Lecture 7: Prime numbers

A natural number n is said to be *prime* if $n \geq 2$ and the only divisors of n are 1 and n itself. A number which is not prime is said to be *composite.*

Warning! The number 1 is not a prime.

The primes have exercised a great fascination ever since they were first studied and continue to pose questions that mathematicians have yet to solve.

The fundamental theorem of arithmetic

In the lectures, I assumed that you were familiar with this result. For those of you who aren't, here are the details.

Lemma 0.1. *Let $n \geq 2$. The smallest divisor $d \geq 2$ of n is a prime. Thus every number $n \geq 2$ has a prime divisor.*

Proof. If n is a prime then n is its own prime divisor. Suppose n is not prime. Let d be the smallest number dividing n which is larger than 1. If d were not prime then d would have a divisor which was not 1 and this divisor would in turn divide n, but this would contradict the fact that d was the smallest divisor of n. Thus d must itself be prime. □

The following was proved by Euclid: it is Proposition 20 of Book IX of the *Elements.*

Theorem 0.2. *There are infinitely many primes.*

Proof. Let $p_1, \ldots, p_n$ be the first n primes. Put

$$N = p_1 \ldots p_n + 1.$$

If N is a prime, then N is a prime bigger than p_n. If N is composite, then by the above lemma N has a prime divisor p. But p cannot equal any of the primes $p_1, \ldots, p_n$ because N leaves remainder 1 when divided by p_i. It follows that p is a prime bigger than p_n. Thus we can always find a bigger prime. It follows that there must be an infinite number of primes. □

The following was discussed in Lecture 4.

Algorithm 0.3. To decide if a number n is prime or composite. Check to see if any prime $p \leq \sqrt{n}$ divides n. If none of them do, the number n is prime.

Let's think about why this works. If a divides n then we can write $n = ab$ for some number b. If $a < \sqrt{n}$ then $b > \sqrt{n}$ whilst if $a > \sqrt{n}$ then $b < \sqrt{n}$. Thus to decide if n is prime or not we need only carry out trial divisions by all numbers $a \leq \sqrt{n}$.

However, this is inefficient because if a divides n and a is not prime then a is divisible by some prime p which must therefore also divide n. It follows that we need only carry out trial divisions by the primes $p \leq \sqrt{n}$.

Example 0.4. Determine whether 97 is prime using the above algorithm. We first calculate the largest whole number less than or equal to $\sqrt{97}$. This is 9. We now carry out trial divisions of 97 by each prime number p where $2 \leq p \leq 9$; by the way, if you aren't certain which of these numbers is prime: just try them all. You'll get the right answer although not as efficiently. You might also want to remember that if m doesn't divide a number neither can any multiple of m. In any event, in this case we carry out trial divisions by $2, 3, 5$ and 7. None of them divides 97 exactly and so 97 is prime.

The following is an immediate consequence of Gauss's Lemma. It is a fundamental property of primes.

Lemma 0.5. *Let $p \mid ab$ where p is a prime. Then $p \mid a$ or $p \mid b$.*

Theorem 0.6 (Fundamental theorem of arithmetic). *Every number $n \geq 2$ can be written as a product of primes in essentially one way. By* product *we allow the possibility that there is only one prime.*

Proof. Let $n \geq 2$. If n is already a prime then there is nothing to prove, so we can suppose that n is composite. Let p_1 be the smallest prime divisor of n. Then we can write $n = p_1 n'$ where $n' < n$. Once again, n' is either prime or composite. Continuing in this way, we can write n as a product of primes.

