AMICABLE NUMBERS

And Their Applications

The intent of this paper is to discuss amicable numbers and its related topics. After recalling the long history of the topic, it will address the important facts about numbers that are and are not amicable. This discussion will include a proof of Thabit's Rule (more specifically, Euler's generalization of the rule), and will mention other specific types of amicable numbers.

1. Introduction

As is the case with most concepts in Number Theory, a pair of amicable numbers (or friendly numbers, as they are otherwise known) is a seemingly straightforward idea which has vastly complex implications and is mired in a compilation of strenuous mathematics. We state precisely what it means to be a pair of amicable number in Definition 1.

> **Definition 1** - Two integers greater than or equal to 1 are said to amicable if the sum of the proper positive divisors of one of the integers is equal to the other integer, and vice versa.

While this treatise will focus on pairs of amicable numbers, there exist other sets of amicable numbers of higher degrees (such as, amicable triples). We revise the above definition to suit these cases, as well.

> **Definition 1.1** - A set S_n of n integers greater than or equal to 1 are said to be amicable if the sum of the proper positive divisors of each element of the set is equal to the sum of the other integers in the set.

In the cases where the size of the set, n, is greater than or equal to 2, we append an additional criterion that an integer in such a set may not equal the sum of its own divisors. Instead, we treat separately the case where an integer forms an amicable set with itself.

We call such an integer a *perfect number*. We demonstrate the properties of both amicable and perfect numbers with a couple of examples.

Example 1 - {220, 284} is a pair of amicable numbers. The proper divisors of 220 are 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, and 110. The sum of these is

$$1+2+4+5+10+11+20+22+44+55+110=284.$$

The proper divisors of 284 are 1, 2, 4, 71, and 142. The sum of these is

$$1+2+4+71+142=220.$$

It is worth noting that there are no non-perfect amicable numbers less than these two integers.

Example 2 - 6 is the smallest a perfect number. This is straightforward. The sum of the proper divisors of 6 is 1+2+3=6. The sum of the proper divisors of 2, 3, 4, and 5 are 1, 1, 3, and 1, respectively. The sum of the proper divisors of 1 is undefined, since 1 does not have any proper divisors. So, 6 is the smallest perfect number.

2. A Brief History

In antiquity, pairs of amicable numbers were thought to have mystical powers, and they were often utilized in religious texts and in magic, particularly in relation to love and friendship (thus, the name amicable). In the Old Testament, for example, it is written that Jacob offered 220 sheep (220 being one of the amicable numbers from Example 1) to his brother as a sign of goodwill. Additionally, Greek astrologers incorporated these numbers into their horoscopes, talismans, and charms.

The first set of amicable numbers (220 and 284) was discovered by Pythagoras in the 6^{th} century, and the properties of these types of numbers were studied extensively by the Pythagoreans throughout the group's existence. While science in the Western world

gave way to more spiritual exploits during Dark Ages, Arabic scholars such as Ibn Tahir al-Baghdadi and al-Madshritti contributed their thoughts to the study of this subject, while also preserving the works of other scholars who came before them (al-Baghdadi's commentary on the works al-Khwarizmi, for example, are particularly important because al-Khwarizmi's original work has been lost to the ages). Perhaps the most important of these Arab scholars is Thabit ibn Qurra, whose formula for constructing amicable numbers we will study in a later section. Other more recognizable mathematicians who studied these types of numbers were René Descartes and Leonhard Euler, both of whom refined Thabit's formula.

3. A Few (Simple) Proofs

The first question that may arrive when studying amicable numbers is "How many amicable numbers are there?" There is, in fact, no proof supporting either that there is a finite quantity of amicable numbers, or that there are infinitely many such integers, and such a proof will not be attempted in this paper. First and foremost, however, we should state a few basic properties of numbers which are not amicable.

Theorem 1 - For a prime p, p is not an amicable number.

Proof: Let p be a prime. Then p has only two divisors, 1 and p. Then 1 is the only proper divisor of p. Suppose p is an amicable number. Then 1 is an amicable number. But, the sum of the proper divisors of 1 is undefined, since 1 has no proper divisors. Then 1 is not amicable. This is a contradiction. So p is not amicable.

That was a rather intuitive, but important, observation. It narrows our search for amicable numbers to composite numbers.

