

The Perfect Number Theorem

Mark IJbema

October 11, 2017

Abstract

This document presents the formal proof of the Perfect Number Theorem. The result can also be found as number 70 on the list of “top 100 mathematical theorems” [Wie]. This document was produced as result of a B.Sc. Thesis under supervision of Jaap Top and Wim H. Hesselink (University of Groningen) in 2009.

Contents

1	Basics needed	1
2	Sum of divisors function	2
3	Perfect Number Theorem	4

1 Basics needed

theory *PerfectBasics*

imports *Main HOL-Computational-Algebra.Primes HOL-Algebra.Exponent*
begin

lemma *sum-mono2-nat*: *finite (B::nat set) $\implies A \leq B \implies \sum A \leq \sum B$*
<proof>

lemma *multiplicity-0 [simp]*: *multiplicity 0 x = 0*
<proof>

lemma *exp-is-max-div*:

assumes *m0*: *m $\neq 0$ and p: prime p*

shows $\sim p \text{ dvd } (m \text{ div } (p^{(\text{multiplicity } p \ m)}))$

<proof>

lemma *coprime-multiplicity*:

assumes *prime (p::nat) and m > 0*

shows *coprime p (m div (p ^ multiplicity p m))*
<proof>

lemma *add-mult-distrib-three: (x::nat)*(a+b+c)=x*a+x*b+x*c*
<proof>

lemma *nat-interval-minus-zero: {0..Suc n} = {0} Un {Suc 0..Suc n}* *<proof>*

lemma *nat-interval-minus-zero2:*

assumes *n>0*

shows *{0..n} = {0} Un {Suc 0..n}* *<proof>*

theorem *simplify-sum-of-powers: (x - 1::nat) * (∑ i=0 .. n . x^i) = x^(n + 1) - 1* *(is ?l = ?r)*
<proof>

end

2 Sum of divisors function

theory *Sigma*

imports *PerfectBasics HOL-Library.Infinite-Set*

begin

definition *divisors :: nat => nat set* **where**
divisors (m::nat) == {n . n dvd m}

definition *sigma :: nat => nat* **where**
sigma m == ∑ n | n dvd m . n

lemma *sigma-divisors: sigma(n) = ∑ (divisors(n))*
<proof>

lemma *divisors-eq-dvd[iff]: (a:divisors(n)) = (a dvd n)*
<proof>

lemma *mult-divisors: (a::nat)*b=c==>a: divisors c*
<proof>

lemma *mult-divisors2: (a::nat)*b=c==>b: divisors c*
<proof>

lemma *divisorsfinite[simp]:*
assumes *n>0*
shows *finite (divisors n)*
<proof>

lemma *divs-of-zero-UNIV[simp]: divisors(0) = UNIV*
<proof>

lemma *sigma0[simp]: sigma(0) = 0*

<proof>

lemma *sigma1[simp]*: $\text{sigma}(1) = 1$

<proof>

lemma *prime-divisors*: $\text{prime } (p::\text{nat}) \longleftrightarrow \text{divisors } p = \{1,p\} \ \& \ p > 1$

<proof>

lemma *prime-imp-sigma*: $\text{prime } (p::\text{nat}) \implies \text{sigma}(p) = p+1$

<proof>

lemma *sigma-third-divisor*:

assumes $1 < a \ a < n \ a : \text{divisors } n$

shows $1+a+n \leq \text{sigma}(n)$

<proof>

lemma *sigma-imp-divisors*: $\text{sigma}(n)=n+1 \implies n > 1 \ \& \ \text{divisors } n = \{n,1\}$

<proof>

lemma *sigma-imp-prime*: $\text{sigma}(n)=n+1 \implies \text{prime } n$

<proof>

lemma *pr-pow-div-eq-sm-pr-pow*:

fixes $p::\text{nat}$

assumes *prime*: $\text{prime } p$

shows $\{d . d \ \text{dvd} \ p^n\} = \{p^f \mid f . f \leq n\}$

<proof>

lemma *rewrite-sum-of-powers*:

assumes $p: (p::\text{nat}) > 1$

shows $(\sum \{p^m \mid m . m \leq (n::\text{nat})\}) = (\sum \ i = 0 .. n . p^i)$ (**is** $?l = ?r$)

<proof>

theorem *sigma-primpower*:

$\text{prime } p \implies (p - 1) * \text{sigma}(p^{(e::\text{nat})}) = (p^{(e+1)} - 1)$

<proof>

lemma *sigma-prime-power-two*: $\text{sigma}(2^{(n::\text{nat})}) = 2^{(n+1)} - 1$

<proof>

lemma *prodsums-eq-sumprods*:

fixes $p :: \text{nat}$ **and** $m :: \text{nat}$

assumes *coprime* $p \ m$

shows $\sum \{p^f \mid f . f \leq n\} * \sum \{b . b \ \text{dvd} \ m\} = \sum \{p^f * b \mid b . f \leq n \wedge b \ \text{dvd} \ m\}$

<proof>

declare $[[\text{simproc } \text{add: } \text{finite-Collect}]]$

lemma *rewrite-for-sigma-semimultiplicative*:
fixes $p::nat$
assumes $prime\ p$
shows $\{p^f * b \mid f \leq n \ \& \ b \text{ dvd } m\} = \{a * b \mid a \text{ dvd } (p^n) \ \& \ b \text{ dvd } m\}$
 $\langle proof \rangle$

lemma *div-decomp-comp*:
fixes $a::nat$
shows $coprime\ m\ n \implies a \text{ dvd } m * n \iff (\exists b\ c. a = b * c \ \& \ b \text{ dvd } m \ \& \ c \text{ dvd } n)$
 $\langle proof \rangle$

theorem *sigma-semimultiplicative*:
assumes $p: prime\ p$ **and** $coprime\ p\ m$
shows $sigma\ (p^n) * sigma\ m = sigma\ (p^n * m)$ (**is** $?l = ?r$)
 $\langle proof \rangle$

end

3 Perfect Number Theorem

theory *Perfect*
imports *Sigma*
begin

definition *perfect* :: $nat \implies bool$ **where**
 $perfect\ m == m > 0 \ \& \ 2 * m = sigma\ m$

theorem *perfect-number-theorem*:
assumes $even: even\ m$ **and** $perfect: perfect\ m$
shows $\exists n. m = 2^n * (2^{n+1} - 1) \wedge prime\ ((2::nat)^{n+1} - 1)$
 $\langle proof \rangle$

theorem *Euclid-book9-prop36*:
assumes $p: prime\ (2^{n+1} - 1)$
shows $perfect\ ((2^n) * (2^{n+1} - 1))$
 $\langle proof \rangle$

end

References

[Wie] Freek Wiedijk. Formalizing 100 theorems. <http://www.cs.ru.nl/~freek/100/>.