

thm_2Eint__arith_2EINT__LINEAR__GCD
(TMUY4wbHd6vvy3DrBUWk1zp3Ky8hcZKsZ1V)

October 26, 2020

Definition 1 We define `c_2Emin_2E_3D` to be $\lambda A. \lambda x \in A. \lambda y \in A. \text{inj_o } (x = y)$ of type $\iota \Rightarrow \iota$.

Definition 2 We define `c_2Ebool_2ET` to be $(\text{ap } (\text{ap } (\text{c_2Emin_2E_3D } (2^2)) (\lambda V 0x \in 2.V 0x)) (\lambda V 1x \in 2.V 1x))$

Let `ty_2Enum_2Enum` : ι be given. Assume the following.

$$\text{nonempty } \text{ty_2Enum_2Enum} \quad (1)$$

Let `c_2Egcd_2Egcd` : ι be given. Assume the following.

$$\text{c_2Egcd_2Egcd} \in ((\text{ty_2Enum_2Enum}^{\text{ty_2Enum_2Enum}})^{\text{ty_2Enum_2Enum}})^{\text{ty_2Enum_2Enum}} \quad (2)$$

Definition 3 We define `c_2Emin_2E_40` to be $\lambda A. \lambda P \in 2^A. \text{if } (\exists x \in A. P \ x) \text{ then } (\text{the } (\lambda x. x \in A \wedge P \ x))$ of type $\iota \Rightarrow \iota$.

Definition 4 We define `c_2Ebool_2E_3F` to be $\lambda A. 27a : \iota. (\lambda V 0P \in (2^{A-27a}). (\text{ap } V 0P \ (\text{ap } (\text{c_2Emin_2E_40 } A)))$

Let `c_2Enum_2EZERO__REP` : ι be given. Assume the following.

$$\text{c_2Enum_2EZERO_REP} \in \text{omega} \quad (3)$$

Let `c_2Enum_2EABS__num` : ι be given. Assume the following.

$$\text{c_2Enum_2EABS_num} \in (\text{ty_2Enum_2Enum}^{\text{omega}}) \quad (4)$$

Definition 5 We define `c_2Enum_2E0` to be $(\text{ap } \text{c_2Enum_2EABS_num } \text{c_2Enum_2EZERO_REP})$.

Definition 6 We define `c_2Earithmetic_2EZERO` to be `c_2Enum_2E0`.

Let `c_2Enum_2EREP__num` : ι be given. Assume the following.

$$\text{c_2Enum_2EREP_num} \in (\text{omega}^{\text{ty_2Enum_2Enum}}) \quad (5)$$

Let `c_2Enum_2ESUC__REP` : ι be given. Assume the following.

$$\text{c_2Enum_2ESUC_REP} \in (\text{omega}^{\text{omega}}) \quad (6)$$

Definition 7 We define $c_2Ebool_2E_21$ to be $\lambda A_27a : \iota. (\lambda V0P \in (2^{A_27a}). (ap (ap (c_2Emin_2E_3D (2^{A_27a})))$

Definition 8 We define c_2Enum_2ESUC to be $\lambda V0m \in ty_2Enum_2Enum. (ap c_2Enum_2EABS_num ($

Let $c_2Earithmetic_2E_2B : \iota$ be given. Assume the following.

$$c_2Earithmetic_2E_2B \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (7)$$

Definition 9 We define $c_2Earithmetic_2EBIT1$ to be $\lambda V0n \in ty_2Enum_2Enum. (ap (ap c_2Earithmetic_2E_2B$

Definition 10 We define $c_2Earithmetic_2ENUMERAL$ to be $\lambda V0x \in ty_2Enum_2Enum. V0x$.

Let $ty_2Epair_2Eprod : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0. nonempty A0 \Rightarrow \forall A1. nonempty A1 \Rightarrow nonempty (ty_2Epair_2Eprod A0 A1) \quad (8)$$

Let $ty_2Einteger_2Eint : \iota$ be given. Assume the following.

$$nonempty ty_2Einteger_2Eint \quad (9)$$

Let $c_2Einteger_2Eint_REP_CLASS : \iota$ be given. Assume the following.

$$c_2Einteger_2Eint_REP_CLASS \in ((2^{(ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum)})^{ty_2Einteger_2Eint}) \quad (10)$$

