ARITHMETICAL FUNCTIONS III: ORDERS OF MAGNITUDE

1. Introduction

Having entertained ourselves with some of the more elementary and then the more combinatorial/algebraic aspects of arithmetical functions, we now grapple with what is fundamentally an analytic number theory problem: for a given arithmetical function f, approximately how large is $f(n)$ as a function of n?

It may at first be surprising that this is a reasonable – and, in fact, vital – question to ask even for the "elementary" functions f for which we have found exact formulas, e.g. $d(n)$, $\sigma(n)$, $\varphi(n)$, $\mu(n)$ (and also $r_2(n)$, which we have not yet taken the time to write down a formula for but could have based upon our study of the Gaussian integers). What we are running up against is nothing less than the multiplicative/additive dichotomy that we introduced at the beginning of the course: for simple multiplicative functions f like d and φ, we found exact formulas. But these formulas were not directly in terms of n, but rather made reference to the standard form factorization $p_1^{a_1} \cdots p_r^{a_r}$. It is easy to see that the behavior of, say, $\varphi(n)$ as a function of "n alone" cannot be so simple. For instance, suppose $N = 2^p - 1$ is a Mersenne prime. Then

$$\varphi(N) = N - 1.$$

But

$$\varphi(N+1) = \varphi(2^p) = 2^p - 2^{p-1} = 2^{p-1} = \frac{N+1}{2}.$$

This is a bit disconcerting: $N + 1$ is the tiniest bit larger than N, but $\varphi(N + 1)$ is half the size of $\varphi(N)$!

Still we would like to say something about the size of $\varphi(N)$ for large N. For instance, we saw that for a prime p there are precisely $\varphi(p - 1)$ primitive roots modulo p, and we would like to know something about how many this is.

Ideal in such a situation would be to have an asymptotic formula for φ: that is, a simple function $g : \mathbb{Z}^+ \to (0, \infty)$ such that $\lim_{n\to\infty} \frac{\varphi(n)}{g(n)} = 1$. (In such a situation we would write $\varphi \sim g$.) But it is easy to see that this is too much to ask. Indeed, as above we have $\varphi(p) = p - 1$, so that restricted to prime values $\varphi(p) \sim p$; on the other hand, restricted to even values of n, $\varphi(n) \leq \frac{n}{2}$, so there is too much variation in φ for there to be a simple asymptotic expression.

This is typical for the classical arithmetical functions; indeed, some of them, like the divisor function, have even worse behavior than φ. In other words, φ has more than one kind of limiting behavior, and there is more than one relevant question to ask. We may begin with the following:

Question 1. *a) Does $\varphi(n)$ grow arbitrarily large as n does?*
b) How small can $\varphi(n)/n$ be for large n?

Part a) asks about the size of φ in an absolute sense, whereas part b) is asking about φ in a relative sense. In particular, since there are $\varphi(p) = p-1$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$, the quantity $\frac{\varphi(p-1)}{p-1}$ measures the chance that a randomly chosen nonzero residue class is a primitive root modulo p. Note we ask "how small" because we know how large $\frac{\varphi(n)}{n}$ can be: arbitrarily close to 1, when n is a large prime.

2. Lower bounds on Euler's totient function

Anyone who works long enough with the φ function (for instance, in computing all n such that $\varphi(n) \leq 10$) will guess the following result:

Proposition 1. *We have* $\lim_{n\to\infty} \varphi(n) = \infty$.

Equivalently: for any $L \in \mathbb{Z}^+$, there are only finitely many n such that $\varphi(n) \leq L$.

The idea of the proof is a simple and sensible one: if a positive integer n is "large", it is either divisible by a large prime p, or it is divisible by a large power a of a prime, or both. To formalize this a bit, consider the set $S(A, B)$ of positive integers n which are divisible only by primes $p \leq A$ and such that $\mathrm{ord}_p(n) \leq B$ for all primes p. Then $S(A, B)$ is a finite set: indeed it has at most $(B+1)^A$ elements. (Also its largest element is at most $\prod_{p\leq A} p^B \leq (A!)^B$, which is, unfortunately, pretty darned large.)

