# Summer High School 2009

Aaron Bertram

## 1. Prime Numbers.

Let's start with some notation:

$\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$ is the (infinite) set of **natural** numbers.

$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ is the set of **integers**.

$\mathbb{Q} = \{\text{rational numbers}\}$

$\mathbb{R} = \{\text{real numbers}\}$

*Question 1.1.* What's a rational number?

*Question 1.2.* What's a real number?

**Well-Ordered Axiom of the Natural Numbers:**
Every subset $S \subseteq \mathbb{N}$ except for the empty set has a smallest element.

*Question 1.3.* Why is it called "well-ordered"?

Axioms are mathematical statements that are accepted without proof. We try to keep these to a minimum! There is one other important one:

**Archimedes' Axiom:**
Each real number is less than some natural number.

**Examples** (of subsets of $\mathbb{N}$):

$S = \{\text{all natural numbers}\}$.
(Smallest element: 1)

$S = \{\text{natural numbers that are divisible by 3}\}$.
(Smallest element: 3)

$S = \{\text{natural numbers that are greater than } \pi\}$.
(Smallest element: 4)

$S = \{\text{natural numbers that are greater than their squares}\}$.
(No smallest element, because it is the empty set!)

**Definition 1.1.**

(a) A natural number $n > 1$ is *prime* if its only divisors are 1 and $n$.

(b) Natural numbers $> 1$ that are not prime are *composite.*

(c) 1 has a multiplicative inverse (itself) and so is called a *unit.*

**Examples:**

*Primes up to 30:* 2,3,5,7,11,13,17,19,23,29

*Composites up to 30:* 4,6,8,9,10,12,14,15,16,18,20,21,22,24,25,26,27,28,30

**Fundamental Theorem of Arithmetic (Part I)** Every natural number other than 1 is a product of finitely many primes.

**Proof:** Let $S$ be the set of all natural numbers other than 1 that are *not* a product of finitely many primes and let $c$ be its smallest element. Then $c = ab$ for some natural numbers $a$ and $b$ not equal to 1 or $n$. In particular, $a < c$ and $b < c$, so $a \notin S$ and $b \notin S$, so $a$ and $b$ *are* both products of finitely many primes. If we write $a = p_1 p_2 \cdots p_m$ and $b = q_1 q_2 \cdots q_n$, then $c = ab = p_1 p_2 \cdots p_m \cdot q_1 q_2 \cdots q_n$ and so $c$ would also be a product of finitely many primes. That's not allowed, so there can be no smallest element of $S$. So $S = \emptyset$ by the well-ordered axiom. Thus *every* natural number $> 1$ is a product of finitely many primes. □

Part II of the Fundamental Theorem of Arithmetic will say that there is *only one way* for a natural number $> 1$ to be a product of primes. We'll prove this later.

*Question 1.4.* How many prime numbers are there?

**Euclid's Theorem:** There are infinitely many primes.

**Proof:** If $p_1, p_2, \ldots, p_n$ are primes, then $N = p_1 p_2 \cdots p_n + 1$ is not divisible by any of the primes $p_1, p_2, \cdots p_n$. So it must be divisible by finitely many new primes, by the fundamental theorem of arithemtic. In other words, no matter how many primes we start with, there are always more primes. So there are infinitely many. □

**Examples:** Starting with $p_1 = 2$, the method of proof gives:

$N_1 = p_1 + 1 = 3$, which is prime. Call it $p_2 = 3$.

$N_2 = p_1 p_2 + 1 = 2 \cdot 3 + 1 = 7$ is prime. Call it $p_3 = 7$.

$N_3 = p_1 p_2 p_3 + 1 = 43$ is prime. Call it $p_4 = 43$.

$N_4 = p_1 p_2 p_3 p_4 + 1 = 1807 = 13 \cdot 139$. Call them $p_5 = 13, p_6 = 139$.

$N_5 = p_1 p_2 \cdots p_6 + 1 = 3263443$ is prime. Etcetera!

*Refined Question 1.4.*

(a) What is the largest known prime?

(b) How do we tell if a number $n$ is prime or not?

(c) How far is it from one prime $p$ to the next (as a function of $p$)?

(d) How many primes are less than $n$ (as a function of $n$)?

Some partial answers (without proof!):

**Mersenne primes** are the largest known primes. Named after Marin Mersenne (1588-1648), a French monk, mathematician, philosopher, and musician, these are primes of the form $2^p - 1$. If $k$ divides $n$, then:

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

so $2^n - 1$ is never a prime if $n$ is composite. On the other hand, $2^p - 1$ may or may not be a prime if $p$ is a prime:

$M_1 = 2^2 - 1 = 3, M_2 = 2^3 - 1 = 7, M_3 = 2^5 - 1 = 31, M_4 = 2^7 - 1 = 127$

are the first four Mersenne primes, but:

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

is not a prime. The largest known prime is the Mersenne prime:

$$2^{43,112,609} - 1$$

which has about 13 million digits (discovered to be prime in 2008). The reason we don't know any other primes of this order of magnitude is that it takes too long to check whether other numbers of this size are prime or not (and it isn't so easy to do it for Mersenne primes, either).

