Number Theoretic Functions

Adithya B., Kevin L., William W., Daniel X.

10/7

§1 Divisor Count

The first function we will consider is the *divisor counting function* $\tau(n)$, which gives the number of positive integer factors of n. The most important fact about this function is the following formula:

Theorem 1.1

If the prime factorization of n is $p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ then

$$\tau(n) = (e_1+1)(e_2+1)\cdots(e_k+1).$$

This formula is enough to tackle most problems relating to the divisor counting function. Let's see it in action:

Example 1.2 (2004 AIME II # 8)

How many positive integer divisors of 2004^{2004} are divisible by exactly 2004 positive integers?

Solution. We can first factorize $2004^{2004} = 2^{4008}3^{2004}167^{2004}$. Since all divisors are in the form of $2^x3^y167^z$, we have the number of divisors to be

$$(x+1)(y+1)(z+1) = 2004 = 2^2 \cdot 3 \cdot 167.$$

Our answer is $\binom{4}{2}\binom{3}{2}\binom{3}{2} = 54$. □

Example 1.3 (2005 AIME I # 12)

For positive integers n, let $\tau(n)$ denote the number of positive integer divisors of n, including 1 and n. For example, $\tau(1) = 1$ and $\tau(6) = 4$. Define $S(n)$ by

$$S(n) = \tau(1) + \tau(2) + ... + \tau(n).$$

Let a denote the number of positive integers $n \leq 2005$ with $S(n)$ odd, and let b denote the number of positive integers $n \leq 2005$ with $S(n)$ even. Find $|a-b|$.

Solution. We wish to characterize each term $\tau(k)$ in the sum mod 2. Note that for $k = p_1^{e_1}p_2^{e_2}\cdots p_i^{e_i}$,

$$\tau(k) = (e_1+1)(e_2+1)\cdots(e_i+1).$$

This is only odd when $e_1, e_2, \ldots, e_i \equiv 0 \pmod 2$, or when k is a perfect square k. Therefore, between perfect squares, $\tau(k)$ is always even, which implies that the parity of $S(n)$ does not change between perfect squares. Also, the parity of $S(n)$ switches at every perfect square.

Let's now try to evaluate some initial terms to see the general trend of the function. Note that $S(1), S(2), S(3)$ are all odd. Then, $S(4), S(5), \ldots, S(8)$ are all even, and then $S(9), S(10), \ldots, S(15)$ are odd, and so on. Let's first find the number of even and odd terms for $n \le 44^2 - 1 = 1935$ as the terms from $1936 \le n \le 2005$ all have the same parity. For the values of n less than or equal to 1935, the number of odd terms is

$$(2^2 - 1^2) + (4^2 - 3^2) + \cdots + (44^2 - 43^2) = 3 + 7 + 11 + \cdots + 87.$$

The number of even terms in this range is

$$(3^2 - 2^2) + (5^2 - 4^2) + \cdots + (43^2 - 42^2) = 5 + 9 + \cdots + 85.$$

There are an additional $2005 - 1936 + 1 = 70$ even terms. Therefore, we find

$$a - b = 3 + (7 - 5) + (11 - 9) + \cdots + (87 - 85) - 70 = 3 + 2 \cdot 21 - 70 = -25.$$

Finally, $|a - b| = \boxed{025}$.

□

Example 1.4 (2016 AIME II # 11)

For positive integers N and k, define N to be k-nice if there exists a positive integer a such that a^k has exactly N positive divisors. Find the number of positive integers less than 1000 that are neither 7-nice nor 8-nice.

