Math 42 Sampler

Rich Schwartz

September 23, 2009

General Information: M42 is a friendly introduction to number theory. This course is designed to appeal to students who are interested in mathematics but who might not actually concentrate in math. The course is very accessible. It starts pretty much from scratch and tries to be as self-contained as possible. M42 comprises a whole bunch of different interesting topics. In this summary, I'll give you a sample of them. So, actually, this is more like a sampler than a summary.

Pythagorean Triples: The Pythagorean Theorem says that $a^2 + b^2 = c^2$, where a and b are the short sides of a right triangle and c is the long side. A *Pythagorean triple* is a solution to this equation where a, b, c are all integers. The best known one is the $3^2 + 4^2 = 5^2$. The triple here is $(3, 4, 5)$. Another triple is $(5, 12, 13)$. It turns out that there are infinitely many Pythagorean triples, even if you assume that a, b, c have no common factors. In M42 you study the Pythagorean triples and find a formula that generates all of them.

Primes and Composites: An integer $p > 1$ is called *prime* if p has no divisors other than 1 and p. That is, no positive integers divide evenly into p except 1 and p itself. The first few primes are $2, 3, 5, 7, 11, 13, 17, 19$. An integer greater than 1 is called *composite* if it is not prime. In M42 you will probably learn two classic results.

- Every integer greater than 1 factors uniqely into primes. For instance $60 = 2 \times 2 \times 3 \times 5$.
- Euclid's Theorem: There are infinitely many primes.

A more advanced result, which you might learn in M42 is Euler's Theorem:

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \ldots = \infty.$$

Here $p_1, p_2, p_3, \ldots$ is the list of primes. Euler's Theorem is a more sophisticated way of saying that there are infinitely many primes.

Perfect Numbers and Mersenne Primes: An integer N is perfect if N equals the sum of its divisors. For instance,

$$6 = 1 + 2 + 3; \qquad 28 = 1 + 2 + 4 + 7 + 14.$$

A *Mersenne Prime* is a number of the form $2^p - 1$ that happens to be prime. Here p is another prime. Nobody knows if there are infinitely many Mersenne primes, though two new ones were found at UCLA last year.

One result you will prove in M42 is that $2^{p-1}(2^p - 1)$ is a perfect number provided that $2^p - 1$ is a Mersenne prime. You will also prove Euler's theorem: If N is an even perfect number than $N = 2^{p-1}(2^p - 1)$ for some prime p. That is, the Mersenne primes account for all the even perfect numbers. Nobody knows about odd perfect numbers.

The Euclidean Algorithm: Given two positive integers a and b, the *greatest common divisor* is the largest integer d such that d divides both a and b. This expression is denoted by (a, b). One way to find (a, b) is to factor both numbers into primes and to pull out the common factors. This works just fine in theory, but it is very slow for large pairs (a, b). There is a much better method, called the *Euclidean Algorithm.* I'll sketch the idea. If $a < b$ then $(a, b - a) = (a, b)$. That is, you don't change the greatest common divisor when you consider the smaller pair $(a, b - a)$ instead of (a, b). Let

$$a' = \min(a, b - a); \qquad b' = \max(a, b - a).$$

Then $(a', b') = (a, b)$. Continuing, let

$$a'' = \min(a', b' - a'); \qquad b'' = \max(a', b' - a').$$

We have $(a'', b'') = (a', b') = (a, b)$. Continuing in this way, we eventually arrive at the pair (d, d). Keeping track of the various subtractions we made, the Euclidean Algorithm also produces a pair of integers (m, n) such that

$am + bn = d$.

Modular Arithmetic: If n divides the difference $a - b$, one writes

$$a \equiv b \mod n.$$

For instance, $7 \equiv 2$ mod 5. To relate this to the previous topic, if $(a, b) = 1$ and m and n are such that $am+bn = 1$ then $am \equiv 1$ mod b. When $(a, b) = 1$, the numbers a and b are said to be *relatively prime*.

In M42 you get practice solving linear equations like $7x + 2 \equiv 5$ mod 17. You also learn several nice theorems concerning modular arithmetic.

- Fermat's Theorem: If p is prime then $a^p \equiv a$ mod p for any integer a.
- If p is prime then Wilson's Theorem: $(p - 1)! \equiv -1$ mod p.

Fermat's Theorem has a nice generalization. For any positive integer N, let $\phi(N)$ denote the number of numbers n in the list $1, ..., N$ such that $(n, N) = 1$. For instance $\phi(6) = 2$ because 1 and 5 are the only numbers between 1 and 6 that are relatively prime to 6. It turns out that

$$a^{\phi(n)} \equiv 1 \mod N$$

provided that $(a, N) = 1$. This result is known as Euler's Theorem.

RSA Crytography: Euler's Theorem is the basis for a famous way of sending encoded messages, known as RSA public key cryptography. Here is the idea. Let p and q be (large) primes and let $N = pq$. In this case, it turns out that $\phi(N) = (p - 1)(q - 1)$. The important point here is that for large primes you can only compute $\phi(N)$ if you know that N factors as pq.

Suppose you own a company and you want to collect encoded messages from people. You want anyone to be able to send you a message, but you don't want strangers to be able to decode the messages. So, you choose p and q as above and you tell the world about $N = pq$ while keeping p and q secret. Next, you choose e such that $(e, \phi(N)) = 1$. You also tell the world about e. The number e is the "encoder".