Definition 11 We define $c_2Einteger_2Eint_REP$ to be $\lambda V0a \in ty_2Einteger_2Eint. (ap (c_2Emin_2E_40 ($

Let $c_2Einteger_2Eint_add : \iota$ be given. Assume the following.

$$c_2Einteger_2Eint_add \in (((ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum)^{ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum})^{ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum}) \quad (11)$$

Let $c_2Einteger_2Eint_eq : \iota$ be given. Assume the following.

$$c_2Einteger_2Eint_eq \in ((2^{(ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum)})^{ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum}) \quad (12)$$

Let $c_2Einteger_2Eint_ABS_CLASS : \iota$ be given. Assume the following.

$$c_2Einteger_2Eint_ABS_CLASS \in (ty_2Einteger_2Eint)^{(2^{(ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum)})} \quad (13)$$

Definition 12 We define $c_2Einteger_2Eint_ABS$ to be $\lambda V0r \in (ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum$

Definition 13 We define $c_2Einteger_2Eint_add$ to be $\lambda V0T1 \in ty_2Einteger_2Eint. \lambda V1T2 \in ty_2Einteger_2Eint$

Let $c_2Einteger_2Eint_neg : \iota$ be given. Assume the following.

$$c_2Einteger_2Eint_neg \in ((ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum)^{ty_2Epair_2Eprod ty_2Enum_2Enum ty_2Enum_2Enum}) \quad (14)$$

Definition 14 We define $c_2Einteger_2Eint_neg$ to be $\lambda V0T1 \in ty_2Einteger_2Eint.(ap\ c_2Einteger_2Eint$.

Let $c_2Earithmetic_2E_2A : \iota$ be given. Assume the following.

$$c_2Earithmetic_2E_2A \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (15)$$

Let $c_2Einteger_2Eint_of_num : \iota$ be given. Assume the following.

$$c_2Einteger_2Eint_of_num \in (ty_2Einteger_2Eint^{ty_2Enum_2Enum}) \quad (16)$$

Let $c_2Einteger_2Etint_mul : \iota$ be given. Assume the following.

$$c_2Einteger_2Etint_mul \in (((ty_2Epair_2Eprod\ ty_2Enum_2Enum\ ty_2Enum_2Enum)^{(ty_2Epair_2Eprod\ ty_2Enum_2Enum\ ty_2Enum_2Enum)})^{(ty_2Epair_2Eprod\ ty_2Enum_2Enum\ ty_2Enum_2Enum)}) \quad (17)$$

Definition 15 We define $c_2Einteger_2Eint_mul$ to be $\lambda V0T1 \in ty_2Einteger_2Eint.\lambda V1T2 \in ty_2Einteger$

Definition 16 We define c_2Ebool_2EF to be $(ap\ (c_2Ebool_2E_21\ 2)\ (\lambda V0t \in 2.V0t))$.

Definition 17 We define $c_2Emin_2E_3D_3D_3E$ to be $\lambda P \in 2.\lambda Q \in 2.inj_o\ (p\ P \Rightarrow p\ Q)$ of type ι .

Definition 18 We define $c_2Ebool_2E_5C_2F$ to be $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap\ (c_2Ebool_2E_21\ 2)\ (\lambda V2t \in 2.V2t$

Definition 19 We define $c_2Ebool_2E_2F_5C$ to be $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap\ (c_2Ebool_2E_21\ 2)\ (\lambda V2t \in 2.V2t$

Definition 20 We define $c_2Ebool_2E_7E$ to be $(\lambda V0t \in 2.(ap\ (ap\ c_2Emin_2E_3D_3D_3E\ V0t)\ c_2Ebool_2E_7E$

Assume the following.

$$True \quad (18)$$

Assume the following.

$$(\forall V0t1 \in 2.(\forall V1t2 \in 2.(((p\ V0t1) \Rightarrow (p\ V1t2)) \Rightarrow (((p\ V1t2) \Rightarrow (p\ V0t1)) \Rightarrow ((p\ V0t1) \Leftrightarrow (p\ V1t2)))))) \quad (19)$$

Assume the following.

$$(\forall V0t \in 2.((p\ V0t) \vee (\neg(p\ V0t)))) \quad (20)$$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0t \in 2.((\exists V1x \in A_27a.(p\ V0t)) \Leftrightarrow (p\ V0t))) \quad (21)$$

Assume the following.

$$(\forall V0t \in 2.(((p\ V0t) \Rightarrow False) \Rightarrow (\neg(p\ V0t)))) \quad (22)$$