Solution. We claim that a number N is k-nice if and only if $N \equiv 1 \pmod k$. First, to show the if direction, note that if $a = 2^{\frac{N-1}{k}}$, then $\left(2^{\frac{N-1}{k}}\right)^k = 2^{N-1}$ has exactly N divisors, as desired. Now, to prove the other direction, we just have to show that the number of divisors of any kth power must be 1 mod k. Note that this is true because the number of divisors of a^k is the product of the $e_i + 1$, where e_i are the exponents in the prime factorization of a^k. However, note that we have that all e_i are multiples of k, so we're multiplying a bunch of 1 mod k numbers, so the product must be 1 mod k. Thus, our claim is proven. Now, we just have to count the number of positive integers less than 1000 that are neither 1 mod 7 or 1 mod 8. Note that this can be counted with complementary counting and PIE as $998 - \left\lfloor \frac{998}{7} \right\rfloor - \left\lfloor \frac{998}{8} \right\rfloor + \left\lfloor \frac{998}{56} \right\rfloor = \boxed{749}$. □

§2 Multiplicative Functions

One general class of functions that you might encounter are *multiplicative* functions. The definition for number theoretic functions is slightly different from the definition you might have seen for real numbers:

Definition 2.1. A function $f : \mathbb{N} \mapsto \mathbb{N}$ is *multiplicative* if $f(mn) = f(m)f(n)$ holds whenever $\gcd(m, n) = 1$.

Note that we place the restriction that m and n must be relatively prime. This allows the definition to apply to a wider array of functions we might consider. For example,

the totient function is multiplicative, as you may want to verify (we discuss the totient function later in this handout).

The key perk of multiplicative functions is that we only need to consider how it behaves on prime powers. If f is multiplicative and we know $f(p^e)$ for every prime p and exponent e, then we know $f(n)$ for any positive integer n: if $n = p_1^{e_1} \cdots p_k^{e_k}$ then $f(n) = f(p_1^{e_1}) \cdots f(p_k^{e_k})$.

Example 2.2 (PUMaC 2016)
Compute the number of positive integers between 2017 and 2017^2 such that $n^n \equiv 1 \pmod{2017}$.

Solution. By Fermat's Little Theorem, we know $n^{2016} \equiv 1 \pmod{2017}$. Therefore, it suffices to find both $n \pmod{2017}$ (for the base of the exponent) and $n \pmod{2016}$ (to reduce the exponent). Let $x \equiv n \pmod{2017}$ and $y \equiv n \pmod{2017}$. As our range for n is a set of $2016 \cdot 2017$ consecutive integers, we can uniquely determine n from x and y using the Chinese Remainder Theorem.

Therefore, it suffices to find the number of pairs (x, y) such that $x^y \equiv 1 \pmod{2017}$. As 2017 is a prime, we know there exists a primitive root g. Let $x = g^k$. Then, we need to count pairs (k, y). Note that $g^{ky} \equiv 1 \pmod{2017}$. As g is a primitive root, this implies that $2016 \mid ky$. We must have $\frac{2016}{\gcd(2016,k)} \mid y$. As y ranges from 0 to 2015, there should be $\frac{2016}{\frac{2016}{\gcd(2016,k)}} = \gcd(2016, k)$ values of y for each value of k. As k ranges from 1 to 2016, the number of pairs (k, y) is

$$\sum_{k=1}^{2016} \gcd(k, 2016).$$

Define $f(n) = \sum_{k=1}^{n} \gcd(k, n)$. We claim that $f(n)$ is multiplicative. We will show that if $\gcd(a, b) = 1$, then $f(a)f(b) = f(ab)$. Note that

$$f(a)f(b) = \left(\sum_{i=1}^{a} \gcd(i, a)\right)\left(\sum_{j=1}^{b} \gcd(j, b)\right) = \sum_{i=1}^{a}\sum_{j=1}^{b} \gcd(i, a)\gcd(j, b).$$

By the Chinese Remainder Theorem, let k be the unique integer such that $k \equiv i \pmod{a}$ and $k \equiv j \pmod{b}$. Note that $\gcd(i, a) = \gcd(k, a)$ and $\gcd(j, b) = \gcd(k, b)$. As the entire residue set $\pmod{ab}$ is covered by k, we can replace the double sum by a single sum over k.