So if we assume that n is sufficiently large – say larger than $(L!)^L$ – then n is divisible either by a prime $p > L$ or by p^{L+1} for some prime p. It is easy to show that if $m \mid n$, $\varphi(m)|\varphi(n)$ – and thus $\varphi(m) \leq \varphi(n)$. So in the first case we have

$$\varphi(n) \geq \varphi(p) = p - 1 \geq L,$$

and in the second case we have

$$\varphi(n) \geq \varphi(p^{L+1}) = p^L(p-1) \geq p^L > L.$$

So we've shown that if $n > (L!)^L$, then $\varphi(n) \geq L$, which proves the result.

It was nice to get an explicit lower bound on φ, but the bound we got is completely useless in practice: to compute all n for which $\varphi(n) \leq 5$ above argument tells us that it suffices to look at n up to $120^5 = 24883200000$. But this is ridiculous: *ad hoc* arguments do much better. For instance, if n is divisible by a prime $p \geq 7$, then $\varphi(n)$ is divisible by $p - 1 \geq 6$, so we must have $n = 2^a 3^b 5^c$. If $c \geq 2$, then $25 \mid n$ so $20 = \varphi(25) \leq \varphi(n)$. Similarly, if $b \geq 2$, then $9 \mid n$ so $6 = \varphi(9) \leq \varphi(n)$, and if $a \geq 4$, then $16 \mid n$ so $8 = \varphi(16) \leq \varphi(n)$. So, if $n = 5m$, then $\varphi(n) = 4\varphi(m)$ so $\varphi(m) = 1$ and thus $m = 1$ or 2. If $n = 3m$, then $\varphi(n) = 2\varphi(m)$, so $\varphi(m) = 1$ or 2, so $n = 3 \cdot 1,\ 3 \cdot 2,\ 3 \cdot 4$. Otherwise n is not divisible by 9 or by any prime $p \leq 5$, so that $b \leq 1$ and $a \leq 3$. This yields the possibilities $n = 1, 2, 4, 8, 3, 6$. In summary, $\varphi(n) \leq 5$ iff

$$n = 1, 2, 3, 4, 5, 6, 8, 10, 12.$$

More practical lower bounds are coming up later.

However, it is interesting to note that essentially the same idea allows us to give us a much better asymptotic lower bound on φ. Namely, we have the following pretty result which once again underscores the importance of keeping an eye out for multiplicativity:

Theorem 2. *Suppose f is a multiplicative arithmetical function such that $f(p^a) \to 0$ as $p^a \to \infty$. Then $f(n) \to 0$ as $n \to \infty$.*

In other words if f is a multiplicative function such that for every $\epsilon > 0$, $|f(p^m)| < \epsilon$ for all sufficiently large prime powers, it follows that $|f(n)| < \epsilon$ for all sufficiently large n, prime power or otherwise.

Remark: As long as our multiplicative function f is never 0, an equivalent statement is that if $f(p^n) \to \infty$ for all prime powers than $f(n) \to \infty$ for all n. (Just apply the theorem to $g = \frac{1}{f}$, which is multiplicative iff f is.) So assuming the theorem, we can just look at

$$\varphi(p^a) = p^{a-1}(p-1) \geq \max(p-1, a-1),$$

and if p^a is large, at least one of p and a is large. But actually we get more:

Corollary 3. *For any fixed δ, $0 < \delta < 1$, we have $\varphi(n)/n^\delta \to \infty$.*

Proof: We wish to show that $f(n) := \frac{n^\delta}{\varphi(n)} \to 0$ as $n \to \infty$. Since both n^δ and $\varphi(n)$ are multiplicative, so is their quotient f, so by the theorem it suffices to show that f approaches zero along prime powers. No problem:

$$f(p^n) = \frac{p^{n\delta}}{p^{n-1}(p-1)} = \frac{p}{p-1} \cdot (p^{\delta-1})^n.$$

Here $\delta - 1 < 0$, so as $p \to \infty$ the first factor approaches 1 and the second factor approaches 0 (just as $x^\alpha \to 0$ as $x \to \infty$ for negative α). On the other hand, if p stays bounded and $n \to \infty$ then the expression tends to 0 exponentially fast.

Now let us prove Theorem 2. We again use the idea that for any $L > 0$, there exists $N = N(L)$ such that $n > N$ implies N is divisible by a prime power $p^a > L$.

