a * x) + (a * y) = a * c0$.

Therefore we have showed

$$\exists c0 : nat, (a * x) + (a * y) = a * c0$$

and so $a|((a * x) + (a * y))$.

We have proved

$$a|((a * x) + (a * y))$$

and so $a|((a * x) + c)$ follows.

We have proved

$$a|((a * x) + c)$$

and so $a|(b + c)$ follows.

and so we have proved $a|(b + c)$.

and so we have proved $a|(b + c)$.

We are done with $a|(b + c)$

We have showed that if

$$Hyp : (a|b) \wedge (a|c)$$

then

$$a|(b + c)$$

a proof of $((a|b) \wedge (a|c)) \Rightarrow (a|(b + c))$.

Lemma 5 (nt4) $nt4\,(n\,m : nat) : \ (odd\,n) \wedge (odd\,m) \ \Rightarrow \ (even\,(m + n))$.

Proof: We will assume

$$Hyp : (oddn) \wedge (oddm)$$

and show

$$even(m + n).$$

Using the definition even, our conclusion becomes

$$\exists c : nat, m + n = 2 * c.$$

Using the definition of odd,

$$Hyp$$

becomes

$$Hyp : (\exists c : nat, n = (2 * c) + 1) \wedge (\exists c : nat, m = (2 * c) + 1)$$

Since we know $Hyp : (\exists c : nat, n = (2 * c) + 1) \wedge (\exists c : nat, m = (2 * c) + 1)$ we also know

$$Hyp0 : \exists c : nat, n = (2 * c) + 1$$

$$Hyp1 : \exists c : nat, m = (2 * c) + 1.$$

We choose a variable

$$x$$

in

$$Hyp0$$

to obtain

$$n, m, x : nat$$

$$Hyp0 : n = (2 * x) + 1.$$

We choose a variable

$$y$$

in

$$Hyp1$$

to obtain

$$y : nat$$

$$Hyp1 : m = (2 * y) + 1.$$

We rewrite the goal using

$$Hyp0$$

to obtain

$$\exists c : nat, m + ((2 * x) + 1) = 2 * c.$$

We rewrite the goal using

$$Hyp1$$

to obtain

$$\exists c : nat, (2 * y) + (1 + ((2 * x) + 1)) = 2 * c.$$

We shall prove $\exists c : nat, (2 * y) + (1 + ((2 * x) + 1)) = 2 * c$ by showing

$$(2 * y) + (1 + ((2 * x) + 1)) = 2 * (x + (y + 1)).$$

This follows immediately from arithmetic.This is done

$$(2 * y) + (1 + ((2 * x) + 1)) = 2 * (x + (y + 1))$$

means that $\exists c : nat, (2 * y) + (1 + ((2 * x) + 1)) = 2 * c$.

We have proved

$$\exists c : nat, (2 * y) + (1 + ((2 * x) + 1)) = 2 * c$$

and so $\exists c : nat, m + ((2 * x) + 1) = 2 * c$ follows.

We have proved

$$\exists c : nat, m + ((2 * x) + 1) = 2 * c$$

and so $\exists c : nat, m + n = 2 * c$ follows.

and so we have proved $\exists c : nat, m + n = 2 * c$.

and so we have proved $\exists c : nat, m + n = 2 * c$.

We are done with $\exists c : nat, m + n = 2 * c$

Therefore we have showed

$$\exists c : nat, m + n = 2 * c$$

and so $even(m + n)$.

We have showed that if

$$Hyp : (oddn) \wedge (oddm)$$

then

$$even(m + n)$$

a proof of $oddn \wedge oddm \Rightarrow even(m + n)$.

Lemma 6 (nt5) $nt5\,(n : nat) :\ odd\,(n\ +\ (n + 1))$.

Proof: Using the definition odd, our conclusion becomes

$$\exists c : nat, n + (n + 1) = (2 * c) + 1.$$

We shall prove $\exists c : nat, n + (n + 1) = (2 * c) + 1$ by showing

$$n + (n + 1) = (2 * n) + 1.$$

This follows immediately from arithmetic.This is done

$$n + (n + 1) = (2 * n) + 1$$

means that $\exists c : nat, n + (n + 1) = (2 * c) + 1$.

