2 Amicable Numbers

In this lecture we look a little more at perfect numbers and the closely related amicable and sociable numbers.

Perfect numbers were known to Euclid and were later studied by Mersenne the Monk whose name is associated with certain prime numbers and who also explored musical scales as we shall see in a later lecture.

Under the banner of amicable in the sense of Friendly, we also say a little about Fermat numbers and Fibonacci numbers; the latter in particular will crop up several times in later lectures.

Perfect numbers

We recall that a number whose factors (apart from the number itself) add up to the number is called a perfect number.

The first two perfect numbers are 6 and 28 since

$$1 + 2 + 3 = 6$$

$$1 + 2 + 4 + 7 + 14 = 28$$

Some mystical properties were attached to these perfect numbers – God made the world in 6 days and the Moon encircles the Earth in 28 days.

Two more were known in antiquity, namely

$$1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496$$

$$1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064 = 8128$$

The next perfect number was discovered in the 15th century but the author seems to be unknown. It is quite a big jump, namely

$$33{,}550{,}336$$

The factors of these perfect numbers are interesting, they are

$$6 = 2\times3$$
$$28 = 2^2\times7$$
$$496 = 2^4\times31$$
$$8128 = 2^6\times127$$
$$33{,}550{,}336 = 2^{12}\times8191$$

J. Barnes, *Nice Numbers*, DOI 10.1007/978-3-319-46831-0_2

We see a pattern emerging. The factors of these perfect numbers all comprise lots of powers of two and one other prime number. Moreover, this other prime number is itself one less than a power of 2. So we have

$6 = 2^1 \times (2^2–1)$
$28 = 2^2 \times (2^3–1)$
$496 = 2^4 \times (2^5–1)$
$8128 = 2^6 \times (2^7–1)$
$33{,}550{,}336 = 2^{12} \times (2^{13}–1)$

So these perfect numbers all have the form $2^{k–1} \times (2^k–1)$. But note that not every number of this form is perfect. It never works if k is even. For example taking $k = 4$ we get $8 \times 15 = 120$ and this is certainly not perfect.

Euclid showed that if $2^k–1$ is a prime number then $2^{k–1} \times (2^k–1)$ is always a perfect number. His proof is Proposition 36 in Book IX of the Elements. But as in the case of showing that primes go on for ever, his discussion is geometrical and very difficult to follow.

Before describing a modern proof it is useful to introduce some algebraic notation. We will denote the sum of all the factors of n by $\sigma(n)$. This includes n itself. Note therefore that $\sigma(n) = s(n) + n$ where $s(n)$ is the sum of all the factors except n itself as introduced in the previous lecture.

So a number is perfect if

$\sigma(n) = 2n$ rule for n to be perfect

A very useful fact is that if two numbers m and n have no common factors (we say they are relatively prime or coprime) then

$\sigma(m \times n) = \sigma(m) \times \sigma(n)$ provided m and n have no common factors

Functions having this property are known as multiplicative functions. We will meet another example in the final lecture.

We can try this multiplicative property on an example. Consider 3, 4, and 12. Now 3 and 4 have no common factors and

$\sigma(3) = 1 + 3 = 4$
$\sigma(4) = 1 + 2 + 4 = 7$
$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28 = 4 \times 7$

So it works. It is not difficult to see why this is the case. Consider writing

$(1 + 3) \times (1 + 2 + 4)$

then every factor of 12 is obtained by taking one item from the first term and one item from the second term. Thus 6 is obtained by taking the 3 from the first term and the 2 from the second. But it only works if the two numbers have no common factors because otherwise we get duplication.

Now to return to Euclid's proposition. We have

$$\sigma(2^{k-1}) = 1 + 2 + 4 + \cdots + 2^{k-1} = 2^k - 1$$
$$\sigma(2^k - 1) = 1 + 2^k - 1 = 2^k$$

The first is because we are just adding up the powers of 2 such as $1 + 2 + 4 = 7$. The second is because we are assuming that $2^k - 1$ is prime and so its only factors are 1 and itself. Moreover, since $2^k - 1$ is prime it has no factors in common with 2^{k-1} and so we can apply the multiplication rule that $\sigma(m \times n) = \sigma(m) \times \sigma(n)$ to these two expressions. We get

$$\sigma(2^{k-1} \times (2^k - 1)) = \sigma(2^{k-1}) \times \sigma(2^k - 1) = (2^k - 1) \times 2^k$$

Now the expression on the right is simply twice that following σ on the left which is precisely the condition for being perfect. So we are done.

A further important fact is that not only are all numbers of Euclid's form perfect but all even perfect numbers are of that form which is perhaps surprising. This was shown by Euler about 2000 years later. The somewhat tricky proof is roughly as follows.