**Open Problem 1.** Are there infinitely many Mersenne primes?
(Only 46 Mersenne primes are known in all!)

**How to Check Primality:** One surefire way to tell whether $n$ is prime is to try to factor it. In other words, for each $k = 2, 3, \ldots, n-1$, simply divide $n$ by $k$ and see if there is a nonzero remainder or not. If there is a remainder of zero (for some $k$) then $n$ is composite. If there is always a nonzero remainder, then $n$ is prime.

**Simplifications:**

(ii) You only need to check this when $k \leq \sqrt{n}$.

(i) You only need to check this when $k = p$ is itself a *prime*.

Evidently, this isn't how large prime numbers are found in practice (it would take too long!). We will talk about more refined primality tests later this week.

*Sample Question:* (Mersenne-like primes in Base 10) We know that:

$$11 \text{ is prime, but } 111 = 3 \cdot 37 \text{ is composite}$$

Notice that $1111 = 11 \cdot 101$, and more generally, whenever $11 \ldots 11$ has a composite number of digits, then it is itself a composite number. But what about when it has a prime number of digits? Is $11,111$ prime? How about $1,111,111$? How about $11,111,111,111$?

To answer the last two questions, we need to keep in mind that the distances between primes jump around "at random," so there aren't going to be nice smooth functions that perfectly pin them down. The *natural logarithm* function, however, comes astoundingly close.

**Definition 1.2:** The *natural logarithm* ("$\ln(a)$" on your calculator) measures the area under the graph of the function $f(x) = 1/x$ and bounded by the lines $x = 1$ and $x = a$.

This is an increasing function, and in a Calculus class you prove that it satisfies the usual properties of log functions:

$$\ln(1) = 0, \quad \ln(ab) = \ln(a) + \ln(b)$$

**Definition 1.3:** The number $e$ (approximately 2.71828) is the unique positive real number with the property that $\ln(e) = 1$.

**The Prime Number Theorem:** *On average*, the distance from one prime number $p$ to the next is approximately $\ln(p)$.

This is a very "deep" theorem which we won't be able to prove here. If you decided to become a math major, it would be a theorem to aspire to understanding by the time you graduate from college. Notice that "on average" is extremely important, since we don't know much at all about the minimum and maximum "gaps" between primes!

On the minimum side, you can't do better than a distance of two (once you clear 2 and 3) because all primes $> 2$ are odd numbers:

**Definition 1.4:** *Twin primes* are primes that differ by two.

*Examples:* 3 and 5, 5 and 7, 11 and 13, 17 and 19.

**Open Problem 2.** Are there infinitely many twin primes?

On the maximum side, little is known. Here are the largest gaps between small primes (relative to their size).

| | Gap |
|---|---|
| 3 to 5 | 2 |
| 7 to 11 | 4 |
| 23 to 29 | 6 |
| 89 to 97 | 8 |
| 113 to 127 | 14 |

**Sample Open Problem 3.** If you could prove that the gap is always:

$$< 2\sqrt{p} + 1$$

then you would be instantly famous (it is suspected to be much smaller, and that would be a consequence of the famous *Riemann Hypothesis*).

**Final Remark:** Let

$$\pi(n) = \text{the number of primes less than or equal to } n$$

The fact that the average distance from $p$ to the next prime is $\ln(p)$ implies that about $1/\ln(p)$ of the numbers near $p$ are prime. Thus we ought to get a good estimate for $\pi(n)$ by taking the area beneath $1/\ln(x)$ from $x = 1$ to $x = n$ (for those of you who know Calculus, $1/\ln(x)$ can't be integrated using any of the tricks of the trade).

This new function is called $Li(x)$. It comes very close to $\pi(n)$.

| n | π(n) | Li(n) (approximately) |
|---|---|---|
| 10 | 4 | 6.1656 |
| 100 | 25 | 30.126 |
| 1000 | 168 | 177.61 |
| 10,000 | 1229 | 1246.1 |
| 100,000 | 9592 | 9629.8 |
| 1,000,000 | 78,498 | 78,728 |

**Really Final Remark:** Gauss and Riemann first observed how close $Li(n)$ came to predicting $\pi(n)$. They conjectured that for all $n$:

$$Li(n) > \pi(n)$$

They were wrong (even the greats can make mistakes once in a while). But the first time the two functions switch so that $Li(n) < \pi(n)$ is probably around $n = 10^{316}$ (that's a 1 followed by 316 zeroes!). It isn't known exactly when it happens. We just know that it does happen (proved by Littlewood in 1914).