Assume the following.

$$(\forall V0t \in 2.((\neg(p V0t)) \Rightarrow ((p V0t) \Rightarrow False))) \quad (23)$$

Assume the following.

$$\begin{aligned} & (\forall V0t \in 2.(((True \Rightarrow (p V0t)) \Leftrightarrow (p V0t)) \wedge (((p V0t) \Rightarrow True) \Leftrightarrow \\ & True) \wedge (((False \Rightarrow (p V0t)) \Leftrightarrow True) \wedge (((p V0t) \Rightarrow (p V0t)) \Leftrightarrow True) \wedge ((\\ & (p V0t) \Rightarrow False) \Leftrightarrow (\neg(p V0t)))))) \end{aligned} \quad (24)$$

Assume the following.

$$\begin{aligned} & ((\forall V0t \in 2.((\neg(\neg(p V0t))) \Leftrightarrow (p V0t))) \wedge (((\neg True) \Leftrightarrow False) \wedge \\ & ((\neg False) \Leftrightarrow True))) \end{aligned} \quad (25)$$

Assume the following.

$$\forall A_27a.nonempty \ A_27a \Rightarrow (\forall V0x \in A_27a.((V0x = V0x) \Leftrightarrow True)) \quad (26)$$

Assume the following.

$$\forall A_27a.nonempty \ A_27a \Rightarrow (\forall V0x \in A_27a.(\forall V1y \in A_27a.((V0x = V1y) \Leftrightarrow (V1y = V0x)))) \quad (27)$$

Assume the following.

$$\begin{aligned} & (\forall V0t \in 2.(((True \Leftrightarrow (p V0t)) \Leftrightarrow (p V0t)) \wedge (((p V0t) \Leftrightarrow True) \Leftrightarrow \\ & (p V0t)) \wedge (((False \Leftrightarrow (p V0t)) \Leftrightarrow (\neg(p V0t))) \wedge (((p V0t) \Leftrightarrow False) \Leftrightarrow (\neg(\\ & p V0t)))))) \end{aligned} \quad (28)$$

Assume the following.

$$\forall A_27a.nonempty \ A_27a \Rightarrow (\forall V0P \in (2^{A_27a}).((\neg(\exists V1x \in A_27a.(p (ap V0P V1x)))) \Leftrightarrow (\forall V2x \in A_27a.(\neg(p (ap V0P V2x)))))) \quad (29)$$

Assume the following.

$$\begin{aligned} & \forall A_27a.nonempty \ A_27a \Rightarrow (\forall V0P \in 2.(\forall V1Q \in (\\ & 2^{A_27a}).(((p V0P) \vee (\exists V2x \in A_27a.(p (ap V1Q V2x)))) \Leftrightarrow (\exists V3x \in \\ & A_27a.((p V0P) \vee (p (ap V1Q V3x)))))) \end{aligned} \quad (30)$$

Assume the following.

$$\begin{aligned} & \forall A_27a.nonempty \ A_27a \Rightarrow \forall A_27b.nonempty \ A_27b \Rightarrow (\\ & \forall V0P \in ((2^{A_27b})^{A_27a}).((\forall V1x \in A_27a.(\exists V2y \in \\ & A_27b.(p (ap (ap V0P V1x) V2y)))) \Leftrightarrow (\exists V3f \in (A_27b^{A_27a}).(\\ & \forall V4x \in A_27a.(p (ap (ap V0P V4x) (ap V3f V4x)))))) \end{aligned} \quad (31)$$

Assume the following.

$$\begin{aligned} & (\forall V0a \in ty_2Enum_2Enum.(\forall V1b \in ty_2Enum_2Enum.(\\ & (ap (ap c_2Egcd_2Egcd V0a) V1b) = (ap (ap c_2Egcd_2Egcd V1b) V0a)))) \end{aligned} \quad (32)$$

Assume the following.

$$(\forall V0a \in ty_2Enum_2Enum.((ap (ap c_2Egcd_2Egcd V0a) c_2Enum_2E0) = V0a)) \quad (33)$$

Assume the following.

$$(\forall V0a \in ty_2Enum_2Enum.((ap (ap c_2Egcd_2Egcd c_2Enum_2E0) V0a) = V0a)) \quad (34)$$

Assume the following.