First we extract all the powers of two so that the perfect number n has the form $2^{k-1} \times m$ where m is odd. As a consequence m has no factors in common with 2^{k-1} and so the multiplication rule can be applied. We get

$$\sigma(n) = \sigma(2^{k-1}) \times \sigma(m) = (2^k - 1) \times \sigma(m)$$

On the other hand since we are given that n is a perfect number we know that $\sigma(n) = 2n = 2^k \times m$. Equating these two expressions for $\sigma(n)$ we get

$$(2^k - 1) \times \sigma(m) = 2^k \times m$$

It follows that $2^k - 1$ must be a factor of m since it has to be a factor of the right hand side and it is obviously not a factor of 2^k (it is odd for one thing). So m must be of the form

$$m = (2^k - 1) \times M$$

Putting this expression for m in the previous equation and cancelling the factor of $2^k - 1$ gives

$$\sigma(m) = 2^k \times M = 2^k \times M - M + M = (2^k - 1)M + M = m + M$$

Now we know that M is a factor of m and moreover m is a factor of m. Therefore $\sigma(m)$ must be at least $m+M$. But since $\sigma(m)$ is exactly $m+M$ there can be no other factors. However, 1 must be a factor and so we conclude that M must be 1 and that m must be prime. That's it. Indeed, it is a somewhat crafty proof!

We have just shown that all even perfect numbers must be of the form

$$n = 2^{k-1} \times (2^k - 1) \text{ where } 2^k - 1 \text{ is prime}$$

What about odd perfect numbers? No odd perfect numbers are known but it has not been proved that there are none. But it seems unlikely. If there are odd perfect numbers then they must be extremely large.

In the search for perfect numbers it was thought for some time that if p were prime then 2^p-1 would be prime as well. It certainly works to start with and gives the first four perfect numbers. Thus

$$2^2-1 = 3$$
$$2^3-1 = 7$$
$$2^5-1 = 31$$
$$2^7-1 = 127$$

and these are all prime. But it is not true for 11 since

$$2^{11}-1 = 2047 = 23 \times 89$$

However, $2^{13}-1 = 8191$ is prime and so the fifth perfect number is $2^{12} \times (2^{13}-1)$ which is 33,550,336 as mentioned earlier.

Modular arithmetic

BEFORE DIVING into perfect numbers in more detail it is helpful to introduce the idea of modular arithmetic. A good example occurs with using a clock (in 12 hour notation).

If the time is 8 o'clock, then what is the time 7 hours later? It is 3 o'clock. And if the time now is 11 o'clock then what is the time 15 hours later? It is 2 o'clock. We throw away multiples of 12 whenever they occur. The numbers just go around in cycles.

We can do this modulo any integer greater than 1. For example we could be working modulo 8 in which case if we add 7 to 5 we get 4. That is because 7 + 5 gives 12 and then we subtract 8 to give 4. We can write this as

$$7 + 5 \equiv 4 \pmod 8$$

We do the same with other operations such as multiplication. Thus since 7 times 5 equals 35 and $35 = 4\times8 + 3$, we have

$$7 \times 5 \equiv 3 \pmod 8$$

We read such statements as "7 times 5 is congruent to 3 mod 8". Note the special symbol ≡ rather than the normal = which is used to distinguish congruence from normal equality.

The key definition is

$a \equiv b \pmod m$ means $a-b$ is exactly divisible by m

It is easy to show various simple consequences, such as

$$a \equiv b \pmod{m} \quad \text{implies} \quad b \equiv a \pmod{m}$$

$$a \equiv b \pmod{m} \quad \text{and} \quad b \equiv c \pmod{m} \quad \text{implies} \quad a \equiv c \pmod{m}$$

The congruency property is preserved by addition, subtraction, and multiplication. So if

$$a \equiv b \pmod{m} \quad \text{and} \quad c \equiv d \pmod{m}$$

then it follows that

$$a + c \equiv b + d \pmod{m}$$

$$a - c \equiv b - d \pmod{m}$$

$$a \times c \equiv b \times d \pmod{m}$$

$$a^n \equiv b^n \pmod{m}$$

But it does not hold for division. For example 3 is congruent to 13 modulo 10 but dividing 12 by 3 and 13 gives different results thus

$$12 \div 3 = 4 \text{ rem } 0 \qquad \text{but} \qquad 12 \div 13 = 0 \text{ rem } 12$$

and neither quotient nor remainder are congruent modulo 10.

However, if $a \equiv b \pmod{m}$ and d is a divisor of m then it follows that $a \equiv b \pmod{d}$. For example, since $25 \equiv 15 \bmod 10$, it follows that $25 \equiv 15 \bmod 5$ and also that $25 \equiv 15 \bmod 2$.

Moreover, if a and m are relatively prime (and so have no common factors) and $ab \equiv ac \pmod{m}$ then we can cancel the a and deduce that $b \equiv c \pmod{m}$.

Also, although division does not preserve congruency in general, a always has an inverse modulo m if a and m are relatively prime, that is we can always find b such that $a \times b \equiv 1 \pmod{m}$. For example, 3 and 7 have no common factors and $3 \times 5 \equiv 1 \pmod{7}$ so that 5 is the "inverse" of 3. This will be proved and used in the final lecture when we discuss cryptography.

Mersenne the monk

THE FRENCH MONK Father Merin Mersenne (1588–1648) was also a famous mathematician. Among many topics he studied numbers of the form

$$M_n = 2^n - 1$$

which are now called Mersenne numbers. If a Mersenne number is prime then it is called a Mersenne prime. Note that it can be proved that if a Mersenne number

M_n is prime then n must be a prime (see the end of this section). But the reverse does not hold since we saw above that M_{11} is not prime.

