

# thm\_2Egcd\_2EGCD\_\_CANCEL\_\_MULT (TM- FJMcxmX6PfBxTVEoeVid8BUCsTwFJaKM3)

October 26, 2020

**Definition 1** We define `c_2Emin_2E_3D` to be  $\lambda A. \lambda x \in A. \lambda y \in A. inj\_o (x = y)$  of type  $\iota \Rightarrow \iota$ .

**Definition 2** We define `c_2Ebool_2ET` to be  $(ap (ap (c_2Emin_2E_3D (2^2)) (\lambda V0x \in 2.V0x)) (\lambda V1x \in 2.V1x))$

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

**Definition 4** We define `c_2Ebool_2E_3F` to be  $\lambda A. 27a : \iota. (\lambda V0P \in (2^{A-27a}). (ap V0P (ap (c_2Emin_2E_40 A P))))$

Let `ty_2Enum_2Enum` :  $\iota$  be given. Assume the following.

$$nonempty\ ty\_2Enum\_2Enum \tag{1}$$

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

$$c\_2Earithmetic\_2E\_2A \in ((ty\_2Enum\_2Enum)^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum} \tag{2}$$

**Definition 5** We define `c_2Ebool_2E_21` to be  $\lambda A. 27a : \iota. (\lambda V0P \in (2^{A-27a}). (ap (ap (c_2Emin_2E_3D (2^{A-27a})) P) V0P))$

**Definition 6** We define `c_2Edivides_2Edivides` to be  $\lambda V0a \in ty\_2Enum\_2Enum. \lambda V1b \in ty\_2Enum\_2Enum. \lambda V2c \in ty\_2Enum\_2Enum. (ap (ap (ap (c_2Emin_2E_3D (2^{A-27a})) P) V0a) V1b) V2c)$

**Definition 7** We define `c_2Emin_2E_3D_3D_3E` to be  $\lambda P \in 2. \lambda Q \in 2. inj\_o (p \Rightarrow Q)$  of type  $\iota$ .

**Definition 8** We define `c_2Ebool_2E_2F_5C` to be  $(\lambda V0t1 \in 2. (\lambda V1t2 \in 2. (ap (c_2Ebool_2E_21 2) (\lambda V2t \in 2. (ap (ap (ap (c_2Emin_2E_3D (2^{A-27a})) P) V0t1) V1t2) V2t))))$

**Definition 9** We define `c_2Egcd_2Eis_gcd` to be  $\lambda V0a \in ty\_2Enum\_2Enum. \lambda V1b \in ty\_2Enum\_2Enum. \lambda V2c \in ty\_2Enum\_2Enum. (ap (ap (ap (c_2Emin_2E_3D (2^{A-27a})) P) V0a) V1b) V2c)$

Let `c_2Enum_2EZERO__REP` :  $\iota$  be given. Assume the following.

$$c\_2Enum\_2EZERO\_REP \in omega \tag{3}$$

Let `c_2Enum_2EABS__num` :  $\iota$  be given. Assume the following.

$$c\_2Enum\_2EABS\_num \in (ty\_2Enum\_2Enum)^{omega} \tag{4}$$

**Definition 10** We define  $c\_2Enum\_2E0$  to be  $(ap\ c\_2Enum\_2EABS\_num\ c\_2Enum\_2EZERO\_REP)$ .

**Definition 11** We define  $c\_2Earithmetic\_2EZERO$  to be  $c\_2Enum\_2E0$ .

Let  $c\_2Enum\_2EREP\_num : \iota$  be given. Assume the following.

$$c\_2Enum\_2EREP\_num \in (\omega^{ty\_2Enum\_2Enum}) \quad (5)$$

Let  $c\_2Enum\_2ESUC\_REP : \iota$  be given. Assume the following.

$$c\_2Enum\_2ESUC\_REP \in (\omega^{\omega}) \quad (6)$$

**Definition 12** 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 13** We define  $c\_2Earithmetic\_2EBIT1$  to be  $\lambda V0n \in ty\_2Enum\_2Enum.(ap\ (ap\ c\_2Earithmetic$

