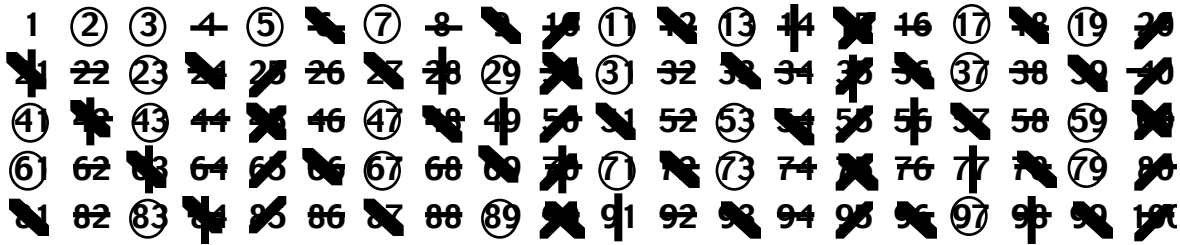


Prime Numbers

The study of prime numbers is as old as mathematics itself. This set of notes has a bunch of facts about primes, or related to primes. Much of this stuff is old--dating back 2-3000 years. We start with possibly the most important question about primes: how many are there?

We have an ancient method for calculating lists of primes, which is still unbelievable good. It is called the "Sieve of Eratosthenes." The idea is as follows: Form an array of numbers 1, 2, 3, Ignore 1 because it is a unit. Circle 2, and cross out every subsequent multiple of 2. Suppose that the last number in your array is n . Repeat the following until you circle a number greater than \sqrt{n} : Find the next number not crossed off, circle it, and cross off every subsequent multiple. Once a number greater than \sqrt{n} is circled, don't cross off any additional numbers, just circle the remaining numbers not crossed off, they will all be prime. For example, to find all primes less than 100 takes 4 steps:

1	②	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	②	③	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	②	③	4	⑤	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100



This algorithm is very fast. I've heard it said that if you are writing a program that makes use of all primes less than 1,000,000 it is faster to use the sieve of Eratosthenes than to read in a preexisting file of primes. One thing that makes the algorithm so fast is that we can stop sieving once we reach \sqrt{n} . The reason for this is the following theorem.

Theorem. If n is not prime, then n has a prime divisor $p \leq \sqrt{n}$.

Proof. Let n be composite and let q be a prime divisor of n . Then $n = q \cdot (n/q)$. If $q < \sqrt{n}$, let $p = q$. Otherwise, $n/q < \sqrt{n}$, so let p be a prime divisor of n/q .

As a consequence of this theorem, we have the following factoring technique: To factor a number n , try dividing n in turn by the primes 2, 3, 5, \dots . We continue until a prime gets larger than the square root of the unfactored part. For example, suppose we wish to factor 1286740. We divide by 2 until an odd number results: $1286740 = 2^2 \cdot 321685$. The unfactored part is not divisible by 3, but it is by 5, so we have $1286740 = 2^2 \cdot 5 \cdot 64337$. Continuing, we have $1286740 = 2^2 \cdot 5 \cdot 7^2 \cdot 1313 = 2^2 \cdot 5 \cdot 7^2 \cdot 13 \cdot 101$. Note that after dividing by 13 to leave an unfactored part of 101, we can stop because $101 < 13^2$. This means that 101 must be prime.

At this point, we have a good way to find all small primes, and a reasonable algorithm for factoring small numbers. We still have not answered the question of how many primes there are. Consider following table:

range	1-100	1000-1100	10^4 - 10^4+100	10^5 - 10^5+100	10^6	10^7
# of primes	25	16	11	6	6	2

This table gives the number of primes in ranges of 100 consecutive integers. Based on

the table, one might expect that the number of primes is finite and that there is some largest prime. However, this is not the case. The following is a result due to Euclid:

Theorem. There are infinitely many primes.

Proof. Suppose not, and let $\{2, 3, \dots, p_k\}$ be a complete list of primes. Let M be the number $M = 2 \cdot 3 \cdot \dots \cdot p_k + 1$. (M is one greater than the product of all primes.) When M is divided by 2 or 3 or \dots or p_k , the remainder will be 1. Thus, M is not divisible by any of the primes in our list. But M is divisible by some prime by the Fundamental Theorem of Arithmetic. This contradicts the assumption that our list was complete, which completes the proof of the theorem.

Given the first k primes, we can define the number $M_k = 2 \cdot 3 \cdot \dots \cdot p_k + 1$. The first several are $M_1 = 3$, $M_2 = 7$, $M_3 = 31$, $M_4 = 211$. These first ones are primes and it is a common conjecture by students that M_k is always prime. But this is not the case: $M_6 = 30031 = 59 \cdot 509$.

