Scribe Notes for *Algorithmic Number Theory*
Class 2—May 19, 1998

Scribes: Lynn Jones, Nick Loehr, and Hussein Suleman

Abstract

This class continued the review of number theory. We defined multiplicative functions, Euler's ϕ-function, and the Möbius function; we also stated the Möbius inversion formula. We introduced some notations relevant to the asymptotic growth rate of functions. Finally, we discussed formulae for approximating sums by integrals, approximating integrals by bounding error terms, and approximating sums of functions over primes.

1 Function Definitions

1.1 Multiplicative functions

A function for which

$$f(mn) = f(m)f(n)$$

whenever m and n are relatively prime, is said to be *multiplicative*. Euler's ϕ-function and the Möbius function (defined below) are each multiplicative.

1.2 Euler's ϕ-Function

Euler's ϕ-function is defined on positive integers as follows:

$$\phi(n) = \sum_{\substack{1 \le k \le n \\ \gcd(k,n) = 1}} 1$$

This function counts the number of integers less than or equal to n that are relatively prime to n. For prime numbers p, all integers less than p are relatively prime to p and so

$$\phi(p) = p - 1$$

More generally (see equation 2.2 in the text), if n has prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $e_i > 0$ for each i, then

$$\phi(n) = \prod_{1 \le i \le k} (p_i - 1) p_i^{e_i - 1}$$

The proof for this equation is given as the solution to exercise 7 in Chapter 2 and may be found on page 319. Table 1 lists values of $\phi(n)$ for $1 \le n \le 10$. As stated earlier, the ϕ function is multiplicative.

n	$\phi(n)$	Values of $k \leq n$ with $\gcd(k,n) = 1$	$\mu(n)$	Comment
1	1	{1}	1	product of 0 primes
2	1	{1,2}	-1	
3	2	{1,2}	-1	
4	2	{1,3}	0	divisible by 2^2
5	4	{1,2,3,4}	-1	
6	2	{1,5}	1	product of 2 primes
7	6	{1,2,3,4,5,6}	-1	
8	4	{1,3,5,7}	0	divisible by 2^2
9	6	{1,2,4,5,7,8}	0	divisible by 3^2
10	4	{1,3,7,9}	1	product of 2 primes

Table 1: Values of $\phi(n)$ and $\mu(n)$ for $1 \leq n \leq 10$.

Example 1.1. Since 2 and 5 are relatively prime,

$$\phi(2)\phi(5) = 1 \times 4 = 4 = \phi(10).$$

However, note that

$$\phi(5) \times \phi(5) = 4 \times 4 = 16 \neq 20 = \phi(25).$$

This inequality does not violate the definition of multiplicative functions, since $\gcd(5,5) \neq 1$.

1.3 Möbius Function

The Möbius function μ is defined for positive integers n as follows.

$$\mu(n) \quad = \quad \begin{cases} 0 & \text{if } n \text{ is divisible by a square larger than 1} \\ (-1)^t & \text{if } n = p_1 p_2 \cdots p_t, \text{ the product of } t \text{ distinct primes.} \end{cases}$$

The Möbius function is also multiplicative. To see this, let m and n be relatively prime. If either m or n is divisible by a square greater than 1, then mn is also divisible by a square greater than 1. So $\mu(mn) = 0 = \mu(m)\mu(n)$, since one of the latter two factors must be zero. If neither m nor n is divisible by a square greater than 1, we have $m = p_1 p_2 \cdots p_t$ and $n = q_1 q_2 \cdots q_s$ for primes $p_1, \ldots, p_t, q_1, \ldots, q_s$. These primes must be *distinct*, since m and n have no common factors. Thus, $\mu(mn) = (-1)^{t+s} = (-1)^t(-1)^s = \mu(m)\mu(n)$, as desired. Table 1 lists values of $\mu(n)$ for some small values of n. Note that for any prime p, $\mu(p) = -1$.

2 The Möbius Inversion Formula

The *Möbius Inversion Formula* is useful when we have a function $g(n)$ that is defined in terms of another function f evaluated at the positive divisors of n, i.e.,

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

Suppose we wish to solve for f in terms of the values of g. The Möbius Inversion formula (Theorem 2.3.1) states that

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Example 2.1. Let $f(n) = n^2$. Set $g(n) = \sum_{d|n} d^2$. For $n = 10$, let us verify explicitly that

$$f(10) = 100 = \sum_{d|10} \mu(d) g\left(\frac{10}{d}\right).$$

First, calculate the values for $g(n)$ at the divisors of 10:

$$\begin{array}{rcccccc} g(10/1) & = & g(10) & = & 1^2+2^2+5^2+10^2 & = & 130 \\ g(10/2) & = & g(5) & = & 1^2+5^2 & = & 26 \\ g(10/5) & = & g(2) & = & 1^2+2^2 & = & 5 \\ g(10/10) & = & g(1) & = & 1^2 & = & 1 \end{array}$$