The next theorem relies on the assumptions that there are no amicable pairs in which either:

a) Both elements of the pair are relatively prime, or

b) The elements of the pair have opposite parity.

Both of these assumptions have been the objects of considerable study, but have yet to be proven. However, every known pair of amicable numbers has been found to have both a greatest common divisor greater than 1 and the same parity. If we can assume there are no such amicable numbers of these types, the subsequent theorems follow.

Theorem 2.1 - There exists no integer k^n for k, n $\in Z_{>1}$ such that k is prime and k^n is an amicable number.

Proof: Suppose k^n is an amicable number for a prime k. Then, the sum of the proper factors of k^n is $t=1+k+k^2+\ldots+k^{n-1}$. Then, t is an amicable number. Then, if it is true that there are no relatively prime pairs of amicable numbers, k^n and t share a prime factor. But k is the only prime factor of k^n. So, if k^n and t are amicable, $k|t$. But $t\equiv 1 \pmod{k}$. So k does not divide t. So k^n is not amicable.

Theorem 2.2 - There exists no integer k^n for k, n $\in Z_{>1}$ such that k is even and k^n is an amicable number.

Proof: Suppose k^n is an amicable number for an even number k. Then, the sum of the proper factors of k^n is $t=1+k+k^2+\ldots+k^{n-1}$. Then, t is an amicable number. Then, if it is true that there are no pairs of amicable numbers with each element in the pair having different parity, k^n and t have the same parity. But, k^n is even. Furthermore, $k+k^2+\ldots+k^{n-1}$ is even. Then $t=1+k+k^2+\ldots+k^{n-1}$ is odd. This is a contradiction. A similar argument can be made for odd k, but only when n is even.

These proofs lack substance, however, with the earlier conjectures still being unproven. But, if one were looking to find a counterexample to the two conjectures from

which we based these theorems, looking for an amicable number k^n for k prime or k even would be a good place to start.

4. Thabit's Rule (Euler's Rule)

While it obviously is not easy to find a pair of amicable numbers, there have been some efforts in formulating an algorithm for finding amicable numbers of a certain type. One such algorithm was created by Thabit ibn Qurra, a 9th century Arabic mathematician. His theorem is as follows:

Theorem 3.1: ***Thabit's Rule***

Let $p=3*2^{n-1}-1$, $q=3*2^n-1$, and $r=9*2^{2n-1}-1$, where n is an integer greater than 1.

Then, if p, q, and r are prime, $\{2^npq, 2^nr\}$ is a pair of amicable numbers.

The form we will prove is Euler's Generalization of Thabit's Rule, published in 1747, which is as follows:

Theorem 3.2: ***Euler's Rule (a Generalization of Thabit's Rule)***

Let $p=2^m(2^{n-m}+1)-1$, $q=2^n(2^{n-m}+1)-1$, and $r=2^{n+m}(2^{n-m}+1)^2-1$, for integers m and n, where $1\leq m<n$. Then, if p, q, and r are prime, $\{2^npq, 2^nr\}$ is a pair of amicable numbers.

With his theorem, Thabit was able to rediscover Pythagoras' amicable pair, {220, 284}, as well as find a new pair, {17296, 18416}. Later, René Descartes would use Thabit's Theorem and discover the pair, {9363584, 9437056}. Using his generalization, Euler discovered the pair {2172649216, 2181168896}. However, after this pair, these theorems do not produce another pair for integers less than 10^{38}.

We now proceed to a proof of Euler's Generalization of Thabit's Theorem. However, before continuing, we must make the following definition and a few observations.

Definition 2 - The Sigma Function - Let σ(s) be the sum of all the factors of s including s itself.

Note that, {n, m} is an amicable pair if and only if σ(m)-m=n and σ(n)-n=m. (i.e., if and only if σ(m)=σ(n)=m+n). Then, if {n, m} is not an amicable pair, either σ(m)≠m+n or σ(n)≠m+n. We will need this later.