It turns out that primes are fairly common. We give a name to the number of primes up to some bound: $\pi(n)$ = the number of primes $\leq n$. for example, $\pi(100) = 25$ because there are 25 primes less than 100. In 1793 at the age of 15, Gauss made the following conjecture about how common prime numbers are:

$$\pi(x) \cong \int_2^x \frac{1}{\ln(t)} dt.$$

This integral has a name, it is called $\text{li}(x)$, the logarithmic integral. A bit over 100 years ago, in 1896, this conjecture was proved simultaneously by Hadamard and de la Vallée Poussin. The exact statement of the result is this:

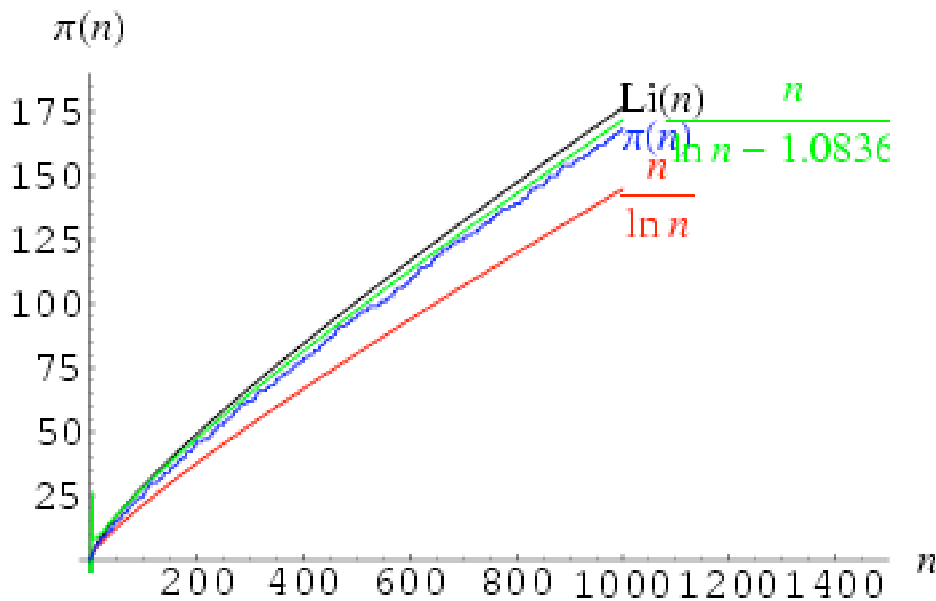
Theorem. (The **Prime Number Theorem**, or **PNT**) $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\text{li}(x)} = 1$.

The integral $\text{li}(x)$ can be approximated by the function $\frac{x}{\ln(x)}$, so usually, we say that

$\pi(x) \cong \frac{x}{\ln(x)}$. The following table gives a feel for the fit:

n	$\pi(n)$	$\frac{n}{\ln(n)}$	$\text{li}(n)$
1000	168	145	177
1,000,000	78,498	72,382	78,626
1,000,000,000	50,847,478	48,254,942	50,849,234

Here are some graphs to give another perspective. This graph came from <http://mathworld.wolfram.com/PrimeNumberTheorem.html>



Perfect Numbers

A number is called a **perfect number** if it equals the sum of its proper divisors. The first several perfect numbers are:

$$6 = 1 + 2 + 3,$$

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

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

$$8192 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064.$$

Based on the prime factorizations: $6 = 2 \cdot 3$, $28 = 2^2 \cdot 7$, $4096 = 2^4 \cdot 31$, $8192 = 2^6 \cdot 127$,

we might be lead to guess that perfect numbers always have the form $2^k p$ where p is a prime number. In fact, p cannot be any old prime number, it must have the form $2^n - 1$ for some n . Let $M(n) = 2^n - 1$. The numbers $M(n)$ are called **Mersenne numbers**. If $M(n)$ is a prime number, it is called a **Mersenne prime**.

Theorem. If $p = 2^n - 1$ is prime, then $m = 2^{n-1} p$ is a perfect number.

Proof: The factors of $2^{n-1} p$ are $1, 2, 4, \dots, 2^{n-1}, p, 2p, 4p, \dots, 2^{n-1} p$. The sum of the factors is $(1 + 2 + 4 + \dots + 2^{n-1}) + p(1 + 2 + 4 + \dots + 2^{n-1}) = (2^n - 1) + p(2^n - 1) = p + p^2 = p(p + 1) = 2^n p = 2m$, as desired. (If we sum up all the factors of a perfect number instead of all the proper factors, we should get twice the number.)