Next, find $\mu(d)$ for the divisors of 10 (cf. Table 1):

$$\begin{array}{rcl} \mu(1) & = & 1 \\ \mu(2) & = & -1 \\ \mu(5) & = & -1 \\ \mu(10) & = & 1 \end{array}$$

Finally, sum the values $\mu(d)g(10/d)$:

$$1 \times 130 - 1 \times 26 - 1 \times 5 + 1 \times 1 = 100$$

We can also write this calculation as

$$(1^2+2^2+5^2+10^2) - (1^2+5^2) - (1^2+2^2) + (1^2) = 10^2.$$

Note that the Möbius Inversion Formula is somewhat reminiscent of the popular Inclusion-Exclusion Principle from CS 5024. The formula can actually be proved as a corollary to that principle. One more useful property of the Möbius function is given by Lemma 2.3.3:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

3 Asymptotic Growth Rates of Functions

In order to better understand the behavior of functions, they can be compared to other well-known functions. These comparisons allow us to infer relationships about the similarity in growth rates of functions as the functional parameter tends to ∞.

We will use the following notation to describe the relative growth rates of functions. Detailed technical definitions of these symbols are given in Definition 2.4.1.

- $f(n) = O(g(n))$ if f grows no faster than g. This 'Big O' relationship is akin to a $\leq$ comparison. Constant factors are ignored in this relationship.

  Example 3.1. $3n^2 + 4n - 7 = O(n^2)$.

- $f(n) = \Omega(g(n))$ if $f(n)$ grows at least as quickly as $g(n)$ ("$f \geq g$").

- $f(n) = \Theta(g(n))$ if $f(n)$ grows at the same rate as $g(n)$, ignoring constant factors ("$f = g$").

- $f(n) = o(g(n))$ if $f(n)$ is smaller than $g(n)$, i.e., $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$. This 'small o' notation is similar to a strict less-than relationship. In this relationship, additive terms are important.

  Example 3.2. Recalling the prime number theorem, we can rewrite it as:

  $$\pi(x) \quad = \quad \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

  Here, the second term represents the error, and it is asymptotically "smaller" than the first term.

- $f(n) \sim g(n)$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$. Note that, in this one case, constant factors *cannot* be ignored.

  Example 3.3. Yet another way of stating the prime number theorem is as follows:

  $$\pi(x) \sim \frac{x}{\log x}.$$

4 Approximation by Integrals

4.1 Euler's Summation Formula (Corollary 2.5.2)

Theorem 4.1. *Let f be continuously differentiable on $[1, x]$. Then*

$$\sum_{1\leq k\leq x} f(k) = \int_1^x f(t)dt + f(1) - (x - \lfloor x \rfloor) + \int_1^x (t - \lfloor t \rfloor) f'(t)dt.$$

Here, k is an integer, and x is real.

For a proof, see Corollary 2.5.2 in Bach & Shallit [1]. The first term represents the general approximation and the other terms compensate for the error incurred in the approximation. The general idea when using this formula is to calculate the approximation term and bound the error terms.

Example 4.2. (Theorem 2.5.3 in Bach & Shallit [1])
Consider the harmonic series, defined by:

$$H_n = \sum_{1\leq k\leq n} \frac{1}{k}$$

It is well known that this series diverges when $n \to \infty$. To approximate this series for integer values of n, we can set $f(x) = \frac{1}{x}$. Then $f'(x) = -\frac{1}{x^2}$.

Now, by Euler's Summation Formula,

$$\begin{aligned} H_n &= \int_1^n \frac{dt}{t} + 1 + \int_1^n -\frac{t - \lfloor t \rfloor}{t^2} dt \\ &= \log n + \left(1 - \int_1^\infty \frac{t - \lfloor t \rfloor}{t^2}\right) + \int_n^\infty \frac{t - \lfloor t \rfloor}{t^2} dt \end{aligned}$$

Let γ denote the constant $(1 - \int_1^\infty \frac{t-\lfloor t \rfloor}{t^2} dt)$, which is called *Euler's constant*. The error has now been reduced to the sum of γ and the integral $\int_n^\infty \frac{t-\lfloor t \rfloor}{t^2} dt$. This integral can be bounded above as follows:

$$\int_n^\infty \frac{t - \lfloor t \rfloor}{t^2} dt < \int_n^\infty \frac{dt}{t^2} = O\left(\frac{1}{n}\right)$$

