The Basics of Number Theory

Dennis Chen

March 2019

1 Divisibility, GCD, and LCM

1.1 Divisibility

Divisibility seems like such a simple idea; if a divides b (which is denoted as $a|b$) then $\frac{b}{a}$ must be an integer. However, this falls apart once we start introducing 0 into the equation. For the purpose of letting our definition stay consistent when 0 is introduced, we say that integers $a|b$ if there exists integer c such that $ac = b$. (We specify a, b as integer for our useful results to stay consistent.)

This means that all $a|0$ and $0 \nmid b$ for all $b \neq 0$, implying $0|0$. (Verify this for yourself.)

1.2 Results

Our rigorous definition of divisibility leaves us with some results that we can prove which we would not have obtained using the intuitive method.

1. If $a|c$ and $b|c$ then $a|c$. (This may be referred to as the "chain rule" of divisibility.)
2. If $a|b$ then $a|bc$ for all integer c.
3. If $a|b$ and $a|c$, then $a|b+c$ and $a|b-c$.

1.3 GCD and LCM

We define $\gcd(a_1, a_2 \dots a_n)$ as the largest positive integer such that

$$\gcd(a_1, a_2 \dots a_n)|a_1, a_2 \dots a_n.$$

Similarly, we define $\operatorname{lcm}(a_1, a_2 \dots a_n)$ as the smallest **positive** integer such that $a_1, a_2 \dots a_n| \operatorname{lcm}(a_1, a_2 \dots a_n)$.

2 Fermat's Little Theorem

Theorem 1. (Fermat's Little Theorem) *Consider a prime p. For relatively prime a, p, $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. (Induction) For the inductive proof, we prove that $a^p \equiv a \pmod{p}$ instead.

This is obviously true for the base case $a = 1$.

Now assume that this is true for $a = n$. Then

$$(n+1)^p \equiv n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + 1.$$

But notice that $\binom{p}{1}, \binom{p}{2} \ldots \binom{p}{p-1}$ are all divisible by p, so

$$n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + 1 \equiv n^p + 1 \equiv n + 1,$$

as desired. □

Proof. (Rearrangement) Notice that $a, 2a, 3a \ldots a(p-1)$ is a rearrangement of $1, 2, 3 \ldots p-1$ taken $\pmod{p}$. We prove this by contradiction. Assume that there are two integers such that $ax \equiv ay \pmod{p}$. Since $\gcd(a, p) = 1$, we can divide both sides by a to yield $x \equiv y$. But this is obviously not possible. Thus, contradiction.

Then we notice that because of our proven rearrangement, $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$. As $\gcd(p, (p-1)!) = 1$, we can divide both sides by $(p-1)!$ to get $1 \equiv a^{p-1} \pmod{p}$, as desired. □

3 The Totient Function

Theorem 2. (Multiplicity) *For relatively prime m, n, $\phi(m) \cdot \phi(n) = \phi(mn)$.*

Theorem 3. (Product Formula) *For $n = {p_1}^{e_1} \cdot {p_2}^{e_2} \ldots {p_n}^{e_n}$, $\phi(n) = n\frac{p_1-1}{p_1} \cdot \frac{p_2-1}{p_2} \cdots \frac{p_n-1}{p_n}$.*

Theorem 4. (Euler's Totient Theorem) *For relatively prime a, n, $a^{\phi(n)} \equiv 1 \pmod{n}$.*

4 Modular Inverses

In normal arithmetic, $a \cdot a^{-1} = 1$. In modular arithmetic, a^{-1} is the number such that $a \cdot a^{-1} \equiv 1 \pmod{n}$. We say that a^{-1} is the inverse of $a \pmod{n}$.

Of course, the modular inverse is defined if and only if $\gcd(a, n) = 1$.

5 Wilson's Theorem

Theorem 5. (Wilson's Theorem) *For prime* p,

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Notice that the numbers $2, 3, 4 \ldots p-2$ all have modular inverses. In addition, modular inverses come in pairs. Since p is odd (the case where $p = 2$ is very easy to deal with), then the modular inverses all multiply to 1. This leaves us with $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$, as desired. $\square$

As an exercise, prove that $(p-2)! \equiv 1 \pmod{p}$. (This is quite easy to do directly with Wilson's.)

6 Homework Problems

1. Find the inverse of 2 $\pmod{p}$ for odd prime p in terms of p.
2. Let n be a 5-digit number, and let q and r be the quotient and the remainder, respectively, when n is divided by 100. For how many values of n is $q + r$ divisible by 11?
3. Prove $\phi(n)$ is composite for $n \geq 7$.
4. How many integer values of $1 \leq x \leq 100$ makes $x^2 + 8x + 5$ divisible by 10?
5. Find the remainder of $(1^3)(1^3 + 2^3)(1^3 + 2^3 + 3^3) \ldots (1^3 + 2^3 + 3^3 \cdots + 99^3)$ when divided by 101.
6. Find all odd n such that $\frac{1}{n}$ expressed in base 8 is a repeating decimal with period 4.
7. Find the remainder of $5^{31} + 5^{17} + 1$ when divided by 31.