Amicable Numbers

Angeliki Koutsoukou-Argyraki

March 17, 2025

Abstract

This is a formalisation of Amicable Numbers, involving some relevant material including Euler's sigma function, some relevant definitions, results and examples as well as rules such as Thābit ibn Qurra's Rule, Euler's Rule, te Riele's Rule and Borho's Rule with breeders.

The main sources are [2] [3]. Some auxiliary material can be found in [1] [4]. If not otherwise stated, the source of definitions is [2]. In a few definitions where we refer to Wikipedia articles [5] [6] [7] this is explicitly mentioned.

Contents

theory *Amicable-Numbers*
imports *HOL−Number-Theory.Number-Theory*
HOL−Computational-Algebra.Computational-Algebra
Pratt-Certificate.Pratt-Certificate-Code
Polynomial-Factorization.Prime-Factorization

begin

1 Miscellaneous

lemma *mult-minus-eq-nat*:
fixes $x::nat$ **and** $y::nat$ **and** $z::nat$
assumes $x+y = z$
shows $-x-y = -z$
⟨*proof*⟩

lemma *minus-eq-nat-subst*: **fixes** $A::nat$ **and** $B::nat$ **and** $C::nat$ **and** $D::nat$ **and** $E::nat$
assumes $A = B-C-D$ **and** $-E = -C-D$
shows $A = B-E$
⟨*proof*⟩

lemma *minus-eq-nat-subst-order*: **fixes** $A::nat$ **and** $B::nat$ **and** $C::nat$ **and** $D::nat$ **and** $E::nat$
assumes $B-C-D > 0$ **and** $A = B-C-D+B$ **shows** $A = 2*B-C-D$
⟨*proof*⟩

lemma *auxiliary-ineq*: **fixes** $x::nat$ **assumes** $x \geq (2::nat)$
shows $x+1 < (2::nat)*x$
⟨*proof*⟩

lemma *sum-strict-mono*:
fixes $A :: nat\ set$
assumes *finite* B $A \subset B$ $0 \notin B$
shows $\sum A < \sum B$
⟨*proof*⟩

lemma *coprime-dvd-aux*:
assumes *gcd m n = Suc 0 na dvd n ma dvd m mb dvd m nb dvd n* **and** *eq*: $ma * na = mb * nb$
shows $ma = mb$
⟨*proof*⟩

2 Amicable Numbers

2.1 Preliminaries

definition *divisor* :: *nat* ⇒*nat* ⇒ *bool* (**infixr** ‹*divisor*› *80*)
where *n divisor m* ≡(*n* ≥ *1* ∧ *n* ≤ *m* ∧ *n dvd m*)

definition *divisor-set*: *divisor-set m* = {*n*. *n divisor m*}

lemma *def-equiv-divisor-set*: *divisor-set* (*n*::*nat*) = *set*(*divisors-nat n*)
⟨*proof*⟩

definition *proper-divisor* :: *nat* ⇒*nat* ⇒ *bool* (**infixr** ‹*properdiv*› *80*)
where *n properdiv m* ≡(*n* ≥ *1* ∧ *n* < *m* ∧ *n dvd m*)

definition *properdiv-set*: *properdiv-set m* = {*n*. *n properdiv m*}

lemma *example1-divisor*: **shows** (*2*::*nat*) ∈ *divisor-set* (*4*::*nat*)
⟨*proof*⟩

lemma *example2-properdiv-set*: *properdiv-set* (*Suc* (*Suc* (*Suc 0*))) = {(*1*::*nat*)}
⟨*proof*⟩

lemma *divisor-set-not-empty*: **fixes** *m*::*nat* **assumes** *m* ≥*1*
shows *m* ∈ *divisor-set m*
⟨*proof*⟩

lemma *finite-divisor-set* [*simp*]: *finite*(*divisor-set n*)
⟨*proof*⟩

lemma *finite-properdiv-set*[*simp*]: **shows** *finite*(*properdiv-set m*)
⟨*proof*⟩

lemma *divisor-set-mult*:
divisor-set (*m*∗*n*) = {*i*∗*j*| *i j*. (*i* ∈ *divisor-set m*)∧(*j* ∈ *divisor-set n*)}
⟨*proof*⟩