Do all perfect numbers have the above form? Here is a partial answer:

Theorem. (Euler) If m is a perfect number and m is even, then $m = 2^{n-1} (2^n - 1)$ where $2^n - 1$ is a prime.

Proof: Let m be a perfect number, and suppose that $m = 2^k Q$, where Q is an odd integer. Suppose that the sum of the divisors of Q is S . Then the sum of the divisors of m is $S(1 + 2 + 4 + \dots + 2^k) = (2^{k+1} - 1)S$. (You should verify this--it is not quite obvious.) We want this sum to be $2m$, so $2m = (2^{k+1} - 1)S$. Solving for S ,

$$S = \frac{2m}{2^{k+1} - 1} = \frac{2^{k+1} Q}{2^{k+1} - 1} = Q + \frac{Q}{2^{k+1} - 1}.$$

But Q and $\frac{Q}{2^{k+1} - 1}$ are both divisors of Q and the only way for these to be the only divisors of Q is if Q is prime. This completes the proof.

At this point, some obvious questions arise:

Question 1: Are there any odd perfect numbers?

Question 2: Are there infinitely many perfect numbers?

No one knows the answers to these questions. The second question can be asked in terms of Mersenne primes: Are there infinitely many Mersenne primes? If we look at

the Mersenne numbers, $M(n) = 2^n - 1$:

n	1	2	3	4	5	6	7	8
$2^n - 1$	1	3	7	15	31	63	127	255

a pattern presents itself: only prime numbers n give rise to primes. We can prove this: suppose that n is not prime, say $n = ab$, where $a, b > 1$. Then we can write

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1),$$

so $2^n - 1$ has the factor $2^a - 1$, and can't be prime. However, $2^p - 1$ is not always prime. For example, $2^{11} - 1 = 2047 = 23 \cdot 89$. As of February 2009, there are 46 known primes p for which $2^p - 1$ is prime. These are:

2, 3, 5, 7, 13 (these were known to the Greeks),

17, 19, 31, 61 (these were discovered before the 20'th century),

89, 107, 127, 521, 607, 1279, 2203, 2281, 3217 (discovered before 1960),

4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497
(discovered before 1980),

86243, 110503, 132049, 216091 (these were found in the 80's),

756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593
(found in the 90's)

13,466,917 (2001), 20,996,011 (2003), 24,036,583 (2004),

25,964,951, 30,402,457 (2005), 32,582,657 (September, 2006)

43,112,609, 37,156,667 (found in August, September, 2008).

It is known that $2^{13466917} - 1$ is the 39th Mersenne prime (that there are no smaller primes that were missed.) From that point on, there could be gaps. All exponents below 16,000,000 have been tested at least once, and everything below 13,466,917 has been double checked. It is possible that there are other exponents between 17,000,000 and 43,112,609 that give Mersenne primes. The following is an algorithm to check if a number $2^p - 1$ is a Mersenne prime: (The Lucas-Lehmer test)

Set $U = 4$.

for i from 3 to p do

replace U by $(U^2 - 2) \bmod (2^p - 1)$

at the end of the loop, if $U = 0$, then $2^p - 1$ is prime,
otherwise, $2^p - 1$ is composite.

For example, if $p = 19$, we have

$$U = 4 \rightarrow 14 \rightarrow 194 \rightarrow 37634 \rightarrow 218767 \rightarrow 510066 \rightarrow 386344 \rightarrow 323156 \rightarrow \\ 218526 \rightarrow 504140 \rightarrow 103469 \rightarrow 417706 \rightarrow 307417 \rightarrow 382989 \rightarrow 275842 \\ \rightarrow 85226 \rightarrow 523263 \rightarrow 0,$$

so $2^{19} - 1$ is a Mersenne prime. However, when $p = 23$, we have

$$U = 4 \rightarrow 14 \rightarrow 194 \rightarrow 37634 \rightarrow 7031978 \rightarrow 7033660 \rightarrow 1174629 \rightarrow 7643358 \\ \rightarrow \\ 3179743 \rightarrow 2694768 \rightarrow 763525 \rightarrow 4182158 \rightarrow 7004001 \rightarrow 1531454 \rightarrow \\ 5888805 \rightarrow 1140622 \rightarrow 4321431 \rightarrow 7041324 \rightarrow 2756392 \rightarrow 1280050 \rightarrow \\ 6563009 \rightarrow 6107895 \neq 0$$

so $2^{23} - 1$ is not a Mersenne prime.