Lemmas I-III - Basic properties of σ

I. σ(mn)=σ(m)σ(n), if gcd(m,n)=1.

II. If m is prime, σ(m)=m+1.

III. If n is prime, $\sigma(n^k)=1+n+n^2\ldots n^k=\frac{n^{k+1}-1}{n-1}$.

Proof: Lemmas II & III are instinctive. If m is prime, then the divisors of m are 1 and m. Then the sum of these divisors is m+1. If n is prime, then the divisors of n^k are1, n, n^2, … n^z for $1\le z\le k$. Then the sum of these divisors is $1+n+n^2+\ldots+n^k$, which can be simplified as shown above. The proof of Lemma I follows from Lemmas II & III. Suppose gcd(m,n)=1. Then $m=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$ and $n=q_1^{L_1}q_2^{L_2}\ldots q_s^{L_s}$ for primes p and q and integers k and L. Furthermore, $p_i\neq q_j$ for any $1\le i\le r$ or $1\le j\le s$. Then,

$$\sigma(mn)=\frac{(p_1^{k_1+1}-1)(p_2^{k_2+1}-1)\ldots(p_r^{k_r+1}-1)(q_1^{L_1+1}-1)(q_2^{L_2+1}-1)\ldots(q_s^{L_s+1}-1)}{(p_1-1)(p_2-1)\ldots(p_r-1)(q_1-1)(q_2-1)\ldots(q_s-1)}$$

by Lemma III. Then, since none of the p_i's or q_j's are equal, this equals

$$\frac{(p_1^{k_1+1}-1)(p_2^{k_2+1}-1)\ldots(p_r^{k_r+1}-1)}{(p_1-1)(p_2-1)\ldots(p_r-1)} * \frac{(q_1^{L_1+1}-1)(q_2^{L_2+1}-1)\ldots(q_s^{L_s+1}-1)}{(q_1-1)(q_2-1)\ldots(q_s-1)}$$

which equals σ(m) σ(n). Now we proceed to the proof of Euler's generalization of Thabit's Rule.

Theorem 3.2: Euler's Rule (a Generalization of Thabit's Rule)

Proof: Let $p=2^m(2^{n-m}+1)-1$, $q=2^n(2^{n-m}+1)-1$, and $r=2^{n+m}(2^{n-m}+1)^2-1$ all be prime (note that, furthermore, they are each odd, since they are each congruent to 1 mod 2). Then $\sigma(p)=2^m(2^{n-m}+1)$, $\sigma(q)=2^n(2^{n-m}+1)$, and $\sigma(r)= 2^{n+m}(2^{n-m}+1)^2$, by Lemma II. Note that, $\sigma(r)=\sigma(p)\sigma(q)$ (i.e. $r+1=(p+1)(q+1)$). Suppose $\{2^npq, 2^nr\}$ is not an amicable pair. Then, recall that if m and n are not amicable, either $\sigma(m)\neq m+n$ or $\sigma(n)\neq m+n$. This means either $\sigma(2^npq)\neq 2^n(pq+r)$ or $\sigma(2^nr)\neq 2^n(pq+r)$.

Suppose $\sigma(2^npq)\neq 2^n(pq+r)$. Then $\sigma(2^n)\sigma(p)\sigma(q)\neq 2^n(pq+r)$, by Lemma I, since 2^n, p, and q are all relatively prime to one another. So, $(2^{n+1}-1)(p+1)(q+1)\neq 2^n(pq+r)$, by Lemmas II and III. So, $(2^{n+1}-1)(r+1)\neq 2^n(2r-p-q)$, substituting (r+1) for (p+1)(q+1) and substituting 2r-p-q for pq+r (since $r+1=(p+1)(q+1)=pq+p+q+1$. Then

$$2^{n+1}r+2^{n+1}-r-1\neq 2^{n+1}r-2^np-2^nq$$

So, $2^{n+1}-(r+1)\neq -2^np-2^nq$. Re-substituting (p+1)(q+1) for (r+1) and dividing by -1 gives us

$$(p+1)(q+1)-2^{n+1}\neq 2^n(p+q).$$

So, $(p+1)(q+1)-2^{n+1}-2^n(p+q)\neq 0$. Substituting our original values for p and q aids us in simplifying the left side of this inequality as follows:

$$\begin{aligned}
&(p+1)(q+1)-2^{n+1}-2^n(p+q)\\
&=(2^m(2^{n-m}+1))(2^n(2^{n-m}+1))-2^{n+1}-2^n(2^m(2^{n-m}+1)+2^n(2^{n-m}+1)-2)\\
&=(2^n+2^m)(2^{2n-m}+2^n)-2^{n+1}-2^n(2^n+2^m+2^{2n-m}+2^n-2)\\
&=2^{3n-m}+2^{2n}+2^{2n}+2^{n+m}-2^{n+1}-2^{2n}-2^{n+m}-2^{3n-m}-2^{2n}+2^{n+1}\\
&=0
\end{aligned}$$