$$f(a)f(b) = \sum_{i=1}^{a}\sum_{j=1}^{b} \gcd(i, a)\gcd(j, b) = \sum_{k=1}^{ab} \gcd(k, a)\gcd(k, b).$$

Finally, since $\gcd(a, b) = 1$, we must have $\gcd(k, a)\gcd(k, b) = \gcd(k, ab)$. Therefore,

$$f(a)f(b) = \sum_{k=1}^{ab} \gcd(k, ab) = f(ab).$$

Now, we want to evaluate $f(2016)$. As f is multiplicative, this is equivalent to finding $f(32)f(9)f(7)$, which can all be individually evaluated. We have

$$f(32) = \sum_{k=1}^{32} \gcd(k, 32) = 16 \cdot 1 + 8 \cdot 2 + 4 \cdot 4 + 2 \cdot 8 + 1 \cdot 16 + 1 \cdot 32 = 112.$$

$$f(9) = \sum_{k=1}^{9} \gcd(k, 9) = 6 \cdot 1 + 2 \cdot 3 + 1 \cdot 9 = 21.$$

$$f(7) = \sum_{k=1}^{9} \gcd(k, 7) = 6 \cdot 1 + 1 \cdot 7 = 13.$$

Therefore, $f(2016) = 112 \cdot 21 \cdot 13 = \boxed{30576}$. □

Example 2.3 (2019 HMMT Algebra and Number Theory #8)
There is a unique function $f : \mathbb{N} \to \mathbb{R}$ such that $f(1) > 0$ and such that

$$\sum_{d|n} f(d) f\left(\frac{n}{d}\right) = 1$$

for all $n \geq 1$. What is $f(2018^{2019})$?

Solution. We begin by letting $n = 1$, so that $f(1) = 1$. We claim that f is multiplicative, that $f(ab) = f(a)f(b)$ for relatively prime a, b. Note that every divisor of ab can be written uniquely as the product $d_1 d_2$, where $d_1 | a$ and $d_2 | b$. Now, we wish to show our claim by induction on ab. Suppose it holds true for all smaller ab. Now, plugging in $n = a, b, ab$ gives us

$$1 = \sum_{d_1|a} f(d_1) f\left(\frac{a}{d_1}\right) \sum_{d_2|b} f(d_2) f\left(\frac{b}{d_2}\right)$$

$$= \sum_{d_1 d_2 | ab} f(d_1 d_2) f\left(\frac{ab}{d_1 d_2}\right) - 2f(1)f(ab) + 2f(a)f(b) = \sum_{d_1 d_2 | ab} f(d_1 d_2) f\left(\frac{ab}{d_1 d_2}\right)$$

Thus, we find $f(ab) = \frac{f(a)f(b)}{f(1)} = f(a)f(b)$, as desired. Now, note that $f(p^k)$ is independent on the prime p, which can be shown by induction on k. Let $a_k = f(p^k)$. Now, consider the generating function $g(x) = a_0 + a_1 x + a_2 x^2 + \cdots$. Note that it satisfies $g(x)^2 = 1 + x + x^2 + \cdots = \frac{1}{1-x}$. Thus, we find that $g(x) = (1-x)^{-\frac{1}{2}}$. By the extended binomial theorem, we note that this gives us $a_n = \binom{-\frac{1}{2}}{n} = \frac{(-1)^n \binom{2n}{n}}{4^n}$. □

§3 General Functions

Some number theory problems present us with a newly defined function and ask us to work with it. In this case, we have no prior knowledge about the properties of the function, unlike well-known functions such as the divisor counting function. For these problems, it is important to understand how these functions behave as a substitute for this lack of prior knowledge. We discussed multiplicativity as one possible way we can work with arbitrary number theoretic functions; in the examples below, we consider other ad-hoc methods of learning about the function.

