# PRIME NUMBERS

LECTURE NOTES: MATH 422 (CSUSM). SPRING 2009. PROF. AITKEN

## 1. Prime Divisors

**Theorem 1.** *If $n > 1$ is composite, then $n$ has a prime divisor $p$ such that $p^2 \leq n$.*

*Remark.* Another way to say this is that a composite integer $n > 1$ has a prime divisor $p$ with $p \leq \sqrt{n}$. So if an integers $n > 1$ is not divisible by any prime $p \leq \sqrt{n}$, we can conclude that $n$ must be a prime.

*Proof.* If $n$ is composite, then $n = ab$ where $a > 1$ and $b > 1$. For convenience, suppose $a \leq b$. Let $p$ be a prime divisor of $a$. Thus $p \leq a \leq b$. So

$$p^2 \leq a^2 \leq ab = n.$$

Since $p \mid a$ and $a \mid n$ we have $p \mid n$. □

*Exercise* 1. Show that if you want to decide if a two digit number is a prime, you only need to check divisibility by 2, 3, 5, and 7. Show that aside from 49, 77, and 91 you only need to check divisibility by 2, 3, and 5.

*Exercise* 2. What is the largest prime that must be checked to show a three digit number is a prime?

## 2. Sieve of Eratosthenes

The Sieve of Eratosthenes is an algorithm to generate all the primes less than or equal to a fixed bound $N$. One starts by making a list of all integers between 2 and $N$. One crosses out all multplies of 2 except 2. Next one crosses out all multiples of 3 except 3. Then one does this for 5. Keep going: after crossing out multiples of $p$ except $p$, the first uncrossed out number $p'$ must be a prime. One then crosses out all multiples of $p'$ except $p'$. One proceeds until the next uncrossed out number has square greater than $N$.

After doing this, all remaining numbers are guarenteed to be primes. Basically you have filtered out all composite numbers, and what is left is a prime. (A sieve is a utensil for separating coarse and fine particles. Here we are separating the composites from the primes.).

*Exercise* 3. Use the Sieve of Eratosthenes to find all primes less than $N = 200$.

---

*Date*: Spring 2009. Version of March 2, 2009.

## 3. Formulas for primes

It has proven very difficult to find a simple formula that generates only prime numbers and does so in an efficient manner. (There are some formulas, for example, formulas involving factorials, that are not at all efficient).

A famous attempt was proposed by Fermat:

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

which, as we will see below, unfortunately fails to give only primes.

One might hope for a polynomial formula $f(x)$ for primes. For example, Euler noticed that $f(x) = x^2 - x + 41$ gives primes for $n = 0, 1, \ldots, 40$. Unfortunately it fails for infinitely many values after that. The following theorem shows that polynomials will never give formula for primes.

**Theorem 2.** *There is no nonconstant polynomial $f(x)$ with integer coefficients such that $f(n)$ is a prime for all $n \in \mathbb{Z}$.*

*Proof.* Suppose such a polynomial $f(x)$ exists. Pick an integer $n$. Then $f(n)$ is prime by assumption. Call this prime $p$. Since $f(n) = p$, we have $f(n) \equiv 0$ modulo $p$. Now $n \equiv n + kp$ modulo $p$ since $p$ divides the difference. So, by the theorem on polynomial substitution,

$$f(n + kp) \equiv f(n) \equiv 0 \mod p.$$

In particular, $p \mid f(n + kp)$ for all $k \in \mathbb{Z}$.

Since $f(n + kp)$ is also a prime by assumption, this implies that $p = f(n + kp)$ for all $k \in \mathbb{Z}$, since the only way one prime can divide another is for them to be equal.

Consider the polynomial $g(x) = f(x) - p$. Observe that $g(n + kp) = 0$ for all $k \in \mathbb{Z}$. Thus $g(x)$ has an infinite number of roots. However, the number of roots of $g(x)$ is bounded by the degree (basic result of concerning polynomials). This gives a contradiction. □

*Exercise* 4. What about polynomials $f(x)$ such that $f(n)$ is prime for all positive $n$? What about polynomials $f(x)$ such that $f(n)$ is prime for all $n \geq B$ where $B$ is some bound? Can the above proof be used to rule out such (nonconstant) polynomials?

## 4. Fermat Primes

Fermat conjectured that $2^{2^n} + 1$ is a prime for all $n \geq 0$. Why did Fermat focus on exponents that are a power of two? The following theorem gives an answer:

**Theorem 3.** *Suppose that $c^n + 1$ is a prime where $c > 1$ and $n > 1$. Then $c$ is even and $n$ is a power of two.*

*Proof.* Suppose $c$ is odd. Then $c > 2$ and $c^n$ is odd. Thus $c^n + 1$ is even, and is greater than 2. So $c^n + 1$ cannot be prime, a contradiction. We conclude that $c$ is even.

Suppose that $n$ is not a power of 2. So there is an odd prime $p$ dividing $n$. Write $n = pm$. Trivially, $(c^m + 1) \mid c^m - (-1)$. So

$$c^m \equiv -1 \mod N$$

where $N = c^m + 1$. Raise each side of the congruence to the $p$ power. This gives

$$(c^m)^p \equiv (-1)^p \mod N.$$

Simplifying gives $c^n \equiv -1$ modulo $N$. Thus $N$ divides the difference $c^n + 1$. Observe that $1 < N < c^n + 1$ since $N = c^m + 1$ and $m < n$. Thus $c^n + 1$ cannot be a prime. □

**Definition 4.** A number of the form $2^{2^n} + 1$ is called a *Fermat number*. A prime that is a Fermat number is called a *Fermat prime*. The first five Fermat numbers are $3, 5, 17, 257$, and $65537$.

