Number Theory I: Worksheet —Solutions

1. **Warmup: Practice with definitions.** The following quickies test your precise understanding of the definitions of divisibility and primes. In answering the questions, make sure to use the appropriate "official" definition from class (as given on the "Number Theory I" class handout), not any preconceived notions about primes and divisibilty, what your high school teacher told you, etc.

   (a) **Primes and composite numbers.** For each of the following numbers determine if it is prime, composite, or neither. For composite numbers, write out their prime factorization.

   $2, \quad -2, \quad 1, \quad 12, \quad 120$

   Solution: *2 is prime, $12 = 2^2 \cdot 3$ and $120 = 2^3 \cdot 3 \cdot 5$ are composite, 1 and -2 are neither.*

   (b) **Divisibility properties of 1 and 0:**
   Which $n \in \mathbb{Z}$ satisfy (i) $1 \mid n$, (ii) $n \mid 1$, (iii) $n \mid 0$?

   Solution: *(i) All $n \in \mathbb{Z}$, (ii) $n = \pm 1$. (iii) All $n \in \mathbb{Z} - \{0\}$.*

   (c) **Divisors of primes and prime powers:**

   (i) Let p be a prime. List all *positive* divisors of p. How many positive divisors are there?

   Solution: *There are 2 divisors, 1 and p.*

   (ii) Let k be a natural number and p be a prime. List all *positive* divisors of p^k. How many positive divisors are there?

   Solution: *There are $k+1$ divisors, $1, p^1, p^2, \dots, p^k$.*

2. **Famous numbers, I: Perfect numbers.** A number n is perfect if it is equal to the sum of its *positive* divisors *excluding n itself.* For example, the positive divisors of 6 are $1, 2, 3, 6$. If we remove 6 from the list and add up the remaining divisors, we get $1 + 2 + 3 = 6$, so 6 is perfect.

   (a) List all positive divisors of 28, and show that 28 is a perfect number.

   Solution: *The positive divisors of 28 are $1, 2, 4, 7, 14, 28$. After removing 28 from the list, the sum of the remaining divisors is $1 + 2 + 4 + 7 + 14 = 28$. Thus, 28 is perfect.*

   (b) More generally, consider numbers of the form $n = 2^k \cdot (2^{k+1} - 1)$. (The above examples, $n = 6$ and $n = 28$, correspond to $k = 1$ and $k = 2$.) Show that such an n is perfect whenever $2^{k+1} - 1$ is a prime number.

   Remark: This is a famous result of Euclid and Euler. In fact, Euler showed the only *even* perfect numbers are those of the above form. Primes of the form $2^k - 1$ form another famous class of numbers, namely *Mersenne primes.*

   Solution: *Write $p = 2^{k+1} - 1$. Assuming p is prime, the positive divisors of $2^k p$ are $2^0, 2^1, \dots, 2^k, p \cdot 2^0, p \cdot 2^1, \dots, p \cdot 2^k$. Adding up these numbers excluding the last one, $2^k p$, we get*

   $$\begin{aligned}&(2^0 + 2^1 + \cdots + 2^k) + p(2^0 + 2^1 + \cdots + 2^{k-1})\\ &\quad = 2^{k+1} - 1 + p(2^k - 1) = p + p(2^k - 1) = 2^k p,\end{aligned}$$

   which is the original number $2^k(2^{k+1} - 1)$. Thus this number is perfect, whenever $2^{k+1} - 1$ is a prime number.

3. **Proof-writing practice: Divisibility properties.** For each of the following statements, give a careful proof *using only the definition of divisibility* ("$a \mid b$" means "there exists $m \in \mathbb{Z}$ such that $b = am$"). Some of these problems will appear in the homework. Others will be worked out in class.

   (In all statements, $a, b, c, d, \ldots$ are assumed to be non-zero integers.)

   (a) If $a \mid b$ and $b \mid c$, then $a \mid c$.

   Solution: *Suppose $a \mid b$ and $b \mid c$. By the definition of divisibility, this means that there exist $m \in \mathbb{Z}$ such that $b = ma$ and $n \in \mathbb{Z}$ such that $c = nb$. Therefore $c = nb = n(ma) = (nm)a$. Since n, m are integers, so is nm. Hence, $c = ka$, where $k = nm$ is an integer. By the definition of divisibility, this means that $a \mid c$.*

   (b) If $d \mid a$ and $d \mid b$, then $d \mid a + b$ and $d \mid a - b$.

   Solution: *Suppose $d \mid a$ and $d \mid b$. By the definition of divisibility, this means that there exist $m \in \mathbb{Z}$ such that $a = md$ and $n \in \mathbb{Z}$ such that $b = nd$. Therefore $a + b = md + nd = (m + n)d$. Since n, m are integers, so is $n + m$. Hence, $a + b = dk$, where $k = n+m$ is an integer. By the definition of divisibility, this means that $d \mid a+b$. The second relation, $d \mid a - b$, is proved analogously.*

   (c) If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

   Solution: *Suppose $a \mid b$ and $b \mid a$. By the definition of divisibility, this means that there exist $m \in \mathbb{Z}$ such that $b = ma$ and $n \in \mathbb{Z}$ such that $a = nb$. Therefore $a = nb = n(ma) = (nm)a$. Since we assumed that a is nonzero, we can divide by a and obtain $nm = 1$. Since n and m are integers, this implies $n = m = 1$ or $n = m = -1$. In the first case, we have $a = b$, and in the second case $a = -b$. Thus, $a \mid b$ and $b \mid a$ implies $a = b$ or $a = -b$, as claimed.*

   (d) (HW) If $d \mid a$ and $d \mid b$, then $d \mid ax + by$ for any $x, y \in \mathbb{Z}$.

   (e) (HW) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

4. **Proof-writing practice: Proof of the Existence Part of FTA.** Using strong induction prove that every integer $n \geq 2$ has a prime factorization. (Pay particular attention to the write-up; be sure to include an appropriate base case, and clearly state the assumptions in the induction step.)

   Solution: *Let $P(n)$ denote the statement "n has a prime factorization." We will use strong induction to prove that $P(n)$ holds for every integer $n \geq 2$.*

   The base case is $n = 2$, which has prime factorization $2 = 2^1$, so $P(2)$ holds

   For the induction step, let $n > 2$ be given and assume that $P(n')$ holds for every *integer n' with $2 \leq n' < n$, i.e., we assume that every such n' has a prime factorization. We seek to show that n also has a prime factorization. We distinguish two cases:*

   - *Case 1: n is prime. In this case n is its own prime factorization and we are done.*
   - *Case 2: n is composite. In this case, by the definition of a composite integer, there exist integers a, b with $1 < a, b < n$ such that $n = ab$. By the induction hypothesis, both a and b have a prime factorization. Multiplying these factorizations together and rearranging terms yields a prime factorization for n.*

   Thus, in either case, n has a prime factorization, so $P(n)$ holds and the induction step is complete. By the principle of strong induction, it follows that $P(n)$ holds for all $n \geq 2$.