The Perfect Number Theorem

Mark IJbema

April 20, 2020

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

theory *PerfectBasics*
imports *Main HOL−Computational-Algebra.Primes HOL−Algebra.Exponent*
begin

lemma *sum-mono2-nat*: *finite* (*B*::*nat set*) $\Longrightarrow$ *A* <= *B* $\Longrightarrow$ $\sum$ *A* <= $\sum$ *B*
⟨*proof*⟩

lemma *multiplicity-0* [*simp*]: *multiplicity 0 x* = *0*
⟨*proof*⟩

lemma *exp-is-max-div*:
assumes *m0*:*m* ≠ *0* **and** *p*: *prime p*
shows ~ *p dvd* (*m div* (*p*ˆ(*multiplicity p m*)))
⟨*proof*⟩

lemma *coprime-multiplicity*:
assumes *prime* (*p*::*nat*) **and** *m* > *0*

shows *coprime p* (*m div* (*p* ˆ *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*) ∗ ($\sum$ *i*=*0* .. *n* . *x*ˆ*i*) = *x*ˆ(*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 == $\sum$ *n* | *n dvd m* . *n*

lemma *sigma-divisors*: *sigma*(*n*) = $\sum$ (*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*]: *sigma*(*1*) = *1*
⟨*proof*⟩

lemma *prime-divisors*: *prime* (*p*::*nat*) ⟷ *divisors p* = {*1*,*p*} & *p*>*1*
⟨*proof*⟩

lemma *prime-imp-sigma*: *prime* (*p*::*nat*) ==> *sigma*(*p*) = *p*+*1*
⟨*proof*⟩

lemma *sigma-third-divisor*:
assumes *1* < *a a* < *n a* : *divisors n*
shows *1*+*a*+*n* <= *sigma*(*n*)
⟨*proof*⟩

lemma *sigma-imp-divisors*: *sigma*(*n*)=*n*+*1* ==> *n*>*1* & *divisors n* = {*n*,*1*}
⟨*proof*⟩

lemma *sigma-imp-prime*: *sigma*(*n*)=*n*+*1* ==> *prime n*
⟨*proof*⟩

lemma *pr-pow-div-eq-sm-pr-pow*:
fixes *p*::*nat*
assumes *prime*: *prime p*
shows {*d* . *d dvd p*ˆ*n*} = {*p*ˆ*f*| *f* . *f*<=*n*}
⟨*proof*⟩

lemma *rewrite-sum-of-powers*:
assumes *p*: (*p*::*nat*)>*1*
shows ($\sum$ {*p*ˆ*m* | *m* . *m*<=(*n*::*nat*)}) = ($\sum$ *i* = *0* .. *n* . *p*ˆ*i*) (**is** *?l* = *?r*)
⟨*proof*⟩

theorem *sigma-primepower*:
prime p ==> (*p* − *1*)∗*sigma*(*p*ˆ(*e*::*nat*)) = (*p*ˆ(*e*+*1*) − *1*)
⟨*proof*⟩

lemma *sigma-prime-power-two*: *sigma*(*2*ˆ(*n*::*nat*)) = *2*ˆ(*n*+*1*) − *1*
⟨*proof*⟩

lemma *prodsums-eq-sumprods*:
fixes *p* :: *nat* **and** *m* :: *nat*
assumes *coprime p m*
shows $\sum${*p* ˆ *f* |*f*. *f* ≤ *n*} ∗ $\sum${*b*. *b dvd m*} = $\sum${*p* ˆ *f* ∗ *b* |*f b*. *f* ≤ *n* ∧ *b dvd m*} (**is** *?lhs* = *?rhs*)
⟨*proof*⟩

declare [[*simproc add*: *finite-Collect*]]

lemma *rewrite-for-sigma-semimultiplicative*:
fixes p::*nat*
assumes *prime* p
shows $\{p\hat{}f*b\ |f\ b.\ f<=n\ \&\ b\ dvd\ m\} = \{a*b\ |a\ b.\ a\ dvd\ (p\hat{}n)\ \&\ b\ dvd\ m\}$
⟨*proof*⟩

lemma *div-decomp-comp*:
fixes a::*nat*
shows *coprime* $m\ n \Longrightarrow a\ dvd\ m*n \longleftrightarrow (\exists\, b\ c.\ a = b * c\ \&\ b\ dvd\ m\ \&\ c\ dvd\ n)$
⟨*proof*⟩

theorem *sigma-semimultiplicative*:
assumes p: *prime* p **and** *cop*: *coprime* $p\ m$
shows *sigma* $(p\hat{}n) *$ *sigma* $m =$ *sigma* $(p\hat{}n * m)$ (**is** $?l = ?r$)
⟨*proof*⟩

end

3 Perfect Number Theorem

theory *Perfect*
imports *Sigma*
begin

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

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

theorem *Euclid-book9-prop36*:
assumes p: *prime* $(2\hat{}(n+1) - (1::nat))$
shows *perfect* $((2\hat{}n)*(2\hat{}(n+1) - 1))$
⟨*proof*⟩

end

References

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