Math 156 Summary

Rich Schwartz

September 27, 2009

General Information: M156 is a course in number theory. There is significant overlap between the topics in M42 and the topics in M156, but M156 discusses things at a higher level and goes much further. In this summary, I'll discuss the main topics taught in M156. The online M156 syllabus has a list of additional advanced topics that are covered if time permits. If you have trouble reading this summary, you might want to read the summary for M42 first.

The Euclidean Algorithm: Given positive integers a and b, the *greatest common divisor* of a and b, denoted (a, b) is the largest integer d which divides both. It turns out that d is the minimum positive value of the set of integer combinations

$$\{ma + bn |\ m, n \in \boldsymbol{Z}\}.$$

In particular, there exist integers m and n such that

$$d = am + bn. \tag{1}$$

Note, however, that m and n are not unique. The *Euclidean Algorithm* produces d and a pair m, n satisfying Equation 1. We order so that $a < b$ and set $a_0 = a$ and $b_0 = b$. Given $a_k < b_k$, produced by the algorithm, we write

$$a_{k+1} = \min(a_k, b_k - a_k); \qquad b_{k+1} = \max(a_k, b_k - a_k).$$

Eventually, we reach $a_n = b_n = d$. Keeping track of the steps in the algorithm–e.g. whether $a_k < b_k - a_k$ at each step, we can produce m and n.

Congruences: We write $a \equiv b \bmod n$ if $a - b$ is divisible by n. Let $\boldsymbol{Z}/n\boldsymbol{Z}$

denote the set of equivalence classes mod n. If m and n are relatively prime, we have a map

$$F : \boldsymbol{Z}/mn\boldsymbol{Z} \to \boldsymbol{Z}/m\boldsymbol{Z} \times \boldsymbol{Z}/n\boldsymbol{Z}.$$

We just take our element of $\boldsymbol{Z}/mn\boldsymbol{Z}$ and list out its class mod m and its class mod n. The Chinese Remainder Theorem says that this map is a bijection.

One can use the Chinese Remainder Theorem to understand relative primality. Let $(\boldsymbol{Z}/n\boldsymbol{Z})^*$ denote those elements in $\boldsymbol{Z}/n\boldsymbol{Z}$ that are relatively prime to n. A number relatively prime to mn is relatively prime to both m and n and vice versa. So, when $(m, n) = 1$, the map above induces a map

$$F^* : (\boldsymbol{Z}/mn\boldsymbol{Z})^* \to (\boldsymbol{Z}/m\boldsymbol{Z})^* \times (\boldsymbol{Z}/n\boldsymbol{Z})^*.$$

This map is a bijection by the Chinese Remainder Theorem. Letting $\phi(n)$ denote the cardinality of $(\boldsymbol{Z}/n\boldsymbol{Z})^*$, we get

$$\phi(mn) = \phi(m)\phi(n) \tag{2}$$

when $(m, n) = 1$. One checks easily that

$$\phi(p^k) = p^k - p^{k-1} \tag{3}$$

when p is prime. Combining Equations 2 and 3 one can easily evaluate $\phi(n)$ provided that n has been factored into primes. The fact that $\phi(n)$ is often hard to compute if n has <u>not</u> been factored into primes is the basis for the famous RSA public key cryptosystem. The M42 summary discusses the RSA system in detail.

In M156 (and also M153) you prove Euler's Theorem:

$$a^{\phi(n)} \equiv 1 \mod n. \tag{4}$$

Here $(a, n) = 1$. As a special case, when $n = p$ is prime, we have $\phi(p) = p-1$, and we get Fermat's Theorem:

$$a^{p-1} \equiv 1 \mod n. \tag{5}$$

The formulas for $\phi(n)$ above make Euler's theorem useful in practice.

Multiplicative Functions: A function $f : \boldsymbol{N} \to \boldsymbol{Z}$ is *multiplicative* if $f(mn) = f(m)f(n)$ when $(m, n) = 1$. We have already seen that Euler's ϕ-function is multiplicative. Here are some other examples.