lemma *divisor-set-1* [*simp*]: *divisor-set* (*Suc 0*) = {*Suc 0*}
⟨*proof*⟩

lemma *divisor-set-one*: **shows** *divisor-set 1* ={*1*}
⟨*proof*⟩

lemma *union-properdiv-set*: **assumes** *n*≥*1* **shows** *divisor-set n* =(*properdiv-set n*)∪{*n*}
⟨*proof*⟩

lemma *prime-div-set*: **assumes** *prime n* **shows** *divisor-set n* = {*n*, *1*}
⟨*proof*⟩

lemma *div-set-prime*:
assumes *prime n*
shows *properdiv-set n* = {*1*}
⟨*proof*⟩

lemma *prime-gcd*: **fixes** *m*::*nat* **and** *n*::*nat* **assumes** *prime m* **and** *prime n* **and** $m \neq n$ **shows** *gcd m n* =*1* ⟨*proof*⟩

We refer to definitions from [5]:

definition *aliquot-sum* :: *nat* ⇒ *nat*
where *aliquot-sum n* ≡ $\sum$ (*properdiv-set n*)

definition *deficient-number* :: *nat* ⇒ *bool*
where *deficient-number n* ≡ (*n* > *aliquot-sum n*)

definition *abundant-number* :: *nat* ⇒ *bool*
where *abundant-number n* ≡ (*n* < *aliquot-sum n*)

definition *perfect-number* :: *nat* ⇒ *bool*
where *perfect-number n* ≡ (*n* = *aliquot-sum n*)

lemma *example-perfect-6*: **shows** *perfect-number 6*

⟨*proof*⟩

2.2 Euler's sigma function and properties

The sources of the following useful material on Euler's sigma function are [2], [3], [4] and [1].

definition *Esigma* :: *nat* ⇒ *nat*
where *Esigma n* ≡ $\sum$ (*divisor-set n*)

lemma *Esigma-properdiv-set*:
assumes $m \geq 1$
shows *Esigma m* = (*aliquot-sum m*) + *m*
⟨*proof*⟩

lemma *Esigmanotzero*:
assumes $n \geq 1$
shows *Esigma n* ≥ *1*
⟨*proof*⟩

lemma *prime-sum-div*:
assumes *prime n*
shows *Esigma n* = *n* +(*1*::*nat*)
⟨*proof*⟩

lemma *sum-div-is-prime*:
assumes *Esigma n* = *n* +(*1*::*nat*) **and** *n* ≥*1*

shows *prime n*

⟨*proof*⟩

lemma *Esigma-prime-sum*:
fixes *k*:: *nat* **assumes** *prime m k* $\geq$*1*
shows *Esigma* $(m^k) = (m^{(k+(1::nat))} - (1::nat)) / (m-1)$

⟨*proof*⟩

lemma *prime-Esigma-mult*: **assumes** *prime m* **and** *prime n* **and** $m \neq n$
shows *Esigma* $(m*n) = $ (*Esigma n*)$*$(*Esigma m*)

⟨*proof*⟩

lemma *gcd-Esigma-mult*:
assumes *gcd m n* = *1*
shows *Esigma* $(m*n) = $ (*Esigma m*)$*$(*Esigma n*)

⟨*proof*⟩

lemma *deficient-Esigma*:
assumes *Esigma m* $< 2*m$ **and** $m \geq 1$
shows *deficient-number m*
⟨*proof*⟩

lemma *abundant-Esigma*:
assumes *Esigma m* $> 2*m$ **and** $m \geq 1$
shows *abundant-number m*
⟨*proof*⟩

lemma *perfect-Esigma*:
assumes *Esigma m* $= 2*m$ **and** $m \geq 1$
shows *perfect-number m*
⟨*proof*⟩

2.3 Amicable Numbers; definitions, some lemmas and examples

definition *Amicable-pair* :: *nat* ⇒*nat* ⇒ *bool* (**infixr** ‹*Amic*› *80*)
where *m Amic n* ≡ ((*m* = *aliquot-sum n*) ∧ (*n* = *aliquot-sum m*))

lemma *Amicable-pair-sym*: **fixes** *m*::*nat* **and** *n* ::*nat*
assumes *m Amic n* **shows** *n Amic m*
⟨*proof*⟩

lemma *Amicable-pair-equiv-def*:
assumes (*m Amic n*) **and** $m \geq 1$ **and** $n \geq 1$
shows (*Esigma m* = *Esigma n*)∧(*Esigma m* = $m+n$)

