Honors 1: Undergraduate Math Lab*

Peter Sarnak[†], Steven Miller[‡], Alex Barnett[§]

September 4^{th}, 2002

Courant Institute of Mathematics
New York University
New York, NY

Abstract

We will review notation, Euclid's Algorithm, Lagrange's Theorem, and prove there are infinitely many primes (three ways: following Euclid, by studying the Riemann Zeta Function $\zeta(s)$ as $s \to 1$, and by analyzing $\zeta(2)$. Lecture by Steven Miller; notes by Alex Barnett and Steven Miller.

1 Notation

- $a|b$: a divides b, *i.e.* the remainder after integer division $\frac{b}{a}$ is 0.
- (a, b) : Greatest Common Divisor (GCD) of a and b. Sometimes written $\gcd(a, b)$.
- $x \equiv y (\bmod n)$: An equality once both sides of the equation have been taken modulo n. Equivalently, there exists an integer a such that $x = y + an$.

---

*Homepage: `http://www.math.nyu.edu/~millerj/`

[†]E-mail: `sarnak@math.princeton.edu`
[‡]E-mail: `millerj@cims.nyu.edu` or `sjmiller@math.princeton.edu`
[§]E-mail: `barnett@nmr.mgh.harvard.edu`

- wlog : 'without loss of generality'. For example, if we have two numbers x and y, it is often convenient to know which is larger and which is smaller. Without loss of generality, we can say $x \leq y$, as the case $x \geq y$ is handled identically (after permuting the variables).
- s.t. : such that.
- $\forall$: for all.
- $\exists$: there exists.
- big O notation : $A(x) = O(B(x))$, read "$A(x)$ is of order $B(x)$", is shorthand for, there is a $C > 0$ (which we can explicitly calculate), s.t. $|A(x)| \leq C\, B(x)$, $\forall x$.
- $|S|$ or $\#S$: number of elements in the set S.
- $\#\{condition\}$: number of objects satisfying the *condition*.
- p : unless otherwise stated, a prime number.
- $\mathbb{Z}$: the set of integers.
- $\mathbb{Z}/n\mathbb{Z}$: the additive group of integers mod n.
- $(\mathbb{Z}/n\mathbb{Z})^*$: the multiplicative group of invertible elements mod n.
- $\mathbb{Q}$: the set of rational numbers. $\mathbb{Q} = \{x : x = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0\}$.
- $\mathbb{R}$: the set of real numbers.
- $\mathbb{C}$: the set of complex numbers.
- $\left(\frac{a}{p}\right)$: Legendre symbol of a and p, defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a, \text{that is, } a = 0 (\text{mod } p) \\ 1, & \text{if } \exists x \text{ s.t. } x^2 = a (\text{mod } p) \\ -1, & \text{if the above does not exist.} \end{cases} \tag{1}$$

  The symbol tests the question, "Does a have a square root in the *field* of arithmetic modulo p?"

- 'weak bound' : an inequality constraining some quantity which does a very poor job of getting close to the true size of the quantity. That is, a not very useful bound.

2 Euclid's algorithm for GCD

Tells you if two positive integers x and y have a GCD greater than 1 by finding it. Therefore it's a 'constructive proof'. It is also 'deterministic' (involves no random choices). A fast procedure, *i.e.* takes only O(log y) steps. Remember that the number of digits $\propto \log y$. wlog we take $y > x$.

Each step is the 'black box' integer division routine we'll call D, which given the pair x, y returns the pair of integers b, r s.t. $r < x$ and satisfying

$$y = bx + r. \tag{2}$$

Note that this step is polynomial in the number of digits (probably $\sim (\log y)^2$ — anyone?).

ALGORITHM:

Start with the pair y, x and perform D to get b_1, r_1.
Perform D on x, r_1 to get b_2, r_2.
Perform D on r_1, r_2 to get b_3, r_3.

$$\vdots$$

Perform D on r_{n-2}, r_{n-1} to get b_n, r_n.

Stop when r_n is either

- 0, in which case r_{n-1} is the GCD, or
- 1, in which case the GCD is 1, that is, x and y are relatively prime.