- Let $I(1) = 1$ and otherwise $I(n) = 0$.
- Let $e(n) = 1$ for all n.
- Let $f(n)$ equal to the sum of the divisors of n. For instance

$$f(6) = 1 + 2 + 3 + 6 = 12.$$

- The *Mobius function* μ such that $\mu(p^n) = (-1)^n$ provided that p is prime. Otherwise $\mu(n) = 0$.

In M156, you see a beautiful "convolution formula" which produces new multiplicative functions out of old:

$$f * g(n) = \sum_{d|n} f(d)g(n-d).$$

The sum takes place over all divisors of n. Once you know that $f * g$ is multiplicative, you can give easy proofs that other functions are multiplicative. Taking our example f from above, we have $f = e * e$. This proves that the "sum of the divisors" is a multiplicative function.

We also have the formula

$$e * \mu = I.$$

This gives the so-called *Mobius inversion formula*:

$$F = f * e \qquad \Longrightarrow \qquad f = F * \mu. \tag{6}$$

Here $F(n)$ is obtained by summing the values of f over all divisors of n. You can think of F as a kind of integral of F. The Mobius inversion formula tells us how to reverse the process and recover f from F.

Primes: In M156, you see the (easy) proof that every positive integer factors uniquely into primes, provided that the primes are written in increasing order. It is also an easy result that there are infinitely many primes: The number $N! + 1$ is not divisible by and number $k \leq N$, so there must be some prime greater than N.

Here is a quick proof that there are infinitely many primes congruent to 3 mod 4. Let $p_1, ..., p_n$ be the list of the first n primes that are congruent to 3 mod 4. Consider the product $4p_1...p_n + 3$. This number is congruent to

3 mod 4 and consequently must be divisible by some prime congruent to 3 mod 4. On the other hand, this number is not divisible by and of our listed primes. So, there is some larger prime congruent to 3 mod 4.

A much more difficult result is *Dirichlet's Theorem*: If $(a, n) = 1$ then there are infinitely many primes congruent to a mod n. One might wonder if there is a trick, similar to the one above, for proving Dirichlet's Theorem in general. The only known proofs are deeper, and are based on *Dirichlet L-functions*. See the Analyic Number Theory section below.

Another beautiful result about the infinitude of primes is *Euler's Theorem:*

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty. \tag{7}$$

This result is also proved by analysis, but the analysis is pretty soft. We sketch a proof in the Analytic Number Theory section.

The famous *Prime Number Theorem* says roughly that there are about $n/\ln(n)$ primes between 1 and n.

Finite Fields: A *field* is a set F together with two operations, addition and multiplication, which satisfy the same algebraic axioms (e.g. distributive law, associative law, existence of inverses...) that the rationals $\boldsymbol{Q}$ satisfy. See the M153 summary for a precise definition.

Amazingly, there are finite fields. For instance, $\boldsymbol{Z}/p\boldsymbol{Z}$ is a finite field when p is prime. As another example, consider the set F of all sums $a + bi$ where $a, b \in \boldsymbol{Z}/5\boldsymbol{Z}$ and i is a formal symbol such that $i^2 = [2]$ in $\boldsymbol{Z}/5\boldsymbol{Z}$. You can add and multiply these expressions together, and you can also divide by nonzero expressions. In short, it turns out that F is a finite field with $25 = 5^2$ elements. Using more sophisticated constructions like this, one shows that there exists a field of order p^n for any prime p and any positive integer n.

Let F be a finite field. In M156 you prove the *Primitive Element Theorem* which shows that there is some element $f \in F$ such that every nonzero element of F is a power of f. That is, $F = \{0, f, f^2, f^3, ...\}$.

Quadratic Reciprocity: For p an odd prime, An integer a is a *quadratic residue* mod p if the equation $x^2 \equiv k$ mod p has a solution. One writes $(k/p) = 1$ if k is a quadratic residue mod p and $(k/p) = -1$ if not. There are a number of interesting results about quadratic residues.

- If p is an odd prime than $(-1/p) = 1$ if and only if $p \equiv 1$ mod 4. This

is closely related to the theorem that p can be written as the sum of two squares if and only if $p \equiv 1 \bmod 4$.