⟨*proof*⟩

lemma *Amicable-pair-equiv-def-conv*:
assumes $m \geq 1$ **and** $n \geq 1$ **and** $(Esigma\ m = Esigma\ n) \wedge (Esigma\ m = m+n)$
shows $(m\ Amic\ n)$
⟨*proof*⟩

definition *typeAmic* :: *nat* ⇒ *nat* ⇒ *nat list*
where *typeAmic n m* =
$[(card\ \{i.\ \exists\ N.\ n = N*(gcd\ n\ m) \wedge prime\ i \wedge i\ dvd\ N \wedge \neg\ i\ dvd\ (gcd\ n\ m)\}),$
$(card\ \{j.\ \exists\ M.\ m = M*(gcd\ n\ m) \wedge prime\ j \wedge j\ dvd\ M \wedge \neg\ j\ dvd\ (gcd\ n\ m)\})]$

lemma *Amicable-pair-deficient*: **assumes** $m > n$ **and** *m Amic n*
shows *deficient-number m*
⟨*proof*⟩

lemma *Amicable-pair-abundant*: **assumes** $m > n$ **and** *m Amic n*
shows *abundant-number n*
⟨*proof*⟩

lemma *even-even-amicable*: **assumes** *m Amic n* **and** $m \geq 1$ **and** $n \geq 1$ **and** *even m* **and** *even n*
shows $(2*m \neq n)$

⟨*proof*⟩

2.3.1 Regular Amicable Pairs

definition *regularAmicPair* :: *nat* ⇒ *nat* ⇒ *bool* **where**
regularAmicPair n m ⟷ (*n Amic m* ∧
$(\exists M\ N\ g.\ g = gcd\ m\ n \wedge m = M*g \wedge n = N*g \wedge squarefree\ M \wedge$
$squarefree\ N \wedge gcd\ g\ M = 1 \wedge gcd\ g\ N = 1))$

lemma *regularAmicPair-sym*:
assumes *regularAmicPair n m* **shows** *regularAmicPair m n*

⟨*proof*⟩

definition *irregularAmicPair* :: *nat* ⇒ *nat* ⇒ *bool* **where**
irregularAmicPair n m ⟷ ((*n Amic m*) ∧ ¬ *regularAmicPair n m*)

lemma *irregularAmicPair-sym*:
assumes *irregularAmicPair n m*
shows *irregularAmicPair m n*
⟨*proof*⟩

2.3.2 Twin Amicable Pairs

We refer to the definition in [6]:

definition *twinAmicPair* :: *nat* ⇒ *nat* ⇒ *bool* **where**
twinAmicPair n m ⟷
(*n Amic m*) ∧ (¬(∃ *k l*. *k* > *Min* {*n*, *m*} ∧ *k* < *Max* {*n*, *m*}∧ *k Amic l*))

lemma *twinAmicPair-sym*:
assumes *twinAmicPair n m*
shows *twinAmicPair m n*
⟨*proof*⟩

2.3.3 Isotopic Amicable Pairs

A way of generating an amicable pair from a given amicable pair under certain conditions is given below. Such amicable pairs are called Isotopic [2].

lemma *isotopic-amicable-pair*:
fixes *m n g h M N* :: *nat*
assumes *m Amic n* **and** *m* ≥ *1* **and** *n* ≥ *1***and** *m*= *g*∗*M* **and** *n* = *g*∗*N*
and *Esigma h* = (*h*/*g*) ∗ *Esigma g* **and** *h* ≠ *g* **and** *h* > *1* **and** *g* > *1*
and *gcd g M* = *1* **and** *gcd g N* = *1* **and** *gcd h M* = *1* **and** *gcd h N* = *1*
shows (*h*∗*M*) *Amic* (*h*∗*N*)

⟨*proof*⟩

lemma *isotopic-pair-example1*:
assumes (*3^3*∗*5*∗*11*∗*17*∗*227*) *Amic* (*3^3*∗*5*∗*23*∗*37*∗*53*)
shows (*3^2*∗*7*∗*13*∗*11*∗*17*∗*227*) *Amic* (*3^2*∗*7*∗*13*∗*23*∗*37*∗*53*)