**Definition 14** We define  $c\_2Earithmetic\_2ENUMERAL$  to be  $\lambda V0x \in ty\_2Enum\_2Enum.V0x$ .

Let  $c\_2Egcd\_2Egcd : \iota$  be given. Assume the following.

$$c\_2Egcd\_2Egcd \in ((ty\_2Enum\_2Enum)^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum} \quad (8)$$

**Definition 15** We define  $c\_2Ebool\_2EF$  to be  $(ap\ (c\_2Ebool\_2E\_21\ 2)\ (\lambda V0t \in 2.V0t))$ .

**Definition 16** We define  $c\_2Ebool\_2E\_5C\_2F$  to be  $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap\ (c\_2Ebool\_2E\_21\ 2)\ (\lambda V2t \in$

**Definition 17** We define  $c\_2Ebool\_2E\_7E$  to be  $(\lambda V0t \in 2.(ap\ (ap\ c\_2Emin\_2E\_3D\_3D\_3E\ V0t)\ c\_2Ebool\_2E$

Assume the following.

$$\begin{aligned} & (\forall V0m \in ty\_2Enum\_2Enum.(\forall V1n \in ty\_2Enum\_2Enum.( \\ & \forall V2p \in ty\_2Enum\_2Enum.((ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m) \\ & (ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V1n)\ V2p)) = (ap\ (ap\ c\_2Earithmetic\_2E\_2A \\ & (ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m)\ V1n))\ V2p)))) \end{aligned} \quad (9)$$

Assume the following.

$$True \quad (10)$$

Assume the following.

$$\begin{aligned} & (\forall V0t1 \in 2.(\forall V1t2 \in 2.(((p\ V0t1) \Rightarrow (p\ V1t2)) \Rightarrow (((p \\ & V1t2) \Rightarrow (p\ V0t1)) \Rightarrow ((p\ V0t1) \Leftrightarrow (p\ V1t2)))))) \end{aligned} \quad (11)$$

Assume the following.

$$\begin{aligned} & (\forall V0t \in 2.(((True \wedge (p\ V0t)) \Leftrightarrow (p\ V0t)) \wedge (((p\ V0t) \wedge True) \Leftrightarrow \\ & (p\ V0t)) \wedge (((False \wedge (p\ V0t)) \Leftrightarrow False) \wedge (((p\ V0t) \wedge False) \Leftrightarrow False) \wedge \\ & (((p\ V0t) \wedge (p\ V0t)) \Leftrightarrow (p\ V0t)))))) \end{aligned} \quad (12)$$

Assume the following.

$$(\forall V0t \in 2.(((True \Rightarrow (p V0t)) \Leftrightarrow (p V0t)) \wedge (((p V0t) \Rightarrow True) \Leftrightarrow True) \wedge (((False \Rightarrow (p V0t)) \Leftrightarrow True) \wedge (((p V0t) \Rightarrow (p V0t)) \Leftrightarrow True) \wedge ((p V0t) \Rightarrow False) \Leftrightarrow (\neg (p V0t)))))) \quad (13)$$

Assume the following.

$$((\forall V0t \in 2.((\neg(\neg(p V0t))) \Leftrightarrow (p V0t))) \wedge ((\neg True) \Leftrightarrow False) \wedge ((\neg False) \Leftrightarrow True)) \quad (14)$$

Assume the following.

$$\forall A\_27a.nonempty A\_27a \Rightarrow (\forall V0x \in A\_27a.(V0x = V0x)) \quad (15)$$

Assume the following.

$$(\forall V0t \in 2.(((True \Leftrightarrow (p V0t)) \Leftrightarrow (p V0t)) \wedge (((p V0t) \Leftrightarrow True) \Leftrightarrow (p V0t)) \wedge (((False \Leftrightarrow (p V0t)) \Leftrightarrow (\neg (p V0t))) \wedge (((p V0t) \Leftrightarrow False) \Leftrightarrow (\neg (p V0t)))))) \quad (16)$$

Assume the following.

$$\forall A\_27a.nonempty A\_27a \Rightarrow (\forall V0P \in 2.(\forall V1Q \in (2^{A\_27a}).(((p V0P) \wedge (\forall V2x \in A\_27a.(p (ap V1Q V2x)))) \Leftrightarrow (\forall V3x \in A\_27a.((p V0P) \wedge (p (ap V1Q V3x))))))) \quad (17)$$