- Euler's Criterion:
$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p.$$

- If p and q are odd primes then $(q/p) = (p/q)$ if and only if $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$.

The last result is the bulk of Gauss's famous *Quadratic Reciprocity Theorem*. The other part of the QRT discusses what happens when one of the primes is 2. The QRT gives you an algorithm for determining whether one number of a quadratic residue mod another one. In M156 you see both the algorithm and a proof of Quadratic Reciprocity.

Diophantine Equations A *Diophantine Equation* asks for integer solutions to polynomial equations. The most famous Diophantine equation is probably $a^2 + b^2 = c^2$. Integer solutions to this equation are known as *Pythagorean Triples*. On easy topic in M1156 is a complete classification of the Pythagorean Triples. This is also done in M42.

The famous Fermat's Last Theorem says that the equation $a^n + b^n = c^n$ has no integer solutions for $n \geq 3$. Andrew Wiles proved this about 10 years ago, but Fermat actually did succeed in proving this result when $n = 4$. His technique is called the *method of descent*. You start with a supposed smallest solution (a, b, c) and through algebraic manipulations produce a smaller solution (a', b', c'), thus arriving at a contradiction. In M156 you apply the method of descent to the equation $a^4 + b^4 = c^4$ and perhaps to some related equations.

Another classic equation is *Pell's Equation*. Pell's equation asks for positive integer solutions to the equation

$$x^2 - Dy^2 = 1.$$

where $D > 0$ is an integer that is not a perfect square. For instance, the pair $(x, y) = (3, 2)$ is a solution to the equation $x^2 - 2y^2 = 1$. Given one solution you can produce infinitely many. For example, if you write

$$(3 + 2\sqrt{2})^n = a_n + b_n\sqrt{2}.$$

Then (a_n, b_n) is also a solution to $x^2 - 2y^2 = 1$. In fact, all solutions to the equation $x^2 - 2y^2 = 1$ arise in this way. In M156, you prove that the general case has infinitely many solutions, and they have the same structure I suggested for the case $D = 2$.

Analytic Number Theory: We already mentioned two applications of analyic number theorem, Dirichlet's Theorem and Equation 7. The proof of Equation 7 is based on the famous *Euler product formula*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod \frac{1}{1 - p^{-s}} \tag{8}$$

and hinges on the fact that both sides of this equation converge when $s > 1$, and diverge as $s \to 1$.

One can use some easy calculus to show that

$$\frac{2}{p_i^s} > \log\left(\frac{1}{1 - p^{-s}}\right), \tag{9}$$

which holds for any $p_i \geq 2$ and $s > 1$. The Euler Product Formula then tells us that

$$\sum \frac{2}{p_i^s} > \sum \log\left(\frac{1}{1 - p^{-s}}\right) = \log\left(\sum \frac{1}{n^s}\right) \to \infty$$

as $s \to 1^+$ and Equation 7 follows.

The left hand side of Equation 8 above is called the *Riemann zeta function*

$$\zeta(s) = \sum \frac{1}{n^s}.$$

The proof of Equation 7 only uses the fact that $\zeta(1) = \infty$, but the proof of the prime number theorem uses the exact behavior of $\zeta(s)$ as $s \to 1$. One classical result is that $\zeta(s)$ is defined and meromorphic (i.e. complex analytic) when s is allowed to be a complex parameter. Probably the most famous conjecture of all time is the *Riemann Hypothesis*: All the zeros of $\zeta(s)$ lie on the line $1/2 + it$. If Jeff Hoffstein teaches M156, he will explain his recent proof of the Riemann Hypothesis.

A classical *Dirichlet L-function* is a generalization of $\zeta(s)$ of the form

$$L(s, \chi) = \sum \frac{\chi(n)}{n^s},$$

where $\chi : \boldsymbol{Z} \to \boldsymbol{C}$ is a homomorphism from $\boldsymbol{Z}$ into the circle of unit complex numbers. The function χ is known as a *character*. The proof of Dirichlet's Theorem on the infinitute of primes congruent to a mod n is based on the knowledge of the analytic behavior of $L(s, \chi)$.