We have seen that all even perfect numbers are of the form

$$2^{k-1} \times (2^k - 1) \text{ where } (2^k - 1) \text{ is prime}$$

and all numbers of this form are perfect.

In other words all perfect numbers are associated with a Mersenne prime and vice versa. Mersenne asserted that M_p was prime for the following values of p: 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. Why he stated this is not known. It was only in 1947 that it was confirmed that he was wrong. The cases of p = 61, 89, and 107 are also prime but 67 and 257 are not.

There is an interesting test for whether a Mersenne number is in fact a prime which was devised by Lucas and Lehmer. The theory was developed by the French teacher Edouard Lucas (1842–1891) and a simple test was devised by the American mathematician Derrick Lehmer (1905–1991). The test goes as follows. We form the series of numbers

$$L_{i+1} = (L_i)^2 - 2, \text{ starting with } L_2 = 4$$

and then M_p is prime if and only if L_p is exactly divisible by M_p. (Some texts define L_0 as 4 and then the test is that M_p is prime if and only if L_{p-2} is exactly divisible by M_p but the difference of 2 is confusing so we have omitted it.)

Let's try this on M_3 and M_5. The first few Ls are

$$L_2 = 4$$
$$L_3 = L_2^2 - 2 = 16 - 2 = 14$$
$$L_4 = L_3^2 - 2 = 14^2 - 2 = 196 - 2 = 194$$
$$L_5 = L_4^2 - 2 = 194^2 - 2 = 37636 - 2 = 37634$$

Now $M_3 = 2^3 - 1 = 7$. Is $L_3 = 14$ divisible by 7? Yes, so M_3 is prime. And from this we get 28 is perfect.

Similarly $M_5 = 2^5 - 1 = 31$. Is $L_5 = 37634$ divisible by 31? Yes it is ($37634 = 31 \times 1214$) so M_5 is prime. And from this we get 496 is perfect.

The numbers rapidly get very large indeed

$$L_6 = L_5^2 - 2 = 37634^2 - 2 = 1416317956 - 2 = 1{,}416{,}317{,}954$$
$$L_7 = L_6^2 - 2 = 1416317954^2 - 2 = 2{,}005{,}956{,}546{,}822{,}746{,}114$$

Now $M_7 = 2^7 - 1 = 127$. Is L_7 divisible by 127? Yes it is since we have

$$L_7 = 2{,}005{,}956{,}546{,}822{,}746{,}114 = 127 \times 15{,}794{,}933{,}439{,}549{,}182$$

and so $M_7 = 127$ is prime. This gives 8128 is perfect.

The next Mersenne number to try is $M_{11} = 2047$. As we saw earlier this is 23×89 and so is not prime. And this is confirmed by the Lucas–Lehmer test. We have

L_{11} =
68,729,682,406,644,277,238,837,486,231,747,530,924,247,154,108,
646,671,752,192,618,583,088,487,405,790,957,964,732,883,069,102,
561,043,436,779,663,935,595,172,042,357,306,594,916,344,606,074,
564,712,868,078,287,608,055,203,024,658,359,439,017,580,883,910,
978,666,185,875,717,415,541,084,494,926,500,475,167,381,168,505,
927,378,181,899,753,839,260,609,452,265,365,274,850,901,879,881,
203,714

and this equals 2047 times

33,575,809,675,937,604,904,170,730,938,811,690,729,969,298,538,
664,715,071,906,506,391,347,575,674,543,701,985,702,434,327,846,
878,868,313,033,543,691,057,729,380,731,463,895,904,418,469,015,
419,986,745,519,437,033,734,832,938,279,608,910,120,948,160,191,
000,813,964,765,860,974,861,301,658,488,764,277,072,487,136,544,
175,563,352,173,792,789,086,765,731,443,754,408,818,222,706,341,
574

plus a remainder of 1736. So since there is a remainder this confirms that M_{11} = 2047 is not prime.

The numbers are getting a bit large now. For M_{13} = 8191 we find that

L_{13} =
22,313,995,867,897,900,769,603,796,342,295,788,566,208,710,409,
165,129,831,038,160,968,311,491,946,220,319,893,407,703,857,721,
437,957,260,314,978,754,160,034,503,401,040,789,215,400,628,158,
170,099,668,522,698,066,550,221,265,307,171,574,634,992,724,727,
060,201,120,758,890,920,172,789,110,609,085,990,337,846,018,634,
451,646,739,004,908,975,710,893,057,017,831,784,106,285,989,578,
600,398,251,364,366,079,398,506,512,806,386,775,247,318,462,388,
007,386,288,293,644,987,819,640,076,171,556,974,003,404,195,908,
596,970,825,853,990,347,990,259,288,695,088,334,854,125,701,652,
040,860,084,239,663,064,263,605,520,384,355,127,215,307,437,936,
591,866,962,296,906,419,378,104,850,899,571,605,034,504,288,737,
636,564,836,267,334,726,723,727,575,106,663,971,046,844,142,763,
512,854,023,937,849,655,467,693,015,631,287,929,701,909,077,381,
005,060,802,853,209,341,459,156,871,829,180,256,316,747,660,704,
875,518,660,035,573,112,882,904,493,746,617,877,304,844,878,674,
402,542,586,943,400,547,464,667,179,926,000,026,596,616,252,849,
884,072,241,228,637,895,801,783,293,732,168,802,374,542,280,341,
992,348,946,606,531,635,000,814,995,246,895,089,041,641,203,184,
136,132,975,956,905,572,518,723,976,402,989,858,509,003,359,081,
748,048,869,560,319,466,898,146,867,908,972,088,453,016,102,089,
761,833,396,052,479,183,215,782,590,173,494,080,725,569,259,056,