Since e and $\phi(N)$ are relatively prime, you can use the Euclidean algorithm to find a pair (d, m) such that

$$ed - m\phi(n) = 1.$$

You keep d and m secret. You don't really care about m, but d is very important. d is the decoder.

Let's think of messages as numerical strings. (For instance $a = 1$ and $b = 2$,. etc.) Someone sends you a message as follows. Let's say that N has 200 digits. The person breaks up their message into a series of pieces $a_1, a_2, ...$, consisting of at most 200 digits each. They then send you the blocks $b_1, b_2, ...$ where

$$b_k = a_k^e \mod N.$$

That is, they raise each block of their message to the eth power and then subtract off multiples of N until the result lies between 0 and N. This is b_k, the kth encoded block.

The miracle is that

$$(b^k)^d = (a_k)^{de} = (a_k)^{1+k\phi} = a_k \times ((a_k)^{\phi})^m \equiv^* a_k \times 1^m = a_k \mod N.$$

Here I've set $\phi = \phi(N)$. The crucial starred equality comes from Euler's Theorem. So, raising the coded message to the dth power decodes the message! In M42 you learn not only about this algorithm but how it is efficiently implemented.

Primality Testing: One needs a supply of large primes for the RSA cryptosystem. One way to find such primes is to pick large integers at random and then test whether they are prime. It turns out that there are rather a lot of primes, as indicated by Euler's Theorem (mentioned above) or a more precise statement called the Prime Number Theorem. In M42 you might learn about how one tests whether a number p is prime. Of course, one could just check that p is prime just by checking that no number smaller than p (or, better $\sqrt{p}$) divides p. However, this is much too slow in practice.

One can verify that p is composite by computing that

$$(*) \qquad a^p \equiv a \mod p$$

fails for some choice of a. If you pick lots of different values of a at random and observe that $(*)$ always holds, you might suspect that p is prime. However, this is not true. There are composite numbers, called *Carmichael numbers*, for which $(*)$ always holds.

There is a more sophisticated test, called *Rabin's statistical primality test*, that is based on the same idea. Every time p passes a modified test for a random choice of a, the chance that p is composite essentially cuts in half. So,if p passes the test for (say) 1000 random inputs, the chances that p is composite are less than the chance that all the molecules in your body will suddenly be transported to the moon due to quantum fluctuations.

Around 10 years ago, M. Agrawal and his student collaborators developed an ironclad (i.e. deterministic) primality test that is just about as fast as Rabin's test. Passing Agrawal's test tells you for sure that p is prime. This test is slightly outside the scope of M42, but it might serve as a special topic for the class.

Multiplicative Functions: The Euler ϕ function has the property that $\phi(mn) = \phi(m)\phi(n)$ provided that m and n are relatively prime. A function with this property is called *multiplicative*. To determine the value of a multiplicative function like ϕ on an integer N, you factor N into primes as

$$N = p_1^{k_1}...p_m^{k_m},$$

and then note that

$$\phi(N) = \phi(p_1^{k_1})...\phi(p_m^{k_m}).$$

In the case of the ϕ function, we have

$$\phi^{p^k} = p^k - p^{k-1}.$$

Combining the last two equations gives a general formula for $\phi(N)$ which agrees with the value $\phi(pq) = (p-1)(q-1)$ discussed above.

There are many other examples of multiplicative functions. For instance, one can define $\alpha(n)$ to be the sum of the divisors of n. For instance $\alpha(6) = 1 + 2 + 3 + 6 = 12$. This function turns out to be multiplicative. In general, if f and g are multiplicative functions, so is the new function

$$f * g(n) = \sum_d f(d)g(n/d).$$

The sum takes place over all numbers d that divide n. In M42 you will study the properties of this weird "product" of multiplicative functions.

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 M42 you might see Pell's Equation Theorem: the general case has infinitely many solutions, and they have the same structure as I suggested for the case $D = 2$.

Square-Triangular Numbers: A number is a *triangular number* if it has the form

$$1 + 2 + 3 + ... + n.$$

On the other hand, a number is a *square number* if it is a perfect square. The number 36 is both a triangular number and a square number, because

$$36 = 1 + ... + 8 = 6^2.$$

It turns out that there are infinitely many integers that are both square and triangular. Using the result for Pell's Equation, you can classify exactly which integers are both square and triangular.

Quadratic Residues: An integer k is a *quadratic residue* mod N if the equation $x^2 \equiv k \bmod N$ has a solution. One writes $(k/N) = 1$ if k is a quadratic residue mod N and $(k/N) = -1$ 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 $p \equiv 1 \bmod 4$. This is closely related to the theorem that p can be written as the sum of two squares if and only if $p \equiv 1 \bmod 4$.
- If p and q are odd primes then $(q/p) = (p/q)$ if and only if $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$. This is part of Gauss's famous *Quadratic Reciprocity Theorem.* Gauss's theorem gives you an algorithm for determining whether one number of a quadratic residue mod another one. In M42 you might learn this algoritm.

The proof of Gauss's theorem is somewhat beyond the scope of M42, though I gave the complete proof when I taught it.