$$(\forall V0n \in ty_2Enum_2Enum.(\forall V1m \in ty_2Enum_2Enum.(\neg(V0n = c_2Enum_2E0)) \Rightarrow (\exists V2p \in ty_2Enum_2Enum.(\exists V3q \in ty_2Enum_2Enum.((ap (ap c_2Earithmetic_2E_2A V2p) V0n) = (ap (ap c_2Earithmetic_2E_2B (ap (ap c_2Earithmetic_2E_2A V3q) V1m)) (ap (ap c_2Egcd_2Egcd V1m) V0n)))))))) \quad (35)$$

Assume the following.

$$(\forall V0x \in ty_2Einteger_2Eint.(\forall V1y \in ty_2Einteger_2Eint.(\forall V2z \in ty_2Einteger_2Eint.((V0x = (ap (ap c_2Einteger_2Eint_add V1y) V2z)) \Leftrightarrow ((ap (ap c_2Einteger_2Eint_add V0x) (ap c_2Einteger_2Eint_neg V1y)) = V2z)))))) \quad (36)$$

Assume the following.

$$(\forall V0x \in ty_2Einteger_2Eint.((ap (ap c_2Einteger_2Eint_add (ap c_2Einteger_2Eint_of_num c_2Enum_2E0)) V0x) = V0x)) \quad (37)$$

Assume the following.

$$(\forall V0x \in ty_2Einteger_2Eint.((ap (ap c_2Einteger_2Eint_add V0x) (ap c_2Einteger_2Eint_of_num c_2Enum_2E0)) = V0x)) \quad (38)$$

Assume the following.

$$(\forall V0x \in ty_2Einteger_2Eint.((ap (ap c_2Einteger_2Eint_mul (ap c_2Einteger_2Eint_of_num (ap c_2Earithmetic_2ENUMERAL (ap c_2Earithmetic_2EBIT1 c_2Earithmetic_2EZERO)))) V0x) = V0x)) \quad (39)$$

Assume the following.

$$(\forall V0x \in ty_2Einteger_2Eint.((ap (ap c_2Einteger_2Eint_mul V0x) (ap c_2Einteger_2Eint_of_num c_2Enum_2E0)) = (ap c_2Einteger_2Eint_of_num c_2Enum_2E0))) \quad (40)$$

Assume the following.

$$\begin{aligned}
& (\forall V0m \in ty_2Enum_2Enum. (\forall V1n \in ty_2Enum_2Enum. (\\
& \quad (ap (ap c_2Integer_2Eint_add (ap c_2Integer_2Eint_of_num \\
V0m)) (ap c_2Integer_2Eint_of_num V1n)) = (ap c_2Integer_2Eint_of_num \\
& \quad (ap (ap c_2Arithmetic_2E_2B V0m) V1n))))))
\end{aligned} \tag{41}$$

Assume the following.

$$\begin{aligned}
& ((\forall V0m \in ty_2Enum_2Enum. (\forall V1n \in ty_2Enum_2Enum. \\
& \quad ((ap (ap c_2Integer_2Eint_mul (ap c_2Integer_2Eint_of_num \\
V0m)) (ap c_2Integer_2Eint_of_num V1n)) = (ap c_2Integer_2Eint_of_num \\
& \quad (ap (ap c_2Arithmetic_2E_2A V0m) V1n)))))) \wedge ((\forall V2x \in ty_2Integer_2Eint. \\
& \quad (\forall V3y \in ty_2Integer_2Eint. ((ap (ap c_2Integer_2Eint_mul \\
& \quad (ap c_2Integer_2Eint_neg V2x)) V3y) = (ap c_2Integer_2Eint_neg \\
& \quad (ap (ap c_2Integer_2Eint_mul V2x) V3y)))))) \wedge ((\forall V4x \in ty_2Integer_2Eint. \\
& \quad (\forall V5y \in ty_2Integer_2Eint. ((ap (ap c_2Integer_2Eint_mul \\
V4x) (ap c_2Integer_2Eint_neg V5y)) = (ap c_2Integer_2Eint_neg \\
& \quad (ap (ap c_2Integer_2Eint_mul V4x) V5y)))))) \wedge ((\forall V6x \in ty_2Integer_2Eint. \\
& \quad ((ap c_2Integer_2Eint_neg (ap c_2Integer_2Eint_neg V6x)) = \\
& \quad V6x))))))
\end{aligned} \tag{42}$$