977,955,738,902,892,341,951,393,866,495,222,420,379,013,713,784,
627,095,469,233,910,359,313,068,881,745,808,900,306,832,764,925,
725,008,680,492,006,161,979,334,986,865,505,218,272,485,914,888,
669,136,966,553,469,714,434

and clearly this exactly equals 8191 times

2,724,208,993,761,189,203,956,024,458,832,351,186,205,434,062,
894,045,883,413,278,106,252,166,029,327,349,516,958,576,957,358,
251,490,326,005,979,581,755,589,610,963,379,415,116,029,865,481,
402,771,293,922,927,367,421,587,262,276,543,959,789,402,115,093,
036,283,862,868,867,161,539,835,076,377,620,069,629,818,827,815,
218,123,152,118,777,801,942,484,807,351,706,969,125,416,431,397,
704,846,569,572,013,927,407,948,542,645,145,498,137,873,087,826,
639,895,774,422,371,503,823,665,007,468,142,714,443,096,593,322,
988,276,257,581,979,043,827,403,160,626,918,365,871,581,699,627,
889,251,627,913,522,532,567,892,262,285,966,930,437,713,031,123,
988,751,918,239,153,512,315,725,167,976,995,678,798,010,534,579,
127,892,178,765,393,081,030,854,300,464,737,391,166,749,376,481,
932,957,395,182,254,871,867,622,148,166,437,300,659,493,233,717,
617,514,443,029,326,009,212,447,426,666,973,538,800,726,121,438,
759,067,105,363,883,910,741,411,853,710,977,643,426,302,634,437,
114,215,918,318,080,887,249,989,888,893,419,610,132,659,779,373,
688,691,520,110,931,253,302,622,792,544,520,669,316,877,338,584,
054,736,777,756,871,155,536,664,020,906,714,087,296,012,843,753,
404,484,553,284,935,364,731,867,168,404,711,251,191,430,027,967,
494,573,174,161,923,997,912,116,575,254,422,181,473,936,772,322,
031,721,816,146,072,418,900,718,177,288,913,939,778,484,832,017,
699,664,966,292,625,118,050,469,279,269,347,139,589,673,265,020,
708,960,501,676,707,405,605,306,907,794,629,337,114,739,685,621,
502,259,636,246,124,546,695,072,028,673,605,813,487,057,247,575,
225,141,858,937,061,374

and as a consequence we confirm that 8191 is prime and this gives rise to the fifth perfect number which as we have seen is 33,550,336.

Actually we don't have to work with such huge numbers since for example if we want to know whether L_5 is divisible by M_5 (= 31) we can keep taking the remainder on dividing by M_5 at each stage. In other words we work entirely using modular arithmetic with modulo 31 as explained in the previous section. The calculation for M_5 then goes

$L_2 = 4$
$L_3 = L_2^2 - 2 = 16 - 2 = 14$
$L_4 = L_3^2 - 2 = 196 - 2 = 194 \equiv 8 \bmod 31$
$L_5 = L_4^2 - 2 = 64 - 2 = 62$

and of course 62 is divisible by 31. Note carefully that we now get a different sequence of Ls according to the value of M_p. Thus for M_7 (= 127) we need to compute L_7 using modulo 127. We get

$$L_2 = 4$$
$$L_3 = L_2^2 - 2 = 16 - 2 = 14$$
$$L_4 = L_3^2 - 2 = 14^2 - 2 = 196 - 2 = 194 \equiv 67 \bmod 127$$
$$L_5 = L_4^2 - 2 = 67^2 - 2 = 4489 - 2 = 4487 \equiv 42 \bmod 127$$
$$L_6 = L_5^2 - 2 = 42^2 - 2 = 1764 - 2 = 1762 \equiv 111 \bmod 127$$
$$L_7 = L_6^2 - 2 = 111^2 - 2 = 12321 - 2 = 12319 = 97 \times 127$$

Again L_7 divides exactly by 127 showing that M_7 is prime but we don't have to deal with such horrendous large numbers as before.

In the same way we can show that M_{11} (= 2047) is not prime. We work modulo 2047 and get

$$L_2 = 4$$
$$L_3 = L_2^2 - 2 = 16 - 2 = 14$$
$$L_4 = L_3^2 - 2 = 14^2 - 2 = 196 - 2 = 194$$
$$L_5 = L_4^2 - 2 = 194^2 - 2 = 37636 - 2 = 37634 \equiv 788 \bmod 2047$$
$$L_6 = L_5^2 - 2 = 788^2 - 2 = 620944 - 2 = 620942 \equiv 701 \bmod 2047$$
$$L_7 = L_6^2 - 2 = 701^2 - 2 = 491401 - 2 = 491399 \equiv 119 \bmod 2047$$
$$L_8 = L_7^2 - 2 = 119^2 - 2 = 14161 - 2 = 14159 \equiv 1877 \bmod 2047$$
$$L_9 = L_8^2 - 2 = 1877^2 - 2 = 3523129 - 2 = 3523127 \equiv 240 \bmod 2047$$
$$L_{10} = L_9^2 - 2 = 240^2 - 2 = 57600 - 2 = 57598 \equiv 282 \bmod 2047$$
$$L_{11} = L_{10}^2 - 2 = 282^2 - 2 = 79524 - 2 = 79522 \equiv 1736 \bmod 2047$$

So we get a remainder of 1736 (luckily the same as when we did it the hard way) and this confirms that 2047 is not prime.