We now prove uniqueness. Suppose that

$$n = p_1 \dots p_s = q_1 \dots q_t$$

are two ways of writing n as a product of primes. Now $p_1 \mid n$ and so $p_1 \mid q_1 \dots q_t$. By the corollary to Gauss's Lemma above, the prime p_1 must divide one of the q_i's and, since they are themselves prime, it must actually equal one of the q_i's. By relabelling if necessary, we can assume that $p_1 = q_1$. Cancel p_1 from both sides and repeat with p_2. Continuing in this way, we see that every prime occurring on the lefthand side occurs on the righthand side. Changing sides, we see that every prime occurring on the righthand side occurs on the lefthand

side. We deduce that the two prime decompositions are identical. □

When we write a number as a product of primes we usually gather together the same primes into a prime power, and write the primes in increasing order. This is illustrated in the example below.

Example 0.7. Let $n = 999,999$. Write n as a product of primes. There are a number of ways of doing this but in this case there is an obvious place to start. We have that

$$n = 3^2 \cdot 111,111 = 3^3 \cdot 37,037 = 3^3 \cdot 7 \cdot 5,291 = 3^3 \cdot 7 \cdot 11 \cdot 481 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37.$$

Thus the prime factorisation of $999,999$ is

$$999,999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37.$$

Primes can be regarded as the *atoms* from which all other numbers can be constructed.

Are there patterns in the set of primes?

The fundamental theorem of arithmetic tells us that every natural number is built up from primes. This suggests that we should study primes in more detail if we want to understand the properties of arbitrary numbers. We also know that there are infinitely many primes. What more can we say? The Fibonacci numbers form an infinite sequence of numbers and for them we found a formula. Could something similar be done for the primes: is there a formula that when n is input will output the nth prime? The answer is no. Mathematicians of course tried to find one and in the process came up with some intesting results. For example, the polynomial

$$p(n) = n^2 - n + 41$$

has the property that its value for $n = 1, 2, 3, 4, \ldots, 40$ is always prime. Of course, for $n = 41$ it is clearly not prime. However, it can be proved that there is no polynomial that will generate all the primes. The closest we can get is a remarkable result by Yuri Matijasevic in 1971, who found a polynomial in 26 variables of degree 25 with the property that when non-negative integers are substituted for the variables the positive values it takes are all and only the primes. However, this polynomial does not generate the primes in any particular order. I have appended a copy of this formula for you delectation.

After centuries of attempts two approaches have yielded some positive results:

(1) Formulae that produce primes (often or sometimes).
(2) A *statistical* approach.

I shall deal with each of these in turn.

Formulae for primes: binomial numbers

Early mathematicians tried to find formulae that would be guaranteed to generate primes. Their starting point was to use algebraic identities which would lead to numbers that had obvious factors (what this means should become clearer in a moment). We shall look at *binomial numbers.* These are numbers of the form

$$N = x^n \pm y^n$$

where x and y are given integer values. We shall look at three cases that will give us the information we need:

(1) $N = x^n - y^n$. We want to factorize this number. Think of x as a variable and y as a constant. If x takes the value y the value of this polynomial will be zero. Thus $x - y$ is a factor. If you carry out the long divison you get

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + x^2y^{n-3} + xy^{n-2} + y^{n-1})$$

which can be verified by multiplying out the righthand side.

(2) $N = x^n + y^n$ where n is odd. Replace y by $-y$ in (1) above. We get that

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \ldots + x^2y^{n-3} - xy^{n-2} + y^{n-1})$$

(3) $N = x^{mn} - y^{mn}$. Replace x by x^m and y by y^m in (1) above. We get that

$$x^{mn} - y^{mn} = (x^m - y^m)(x^{m(n-1)} + x^{m(n-2)}y^m + \ldots + y^{m(n-1)}).$$

Observe that identity (1) is the key and that (2) and (3) are special cases.