First let's set things up: since $f(p^m) \to 0$ we have that f is bounded on prime powers, say $|f(p^m)| \leq C$. Moreover, there exists a b such that $|f(p^m)| \leq 1$ for all $p^m \geq b$; and finally, for every $\epsilon > 0$ there exists $L(\epsilon)$ such that $p^m > L(\epsilon)$ implies $|f(p^m)| < \epsilon$. Now write $n = p_1^{a_1} \cdots p_r^{a_r}$, so that

$$f(n) = f(p_1^{a_1}) \cdots f(p_r^{a_r}).$$

Since there are at most b indices i such that $p_i^{a_i} \leq B$, there are at most b factors in the product which are at least 1 in absolute value, so that the product over these "bad" indices has absolute value at most C^b. Every other factor has absolute value at most 1. Moreover, if n is sufficiently large with respect to $L(\epsilon)$ (explicitly, if $n > L(\epsilon)!^{L(\epsilon)}$, as above), then the largest prime power divisor $p_r^{a_r}$ of n is greater than $L(\epsilon)$ and hence $|f(p_r^{a_r})| < \epsilon$. This gives

$$|f(n)| = |f(p_1^{a_1} \cdots p_r^{a_r})| \leq C^b \cdot \epsilon.$$

Since C and b are fixed and ϵ is arbitrary, this shows that $f(n) \to 0$ as $n \to \infty$.

A nice feature of Theorem 2 is that it can be applied to other multiplicative functions. For instance, it allows for a quick proof of the following useful upper bound on the divisor function:

Theorem 4. *For every fixed $\delta > 0$, we have*

$$\lim_{n \to \infty} \frac{d(n)}{n^\delta} = 0.$$

Proof: Exercise!

Note that Corollary 3 is equivalent to the following statement: for every $0 < \delta < 1$, there exists a positive constant $C(\delta)$ such that for all n,

$$\varphi(n) \geq C(\delta) n^{\delta}.$$

Still equivalent would be to have such a statement for all $n \geq N_0$. This would be very useful provided we actually knew an acceptable value of $C(\delta)$ for some δ, possibly with an explicitly given and reasonably small $N_0(\delta)$ of excluded values. We quote without proof the following convenient result for $\delta = \frac{1}{2}$:

Theorem 5. *For all $n > 6$, $\varphi(n) \geq \sqrt{n}$.*

So in other words, to find all n for which $\varphi(n) \leq 10$, according to this result we need only look at n up to 100, which is fairly reasonable. Of course if you are interested in very large values of φ you will want even stronger bounds. The "truth" is coming up later: there is a remarkable explicit lower bound on $\varphi(n)$.

3. Upper bounds on Euler's φ function

Proposition 6. *For any $\epsilon > 0$, there is an n such that $\varphi(n)/n \leq \epsilon$.*

Proof. Recall that one of our formulas for $\varphi(n)$, or rather for $\varphi(p_1^{a_1} \cdots p_r^{a_r})$, is really a formula for $\varphi(n)/n$:

$$\varphi(n)/n = \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

Just for fun, let's flip this over:

$$\frac{n}{\varphi(n)} = \prod_{i=1}^{r} (1 - \frac{1}{p_i});$$

now what we need to show is that for any $L > 0$, we can choose primes $p_1, \ldots, p_r$ such that $\prod_{i=1}^{r} (\frac{p_i - 1}{p_i})^{-1} > L$.

Well, at the moment we (sadly for us) don't know much more about the sequence of primes except that it is infinite, so why don't we just take n to be the product of the first r primes $p_1 = 2, \ldots, p_r$? And time for a dirty trick: for any i, $1 \leq i \leq r$, we can view $\frac{1}{1 - \frac{1}{p_i}}$ as the sum of a geometric series with ratio $r = \frac{1}{p_i}$. This gives

$$\frac{n}{\varphi(n)} = \prod_{i=1}^{r} (1 - \frac{1}{p_i})^{-1} = \prod_{i=1}^{r} (1 + p_i^{-1} + p_i^{-2} + \ldots).$$