Example 3.1 (2014 AIME II # 15)

For any integer $k \geq 1$, let $p(k)$ be the smallest prime which does not divide k. Define the integer function $X(k)$ to be the product of all primes less than $p(k)$ if $p(k) > 2$, and $X(k) = 1$ if $p(k) = 2$. Let $\{x_n\}$ be the sequence defined by $x_0 = 1$, and $x_{n+1}X(x_n) = x_n p(x_n)$ for $n \geq 0$. Find the smallest positive integer, t such that $x_t = 2090$.

Solution. Our main concern is the sequennce x_i; as such, let us rewrite the recursion so that we may solve for x_{n+1} in terms of x_n:

$$x_{n+1} = \frac{x_n p(x_n)}{X(x_n)}.$$

Since we're given rather obscure functions p and X in this recursion, let's stop to think about what this equation means. Given x_n, if we multiply by the smallest prime not dividing x_n and then divide by all smaller primes, we obtain x_{n+1}. This perspective is helpful with computing the first few terms of the sequence. It also encourages us to consider the prime factorization of the terms, as the recursion involves multiplying and dividing by primes. We obtain:

$$\begin{aligned}
x_1 &= 2 \\
x_2 &= 3 \\
x_3 &= 6 = 2 \cdot 3 \\
x_4 &= 5 \\
x_5 &= 10 = 2 \cdot 5 \\
x_6 &= 15 = 3 \cdot 5 \\
x_7 &= 30 = 2 \cdot 3 \cdot 5 \\
x_8 &= 7.
\end{aligned}$$

Considering the prime factorization, we see that the recursion involves finding the smallest prime not in the factorization, adding it, and deleting all smaller primes.

This sounds a lot like addition in binary! When we add 1 to an integer in binary, we identify the rightmost zero, switch it to a 1, and switch all digits to the right to zero. The connection is much more clear if we write the prime factorizations as follows:

$$\begin{aligned}
x_1 &= 7^0 \cdot 5^0 \cdot 3^0 \cdot 2^1 \\
x_2 &= 7^0 \cdot 5^0 \cdot 3^1 \cdot 2^0 \\
x_3 &= 7^0 \cdot 5^0 \cdot 3^1 \cdot 2^1 \\
x_4 &= 7^0 \cdot 5^1 \cdot 3^0 \cdot 2^0 \\
x_5 &= 7^0 \cdot 5^1 \cdot 3^0 \cdot 2^1 \\
x_6 &= 7^0 \cdot 5^1 \cdot 3^1 \cdot 2^0 \\
x_7 &= 7^0 \cdot 5^1 \cdot 3^1 \cdot 2^1 \\
x_8 &= 7^1 \cdot 5^0 \cdot 3^0 \cdot 2^0.
\end{aligned}$$

It's now clear that if $\overline{e_k e_{k-1} \cdots e_0}$ is the binary representation of n then $x_n = p_k^{e_k} p_{k-1}^{e_{k-1}} \cdots p_0^{e_0}$ (where $p_1 < p_2 < \cdots$ is the sequence of primes). We can turn this into a rigorous proof, but it is basically the same as this intuition: if we write out the prime factorization, to

find x_{n+1} we find the first zero in x_n, change it to a one, and change everything to the right to a zero.

With this description, we can compute the answer. First, we factorize $2090 = 2 \cdot 5 \cdot 11 \cdot 19$, or

$$2090 = 19^1 \cdot 17^0 \cdot 13^0 \cdot 11^1 \cdot 7^0 \cdot 5^1 \cdot 3^0 \cdot 2^1.$$

Thus if $x_t = 2090$ then $t = 10010101_2 = \boxed{149}$. □

Example 3.2 (2013 AIME II # 14)

For positive integers n and k, let $f(n, k)$ be the remainder when n is divided by k, and for $n > 1$ let $F(n) = \max_{1 \le k \le \frac{n}{2}} f(n, k)$. Find the remainder when $\sum_{n=20}^{100} F(n)$ is divided by 1000.

§4 Totient

The final function (along with possibly the most difficult examples) we will consider is the *totient* function, denoted $\varphi(n)$.