Mersenne primes

Let's look first at numbers of the form $a^n - b^n$. By (1) above we see that $a - b$ is a factor. Take the special case where $b = 1$. Then if $a > 2$ numbers of the form $a^n - 1$ cannot be prime. Thus a necessary condition for a number of the form $a^n - 1$ to be prime is that $a = 2$. However, by (3) above if n is composite then $2^n - 1$ is composite. Thus we are led to consider numbers of the form $M_p = 2^p - 1$ where p is a prime. These are called *Mersenne numbers.* Observe that for $p = 2, 3, 5, 7$, the numbers M_p are also prime. However $M_{11} = 2047 = 23 \cdot 89$ is not prime. It is not true that M_p is always prime but when it is it is called a *Mersenne prime.* However, Mersenne numbers have been a happy hunting ground for finding really large prime numbers and new Mersenne primes are announced every so often. It is not known if there

are infinitely many. As of writing (2010), the latest Mersenne prime to have been discovered is

$$M_{42643801}.$$

In the exercises, I shall ask you to develop the connection between Mersenne primes and perfect numbers: another topic that Euclid covered.

Fermat primes

We now look at numbers of the form $a^n + 1$. If $a > 2$ and odd then a^n is odd and so $a^n + 1$ is even. In particular, it is divisible by 2 and so cannot possibly be prime. Thus if $a^n + 1$ is to be odd we need that a^n be even. Also by (2) above we must have that n is even and have no odd divisors. Thus n must be a power of 2. Thus we look at numbers of the form $F_m = 2^{2^m} + 1$ called *Fermat numbers.* When $m = 0$ we get that $F_0 = 3$ and subsequently $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ which are all prime, which you should check. On the basis of this, Fermat conjectured that all Fermat numbers were prime. Childs describes this as "one of the least accurate famous conjectures in the history of mathematics" because not only did Euler show that F_5 was composite but no further examples of Fermat primes have been found. Of course, this still leaves open that there might be more but we won't know for certain until theorems are proved.

Fermat primes have an unexpected geometric connection. Euclid proved that an equilateral triangle and a pentagon could be constructed using only a straightedge and compass. As a very young man, Gauss figured out how to construct a regular polygon having 17 sides using only a straightedge and compass. It is no accident that these polygons have a number of side equal to a Fermat prime. Gauss proved the following general theorem.

Theorem 0.8 (Gauss). *A regular polygon with n sides can be constructed by means of a straightedge and compass if and only if $n = 2^r p_1 \dots p_m$ where the p_i are distinct Fermat primes.*

The power of two comes about because we can bisect angles using a straightedge and compass.

In the exercises, we shall look at some other applications of Fermat numbers.

The prime number theorem

I shall now turn to what I called above the *statistical approach.* The idea is that for each natural number n we count the number of primes $\pi(n)$ less than or equal to n. If we are going to do this then our first

problem is to compile a table of sufficiently many of them. The simplest way of doing this is to use the *Sieve of Eratosthenes.* Suppose we want to construct a table of all primes up to the number N. We begin by listing all numbers from 2 to N inclusive. Mark 2 as prime and then cross out from the table all numbers which are multiples of 2. The first number after 2 which we have not crossed out is 3. We mark this as prime and then cross out all multiples of 3. The first number after 3 not crossed out is 5. We mark this as prime and continue in the same way. We stop when we have crossed out all multiples of the largest prime less than or equal to $\sqrt{N}$. All marked numbers will be prime as well as those numbers which remain not crossed out.

If you compile tables of primes in this way, you can calculate the function $\pi(x)$. Its graph has a staircase shape — it certainly isn't smooth — but as you zoom away it begins to look smoother and smoother: see the two pictures at the end of this lecture. This raises the question whether there is a smooth function that is a good approximation to $\pi(n)$.

This seems to have been what Gauss did. He set up a table something like the following (this is taken from LeVeque's book *Fundamentals of number theory*, Dover, 1977) where

$$\Delta(x) = \frac{\pi(x) - \pi(x - 1000)}{1000}$$

represents an approximate slope of the *curve* $\pi(x)$.