⟨*proof*⟩

2.3.4 Betrothed (Quasi-Amicable) Pairs

We refer to the definition in [7]:

definition *QuasiAmicable-pair* :: *nat* ⇒ *nat* ⇒ *bool* (**infixr** ‹*QAmic*› *80*)
where *m QAmic n* ⟷ (*m* + *1* = *aliquot-sum n*) ∧ (*n* + *1* = *aliquot-sum m*)

lemma *QuasiAmicable-pair-sym* :
assumes *m QAmic n* **shows** *n QAmic m*
⟨*proof*⟩

lemma *QuasiAmicable-example*:
shows *48 QAmic 75*

⟨*proof*⟩

2.3.5 Breeders

definition *breeder-pair* :: *nat* ⇒*nat* ⇒ *bool* (**infixr** ‹*breeder*› *80*)

where *m breeder n* ≡ (∃ *x*∈ℕ. *x* > *0* ∧ *Esigma m* = *m* + *n*∗*x* ∧ *Esigma m* = (*Esigma n*)∗(*x*+*1*))

lemma *breederAmic*:
fixes *x* :: *nat*
assumes *x* > *0* **and** *Esigma n* = *n* + *m*∗*x* **and** *Esigma n* = *Esigma m* ∗ (*x*+*1*)

and *prime x* **and** ¬(*x dvd m*)
shows *n Amic* (*m*∗*x*)

⟨*proof*⟩

2.3.6 More examples

The first odd-odd amicable pair was discovered by Euler [2]. In the following proof, amicability is shown using the properties of Euler's sigma function.

lemma *odd-odd-amicable-Euler*: *69615 Amic 87633*
⟨*proof*⟩

The following is the smallest odd-odd amicable pair [2]. In the following proof, amicability is shown directly by evaluating the sets of divisors.

lemma *Amicable-pair-example-smallest-odd-odd*: *12285 Amic 14595*
⟨*proof*⟩

3 Euler's Rule

We present Euler's Rule as in [2]. The proof has been reconstructed.

theorem *Euler-Rule-Amicable*:
fixes *k l f p q r m n* :: *nat*
assumes *k* > *l* **and** *l* ≥ *1* **and** *f* = *2*^*l*+*1*
and *prime p* **and** *prime q* **and** *prime r*
and *p* = *2*^(*k*−*l*) ∗ *f* − *1* **and** *q* = *2*^*k* ∗ *f* − *1* **and** *r* = *2*^(*2*∗*k*−*l*) ∗ *f*^*2* − *1*
and *m* = *2*^*k* ∗ *p* ∗ *q* **and** *n* = *2*^*k* ∗ *r*
shows *m Amic n*

⟨*proof*⟩

Another approach by Euler [2]:

theorem *Euler-Rule-Amicable-1*:
fixes *m n a* :: *nat*
assumes *m* ≥ *1* **and** *n* ≥ *1* **and** *a* ≥ *1*
and *Esigma m* = *Esigma n* **and** *Esigma a* ∗ *Esigma m* = *a*∗(*m*+*n*)
and *gcd a m* =*1* **and** *gcd a n* =*1*
shows (*a*∗*m*) *Amic* (*a*∗*n*)

⟨*proof*⟩

4 Thābit ibn Qurra's Rule and more examples

Euler's Rule (theorem Euler_Rule_Amicable) is actually a generalisation of the following rule by Thābit ibn Qurra from the 9th century [2]. Thābit ibn Qurra's Rule is the special case for $l = 1$ thus $f = 3$.

corollary *Thabit-ibn-Qurra-Rule-Amicable*:
fixes $k\ l\ f\ p\ q\ r :: nat$
assumes $k > 1$ **and** *prime* p **and** *prime* q **and** *prime* r
and $p = 2\hat{}(k-1) * 3 - 1$ **and** $q = 2\hat{}k * 3 - 1$ **and** $r = 2\hat{}(2*k-1) * 9 - 1$
shows $((2\hat{}k)*p*q)$ *Amic* $((2\hat{}k)*r)$

⟨*proof*⟩

In the following three example of amicable pairs, instead of evaluating the sum of the divisors or using the properties of Euler's sigma function as it was done in the previous examples, we prove amicability more directly as we can apply Thābit ibn Qurra's Rule.