So $(p+1)(q+1)-2^{n+1}-2^n(p+q)=0$, which is a contradiction. So $\sigma(2^npq)$ must equal $2^n(pq+r)$. But, $\sigma(2^npq)=(2^{n+1}-1)(p+1)(q+1)= (2^{n+1}-1)(r+1)=\sigma(2^nr)$. So $\sigma(2^nr)$ must equal $2^n(pq+r)$, as well. Then, $\{2^npq, 2^nm\}$ is a pair of amicable numbers.

While Euler's Rule does not help us find all possible amicable numbers (for instance, the pair {1184, 1210}, which was found by a sixteen year old Italian boy 83 years after Euler's death, is not of this form) and though it does not produce a pair for every m and n, it does provide us with a reliable way of finding some amicable pairs. Also, if one were able to prove there are infinitely many prime triplets p, q, and r of the form $p=2^m(2^{n-m}+1)-1$, $q=2^n(2^{n-m}+1)-1$, and $r=2^{n+m}(2^{n-m}+1)^2-1$, then they will have proven the existence of infinitely many amicable numbers.

5. Perfect Numbers

We will continue with a short discussion about integers which form an amicable pair with themselves. In a previous example, we showed that 6 is the smallest perfect number. In fact, there are only 4 perfect numbers less than 10000: 6, 28, 496, and 8128. Note that, if a number n is a perfect number, then $\sigma(n)-n=n$. Then, $\sigma(n)=2n$. We proceed with a few proofs involving perfect numbers.

Theorem 4 - If 2^k-1 is prime for k greater than 1, then $2^{k-1}(2^k-1)$ is perfect and every even perfect number is of this form.

Proof: Suppose 2^k-1 is prime. Then

$$\sigma(2^{k-1}(2^k-1))= \sigma(2^{k-1})\sigma(2^k-1), \text{ because } 2^{k-1} \text{ and } 2^k-1 \text{ are relatively prime.}$$

So,

$$\sigma(2^{k-1}(2^k-1))=(2^k-1)(2^k), \text{ by Lemmas II \& III.}$$

But,

$$(2^k-1)(2^k)=2*(2^{k-1}(2^k-1)).$$

So, setting $2^{k-1}(2^k-1)=n$, $\sigma(n)=2n$. So $n=2^{k-1}(2^k-1)$ is a perfect number.

Moreover, suppose n is an even perfect number. Then $n=2^{k-1}m$ for k greater than or equal to 2, with m being odd. Then,

$\sigma(2^{k-1}m)=\sigma(2^{k-1})\sigma(m)=(2^k-1)\sigma(m)$, by Lemmas I and III.

But, $2^{k-1}m$ is perfect. So, $\sigma(2^{k-1}m)=2(2^{k-1}m)=2^km$. Then, $(2^k-1)\sigma(m)=2^km$. Then, $2^k-1|2^km$. So, $2^k-1|2^k$ or $2^k-1|m$. But, since the only prime factor of 2^k is 2 and 2^k-1 is odd, 2^k and 2^k-1 are relatively prime. So $^{2k-1}$ cannot divide 2^k. So, $2^{k-1}|m$. Then, $m=(2^{k-1})z$ for $z \in \mathbf{Z}$. Then, since $(2^k-1)\sigma(m)=2^km$,

$$(2^k-1)\sigma(m)=2^k(2^{k-1})z.$$

Then,

$$\sigma(m)=2^kz.$$

Note that, m and z are unequal divisors of m. Then

$$2^kz=\sigma(m)\geq m+z=(2^k-1)z+z=2^kz.$$

Then, $\sigma(m)=m+z$. Then, by the definition of σ, m has only two divisors, m and z. Then $z=1$, and m is prime. So, since $m=(2^k-1)z$, $m=2^k-1$. So $n=2^{k-1}(2^k-1)$ for a prime 2^k-1, thus completing our proof that every even perfect number is of this form. We will use the second part of this proof shortly. First, however, we must prove the following.

Theorem 5 - If a^k-1 is prime for a positive integer *a* and an integer *k* greater than or equal to 2, then a=2 and k is prime.