The procedure works because the D step gives an r which inherits *all* common divisors of y and x. This is easy to see by writing D as $r = y - bx$. Therefore all the adjacent pairs in the sequence $y, x, r_1, r_2 \cdots r_{n-1}$ share the same GCDs. The sequence is also descending $y > x > r_1 > r_2 > \cdots > r_{n-1}$, so must reach the case that $r_{n-1} | r_{n-2}$, in which case r_{n-1} is the GCD and $r_n = 0$, or that a remainder of 1 is reached, which implies no common divisors. We have a worst-case scenario that each remainder is smaller than the previous by a constant factor $c < 1$ (I believe this is the inverse of the Golden Ratio $(\sqrt{5}-1)/2 \approx 0.618 \cdots$ — anyone?), giving geometric (exponential) shrinkage of the r's. Therefore the worst case is that the answer is reached in $n = O(\log\ y)$ steps, and the whole algorithm is therefore polynomial in $\log y$.

3 Lagrange's Theorem

3.1 Basic group theory

Group G is a set of elements g_i satisfying the four conditions below, relative to some binary operation. We often use multiplicative notation ($g_1 g_2$) or additive notation (g_1+g_2) to represent the binary operation. For definiteness, we use multiplicative notation below; however, one could replace xy with $b(x, y)$ below.

If the elements of G satisfy the following four properties, then G is a group.

1. $\exists e \in G$ s.t. $\forall g \in G : eg = ge = g$. (Identity.) We often write $e = 1$ for multiplicative groups, and $e = 0$ for additive groups.
2. $\forall x, y, z \in G :\ (xy)z = x(yz)$. (Associativity.)
3. $\forall x \in G, \exists y \in G$ s.t. $xy = yx = e$. (Inverse.) We write $y = x^{-1}$ for multiplication, $y = -x$ for addition.
4. $\forall x, y \in G : xy \in G$. (Closure.)

If commutation holds ($\forall x, y \in G$, $xy = yx$), we say the group is Abelian. Non-abelian groups exist and are important. For example, consider the group of $N \times N$ matrices with real entries and non-zero determinant. Prove this is a group under matrix multiplication, and show this group is not commutative.

H is a *subgroup* of G if it is a group and its elements form a subset of those of G. The identity of H is the same as the identity of G. Once you've shown the elements of H are closed (ie, under the binary operation, $b(x, y) \in H$ if $x, y \in H$), then associativity in H follows from closure in H and associativity in G.

For the application to Fermat's Little Theorem you will need to know that the set $\{1, x, x^2, \cdots x^{n-1}\}$ where n is the lowest positive integer s.t. $x^n = 1$, called the *cyclic group*, is indeed a subgroup of any group G containing x, as well as n divides the order of G.

For a nice introduction to group theory see: M. Tinkham, *Group Theory and Quantum Mechanics*, (McGraw-Hill, 1964) or S. Lang, *Undergraduate Algebra*.

3.2 Lagrange's Theorem

The theorem states that if H is a subgroup of G then $|H|$ divides $|G|$.

First show that the set hH, *i.e.* all the elements of H premultiplied by one element, is just H rearranged (Cayley's theorem). By closure hH falls within H. We only need to show that hh_i can never equal hh_j for two different elements $i \neq j$. If it were true, since a unique h^{-1} exists we could premultiply the equation $hh_i = hh_j$ by h^{-1} to give $h_i = h_j$, which is false. Therefore $hh_i \neq hh_j$, and we have guaranteed a 1-to-1 mapping from H to hH, so $hH = H$.

Next we show that the sets g_iH and g_jH must either be completely disjoint, or identical. Assume there is some element in both. Then $g_ih_1 = g_jh_2$. Multiplying on the right by $h_i^{-1} \in H$ (since H is a subgroup) gives $g_i = g_jh_2h_1^{-1}$. As H is a subgroup, $\exists h_3 \in H$ such that $h = h_2h_1^{-1}$. Thus $g_i = g_jh_3$. Therefore, as $h_3H = H$, $g_iH = g_jh_3H = g_jH$, and we see if the two sets have one element in common, they are identical. We call a set gH a *coset* (actually, a left coset) of H.

Clearly

$$G = \bigcup_{g \in G} gH \tag{3}$$

Why do we have an equality? As $g \in G$ and $H \subset G$, every set on the right is contained in G. Further, as $e \in H$, given $g \in G$, $g \in gH$. Thus, G is a subset of the right side, proving equality.

There are only finitely many elements in G. As we go through all g in G, we see if the set gH equals one of the sets already in our list (recall we've shown two cosets are either identical or disjoint). If the set equals something already on our list, we do not include it; if it is new, we do. Continuing this process, we obtain

$$G = \bigcup_{i=1}^{k} g_iH \tag{4}$$

for some finite k. If $H = \{e\}$, k is the number of elements of G; in general, however, k will be smaller.