The following is the first example of an amicable pair known to the Pythagoreans and can be derived from Thābit ibn Qurra's Rule with $k = 2$ [2].

lemma *Amicable-Example-Pythagoras*:
shows *220 Amic 284*

⟨*proof*⟩

The following example of an amicable pair was (re)discovered by Fermat and can be derived from Thābit ibn Qurra's Rule with $k = 4$ [2].

lemma *Amicable-Example-Fermat*:
shows *17296 Amic 18416*

⟨*proof*⟩

The following example of an amicable pair was (re)discovered by Descartes and can be derived from Thābit ibn Qurra's Rule with $k = 7$ [2].

lemma *Amicable-Example-Descartes*:
shows *9363584 Amic 9437056*

⟨*proof*⟩

In fact, the Amicable Pair (220, 284) is Regular and of type (2,1):

lemma *regularAmicPairExample*: *regularAmicPair 220 284* $\wedge$ *typeAmic 220 284* $= [2,\ 1]$
⟨*proof*⟩

lemma *abundant220ex*: *abundant-number 220*
⟨*proof*⟩

lemma *deficient284ex*: *deficient-number 284*
⟨*proof*⟩

5 Te Riele's Rule and Borho's Rule with breeders

With the following rule [2] we can get an amicable pair from a known amicable pair under certain conditions.

theorem *teRiele-Rule-Amicable*:
fixes $a\ u\ p\ r\ c\ q$ :: *nat*
assumes $a \geq 1$ **and** $u \geq 1$
and *prime p* **and** *prime r* **and** *prime c* **and** *prime q* **and** $r \neq c$
and $\neg(p\ dvd\ a)$ **and** $(a*u)$ *Amic* $(a*p)$ **and** *gcd* $a\ (r*c)=1$
and $q = r+c+u$ **and** *gcd* $(a*u)\ q = 1$ **and** $r*c = p*(r+c+u) + p+u$
shows $(a*u*q)$ *Amic* $(a*r*c)$

⟨*proof*⟩

By replacing the assumption that $(a*u)$ *Amic* $(a*p)$ in the above rule by te Riele with the assumption that $(a*u)$ *breeder u*, we obtain Borho's Rule with breeders [2].

theorem *Borho-Rule-breeders-Amicable*:
fixes $a\ u\ r\ c\ q\ x$ :: *nat*
assumes $x \geq 1$ **and** $a \geq 1$ **and** $u \geq 1$
and *prime r* **and** *prime c* **and** *prime q* **and** $r \neq c$
and *Esigma* $(a*u) = a*u + a*x$ *Esigma* $(a*u) = ($*Esigma* $a)*(x+1)$ **and** *gcd* $a\ (r * c) = 1$
and *gcd* $(a*u)\ q = 1$ **and** $r * c = x+u + x*u + r*x + x*c$ **and** $q = r+c+u$
shows $(a*u*q)$ *Amic* $(a*r*c)$

⟨*proof*⟩

no-notation *divisor* (**infixr** ‹*divisor*› *80*)

6 Acknowledgements

The author was supported by the ERC Advanced Grant ALEXANDRIA (Project 742178) funded by the European Research Council and led by Professor Lawrence Paulson at the University of Cambridge, UK. Many thanks to Lawrence Paulson for his help and suggestions. Number divisors were initially looked up on https://onlinemathtools.com/find-all-divisors.

end

References

[1] E. Escott. Amicable numbers. *Scripta Mathematica*, 12:61–72, 1946.

[2] M. García, J. Pedersen, and H. te Riele. Amicable pairs, a survey. *REPORT MAS-R0307*, 2003.

[3] M. García, J. Pedersen, and H. te Riele. Amicable pairs, a survey. *Fields Institute Communications*, 41:1–19, 2004.

[4] E. Sandifer. Amicable pairs. 2005. How Euler Did It, The Euler Archive.

[5] Wikipedia. Aliquot sum. https://en.wikipedia.org/wiki/Aliquot_sum, 2020.

[6] Wikipedia. Amicable numbers. https://en.wikipedia.org/wiki/Amicable_numbers, 2020.

[7] Wikipedia. Betrothed numbers. https://en.wikipedia.org/wiki/Betrothed_numbers, 2020.