x	$\pi(x)$	$\Delta(x)$	$\frac{1}{\ln(x)}$
1000	168	$0 \cdot 168$	$0 \cdot 145$
2000	303	$0 \cdot 135$	$0 \cdot 132$
3000	430	$0 \cdot 127$	$0 \cdot 125$
4000	550	$0 \cdot 120$	$0 \cdot 121$
5000	669	$0 \cdot 119$	$0 \cdot 117$
6000	783	$0 \cdot 114$	$0 \cdot 115$
7000	900	$0 \cdot 117$	$0 \cdot 113$
8000	1007	$0 \cdot 107$	$0 \cdot 111$
9000	1117	$0 \cdot 110$	$0 \cdot 110$
10000	1229	$0 \cdot 112$	$0 \cdot 109$

What Gauss noticed, because he was that kind of guy, was that the *slope* of $\pi(x)$ looked very much like $\frac{1}{\ln(x)}$. This suggests that the function, defined by integrating these *slopes*, is given by

$$\mathrm{li}(x) = \int_{t=2}^{x} \frac{1}{\ln(t)} dt$$

should be an approximation to $\pi(x)$. It is called the *logarithmic integral.*

Of course, this is not a theorem: it is a conjecture. It was proved in 1896 by two mathematicians: Hadamard in France and de la Vallée Poussin in Belgium.

Theorem 0.9 (The Prime Number Theorem: version 1)**.**

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1.$$

This version of the PNT is not that easy for us to use. The following lemma will enable us to get a second version of the PNT that is easy to use.

Lemma 0.10.

$$\lim_{x\to\infty} \frac{\mathrm{li}(x)}{x/\ln(x)} = 1.$$

Proof. By l'Hôpital's rule, this limit is equal to the limit of the fraction of functions obtained by differentiating numerator and denominator. The remainder of the proof is set as an exercise. □

If we assume the first version of the PNT and use the lemma above, we obtain the second version of the PNT. We use the fact that the limit of a product is the product of the limits.

Theorem 0.11 (The Prime Number Theorem: version 2)**.**

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

The above theorem can be interpreted as saying that for large values of x the value of $\pi(x)$ is approximately given by $\frac{x}{\ln(x)}$. In fact, $\mathrm{li}(x)$ is a better approximation but we can't compute it as easily on a calculator.

from American Mathematical Monthly 83 (1976), 449-464.

DIOPHANTINE REPRESENTATION OF THE SET OF PRIME NUMBERS

JAMES P. JONES, DAIHACHIRO SATO, HIDEO WADA AND DOUGLAS WIENS

1. Introduction. Martin Davis, Yuri Matijasevič, Hilary Putnam and Julia Robinson [4] [8] have proven that every recursively enumerable set is Diophantine, and hence that the set of prime numbers is Diophantine. From this, and work of Putnam [12], it follows that the set of prime numbers is representable by a polynomial formula. In this article such a prime representing polynomial will be exhibited in explicit form. We prove (in Section 2)

THEOREM 1. *The set of prime numbers is identical with the set of positive values taken on by the polynomial*

$$
\begin{aligned}
(1)\quad & (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)\cdot(h+j)+h-z]^2-[2n+p+q+z-e]^2\\
& -[16(k+1)^3\cdot(k+2)\cdot(n+1)^2+1-f^2]^2-[e^3\cdot(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2\\
& -[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2\\
& -[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\\
& -[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}
\end{aligned}
$$

as the variables range over the nonnegative integers.

(1) is a polynomial of degree 25 in 26 variables, $a, b, c, \ldots, z$. When nonnegative integers are substituted for these variables, the positive values of (1) coincide exactly with the set of all prime numbers 2,3,5,.... The polynomial (1) also takes on negative values, e.g., -76.

In 1971, Yuri Matijasevič [10] outlined the construction of a prime representing polynomial in 24 variables and degree 37, using the Fibonacci numbers. In the addendum to his paper, an improvement to 21 variables and degree 21 was made. (These polynomials were not written out explicitly.) Our construction here yields a polynomial in 19 variables and degree 29. It also yields a polynomial in 42 variables and degree 5. Thus we might ask what is the smallest possible degree and how few variables are actually necessary to represent primes?