Thus,

$$H_n = \log n + \gamma + O\left(\frac{1}{n}\right).$$

5 Asymptotic Approximation of Integrals

Theorem 2.6.1 in Bach and Shallit [1] provides useful formulae for approximating the asymptotic behavior of certain integrals. Assume that f is a continuously differentiable function on $[a, \infty)$. Assume further that

$$\frac{f'(x)}{f(x)} \sim \frac{\mu}{x}$$

for some real constant $\mu > -1$. If $\mu \neq 0$, then

$$\int_a^x f(t)dt \sim \frac{xf(x)}{\mu + 1}. \tag{1}$$

If $\mu = 0$, the same formula holds *provided* that $f'(x)/f(x)$ approaches zero "quickly" enough. Formally, we have

$$\int_a^x f(t)dt \sim xf(x) \tag{2}$$

provided that $f'(x)/f(x) = o(1/x)$.

To gain an intuitive understanding of these formulae, suppose $f(x)$ is the polynomial x^μ. Then $f'(x) = \mu x^{\mu-1}$ and so $f'(x)/f(x)$ exactly equals μ/x. The formula $xf(x)/(\mu + 1)$ is simply the antiderivative of $f(x)$ evaluated at the upper limit x. (Note that evaluating the antiderivative at the lower limit a only changes the definite integral by an additive constant. So we may disregard this limit when finding asymptotic approximations.) Roughly speaking, the theorem states that the formula $xf(x)/(\mu + 1)$ still gives a good approximation for the integral, assuming that the growth rate of f is "similar to" the growth rate of x^μ.

Example 5.1. Consider the integral $\int_2^x \frac{dt}{\log t}$. Let $f(x) = 1/(\log x)$; then $f'(x) = -1/(x \log^2 x)$ and we find that

$$\frac{f'(x)}{f(x)} = \frac{-1}{x \log x} = o\left(\frac{1}{x}\right).$$

Using formula (2) gives

$$\int_2^x \frac{dt}{\log t} \sim x f(x) = \frac{x}{\log x}. \tag{3}$$

Example 5.2. Consider the integral $\int_2^x \frac{t\,dt}{\log t}$. Now let $f(x) = x/(\log x)$; an easy calculation shows that $f'(x) = (\log x - 1)/\log^2 x$ and

$$\frac{f'(x)}{f(x)} = \frac{\log x - 1}{x \log x} = \frac{1}{x} + o\left(\frac{1}{x}\right).$$

So $f'(x)/f(x) \sim 1/x$. Taking $\mu = 1$ in formula (1) gives

$$\int_2^x \frac{t\,dt}{\log t} \sim \frac{x f(x)}{\mu + 1} = \frac{x^2}{2 \log x}. \tag{4}$$

6 Evaluating Summations over Primes

Suppose we wish to approximate the summation $\sum_{p \le x} f(p)$, where p runs over all the primes not exceeding x. Theorem 2.7.1 in Bach and Shallit [1] gives an approximation formula for such sums. Recall that, by the Prime Number Theorem,

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

By Example 5.1, we know that

$$\int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}.$$

So we may write

$$\pi(x) = \int_2^x \frac{dt}{\log t} + \epsilon(x)$$

where the error term $\epsilon(x)$ is $o(x/\log x)$. Then Theorem 2.7.1 states that

$$\sum_{p \le x} f(p) = \int_2^x \frac{f(t)dt}{\log t} + \epsilon(x) f(x) - \int_2^x \epsilon(t) f'(t) dt. \tag{5}$$

The first term on the right hand side gives an asymptotic approximation for the sum, assuming we can bound the remaining two error terms.

Example 6.1. Consider the sum of the primes not exceeding x. Using the formula (5) with $f(x) = x$, we get

$$\sum_{p \le x} p = \int_2^x \frac{t\,dt}{\log t} + x\epsilon(x) - \int_2^x \epsilon(t) dt.$$

We saw earlier (Example 5.2) that the first integral on the right hand side can be asymptotically approximated by $x^2/(2\log x)$. Since $\epsilon(x) = o(x/\log x)$, it is clear that the terms $x\epsilon(x)$ and $\int_2^x \epsilon(t)dt$ are each $o(x^2/\log x)$. Thus, we obtain the approximation

$$\sum_{p \le x} p \sim \frac{x^2}{2\log x},$$

which is correct up to an additive error term.

7 Next Time

The next class will cover important algebraic structures such as groups, rings, and fields.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, The MIT Press, Cambridge, Massachusetts, 1996.