Assume the following.

$$(\forall V0a \in ty\_2Enum\_2Enum.(\forall V1b \in ty\_2Enum\_2Enum.(\forall V2c \in ty\_2Enum\_2Enum.(((p (ap (ap c\_2Edivides\_2Edivides V0a) V1b)) \wedge (p (ap (ap c\_2Edivides\_2Edivides V1b) V2c))) \Rightarrow (p (ap (ap c\_2Edivides\_2Edivides V0a) V2c)))))) \quad (18)$$

Assume the following.

$$(\forall V0a \in ty\_2Enum\_2Enum.(p (ap (ap c\_2Edivides\_2Edivides (ap c\_2Earithmetic\_2ENUMERAL (ap c\_2Earithmetic\_2EBIT1 c\_2Earithmetic\_2EZERO)) V0a))) \quad (19)$$

Assume the following.

$$(\forall V0a \in ty\_2Enum\_2Enum.(\forall V1b \in ty\_2Enum\_2Enum.(\forall V2c \in ty\_2Enum\_2Enum.(\forall V3d \in ty\_2Enum\_2Enum.(((p (ap (ap (ap c\_2Egcd\_2Eis\_gcd V0a) V1b) V2c)) \wedge (p (ap (ap (ap c\_2Egcd\_2Eis\_gcd V0a) V1b) V3d))) \Rightarrow (V2c = V3d)))))) \quad (20)$$

Assume the following.

$$(\forall V0a \in ty\_2Enum\_2Enum.(\forall V1b \in ty\_2Enum\_2Enum.(p (ap (ap (ap c\_2Egcd\_2Eis\_gcd V0a) V1b) (ap (ap c\_2Egcd\_2Egcd V0a) V1b)))))) \quad (21)$$

Assume the following.

$$\begin{aligned}
& (\forall V0a \in ty\_2Enum\_2Enum. (\forall V1b \in ty\_2Enum\_2Enum. ( \\
& \quad \forall V2c \in ty\_2Enum\_2Enum. (((ap (ap c\_2Egcd\_2Egcd V0a) V1b) = \\
& (ap c\_2Earithmetic\_2ENUMERAL (ap c\_2Earithmetic\_2EBIT1 c\_2Earithmetic\_2EZERO)))) \wedge \\
& (p (ap (ap c\_2Edivides\_2Edivides V1b) (ap (ap c\_2Earithmetic\_2E\_2A \\
& \quad V0a) V2c)))) \Rightarrow (p (ap (ap c\_2Edivides\_2Edivides V1b) V2c))))))
\end{aligned} \tag{22}$$

Assume the following.

$$(\forall V0t \in 2. ((\neg(\neg(p V0t))) \Leftrightarrow (p V0t))) \tag{23}$$

Assume the following.

$$(\forall V0A \in 2. ((p V0A) \Rightarrow ((\neg(p V0A)) \Rightarrow False))) \tag{24}$$

Assume the following.

$$\begin{aligned}
& (\forall V0A \in 2. (\forall V1B \in 2. (((\neg((\neg(p V0A) \vee (p V1B)))) \Rightarrow False) \Leftrightarrow \\
& ((p V0A) \Rightarrow False) \Rightarrow ((\neg(p V1B)) \Rightarrow False))))))
\end{aligned} \tag{25}$$

Assume the following.

$$\begin{aligned}
& (\forall V0A \in 2. (\forall V1B \in 2. (((\neg((\neg(p V0A) \vee (p V1B)))) \Rightarrow False) \Leftrightarrow \\
& ((p V0A) \Rightarrow ((\neg(p V1B)) \Rightarrow False))))))
\end{aligned} \tag{26}$$

Assume the following.

$$(\forall V0A \in 2. (((\neg(p V0A)) \Rightarrow False) \Rightarrow (((p V0A) \Rightarrow False) \Rightarrow False))) \tag{27}$$

Assume the following.