The next Mersenne primes are $M_{13} = 2^{13}-1 = 8191$, $M_{17} = 2^{17}-1 = 131{,}071$ and $M_{19} = 2^{19}-1 = 524{,}287$.

The largest prime number that Mersenne himself correctly predicted was M_{127}. Its value is

$$M_{127} = 170{,}141{,}183{,}460{,}469{,}231{,}731{,}687{,}303{,}715{,}884{,}105{,}727$$

and the corresponding perfect number (the twelfth) is

$$14{,}474{,}011{,}154{,}664{,}524{,}427{,}946{,}373{,}126{,}085{,}988{,}481{,}573{,}677{,}491{,}$$
$$474{,}835{,}889{,}066{,}354{,}349{,}131{,}199{,}152{,}128$$

M_{127} was the largest known prime from its discovery in 1876 by Lucas (confirmation really, since Mersenne predicted it two centuries earlier) until in 1952 (using a computer of course) it was shown that M_{521} was prime. It was quite a big jump since it has nearly four times as many digits as M_{127}.

It has almost always been the case throughout history that the largest known prime is a Mersenne prime. It is easy to see why. The problem with large primes is proving that they are prime. But we have the totally reliable Lucas–Lehmer test in the case of Mersenne numbers and this is easy to apply using modern fast computers.

Sometimes we might know that a number is not prime but yet not know its factors. Thus Lucas showed that M_{67} was not prime in 1876 but the factors were only discovered by the American mathematician Frederick Nelson Cole (1861–1927) in 1903. Cole astounded a meeting of the American Mathematical Society by giving a lecture in which he simply by hand and in silence on one blackboard worked out

$$2^{67}-1 = 147,573,952,589,676,412,927$$

and then on another board worked out

$$193,707,721 \times 761,838,257,287$$

They were the same. Note that both factors are themselves prime.

What is the point in finding large primes? Until recently it was just for fun like climbing Mt Everest. But now they are used in cryptography as we shall discuss in the last lecture.

Since 1952 many more Mersenne primes have been discovered. At the time of writing the largest known prime number is the 49th known Mersenne prime which was discovered in January 2016. It is $M_{74207281}$ and has 22,338,618 digits. Note that we have to say 49th *known* Mersenne prime since there may be other smaller Mersenne primes that have not yet been discovered. The corresponding 49th known perfect number has twice as many digits.

A little fact that the reader is invited to prove is that the remainder on dividing any perfect number by 3 is always 1 and never 2. This does not apply to the first perfect number which is 6. But it does apply to all the others.

Here is a simple proof that if M_n is prime then n must be prime as well. We use the technique known as *Reductio ad Absurdum* in which we make an assumption and then deduce a contradiction thereby showing that the assumption was false.

Suppose that M_n is prime and that n is not prime but equal to st. Then

$$M_n = 2^n-1 = 2^{st}-1 = (2^s)^t-1$$

Now consider the following giant expression

$$E = (2^s-1)\{\ (2^s)^{t-1} + (2^s)^{t-2} + (2^s)^{t-3} + (2^s)^{t-4} + \cdots + (2^s)^2 + (2^s) + 1\ \}$$

If we multiply it out we get

$$E = (2^s)^t + (2^s)^{t-1} + (2^s)^{t-2} + (2^s)^{t-3} + \cdots + (2^s)^3 + (2^s)^2 + (2^s) \\ - (2^s)^{t-1} - (2^s)^{t-2} - (2^s)^{t-3} - (2^s)^{t-4} - \cdots - (2^s)^2 - (2^s) - 1$$

$$= (2^s)^t - 1$$

Note how almost all terms cancel in pairs leaving just $(2^s)^t-1$ which of course is 2^n-1 and so E is in fact M_n. However, by construction E is divisible by 2^s-1 and so M_n is not prime. This is a contradiction so n must have been prime.

Amicable numbers

AT LAST we get to the real subject matter of this lecture. An amicable pair of numbers are two numbers, each of which equals the sum of the factors of the other. The smallest pair are 220 and 284. We have

$220 = 2^2.5.11$
$284 = 2^2.71$

The factors of 220 are therefore

1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110 which add to 284

and the factors of 284 are

1, 2, 4, 71, 142 which add to 220.

We can think of perfect numbers as being amicable with themselves (sounds somewhat introvert).