Assume the following.

$$(\forall V0t \in 2. ((\neg(\neg(p V0t))) \Leftrightarrow (p V0t))) \tag{43}$$

Assume the following.

$$(\forall V0A \in 2. ((p V0A) \Rightarrow ((\neg(p V0A)) \Rightarrow False))) \tag{44}$$

Assume the following.

$$\begin{aligned}
& ((\forall V0A \in 2. (\forall V1B \in 2. (((\neg(\neg(p V0A) \vee (p V1B))) \Rightarrow False) \Leftrightarrow \\
& \quad (((p V0A) \Rightarrow False) \Rightarrow ((\neg(p V1B)) \Rightarrow False))))))
\end{aligned} \tag{45}$$

Assume the following.

$$\begin{aligned}
& ((\forall V0A \in 2. (\forall V1B \in 2. (((\neg(\neg(\neg(p V0A)) \vee (p V1B))) \Rightarrow False) \Leftrightarrow \\
& \quad ((p V0A) \Rightarrow ((\neg(p V1B)) \Rightarrow False))))))
\end{aligned} \tag{46}$$

Assume the following.

$$(\forall V0A \in 2. (((\neg(p V0A)) \Rightarrow False) \Rightarrow (((p V0A) \Rightarrow False) \Rightarrow False))) \tag{47}$$

Assume the following.

$$\begin{aligned}
& ((\forall V0p \in 2. (\forall V1q \in 2. (\forall V2r \in 2. (((p V0p) \Leftrightarrow (\\
& \quad (p V1q) \Leftrightarrow (p V2r))) \Leftrightarrow (((p V0p) \vee ((p V1q) \vee (p V2r))) \wedge (((p V0p) \vee ((\neg \\
& \quad p V2r)) \vee (\neg(p V1q)))) \wedge (((p V1q) \vee ((\neg(p V2r)) \vee (\neg(p V0p)))) \wedge ((p V2r) \vee \\
& \quad ((\neg(p V1q)) \vee (\neg(p V0p))))))))))
\end{aligned} \tag{48}$$

Assume the following.

$$\begin{aligned}
& (\forall V0p \in 2. (\forall V1q \in 2. (\forall V2r \in 2. (((p \ V0p) \Leftrightarrow (\\
& (p \ V1q) \vee (p \ V2r))) \Leftrightarrow (((p \ V0p) \vee \neg(p \ V1q)) \wedge ((p \ V0p) \vee \neg(p \ V2r))) \wedge \\
& ((p \ V1q) \vee ((p \ V2r) \vee \neg(p \ V0p))))))))))
\end{aligned} \tag{49}$$

Assume the following.

$$\begin{aligned}
& (\forall V0p \in 2. (\forall V1q \in 2. (\forall V2r \in 2. (((p \ V0p) \Leftrightarrow (\\
& (p \ V1q) \Rightarrow (p \ V2r))) \Leftrightarrow (((p \ V0p) \vee (p \ V1q)) \wedge ((p \ V0p) \vee \neg(p \ V2r))) \wedge ((\\
& \neg(p \ V1q) \vee ((p \ V2r) \vee \neg(p \ V0p))))))))))
\end{aligned} \tag{50}$$

Assume the following.

$$\begin{aligned}
& (\forall V0p \in 2. (\forall V1q \in 2. (((p \ V0p) \Leftrightarrow \neg(p \ V1q))) \Leftrightarrow (((p \ V0p) \vee \\
& (p \ V1q)) \wedge (\neg(p \ V1q) \vee \neg(p \ V0p))))))
\end{aligned} \tag{51}$$

Theorem 1

$$\begin{aligned}
& (\forall V0n \in ty_2Enum_2Enum. (\forall V1m \in ty_2Enum_2Enum. (\\
& \exists V2p \in ty_2Einteger_2Eint. (\exists V3q \in ty_2Einteger_2Eint. \\
& ((ap (ap c_2Einteger_2Eint_add (ap (ap c_2Einteger_2Eint_mul \\
& V2p) (ap c_2Einteger_2Eint_of_num V0n))) (ap (ap c_2Einteger_2Eint_mul \\
& V3q) (ap c_2Einteger_2Eint_of_num V1m))) = (ap c_2Einteger_2Eint_of_num \\
& (ap (ap c_2Egcd_2Egcd V0n) V1m))))))
\end{aligned}$$