Primes and Counting

Adapted from a worksheet by Don Laackman

May 16, 2021

1 Divisors

Definition 1. The sigma function $\sigma(n)$ is defined as the sum of the divisors of the positive integer n. The divisor function $\tau(n)$ is defined as the number of divisors n has. Putting these into equation form,

$$\sigma(n) = \sum_{d|n} d$$
$$\tau(n) = \sum_{d|n} 1$$

Problem 2. Compute $\sigma(8), \tau(42)$, and $\sigma(81)$.

Problem 3. Come up with formulas for $\sigma(p^k)$ and $\tau(p^k)$ for p a prime number; prove that your formulas always hold.

Problem 4. Prove that if m, n are relatively prime numbers, then $\sigma(mn) = \sigma(m)\sigma(n)$ and $\tau(mn) = \tau(m)\tau(n)$.

Definition 5. A *perfect number* is a number n such that $\sigma(n) = 2n$; put another way, it is a number whose proper divisors sum to the number itself.

Problem 6. Find all the perfect numbers less than 30.

Problem 7. The next two perfect numbers after the ones found above are 496 and 8128. What can you say about the prime factorizations of the perfect numbers you have seen so far?

Definition 8. A *Mersenne prime* is a prime number p that can be expressed as $p = 2^n - 1$ for some natural number n. It is still unknown whether there are infinitely many of these!

PROBLEM 9. Prove that any number of the form you discovered in Problem 7 is a perfect number. Conclude that if there are infinitely many Mersenne primes, there are infinitely many perfect numbers.

PROBLEM 10. Prove that any even perfect number is of the form discovered in Problem 7 (hint: use Problem 3).

2 Bounds on σ and τ

DEFINITION 11. We say that $f(n) = O(g(n))$ if there are some constants N, c such that for all $n > N$, $f(n) < c \cdot g(n)$.

PROBLEM 12. Show that $\sigma(n) = O(n \cdot \log(n))$ (you can use the fact that $\sum_{k=1}^{n} \frac{1}{k} \leq \log(n)$).

PROBLEM 13. Show that $\tau(n) = O(\sqrt{n})$ (in fact, it's actually true that $\tau(n) = O(n^{1/k}$ for any $k > 0$, but that's harder to prove).

PROBLEM 14. Disprove that $\sigma(n) = O(n)$ (This means that for any constant coefficient c, you need to come up with arbitrarily large counterexamples. (Hint: You may use the result of Problem 23.)

PROBLEM 15. Disprove that $\tau(n) = O(1)$.

3 Average Values of Arithmetic Functions

DEFINITION 16. We can extend our Big O notation to show that two functions grow similarly. We write $f(n) = h(n) + O(g(n))$ to mean that $f(n) - h(n) = O(g(n))$, which can be interpreted as "$f(n)$ is approximated by $h(n)$ with an error of order at most $g(n)$." Such equations can be manipulated: multiplying both sides by a term, or adding a term to both sides, maintains the equality.

Also, if $f(n) = O(g(n))$ and $g(n) = O(f(n))$, then we say that $f(n) = \Theta(g(n))$. This means that there is some constant α such that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = \alpha$.

PROBLEM 17. Prove that $H(n) = \sum_{i=1}^{n} \frac{1}{n} = \Theta(\log(n))$. There is a calculus proof (that uses the fact that $H(n) = \Theta(H(n+1))$), but you can also try to find upper and lower bounds for $H(2^k)$ in terms of $k = \log_2(2^k)$, and noting that the natural log is a multiple of the base-2 log.

PROBLEM 18. Confirm that the following argument holds:

If $F(n) = \sum_{d|n} f(d)$ for some function $f : \mathbb{N} \to \mathbb{R}$, then

$$\sum_{n \le x} F(n) = \sum_{d \le x} f(d) \sum_{n \le x, d|n} 1 = \sum_{d \le x} f(d) \lfloor x/d \rfloor = x \sum_{d \le x} \frac{f(d)}{d} + O\left(\sum_{d \le x} |f(d)| \right)$$

PROBLEM 19. Use Problem 18 to show that $\sum_{k \le n} \tau(k) = n \cdot \log(n) + O(n)$, so the average value of $\tau(n)$ is approximately $\log(n)$.

Even though the function τ can jump up and down pretty wildly, averaging makes it much more regular.

PROBLEM 20. Say that $f(n)$ is approximately cn for some constant c. Find an approximation for $\frac{1}{x} \sum_{n \le x} f(n)$. Conversely, if you have a function $f(n)$ such that $\frac{1}{x} \sum_{n \le x} f(n)$ is approximately cx, find an approximation for $f(n)$ on average.

PROBLEM 21. Use Problem 18 to show that on average, $\sigma(n)$ is between n and $2n$. (You will have to think harder about the behavior of the error term.

PROBLEM 22. Challenge: If $\zeta(s)$ is defined as $\sum_{n=1}^{\infty} \frac{1}{n^s}$, then get a better approximation of the average value of $\sigma(n)$ in terms of $\zeta(2) = \frac{\pi^2}{6}$. (This $\zeta(s)$ is the famous Riemann zeta function.)