The point here is that if we formally extended this product over all primes:

$$\prod_{i=1}^{\infty} (1 + p_i^{-1} + p_i^{-2} + p_i^{-3} + \ldots)$$

and multiplied it all out, what would we get? A moment's reflection reveals a beautiful surprise: the uniqueness of the prime power factorization is precisely equivalent to the statement that multiplying out this infinite product we get the infinite series $\sum_{n=1}^{\infty} \frac{1}{n}$, i.e., the harmonic series! Well, except that the harmonic series is divergent. That's actually a good thing; but first let's just realize that if we multiply out the finite product $\prod_{i=}^{r} (1 - \frac{1}{p_i})^{-1}$ we get exactly the sum of the reciprocals of the integers n which are divisible only by the first r primes. In particular – since of course $p_r \geq r$, this sum contains the reciprocal of the first r integers, so: with $n = p_1 \cdots p_r$,

$$\frac{n}{\varphi(n)} \geq \sum_{n=1}^{r} \frac{1}{n}.$$

But now we're done, since as we said before the harmonic series diverges – recall that a very good approximation to the rth partial sum is $\log r$, and certainly $\lim_{r \to \infty} \log r = \infty$. This proves the result. □

To summarize, if we want to make $\varphi(n)/n$ arbitrarily small, we can do so by taking n to be divisible by sufficiently many primes. On the other hand $\varphi(n)/n$ doesn't have to be small: $\varphi(p)/p = \frac{p-1}{p} = 1 - \frac{1}{p}$, and of course this quantity approaches 1 as $p \to \infty$. Thus the relative size of $\varphi(n)$ compared to n depends quite a lot on the shape of the prime power factorization of n.

Contemplation of this proof shows that we had to take n to be pretty darned large in order for $\varphi(n)$ to be significantly smaller than n. In fact this is not far from the truth.

4. The truth about Euler's φ function

It is the following:

Theorem 7. *a) For any $\epsilon > 0$ and all sufficiently large n, one has*

$$\frac{\varphi(n) \log \log n}{n} \geq e^{-\gamma} - \epsilon.$$

b) There exists a sequence of distinct positive integers n_k such that

$$\lim_{k \to \infty} \frac{\varphi(n_k) \log \log n_k}{n_j} = e^{-\gamma}.$$

Comments: (a) Here γ is our friend the Euler-Mascheroni constant, i.e.,

$$\lim_{n \to \infty} \sum_{k=1}^{n} (\frac{1}{k}) - \log n \approx 0.5772.$$

(b) What the result is really saying is that $n/\varphi(n)$ can be, for arbitrarily large n, as large as a constant times $\log \log n$, but no larger.

In stating the result in two parts we have just spelled out a fundamental concept from real analysis (which however is notoriously difficult for beginning students to understand): namely, if for any function $f : \mathbb{Z}^+ \to \mathbb{R}$ we have a number L with the property: for every $\epsilon > 0$, then
(i) for all sufficiently large n one has

$$f(n) > L - \epsilon,$$

and (ii) for all $L' < L$ there are only finitely many n such that $f(n) < L'$, then one says that L is the **lower limit** (or limit inferior) of $f(n)$, written

$$\liminf_{n \to \infty} f(n) = L.$$

There is a similar definition of the **upper limit** (or limit superior) of a function: it is the largest L such that for any $\epsilon > 0$, for all but finitely many n we have $f(n) < L + \epsilon$. A function which is unbounded below (i.e., takes arbitrarily small values) has no lower limit according to our definition, so instead one generally says that $\liminf f = -\infty$, and similarly we put $\limsup f = +\infty$ when f is unbounded above. With these provisos, the merit of the upper and lower limits is that they *always* exist; moreover one has

$$\liminf f \leq \limsup f$$

always, and equality occurs iff $\lim_{n\to\infty} f$ exists (or is $\pm\infty$). Using this terminology we can summarize the previous results much more crisply:

Since $\varphi(p) = p - 1$, we certainly have

$$\limsup \varphi(n)/n = 1,$$

so we are only interested in how small $\varphi(n)$ can be for large n. We first showed that $\lim_{n\to\infty} \varphi(n) = +\infty$, and indeed that for any $\delta < 1$,

$$\lim_{n\to\infty} \varphi(n)/n^{\delta} = \infty.$$

However, for $\delta = 1$,

$$\lim \inf_{n\to\infty} \varphi(n)/n = 0.$$

Thus the "lower order" of $\varphi(n)$ lies somewhere between n^{δ} for $\delta < 1$ (i.e., φ is larger than this for all sufficiently large n) and n (i.e., φ is smaller than this for infinitely many n). In general, one might say that an arithmetical function f has **lower order** $g : \mathbb{Z}^+ \to (0, \infty)$ (where g is presumably some relatively simple function) if

$$\liminf_{n\to\infty} \frac{f}{g} = 1.$$

So the truth is that the lower order of φ is $\frac{e^{\gamma} n}{\log\log n}$. We will not prove this here.