We recall that defining $\sigma(n)$ to be the sum of the factors of n including n itself then we have the rule that if m and n have no common factors (that is are relatively prime or coprime to each other) then

$$\sigma(m \times n) = \sigma(m) \times \sigma(n)$$

This is useful for working out the sum of factors since we can apply it several times; thus the sum of the factors of 220 is

$$\sigma(220) = \sigma(2^2).\sigma(5).\sigma(11) = (2^3-1).(5+1).(11+1) = 7.6.12 = 504$$

and the sum of the factors of 284 is

$$\sigma(284) = \sigma(2^2).\sigma(71) = (2^3-1).(71+1) = 7.72 = 504$$

(Remember that we often use . rather than × for multiplication in order to save space.)

We see therefore that we can also define an amicable pair of numbers as a pair m and n such that

$$\sigma(m) = \sigma(n) = m + n$$

Pairs of amicable numbers are much more common than perfect numbers. There are no more before we get to 496 which is the next perfect number but then there are four pairs before the next perfect number after that which is 8128. They are (with prime factors in brackets)

1184 (2^5.37) and 1210 (2.5.11^2)
2620 (2^2.5.131) and 2924 (2^2.17.43)
5020 (2^2.5.251) and 5564 (2^2.13.107)
6232 (2^3.19.41) and 6368 (2^5.199)

Unlike the perfect numbers which all have the same form, the amicable numbers have an extraordinary range of factors with little discernable pattern.

The first pair (220; 284) was known to Pythagoras but curiously enough the next pair (1184; 1210) was only found as recently as 1866 by an Italian schoolboy, Nicolo Paganini. However, two other quite large pairs were known before the middle of the 17th century namely

17,296 (2^4.23.47) and 18,416 (2^4.1151)
9,363,584 (2^7.191.383) and 9,437,056 (2^7.73,727)

Amicable numbers are mysterious. In a sense we know all about even perfect numbers. We can generate them from the corresponding Mersenne primes and we have the Lucas–Lehmer test for these. And we suspect that there are no odd perfect numbers. On the other hand we have no known way of generating all amicable pairs.

Most amicable pairs are even. But some are odd, the smallest being

12,285 (3^3.5.7.13) and 14,595 (3.5.7.139)

Amicable pairs have factors of various forms. There are usually, but not always, many powers of 2, some small prime numbers and often one or more very large ones.

However, although amicable numbers often have very large primes, the sums of the pairs do not. Thus in the table opposite we see that the largest prime in the sums of the first twelve pairs is 31. But the largest prime in the pairs themselves is never less than 37.

The odd behaviour may be related to a characteristic known as smoothness. A number is smooth if it has only small prime factors. In particular we say that it is 7-smooth if it has no factors larger than 7 and so on. It seems that amicable numbers themselves are somewhat rough but their sums are smoother.

m	factors	n	factors	$m+n$	factors
220	$2^2.5.11$	284	$2^2.71$	504	$2^3.3^2.7$
1184	$2^5.37$	1210	$2.5.11^2$	2394	$2.3^2.7.19$
2620	$2^2.5.131$	2924	$2^2.17.43$	5544	$2^3.3^2.7.11$
5020	$2^2.5.51$	5564	$2^2.13.107$	10584	$2^3.3^3.7^2$
6232	$2^3.19.41$	6368	$2^5.199$	12600	$2^3.3^2.5^2.7$
10744	$2^3.17.79$	10856	$2^3.23.59$	21600	$2^5.3^3.5^2$
12285	$3^3.5.7.13$	14595	$3.5.7.139$	26880	$2^8.3.5.7$
17296	$2^4.23.37$	18416	$2^4.1151$	35712	$2^7.3^2.31$
63020	$2^2.5.23.137$	76084	$2^2.23.827$	139104	$2^5.3^3.7.23$
66928	$2^4.47.89$	66992	$2^4.53.79$	133920	$2^5.3^3.5.31$
67095	$3^3.5.7.71$	71145	$3^3.5.17.31$	138240	$2^{10}.3^3.5$
69615	$3^2.5.7.13.17$	87633	$3^2.7.13.107$	157248	$2^6.3^3.7.13$

The first dozen amicable pairs, their sum and factors.

Note that the sums are often a multiple of 126. Indeed the first five pairs add to multiples of 126 thus

$$220 + 284 = 504 = 126 \times 4$$
$$1184 + 1210 = 2394 = 126 \times 19$$
$$2620 + 2924 = 5544 = 126 \times 44$$
$$5020 + 5564 = 10584 = 126 \times 84$$
$$6232 + 6368 = 12600 = 126 \times 100$$

But it doesn't work for the next pair which are 10744 and 10856 since their sum is $21600 = 2^5.3^3.5^2$. Note that $126 = 7 \times 18$ and 7 is not a factor of 21600.

Another curious thing is that since perfect numbers can be seen as amicable with themselves one might think that double a perfect number might exhibit some degree of smoothness. But this is not so since a perfect number is always a power of 2 multiplied by a Mersenne prime and is decidedly rough.

Although we know no way of generating all amicable numbers, there are formulae that generate some pairs. The Arabic mathematician Thabit ibn Qurra (824–901) showed that if

$$p = 3.2^{n-1} - 1$$
$$q = 3.2^n - 1$$
$$r = 9.2^{2n-1} - 1$$

are all prime then the pair

$$M\,(2^n.p.q) \text{ and } N\,(2^n.r)$$

are always amicable.