4 Series

The sum of the reciprocals of the integers diverges; the sum of the reciprocals of the squares converges. This gives a first-order way to estimate how frequently a sequence appears in the integers; in particular, the primes are more common than the squares:

PROBLEM 23. Prove that the series $\sum_{i=1}^{\infty} \frac{1}{p_i}$ summing up the reciprocals of all the prime numbers diverges as follows:

- Assuming that $\sum_{i=1}^{\infty} \frac{1}{p_i}$ converges, explain why there must be some k such that $\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$.
- For any positive integer x, let M_x denote the set of integers in $\{1, 2, \ldots, x\}$ which are not divisible by any prime greater than p_k. Show that $|M_x| \le 2^k \sqrt{x}$ (Hint: a number in M_x is a square number, times some number of primes, each of which is at most p_k. How many ways are there to choose each of those?)
- Show that $\frac{x}{2} < |M_x|$ by over-counting the number of integers at most x which aren't in M_x. (Hint: in particular, each must be divisible by at least one prime greater than p_k; how many numbers less than x are there for each such prime?)

- Conclude that, for sufficiently large x, we have a contradiction.

So, now that the primes are reasonably dense, the question becomes: exactly how dense?

DEFINITION 24. The *prime counting function* $\pi(x)$ is defined to be the number of distinct prime numbers less than or equal to x.

One of the great results of number theory is the Prime Number Theorem, which says that the ratio between $\pi(x)$ and $\frac{x}{log(x)}$ approaches 1 as x goes to infinity. This result is beyond our scope today, but we will prove that $\pi(x) = \Theta\left(\frac{x}{\log(x)}\right)$.

PROBLEM 25. Prove that $2^{2n} > \binom{2n}{n}$.

PROBLEM 26. Prove that the product of all prime numbers between n and $2n$, $\prod_{n<p\leq 2n} p$, divides $\binom{2n}{n}$.

PROBLEM 27. In terms of the prime counting function, what is a number k such that $n^k < \prod_{n<p\leq 2n} p$?

PROBLEM 28. Put together the past three problems into an upper bound for $\pi(2n) - \pi(n)$.

PROBLEM 29. Prove, by induction on n, that $\pi(n) = O\left(\frac{n}{\log(n)}\right)$. Note that the coefficients cannot increase as n increases! It is feasible to show that $\pi(n) \leq 2\left(\frac{n}{\log(n)}\right)$, but feel free to replace 2 by a larger number if that's easier.

To prove the reverse bound, we'll need some new notation.

DEFINITION 30. If a is a real number, the integer part of a, $\lfloor a \rfloor$, is the largest integer such that $\lfloor a \rfloor \leq a$. For any prime number p and integer n, $v_p(n)$ is defined to be the largest power of p dividing n.

PROBLEM 31. Show that

$$v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots = \sum_{j=1}^{\infty} \lfloor n/p^j \rfloor$$

(Hint: note that, for any given n, this is actually a finite sum, plus an infinite number of 0s.)

PROBLEM 32. Prove that for any real numbers a and b, $\lfloor a+b \rfloor - \lfloor a \rfloor - \lfloor b \rfloor$ is either 0 or 1.

PROBLEM 33. Prove that for any integers n and k, $p^{v_p\left(\binom{n}{k}\right)} \leq n$. (Hint: first express $v_p\left(\binom{n}{k}\right)$ in terms of $v_p(n!)$, $v_p((n-k)!)$, and $v_p(k!)$, then use this to get an upper bound for $v_p\left(\binom{n}{k}\right)$.)

PROBLEM 34. Prove that $\binom{n}{k} \leq n^{\pi(n)}$ for any n and k.

PROBLEM 35. Prove that $2^n \leq (n+1)n^{\pi(n)}$ for any n.

PROBLEM 36. Prove that $\frac{1}{2}\frac{n}{\log(n)} < \pi(n)$ for any $n \geq 15$; then conclude that $\pi(n) = O\left(\frac{n}{\log(n)}\right)$.

5 Convolution

As we've seen in the past, $\tau(n)$ and $\sigma(n)$ are examples of *arithmetic functions*: their domain is the set of (positive) natural numbers $\mathbb{N}$.

DEFINITION 37. Given two arithmetic functions f, g, we define their *convolution* as

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

PROBLEM 38. Let $u(n) = 1$ for all n. What is $u * u(n)$?

PROBLEM 39. Let $N(n) = n$. What is $N * u(n)$?

PROBLEM 40. What function $e(n)$ has the property that $f * e(n) = f(n)$ for all arithmetic functions f and positive integers n?

PROBLEM 41. What function $\mu(n)$ has the property that $\mu * u(n) = e(n)$ for all positive integers n?

PROBLEM 42. Prove that convolution is both commutative and associative.

PROBLEM 43. Möbius Inversion on arithmetic functions is the following statement: if f and g are arithmetic functions, then

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

is true if and only if

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

- Re-phrase Möbius inversion just in terms of convolution of functions, without any sums.
- Prove that Möbius inversion holds for all arithmetic functions f.