Prime Numbers

Theorems about prime numbers:

1. Euclid's theorem

There are an infinite number of prime numbers

Proof

Eric says $2,3,5,7,11$ is a list of all the prime numbers.

But consider the number $N=(2\times3\times5\times7\times11)+1$

If N is prime, then Eric's list is not complete.

If N is not prime, then it is a multiple of primes. But N is not a multiple of 2, 3, 5, 7 or 11 so N is a multiple of some other primes. So Eric's list is not complete.

We can repeat this argument for any list that Eric can come up with. So it is impossible to write down a list of all the primes. So there must be an infinite number of primes.

2. We can find an arbitrarily long sequence of consecutive non-primes.

Proof

$6!$ is a multiple of 2, so $2+6!$ is a multiple of 2.

$6!$ is a multiple of 3, so $3+6!$ is a multiple of 3

...

$6!$ is a multiple of 6, so $6+6!$ is a multiple of 6

So we have found a sequence of 5 consecutive non-primes.

In general:

$(2+n!),(3+n!),(4+n!),...(n+n!)$ is a sequence of $n-1$ consecutive non-primes for any positive integer n

3. We cannot find an arithmetic sequence where all the terms are primes.

Proof

Here is an arithmetic sequence: $7,157,307,457,607,757,907\ldots$

The first seven terms are all primes.

Now:

$a=7$ and $d=150$ and $u_n=7+(n-1)150$

So:

$u_8=7+(7)150$ and this is a multiple of 7 and therefore not a prime.

In general:

Consider the arithmetic sequence; $a,a+d,a+2d,a+3d,...$

Now:

$u_n = a + (n-1)d$ so $u_{a+1} = a + ad$ and this is a multiple of a and therefore not prime.

Note:

if $a = 1$ our proof does not work but if $a = 1$ then the first term of the arithmetic sequence is not prime.

Dirichlet's theorem:

If a and d have no common factor then the arithmetic sequence $a, a+d, a+2d, a+3d, \ldots$ will contain an infinite number of primes.

So the terms of $7, 157, 307, 457, 607, 757, 907 \ldots$ cannot all be prime, only an infinite number of them.

It is difficult to prove Dirichlet's theorem but we can prove that there are an infinite number of primes in the arithmetic sequence:

$5, 9, 13, 17, 21, 23, \ldots$

These are the integers of the form $4k+3$

So we want to prove that there are an infinite number of primes of the form $4k+3$

Before we start the proof:

All primes (except 2) are of the form $4k+1$ or $4k+3$

The product of primes of the form $4k+1$ is also of this form because:

$(4k+1)(4q+1) = \ldots = 4(4kq+k+q)+1$

Proof

Eric says $3, 7, 11, 19, 23$ is a list of all the $4k+3$ primes.

But consider the number $N = 4(3 \times 7 \times 11 \times 19 \times 23) + 3$

N is of the form $4k+3$

If N is prime, then Eric's list is not complete.

If N is not prime, then it is a multiple of primes. But N is not a multiple of 3, 7, 11, 19 or 23 so N is a multiple of some other primes. If these other primes were all of the form $4k+1$ then N would be of the form $4k+1$ as we saw above. So at least one of these other primes must be of the form $4k+3$ So Eric's list is not complete.

We can repeat this argument for any list that Eric can come up with. So it is impossible to write down a list of all the $4k+3$ primes. So there must be an infinite number of $4k+3$ primes.

4.

$f(n) = n^2 - n + 41$ is prime for $n = 1, 2, 3, \ldots 40$

and

$f(n)=n^2-79n+1601$ is prime for $n=1,2,3,\ldots 79$

But:

No quadratic polynomial $f(n)$ with integer coefficients, is prime for all values of n

Proof

$f(n)=an^2+bn+c$ where a,b,c are integers

$f(1)=a+b+c$ let $q=a+b+c$

$f(q+1)=a(q+1)^2+b(q+1)+c=\ldots=q(aq+2a+b+1)$

If $q=0$ then $f(1)=0$ and therefore not a prime.