Proof: Note that $a^k-1=(a-1)(a^{k-1}+a^{k-2}+\ldots+a+1)$. Furthermore,

$$a^{k-1}+a^{k-2}+\ldots+a+1>a+1>1.$$

So, because a^k-1 is prime, and we know it has a factor $a^{k-1}+a^{k-2}+\ldots+a+1>1$, it must be that $a^k-1=a^{k-1}+a^{k-2}+\ldots+a+1$ and that a-1,the other factor of a^k-1, equals 1. So a=2.

Suppose k is a composite. Then, $a^k-1=a^{rs}-1$ for integers r and s, both greater than 1.

But, $a^{rs}-1=(a^r-1)(a^{r(s-1)}+a^{r(s-2)}+\ldots a^r+1)$. Then, since a=2, both of these factors are greater than 1. Then, $a^{rs}-1$ is not prime. Then a^k-1 is not prime. This is a contradiction. So k is not a composite, and k is greater than or equal to 2. So k is prime.

Using the previous two proofs, we will prove the following:

Theorem 6 - If n is an even perfect number, then the last digit of n is either 6 or 8.

Proof: Suppose n is an even perfect number. Then, by Theorem 4, $n=2^{k-1}(2^k-1)$ for some prime 2^k-1. Then, by Theorem 5, k is prime. Then k=2 or k is congruent to either 1 or 3 mod 4.

Suppose k=2. Then n=2*3=6.

Suppose $k\equiv 1 \pmod 4$. Then k=4x+1 for an integer x. Then,

$$n=2^{4x}(2^{4x+1}-1)$$
$$=2^{8x+1}-2^{4x}$$
$$=2*2^{8x}-2^{4x}$$
$$=2*16^{2x}-16^x$$
$$\equiv 2*6^{2x}-6^x \pmod{10}$$
$$\equiv 2*6-6 \pmod{10}$$

since the product of any two numbers congruent to 6 mod 10 is congruent to 6 mod 10, as well. Then,

$$\equiv 12-6\equiv 6 \pmod{10}.$$

So, if $k\equiv 1 \pmod 4$, $n\equiv 6 \pmod{10}$ (i.e. the last digit of n is 6).

Suppose $k\equiv 3 \pmod 4$. Then k=4x+3 for an integer x. Then,

$$n=2^{4x+2}(2^{4x+3}-1)$$

$=2^{8x+5}-2^{4x+2}$

$=2*2^{8x+4}-4*2^{4x}$

$=2*16^{2x+1}-4*16^{x}$

By the same argument from before, this is congruent to

$\equiv 2*6-4*6 \pmod{10}$

$\equiv -12 \pmod{10} \equiv 8 \pmod{10}$.

So, if $k \equiv 3 \bmod 4$, $n \equiv 8 \bmod 10$ (i.e. the last digit of n is 8). Thus, if n is an even perfect number, n ends in the digit 6 or 8.

6. Applications of Amicable Numbers

Though they have been studied for nearly one and a half millennia, there are, as of the present, no significant practical applications for amicable numbers, other than recreational mathematics. However, most of what is now a part of the field of mathematics was spawned out of the study of certain numbers with specific properties. What's more, the fact that amicable numbers are an application of factorization may naturally lead to there use in the field of cryptography and the domain of unique factorization into primes. As much as any other discipline of number theory, the area of amicable numbers is ripe for a breakthrough discovery.

References

Information on Perfect Numbers

[1] D. Burton, *Elementary Number Theory,* 6th Edition, McGraw Hill Higher Education, New York 2007.

Historical Information, et al

[2] T. Andreescu. University of Illinois at Champaign. "Number Theory Trivia: Amicable Numbers." http://britton.disted.camosun.bc.ca/amicable.html

[3] C. Caldwell. University of Tennessee at Martin. "The Prime Glossary." http://primes.utm.edu/glossary/page.php?sort=AmicableNumber 1997.

[4] S. Gupta. "Amicable Numbers." http://www.shyamsundergupta.com/amicable.htm

[5] J. O'Connor and E. Robinson. University of St. Andrews (Scotland). http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Perfect_numbers.html December 2001

[6] E. Sandifer. "How Euler Did It: Amicable Numbers." http://www.maa.org/editorial/euler/How%20Euler%20Did%20It%2025%20amicable%20numbers.pdf November 2005.

[7] Weisstein, E. "Euler's Rule." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/EulersRule.html 2004.