Let us consider first the question of the degree. We know that a prime representing polynomial of degree 5 is possible. All that is necessary to reduce the degree to 5 is the Skolem substitution method (cf. [3], p. 263). However, this procedure increases the number of variables (to 42 when applied to (1)). We do not know whether there is a prime representing polynomial of degree < 5.

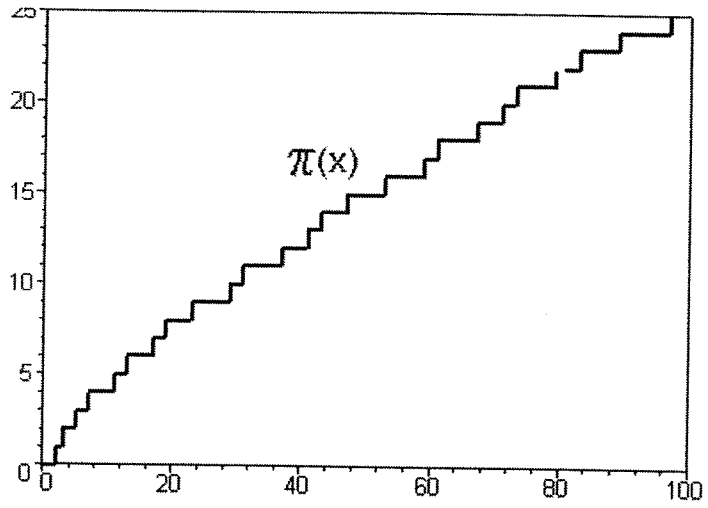
The question of the minimum number of variables is also open. A simple argument shows that at least 2 variables are necessary. But we do not know the minimum number. The method of proof of Theorem 1 yields a polynomial in 16 variables. To reduce the number of variables below 16 requires an entirely different construction. The best result we were able to obtain is a polynomial in 12 variables. We shall prove

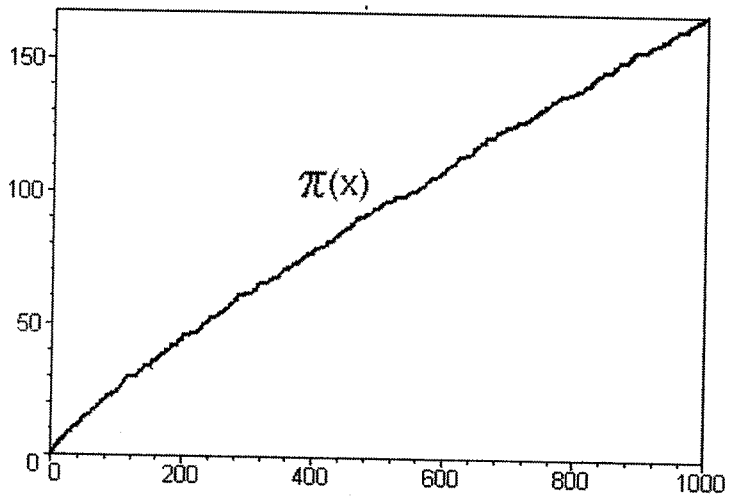
THEOREM 2. *There exists a prime representing polynomial in* 12 *variables.*

This result was reportedly known to Yuri Matijasevič in 1973, although no literature is available concerning this. Our proof uses methods developed by Yuri Matijasevič and Julia Robinson in [11]. The construction is carried out in §3. The polynomial constructed has very large degree.

The proofs of Theorem 1 and 2 are both based on Wilson's Theorem. In each case we show that the set of prime numbers is Diophantine; i.e., that there exists a Diophantine equation solvable only for prime values of a parameter. We construct a polynomial $M(k, x_1, \cdots, x_n)$ with the property that for each nonnegative integer k

$$
(3)\qquad k+2 \text{ is prime} \leftrightarrow M(k, x_1, \cdots, x_n) = 0 \text{ is solvable in nonnegative integers.}
$$





These graphs were taken from

http://primes.utm.edu/howmany.shtml