Fermat checked that all such numbers up to $2^{16} + 1 = 65537$ are prime, and conjectured that all of them are prime. This was disproved by Euler who showed that the next Fermat number $2^{32} + 1 = 4294967297$ is composite and is divisible by 641 (this can be checked with a good calculator). Today, we know of several other Fermat numbers that are composite. In fact, to this day, $2^{16} + 1$ is the largest known Fermat prime. Is the set of Fermat primes finite or infinite? This is still an open question.

Gauss, around 1800, showed an interesting relationship between Fermat primes and constructible $n$-gons. He proved that if $p$ is a prime, then the $p$-gon is constructible by ruler and compass (in the ancient Greek style) if and only if $p$ is a Fermat prime. Thus triangles, pentagons, 17-gons are constructible, but 7-gons (heptagons) are not. Before Gauss, no one knew how to construct a 17-gon with ruler and compass, and no one knew how to prove that one could not construct a 7-gon. Gauss was so proud of this discovery, that he decided to pursue a career in mathematics (instead of ancient languages). He is said to have requested that a 17-gon be engraved on his tombstone.

## 5. Mersenne Primes

Mersenne was interested in primes of the form $2^p - 1$ where $p$ is a prime. Why did Mersenne focus on exponents that are a prime? The following theorem gives an answer:

**Theorem 5.** *Suppose $c > 1$ and $n > 1$ are such that $c^n - 1$ is a prime, then $c = 2$ and $n$ is a prime.*

*Proof.* Since $c^n - 1 = (c-1)(c^{n-1} + \ldots + c^2 + c + 1)$ we have that $c - 1$ divides $c^n - 1$. Since $c - 1 < c^n - 1$ and $c^n - 1$ is a prime, we must have $c - 1 = 1$. Thus $c = 2$.

Now we show that $n$ is prime. Suppose otherwise that $k = ab$ where $a > 1$ and $b > 1$. Then $N = (c^a - 1)$ divides $c^a - 1$ (reflective property of division). So $c^a \equiv 1$ modulo $N$. Hence $(c^a)^b \equiv 1^b$ modulo $N$. Simplifying gives $c^n \equiv c^{ab} \equiv 1$ modulo $N$. Thus $N$ divides the difference $c^n - 1$. Since $a > 1$ and $b > 1$ we have $1 < c^a - 1 < c^{ab} - 1$. In other words $1 < N < c^n - 1$, contradicting the assumption that $c^n - 1$ is a prime. □

**Definition 6.** A number of the form $2^p - 1$ with $p$ prime is called a *Mersenne number*. A prime that is a Mersenne number is called a *Mersenne prime*. Examples of Mersenne numbers include $3, 7, 31$, and $127$ (all prime), and $2^1 1 - 1 = 2047 = 23 \cdot 89$ (composite).

Mersenne primes are connected with perfect numbers. In fact, Euclid proved that if $M$ is a Mersenne prime then $M(M+1)/2$ is a perfect number. (However, Euclid did not speak in terms of Mersenne primes). Euler later showed that every even perfect number is of that form. There are conjectured not to be any odd perfect numbers.

*Exercise* 5. Show that 3 is the only number that is both a Mersenne number and a Fermat number.

In an ongoing project, the Great Internet Mersenne Prime Search (GIMPS), volunteers run software that searches for new Mersenne primes (when the volunteers are not using their computers). According to the GIMPS website "On August 23rd [2008], a UCLA computer in the GIMPS PrimeNet network discovered the 45th known Mersenne prime, $2^{43,112,609} - 1$, a mammoth 12,978,189 digit number! The prime number qualifies for the Electronic Frontier Foundation's $100,000 award for discovery of the first 10 million digit prime number. Congratulations to Edson Smith, who was responsible for installing and maintaining the GIMPS software on the UCLA Mathematics Department's computers." Since then another (smaller) Mersenne prime has been discovered. So there are now 46 known Mersenne primes. It is conjectured that there are an infinite number of such primes. This is a significant unsolved problem, which would imply, as a corollary, the existence of an infinite number of perfect numbers.

## 6. Prime number theorem

Let $\pi(x)$ be the number of prime $p \leq x$. There is no good exact formula for $\pi(x)$. However, the *prime number theorem* asserts that

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

This means that when $x$ is large, the expression $x/\ln x$ is a good approximation for $\pi(x)$.

The prime number theorem gives the following approximations

$$\pi(1000) \approx 144.8 \qquad \pi(1,000,000) \approx 72,382.4 \qquad \pi(1,000,000,000) \approx 48,254,942.4$$

The actual values of $\pi(x)$ (according to Hardy and Wright) are

$$168 \qquad 78,498 \qquad 50,847,478.$$

The ratios are

$$1.160 \qquad 1.084 \qquad 1.0537$$

which we see are gradually getting closer to 1. Thus the first estimate is 16% too large, the second is 8.4% too large, and the last is only 5.4% too large.

A related result says that the $n$th prime is approximately equal to $n \ln n$.