Therefore we have showed

$$\exists c : nat, n + (n + 1) = (2 * c) + 1$$

and so $odd(n + (n + 1))$.

Lemma 7 (nt6) $nt6\,(n : nat) :\ even\,n \lor odd\,n$.

Proof: Using the definition even, our conclusion becomes

$$(\exists c : nat, n = 2 * c) \lor (oddn).$$

Using the definition odd, our conclusion becomes

$$(\exists c : nat, n = 2 * c) \lor (\exists c : nat, n = (2 * c) + 1).$$

Prove by induction. We first prove the base case

$$(\exists c : nat, 0 = 2 * c) \lor (\exists c : nat, 0 = (2 * c) + 1).$$

We will prove the left hand side of $(\exists c : nat, 0 = 2 * c) \lor (\exists c : nat, 0 = (2 * c) + 1)$. That is we need to prove

$$\exists c : nat, 0 = 2 * c.$$

We shall prove $\exists c : nat, 0 = 2 * c$ by showing

$$0 = 2 * 0.$$

This follows immediately from arithmetic.This is done

$$0 = 2 * 0$$

means that $\exists c : nat, 0 = 2 * c$.

We have proved

$$\exists c : nat, 0 = 2 * c$$

and so $(\exists c : nat, 0 = 2 * c) \lor (\exists c : nat, 0 = (2 * c) + 1)$ follows.

Assume

$$IHn : (\exists c : nat, n = 2 * c) \lor (\exists c : nat, n = (2 * c) + 1)$$

and prove

$$(\exists c : nat, (n+1) = 2*c) \vee (\exists c : nat, (n+1) = (2*c)+1).$$

Since we know $IHn : (\exists c : nat, n = 2*c) \vee (\exists c : nat, n = (2*c)+1)$ we can consider two cases:

Case 1

$$Hyp : \exists c : nat, n = 2*c$$

We will prove the right hand side of $(\exists c : nat, (n+1) = 2*c) \vee (\exists c : nat, (n+1) = (2*c)+1)$. That is we need to prove

$$\exists c : nat, (n+1) = (2*c)+1.$$

We choose a variable

$$c$$

in

$$Hyp$$

to obtain

$$n, c : nat$$

$$Hyp : n = 2*c.$$

We rewrite the goal using

$$Hyp$$

to obtain

$$\exists c0 : nat, (2*c+1) = (2*c0)+1.$$

We shall prove $\exists c0 : nat, (2*c+1) = (2*c0)+1$ by showing

$$(2*c+1) = (2*c)+1.$$

This follows immediately from arithmetic.This is done

$$(2*c+1) = (2*c)+1$$

means that $\exists c0 : nat, (2*c+1) = (2*c0)+1$.

We have proved

$$\exists c0 : nat, (2*c+1) = (2*c0)+1$$

and so $\exists c0 : nat, (n+1) = (2*c0)+1$ follows.

and so we have proved $\exists c : nat, (n+1) = (2*c)+1$.

We are done with

$$\exists c : nat, (n+1) = (2*c)+1$$

and so $(\exists c : nat, (n+1) = 2*c) \vee (\exists c : nat, (n+1) = (2*c)+1)$ follows.

Case 2

$$Hyp0 : \exists c : nat, n = (2*c)+1$$

We will prove the left hand side of $(\exists c : nat, (n+1) = 2*c) \vee (\exists c : nat, (n+1) = (2*c)+1)$. That is we need to prove

$$\exists c : nat, (n+1) = 2*c.$$

We choose a variable

$$c$$

in

$$Hyp0$$

to obtain

$$n, c : nat$$

$$Hyp0 : n = (2*c)+1.$$

We rewrite the goal using

$$Hyp0$$

to obtain

$$\exists c0 : nat, ((2*c)+1+1) = 2*c0.$$

We shall prove $\exists c0 : nat, ((2*c)+1+1) = 2*c0$ by showing

$$((2*c)+1+1) = 2*(c+1).$$

This follows immediately from arithmetic.This is done

$$((2*c)+1+1) = 2*(c+1)$$

means that $\exists c0 : nat, ((2*c)+1+1) = 2*c0$.