It's quite amazing that Thabit discovered this so early. If we try $n = 2$, then $p = 5$, $q = 11$, $r = 71$ and these are all prime and this gives the first pair (220; 284).

The case $n = 4$ gives $p = 23$, $q = 47$, $r = 1151$ and thus the pair (17,296; 18,416). This was discovered in the early 14th century. The case $n = 7$ gives $p = 191$, $q = 383$, $r = 73{,}727$ and thus the pair (9,363,584; 9,437,056). This was discovered in the 17th century. Recently it has been shown by brute force that no other values of n less than 20,000 give amicable pairs.

Lots of things are not known about amicable pairs. For example, it is not known whether

any amicable pairs are relatively prime to each other,

any amicable pairs are one odd and one even,

any amicable pairs have only one divisible by 3,

any amicable pairs have all factors greater than 5.

But it is known that some odd amicable pairs are not divisible by 3. And it is known that even amicable pairs never have a factor of 3 (that's very strange).

Amicable multiplets

IN A SIMILAR WAY we can also define amicable triplets, amicable quadruplets and indeed amicable multiplets. By analogy with the formula

$$\sigma(m) = \sigma(n) = m + n$$

we can define an amicable triplet as three numbers l, m, n such that

$$\sigma(l) = \sigma(m) = \sigma(n) = l + m + n$$

There are many examples of such triplets such as

1980; 2016; 2556
9180; 9504; 11,556
21,168; 22,200; 27,312

We can similarly define amicable multiplets such as the quadruplet

554,130,720 ($2^5.3^3.5.11.13.23.29$),
444,169,440 ($2^5.3^3.5.11.13.719$),
481,546,080 ($2^5.3^3.5.17.79.83$),
491,153,760 ($2^5.3^3.5.41.47.59$)

Such multiplets up to order 7 are known.

Sociable cycles

ANOTHER GROUPING is to consider cycles. Is it possible to find a cycle of numbers such that each is the sum of the factors of the previous one and for the first to be the sum of the factors of the last? Yes it is and these are called sociable cycles. Amicable numbers are of course simply two-cycles and perfect numbers are one-cycles.

The history of sociable cycles is quite brief. The first two sociable cycles were discovered in 1910 by the Belgian mathematician Paul Poulet (1887–1946). They involve the smallest numbers of any sociable cycles. They are a 5-cycle and a 28-cycle. Thus the multiple cycle with the smallest numbers is the 5-cycle.

12,496; 14,288; 15,472; 14,536; 14,264; and then 12,496 again

and the next cycle is an amazing 28-cycle thus

14,316; 19,116; 31,704; 47,616; 83,328; 177,792; 295,488;
629,072; 589,786; 294,896; 358,336; 418,904; 366,556; 274,924;
275,444; 243,760; 376,736; 381,028; 285,778; 152,990; 122,410;
97,946; 48,976; 45,946; 22,976; 22,744; 19,916; 17,716

What is very surprising is that despite the 28-cycle being one of the first two sociable cycles ever discovered, no longer cycle or indeed any cycle half as long has been found in the more than 100 years that have followed.

Over a hundred 4-cycles are known, the first few are

1,264,460; 1,547,860; 1,727,636; 1,305,184
2,115,324; 3,317,740; 3,649,556; 2,797,612
2,784,580; 3,265,940; 3,707,572; 3,370,604
4,938,136; 5,753,864; 5,504,056; 5,423,384
7,169,104; 7,538,660; 8,292,568; 7,520,432

Although there are many 4-cycles, no 3-cycles are known, and it is thought, although it has not been proved, that maybe there are no 3-cycles.

At the time of writing, other cycles known are five 6-cycles, three 8-cycles and one 9-cycle. Their smallest numbers are

21,548,919,483	start of 6-cycle
90,632,826,380	start of 6-cycle
1,771,414,411,016	start of 6-cycle
3,524,434,872,392	start of 6-cycle
4,773,123,705,616	start of 6-cycle
1,095,447,416	start of 8-cycle
1,276,254,780	start of 8-cycle
7,914,374,573,864	start of 8-cycle
805,984,760	start of 9-cycle

Just as for amicable pairs all members of known cycles have the same parity – that is either they are all even or all odd. Most cycles are even but one of the 6-cycles is odd and several 4-cycles are odd.

The cycles are intriguing. Having found the 5-cycle and 28-cycle with fairly small numbers, one might expect lots of other cycles of many different lengths. It is disappointing therefore that most of the rest are 4-cycles. There is clearly scope for the reader to look for some others.

One thing that is different from amicable pairs is that whereas no even amicable pair ever has 3 as a factor, this does not apply to sociable cycles. Many of the numbers in the 28-cycle are divisible by 3 (such as $14316 = 2^2.3.1193$).

The fact that there are no 3-cycles is surprising but perhaps reflects the fact that two is company but three is a crowd.

Fermat numbers

PIERRE DE FERMAT (1601–1665) was a lawyer and magistrate and also a brilliant "amateur" mathematician. He didn't bother about winning fame but did mathematics for the fun of it. As a consequence some of his work has come down to us in a sketchy format. The most famous of course is his Last Theorem which says that the equation

$$x^n + y^n = z^n$$

where x, y, z, and n are integers does not have any solutions for n greater than 2. Of course if n is 2 then there are a host of solutions corresponding to Pythagoras such as $3^2 + 4^2 = 5^2$. Fermat claimed to have found a proof but that the margin of his paper was too small to give it. It was only proved very recently by Andrew Wiles in 1995.