Each set g_iH has $|H|$ elements. Thus, $|G| = k|H|$, proving $|H|$ divides $|G|$.

4 Introduction to Riemann zeta function

4.1 Prelude: Euclid's proof of infinity of primes

Given the set of primes $p_1 \cdots p_n$ you can always construct the number $\prod_{i=1}^{n} p_i + 1$ which is indivisible by any of the given $p_1 \cdots p_n$. Therefore this number must be divisible only by primes greater than p_n, or must be prime itself. Therefore there exists a prime greater than p_n. An analysis of this proof gives a very weak lower bound on the number of primes less than x. The worst case scenario is that $\prod_{i=1}^{n} p_i + 1$ is the next prime. Thus, if we had $n-1$ primes up to $x = \prod_{i=1}^{n-1} p_i + 1$, we would have n primes up to

$$\prod_{i=1}^{n-1} p_i \cdot \Big(\prod_{j=1}^{n} p_j + 1 \Big) + 1 \tag{5}$$

Thus, having at least $n-1$ primes less than x, we have at least n primes less than (basically) x^2. One can quantify this further. One should get something like there are at least n primes less than 2^n or 4^n.

The zeta function will give us other ways to prove this, and to get a better estimate on the *prime counting function*,

$$\pi(x) \;\equiv\; \#\{p < x\}, \tag{6}$$

giving the number of primes below any number x.

4.2 Definition, two forms

The Riemann zeta function $\zeta(s)$ is defined, for $\mathrm{Re}(s) > 1$, by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{7}$$

We prove the useful fact that, for $\mathrm{Re}(s) > 1$,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \;=\; \zeta(s) \;=\; \prod_{\substack{\text{primes}\\ p}} \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{8}$$

which we call LHS and RHS. We call the product over primes an Euler Product.

To show equivalence, we use the Fundamental Theorem of Algebra (FTA) that all positive integers can be expressed as a single, unique, product of prime factors. Expanding all reciprocals in the RHS using the geometric series sum formula $(1-x)^{-1} = 1 + x + x^2 + x^3 + \cdots$, gives for the RHS,

$$(1 + 2^{-s} + 2^{-2s} + 2^{-3s} + \cdots)(1 + 3^{-s} + \cdots)(1 + 5^{-s} + \cdots)\cdots.$$

Remarkably, due to the FTA, we can associate 1-to-1 each term (choice of prime factors) on the RHS with each n on the LHS. For instance, $n = 12$ from LHS is accounted for by the RHS term,

$$2^{-2s} \cdot 3^{-s} \cdot 1 \cdot 1 \cdot 1 \cdots = \frac{1}{(2^2 \cdot 3)^s} = \frac{1}{12}.$$

Each combination of RHS terms corresponds uniquely to a single n.

4.3 $\zeta(s)$'s Behaviour and the Infinitude of Primes

We take the limit of s going to 1 and compare sides. LHS gives

$$\lim_{s\to 1} \zeta(s) \;=\; \lim_{s\to 1} \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n}. \tag{9}$$

This sum diverges. Why? Crudely, $\sum_{n=1}^{N} n^{-1}$ is close to $\int_1^N \frac{dy}{y}$ which equals $\log N$. The definition of 'close' can be tightened up. For instance, you can create upper and lower bounds by approximating the integral by rectangular strips, getting

$$\sum_{n=2}^{N} \frac{1}{n} \leq \int_1^N \frac{dy}{y} \leq \sum_{n=1}^{N-1} \frac{1}{n}. \tag{10}$$

As the two sums differ by a bounded amount, we see the sum grows like $\log N$.

As s goes to 1, if there are only finitely many primes than the product over primes is well behaved (ie, finite). Therefore, there must be infinitely many primes!

Further study of the zeta function will lead us to a good estimate for $\pi(x)$.

A second proof follows from the fact that $\zeta(2m)$ = rational $\cdot\pi^{2m}$, for integer m. This is known as a *Special Values* proof, as we are using the value of $\zeta(s)$ at a special value. We need the fact that π^2 is irrational. $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, which is irrational. Thus, the right hand side (the product over primes) must also be irrational; however, if there are only finitely many primes, when $s = 2$ the right hand side is rational! Thus, there must be infinitely many primes.

Please see Steve's notes, and URLs for more information on all of the above.