If $q=1$ then $f(1)=1$ and therefore not a prime.

If $q\geq 2$ then $f(q+1)$ is a multiple of q and therefore not a prime.

In general:

No polynomial $f(n)$ with integer coefficients, is prime for all values of n

5. For every integer $n\geq 1$ there is a prime p where $n\leq p\leq 2n$

Proof – too difficult

6. x and n are positive integers

If x^n-1 is prime then $x=2$

For example, when $n=5$

$x^5-1=(x-1)(x^4+x^3+x^2+x+1)$

So $(x-1)$ is a factor of (x^5-1) so (x^5-1) cannot be prime unless $(x-1)=1$ so $x=2$

So we can see that if $x\neq 2$ then x^n-1 is not prime.

Note: This does not mean, if $x=2$ then x^n-1 is prime - try $n=4$

7. n is a positive integer

If 2^n-1 is prime then n is prime.

For example, when $n=15$

$2^{15}-1=(2^3)^5-1=8^5-1$ and this is not prime by theorem 6.

So we can see that if n is not prime then 2^n-1 is not prime.

Note: This does not mean, if n is prime then 2^n-1 is prime - try $n=11$

Primes of the form 2^n-1 are called Mersenne primes.
Some people like looking for large primes. Many of these are Mersenne primes, such as $2^{82589933}-1$ because there are short cuts to check if numbers of the form 2^n-1 are prime, such as the Lucas – Lehmer test (look it up!)

8. x and n are positive integers
If x^n+1 is prime then n is even

For example, when $n=5$
$x^5+1=(x+1)(x^4-x^3+x^2-x+1)$
So (x+1) is a factor of (x^5+1) so (x^5+1) cannot be prime.
So we can see that if n is odd then x^n+1 is not prime.

Note: This does not mean, if n is even then x^n+1 is prime – try $x=3$ and $n=2$

9. n is a positive integer
If 2^n+1 is prime then $n=2^k$ for some positive integer k

For example, when $n=28$
$2^{28}+1=(2^4)^7+1=16^7+1$ and this cannot be prime by theorem 8.
So we can see that if $n\neq 2^k$ then 2^n+1 is not prime.

Note: this does not mean, if $n=2^k$ then 2^n+1 is prime – try $n=32$

Numbers of the form 2^n+1 where $n=2^k$ are called Fermat numbers.

The first five Fermat numbers are all prime but the sixth Fermat number is 4,294,967,297 and Euler showed that this is not prime. In fact, no other Fermat primes have been discovered.

Conjectures about primes:
1. There are an infinite number of Mersenne primes.
2. There are an infinite number of Fermat primes.

3. There are an infinite number of Fibonacci primes.

4. There are an infinite number of prime pairs (primes like 17 and 19 that differ by 2).

5. For every positive integer n there is a prime p where $n^2 < p < (n+1)^2$

6. There are infinitely many primes of the form n^2+1 where n is a positive integer

7. $2^k - 2$ is a multiple of k if and only if k is a prime number.

Actually this is not a conjecture. The statement is true for $k = 1, 2, 3, 4, \ldots 340$ but not for $k = 341$

8. The Goldbach conjecture

Every even integer, greater than 4, is the sum of two odd primes.

$6 = 3+3$ $8 = 3+5$ $10 = 3+7$ etc

This is the most famous conjectures about primes. It arose in a letter Goldbach wrote to Euler in 1742. In 1931, Schnirelmann proved that every even integer, greater than 4, is the sum of no more than 300,000 primes, which is a start.

Incidently, Goldbach had another conjecture:

Every odd positive integer, greater than 1, is a prime or the sum of a prime and twice a square.

$9 = 7+2(1^2)$ $15 = 7+2(2^2)$ $21 = 3+2(3^2)$ $25 = 7+2(3^2)$ etc

We now know that this conjecture is false. The smallest counter-example is 5777.