Fermat was interested in numbers of the form

$$F_n = 2^{2^n} + 1$$

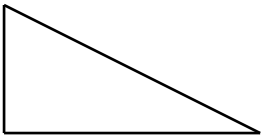
which are somewhat similar to the Mersenne numbers $M_n = 2^n - 1$ discussed earlier. In the case of the Fermat numbers the first few are

$$F_1 = 2^2+1 = 5,\ F_2 = 2^4+1 = 17,\ F_3 = 2^8+1 = 257,\ F_4 = 2^{16}+1 = 65{,}537$$

and these are all prime. Fermat accordingly conjectured that all Fermat numbers are prime. However, this is not the case, as was shown by Euler who found in 1732 that

$$F_5 = 2^{32} + 1 = 4{,}294{,}967{,}297 = 641 \times 6{,}700{,}417$$

Observe that 6,700,417 is indeed prime. It is believed although it has not been proved that all Fermat numbers after F_4 are composite.



A right-angled triangle with sides 1, 2, and √5.

An interesting fact regarding Fermat primes is that a regular polygon can be constructed using ruler and compasses alone if the number of its sides is a Fermat prime. So a 17-gon can in principle be constructed although measurement errors make it somewhat tricky.

The basic reason why the constructions can be done is that we have to solve an equation of degree F–1. In the case of the 17-gon we thus have to solve an equation of degree 16. It turns out that this can be done by solving a series of nested quadratic equations since $16 = 2^4$. The roots of a quadratic equation just involve square roots and these can be found by ruler and compasses alone.

In the case of a pentagon we need to find the square root of 5 and this is easily done since the hypotenuse of a right-angled triangle whose other sides are 1 and 2 is of course √5 using Pythagoras as shown above.

From this we can construct the Golden Number $\tau = (\sqrt{5} + 1)/2$. Now the diagonal of a pentagon of side 1 is simply $2\tau + 1$ and hence we can then construct the pentagon itself. See for example *Gems of Geometry* by the author.

In the case of the 17-gon we need to find the value of a nasty expression involving the square root of 17. See the references for details.

Fibonacci numbers

In 1202, Leonardo of Pisa (c 1175–1250) who was commonly called Fibonacci, meaning son of good fortune, produced a book entitled *Liber Abbaci*. One topic concerned the breeding of rabbits and in particular introduced a series of numbers now called Fibonacci numbers. It is a series in which each number is the sum of the previous two and the first two are both one. So the series begins

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

An important property of the series is that the ratios of successive pairs are closer and closer approximations to the golden number τ just mentioned in connection with Fermat numbers. The ratios are

1/1 = 1; 2/1 = 2; 3/2 = 1.5; 5/3 = 1.666...; 8/5 = 1.6; 13/8 = 1.625;

and so on.

The golden number τ is 1.618033989.... It has many neat properties such as

$$\tau - 1 = 1/\tau \quad \text{and} \quad \tau + 1 = \tau^2.$$

We will encounter the Fibonacci numbers again in Lecture 4 on Fractions when we discuss Egyptian fractions and continued fractions, and in Lecture 8 on Primes when we discuss the greatest common divisor. They also turn up in Appendix B and Appendix G. In particular, Appendix G gives an explicit formula for the *n*th member of the series.

Further reading

A COMPREHENSIVE BOOK on this topic is *Perfect, Amicable and Sociable Numbers* by Song Yan – this is not for the faint-hearted. Various websites are interesting. See for example http://mathworld.com/SociableNumbers.html. A list of all known cycles will be found at http://djm.cc/sociable.txt. The topic of smoothness is discussed at http://en.wikipedia.org/wiki/Smooth_number.

The Mersenne, Fermat, and Fibonacci numbers are discussed in *Elementary Number Theory* by David M Burton and also in *Elementary Number Theory and its Applications* by Kenneth E Rosen.

The construction of polygons with a Fermat prime number of sides is discussed in *Introduction to Geometry* by Coxeter and also in *Makers of Mathematics* by Hollingdale. Coxeter gives the explicit construction for the 17-gon and Hollingdale outlines the nasty process of solving the nested quadratic equations.

Exercises

1 Show that $12496 = 2^4.11.71$. Hence show that its factors (all of them, not just the prime ones) add to 14288. Then find the factors of 14288 (its largest prime factor is 47) and show that they add to 15472. And similarly show that the factors of 15472 (largest prime is 967) add to 14536 and that those of 14536 (largest prime 79) add to 14264. Finally, show that the factors of 14264 (largest prime 1783) add to 12496 thus completing the cycle of 5.

2 Show that the remainder on dividing an even perfect number (other than 6) by 3 is always 1.

http://www.springer.com/978-3-319-46830-3

Nice Numbers
Barnes, J.
2016, XIII, 329 p. 152 illus., 39 illus. in color., Hardcover
ISBN: 978-3-319-46830-3
A product of Birkhäuser Basel