$$\begin{aligned}
& (\forall V0p \in 2. (\forall V1q \in 2. (\forall V2r \in 2. (((p V0p) \Leftrightarrow ( \\
& (p V1q) \Leftrightarrow (p V2r))) \Leftrightarrow (((p V0p) \vee ((p V1q) \vee (p V2r))) \wedge (((p V0p) \vee ((\neg \\
& p V2r) \vee (\neg(p V1q)))) \wedge ((p V1q) \vee ((\neg(p V2r)) \vee (\neg(p V0p)))) \wedge ((p V2r) \vee \\
& ((\neg(p V1q)) \vee (\neg(p V0p))))))))))
\end{aligned} \tag{28}$$

Assume the following.

$$\begin{aligned}
& (\forall V0p \in 2. (\forall V1q \in 2. (\forall V2r \in 2. (((p V0p) \Leftrightarrow ( \\
& (p V1q) \wedge (p V2r))) \Leftrightarrow (((p V0p) \vee ((\neg(p V1q)) \vee (\neg(p V2r)))) \wedge (((p V1q) \vee \\
& (\neg(p V0p))) \wedge ((p V2r) \vee (\neg(p V0p))))))))))
\end{aligned} \tag{29}$$

Assume the following.

$$\begin{aligned}
& (\forall V0p \in 2. (\forall V1q \in 2. (\forall V2r \in 2. (((p V0p) \Leftrightarrow ( \\
& (p V1q) \vee (p V2r))) \Leftrightarrow (((p V0p) \vee (\neg(p V1q))) \wedge (((p V0p) \vee (\neg(p V2r))) \wedge \\
& ((p V1q) \vee ((p V2r) \vee (\neg(p V0p))))))))))
\end{aligned} \tag{30}$$

Assume the following.

$$(\forall V0p \in 2. (\forall V1q \in 2. (\forall V2r \in 2. (((p V0p) \Leftrightarrow (p V1q) \Rightarrow (p V2r)) \Leftrightarrow (((p V0p) \vee (p V1q)) \wedge (((p V0p) \vee \neg(p V2r))) \wedge (\neg(p V1q)) \vee ((p V2r) \vee \neg(p V0p)))))))) \quad (31)$$

Assume the following.

$$(\forall V0p \in 2. (\forall V1q \in 2. (((p V0p) \Leftrightarrow \neg(p V1q)) \Leftrightarrow (((p V0p) \vee (p V1q)) \wedge (\neg(p V1q)) \vee \neg(p V0p)))))) \quad (32)$$

Assume the following.

$$(\forall V0p \in 2. (\forall V1q \in 2. (\neg((p V0p) \Rightarrow (p V1q))) \Rightarrow (p V0p))) \quad (33)$$

Assume the following.

$$(\forall V0p \in 2. (\forall V1q \in 2. (\neg((p V0p) \Rightarrow (p V1q))) \Rightarrow \neg(p V1q))) \quad (34)$$

Assume the following.

$$(\forall V0p \in 2. (\forall V1q \in 2. (\neg((p V0p) \vee (p V1q))) \Rightarrow \neg(p V0p))) \quad (35)$$

Assume the following.

$$(\forall V0p \in 2. (\forall V1q \in 2. (\neg((p V0p) \vee (p V1q))) \Rightarrow \neg(p V1q))) \quad (36)$$

Assume the following.

$$(\forall V0p \in 2. (\neg(\neg(p V0p))) \Rightarrow (p V0p)) \quad (37)$$

**Theorem 1**

$$(\forall V0m \in ty\_2Enum\_2Enum. (\forall V1n \in ty\_2Enum\_2Enum. (\forall V2k \in ty\_2Enum\_2Enum. (((ap (ap c\_2Egcd\_2Egcd V0m) V2k) = (ap c\_2Earithmetic\_2ENUMERAL (ap c\_2Earithmetic\_2EBIT1 c\_2Earithmetic\_2EZERO))) \Rightarrow (((ap (ap c\_2Egcd\_2Egcd V0m) (ap (ap c\_2Earithmetic\_2E\_2A V2k) V1n)) = (ap (ap c\_2Egcd\_2Egcd V0m) V1n)))))))$$