Remark: all statements about limits, lim inf's lim sup's and so on of a function f, by their nature are independent of the behavior of f on any fixed finite set of values: if we took any arithmetical function and defined it completely randomly for the first $10^{10^{10}}$ values, then we would not change its lower/upper order. However in practice we would like inequalities which are true for all values of the function, or at least are true for an explicitly excluded and reasonably small finite set of values. In the jargon of the subject one describes the latter, better, sort of estimate as an **effective bound**. You can always ask the question "Is it effective?" at the end of any analytic number theory talk and the speaker will either get very happy or very defensive according to the answer. So here we can ask if there is an effective lower bound for φ of the right order of magnitude, and the answer is a resounding yes. Here is a nuclear-powered lower bound for the totient function:

Theorem 8. *For all $n > 2$ we have*

$$\varphi(n) > \frac{n}{e^{\gamma} \log\log n + \frac{3}{\log\log n}}.$$

5. Similar results for other functions

5.1. **The sum of divisors function σ.** The story for the function σ is quite similar to that of φ. In fact there is a very close relationship between the size of σ and the size of φ coming from the following beautiful double inequality.

Proposition 9. *For all n, we have*

$$\frac{1}{\zeta(2)} < \frac{\sigma(n)\varphi(n)}{n^2} < 1.$$

Proof: Indeed, if $n = \prod_i p_i^{a_i}$, then

$$\sigma(n) = \prod_i \frac{p_i^{a_i+1} - 1}{p_i - 1} = n \prod_i \frac{1 - p^{-a_i-1}}{1 - p_i^{-1}},$$

whereas

$$\varphi(n) = n \prod_i (1 - p_i^{-1}),$$

so

$$\frac{\sigma(n)\varphi(n)}{n^2} = \prod_i (1 - p_i^{-a_i-1}).$$

We have a product of terms in which each factor is less than one; therefore the product is at most 1. Conversely, each of the exponents is less than or equal to -2, so the product is at least as large as the product $\prod_p (1 - p^{-2})$. Now in general, for $s > 1$ we have

$$\prod_p (1 - p^{-s})^{-1} = \prod_p (1 + p^{-s} + p^{-2s} + \ldots) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s),$$

so the last product is equal to $\frac{1}{\zeta(2)}$. This completes the proof.

Remark: Recall that $\zeta(2) = \frac{\pi^2}{6}$, so that $\frac{1}{\zeta(2)} = \frac{6}{\pi^2}$.

From this result and the corresponding results for φ we immediately deduce:

Theorem 10. *For every $\delta > 0$, $\frac{\sigma(n)}{n^{1+\delta}} \rightarrow 0$.*

In fact we can prove this directly, the same way as for the φ function.

The "truth" about the lower order of φ dualizes to give the true upper order of σ, up to an ambiguity in the multiplicative constant, which will be somewhere between $\zeta(2)^{-1}e^{-\gamma}$ and $e^{-\gamma}$. In fact the latter is correct:

Theorem 11.

$$\limsup_{n\to\infty} \frac{e^{-\gamma}\sigma(n)}{n \log\log n} = 1.$$

And again, because $\sigma(p) = p + 1 \sim p$ for primes, we find that the lower order of $\sigma(n)$ is just n.

5.2. **The divisor function.** The divisor function $d(n)$ is yet more irregularly behaved than φ and σ, as is clear because $d(p) = 2$ for all primes 2, but of course d takes on arbitrarily large values. In particular the lower order of d is just the constant function 2. As regards the upper order, we limit ourselves to the following two estimates, which you are asked to establish in the homework:

Theorem 12. *For any $\delta > 0$, $\lim_{n\to\infty} \frac{d(n)}{n^\delta} = 0$.*

In other words, for large n, the number of divisors of n is less than any prearranged power of n. This makes us wonder whether its upper order is logarithmic or smaller, but in fact this is not the case either.

Proposition 13. *For any $k \in \mathbb{Z}^+$ and any real number C, there exists an n such that $d(n) > C(\log n)^k$.*

Thus the upper order of $d(n)$ is something greater than logarithmic and something less than any power function. We leave the matter there, although much more could be said.