We have proved

$$\exists c0 : nat, ((2*c)+1+1) = 2*c0$$

and so $\exists c0 : nat, (n+1) = 2*c0$ follows.

and so we have proved $\exists c : nat, (n+1) = 2*c$.

We have proved
$$\exists c : nat, (n + 1) = 2 * c$$
and so $(\exists c : nat, (n + 1) = 2 * c) \vee (\exists c : nat, (n + 1) = (2 * c) + 1)$ follows.

Since we proved both cases, we are done with $(\exists c : nat, (n+1) = 2*c) \vee (\exists c : nat, (n + 1) = (2 * c) + 1)$

this finishes the induction.

Therefore we have showed

$$(\exists c : nat, n = 2 * c) \vee (\exists c : nat, n = (2 * c) + 1)$$

and so $(\exists c : nat, n = 2 * c) \vee (oddn)$.

Therefore we have showed

$$(\exists c : nat, n = 2 * c) \vee (oddn)$$

and so $(evenn) \vee (oddn)$.

Lemma 8 (nt7) $nt7\,(n : nat) :\ even\,(n * (n + 1))$.

Proof: Using the definition even, our conclusion becomes

$$\exists c : nat, n * (n + 1) = 2 * c.$$

n and $(nt6)$ imply
$$H : (evenn) \vee (oddn).$$
Since we know $H : (evenn) \vee (oddn)$ we can consider two cases:

Case 1
$$Hyp : evenn$$

Using the definition of even,

$$Hyp$$

becomes
$$Hyp : \exists c : nat, n = 2 * c$$
We choose a variable
$$c$$
in
$$Hyp$$
to obtain
$$n, c : nat$$

$$Hyp : n = 2 * c.$$

We rewrite the goal using

$$Hyp$$

to obtain

$$\exists c0 : nat, 2 * (c * ((2 * c) + 1)) = 2 * c0.$$

We shall prove $\exists c0 : nat, 2 * (c * ((2 * c) + 1)) = 2 * c0$ by showing

$$2 * (c * ((2 * c) + 1)) = 2 * (c * ((2 * c) + 1)).$$

This is trivial!!

$$2 * (c * ((2 * c) + 1)) = 2 * (c * ((2 * c) + 1))$$

means that $\exists c0 : nat, 2 * (c * ((2 * c) + 1)) = 2 * c0$.

We have proved

$$\exists c0 : nat, 2 * (c * ((2 * c) + 1)) = 2 * c0$$

and so $\exists c0 : nat, n * (n + 1) = 2 * c0$ follows.

and so we have proved $\exists c : nat, n * (n + 1) = 2 * c$.

Case 2

$$Hyp0 : oddn$$

Using the definition of odd,

$$Hyp0$$

becomes

$$Hyp0 : \exists c : nat, n = (2 * c) + 1$$

We choose a variable

$$c$$

in

$$Hyp0$$

to obtain

$$n, c : nat$$

$$Hyp0 : n = (2 * c) + 1.$$

We rewrite the goal using

$$Hyp0$$

to obtain

$$\exists c0 : nat, ((2 * c) + 1) * ((2 * c) + (1 + 1)) = 2 * c0.$$

We shall prove $\exists c0 : nat, ((2 * c) + 1) * ((2 * c) + (1 + 1)) = 2 * c0$ by showing

$$((2 * c) + 1) * ((2 * c) + (1 + 1)) = 2 * (((2 * c) + 1) * (c + 1)).$$

This follows immediately from arithmetic.This is done

$$((2 * c) + 1) * ((2 * c) + (1 + 1)) = 2 * (((2 * c) + 1) * (c + 1))$$

means that $\exists c0 : nat, ((2 * c) + 1) * ((2 * c) + (1 + 1)) = 2 * c0$.

We have proved

$$\exists c0 : nat, ((2 * c) + 1) * ((2 * c) + (1 + 1)) = 2 * c0$$

and so $\exists c0 : nat, n * (n + 1) = 2 * c0$ follows.

and so we have proved $\exists c : nat, n * (n + 1) = 2 * c$.

Since we proved both cases, we are done with $\exists c : nat, n * (n + 1) = 2 * c$

Therefore we have showed

$$\exists c : nat, n * (n + 1) = 2 * c$$

and so $even(n * (n + 1))$.This is done