Definition 4.1. $\varphi(n)$ is the number of integers in $\{1, 2, \ldots, n\}$ that are relatively prime to n.

We can find a formula for $\varphi(n)$ given the prime factorization of n:

Theorem 4.2

If $p_1, p_2, \ldots, p_k$ are the distinct primes dividing n then

$$\varphi(n) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) n.$$

We leave the proof as an instructive exercise in the principle of inclusion-exclusion (and a little bit of factoring). With just this formula and the basic definition, we can derive a number of interesting properties of this function. For example, recall:

Theorem 4.3 (Euler)

If $\gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

We consider several other properties and uses of the totient function below.

Example 4.4 (classical)

Show that

$$\sum_{d \mid n} \varphi(d) = n.$$

Solution. Consider the fractions $\frac{t}{n}$ in reduced form where $1 \le t \le n$. The number of fractions in simplified form with denominator d is exactly $\phi(d)$. This is because the

numerator of the fraction has to be relatively prime with d in order for the fraction to be reduced. Since there are $\phi(d)$ integers less than or equal to d that are relatively prime to d, there are $\phi(d)$ fractions with denominator d. As the denominator must be a divisor of n, we have that there are $\sum_{d|n} \varphi(d)$ fractions in total, so $\sum_{d|n} \varphi(d) = n$. □

Example 4.5

Let n be a positive integer. Prove that

$$\sum_{k\geq 1} \varphi(k) \left\lfloor \frac{n}{k} \right\rfloor = \frac{1}{2} n(n+1).$$

Solution. We will try to prove this problem with induction. Let $f(n)$ equal the sum in the example. To use induction properly, we wich to find an expression for the difference $f(n) - f(n-1)$. Note that

$$f(n) - f(n-1) = \sum_{k\geq 1} \varphi(k) \left(\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor \right).$$

Now, the difference of the two floors is only nonzero when k divides n. When k divides n, the difference is exactly equal to 1. Therefore, we can rewrite the sum as

$$f(n) - f(n-1) = \sum_{k|n} \varphi(k) = n$$

due to the previous example. As $f(n) - f(n-1) = n$, we can now use induction to prove the result. The proof is shown below:

The base case is $f(1) = 1$, which is easy to verify. For $n = k$, assume that $f(k) = \frac{1}{2}k(k+1)$. We know that $f(k+1) - f(k) = k+1$. Therefore,

$$f(k+1) = f(k) + f(k+1) - f(k) = \frac{1}{2}k(k+1) + k + 1 = \frac{1}{2}(k+1)(k+2),$$

which completes the induction. □

Example 4.6 (USA TST 2018/1)

Let $n \geq 2$ be a positive integer, and let $\sigma(n)$ denote the sum of the positive divisors of n. Prove that the n^{th} smallest positive integer relatively prime to n is at least $\sigma(n)$, and determine for which n equality holds.

Solution. Suppose the divisors of n are $d_1, d_2, \ldots, d_k$. We care about the interval $[1, d_1 + d_2 + \cdots + d_k]$. A single interval of size $d_1 + d_2 + \cdots + d_k$ is quite awkward, but k intervals of sizes $d_1, d_2, \ldots, d_k$ are much simpler. The number of values in an interval of size d_i relativly prime to n is at most $\varphi(d_i)$, since there are at most as many that are relatively prime to d_i. Now, summing this over all intervals gives us $\sum_{i=1}^{k} \varphi(d_i) = n$. Thus, there are at most n values in the whole interval of size $\sigma(n)$ that are relatively prime to n. Thus, the nth smallest value relatively prime to n is at least $\sigma(n)$, since there are at most n values up to that point. Now, we claim that equality only holds for n equal to a prime power. It is easily checked that equality is true for prime powers. For n not a prime

power, suppose we have distinct primes p, q such that $pq|n$.WLOG, assume $p < q$. Now, if we were to make our first interval of size q, there would be a value in that interval relatively prime with the interval size but not relatively prime with n (in particular, p). Thus, equality cannot hold. $\square$