MATH CIRCLE HIGH SCHOOL 2 GROUP, WINTER 2018
WEEK 4: NUMBER THEORY, PART 1

DON LAACKMAN

1. Divisors

Definition. *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 1. *Compute* $\sigma(8), \tau(42)$*, and* $\sigma(81)$

Problem 2. *Come up with formulas for* $\sigma(p^k)$ *and* $\tau(p^k)$ *for* p *a prime number; prove that your formulas always hold.*

Problem 3. *Prove that if* m, n *are relatively prime numbers, then* $\sigma(mn) = \sigma(m)\sigma(n)$ *and* $\tau(mn) = \tau(m)\tau(n)$

Definition. *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 4. *Find all the perfect numbers less than 30.*

Problem 5. *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?*

Problem 6. *Prove that any number of the form you discovered in problem 5 is a perfect number.*

Problem 7. *Prove that any even perfect number is of the form discovered in problem 5 (hint: use problem 3).*

2. Arithmetic Functions

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

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

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

Problem 8. *Let $u(n) = 1$ for all n. What is $u * u(n)$?*

Problem 9. *Let $N(n) = n$. What is $N * u(n)$?*

Problem 10. *What function $e(n)$ has the property that $f * e(n) = f(n)$ for all arithmetic functions f and positive integers n?*

Problem 11. *What function $\mu(n)$ has the property that $\mu * u(n) = e(n)$ for all positive integers n?*

Problem 12. *Prove that convolution is both commutative and associative.*

Problem 13. Mobius 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

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

(1) *Re-phrase Mobius inversion just in terms of convolution of functions, without any sums.*

(2) *Prove that mobius inversion holds for all functions.*

3. Primes

Problem 14. *Prove* Wilson's Theorem*: $(p-1)! \equiv -1$ (mod p) for any prime number p.*

Problem 15. *Euler's totient function $\phi(n)$ is defined as the number of numbers less than n which are relatively prime to n. Compute $\phi(p)$ for any prime p and prove that if a, b are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$.*

Problem 16. *Prove* Fermat's Little Theorem*: If x and m are relatively prime, then $x^{\phi(m)} \equiv 1$ (mod m)*

Problem 17. *When does the linear diophantine equation $ax + by = c$, with $a, b, c \in \mathbb{Z}$, have integer solutions for x and y?*

Problem 18. *Can you find any interesting relationships involving the totient function and convolution?*