Lecture Notes: Introduction to Number Theory

Montgomery Blair Math Team
1/6/2016

1. Divisors

Any natural number $x > 1$ can be expressed as a product of primes: $x = p_1^{q_1}...p_n^{q_n} = \prod_i^n p_i^{q_i}$ for some n, primes p_i, and positive natural numbers q_i. The primes p_i are referred to as the prime factors of x. The process of decomposing a positive integer into its prime factors and exponents on those factors is known as *factorization*.

A divisor of x is any number y such that x/y has no fractional remainder; equivalently, $x \equiv 0 \pmod{y}$. It is also true that all divisors y of $x = \prod_i^n p_i^{q_i}$ can be expressed as $y = \prod_i^n p_i^{q_i'}$ for some selection of $0 \leq q_i' \leq q_i$.

Because $\prod_i^n p_i^{q_i'}$ is a divisor of $x = \prod_i^n p_i^{q_i}$ for any values $0 \leq q_i' \leq q_i$, the total number of divisors can be determined combinatorially: $d(x) = \sigma_0(x) = \prod_i^n (q_i + 1)$. The sum of all divisors can be determined by creating a product of sums form which would expand to be the sum of all divisors:

$$\sigma_1(x) = \left(1 + p_1 + p_1^2 + ... + p_1^{q_1}\right) ... \left(1 + p_n + p_n^2 + ... + p_n^{q_n}\right) = \prod_{i=1}^{n} \sum_{j=0}^{q_i} p_i^j$$

2. GCD and LCM

The **greatest common divisor** of two positive integers x and y is the greatest number z such that $z|x$ and $z|y$ ($a|b$ means a divides b or, formally, $b \equiv 0 \pmod{a}$).

The **least common multiple** of two positive integers x and y is the smallest number z such that $x|z$ and $y|z$. One should note that $\gcd(x, y) \cdot \operatorname{lcm}(x, y) = xy$ for all positive integers x and y.

3. Chinese Remainder Theorem

Theorem 3.1 (Chinese Remainder Theorem)**.** *For relatively prime r and s and any integers $0 \leq a < r$ and $0 \leq b < s$, there exists exactly one $0 \leq n < rs$ such that $n \equiv a \pmod{r}$ and $n \equiv b \pmod{s}$. Furthermore, the set of all integers k such that $k \equiv a \pmod{r}$ and $k \equiv b \pmod{s}$ is the set of all k such that $k \equiv n \pmod{rs}$.*

Proof. First we show that there cannot be more than one such n. Suppose that $0 \leq n_1, n_2 < rs$, $n_1 \neq n_2$, and $n \equiv n_2 \equiv a \pmod{r}$ and $n_1 \equiv n_2 \equiv b \pmod{s}$. Consider $x = n_1 - n_2$. Clearly, since $n_1 \neq n_2$, x is not divisible by rs. However, $n_1 - n_2 \equiv 0 \pmod{r}$, so x is divisible by r, and similarly x is divisible by s. Since r and s are relatively prime, it follows that x is divisible by rs. This is a contradiction. Thus, there is at most one such n.

Next we show that there exists at least one such n. As we proved above, for each $0 \leq n < rs$, there is a different pair (a, b) such that $n \equiv a \pmod{r}$ and $n \equiv b \pmod{s}$. Since there are rs values that n can take on, and there are rs possible values of (a, b), it follows that each value of (a, b) corresponds to exactly one value of n.

Finally, since adding rs to a number does not change its value mod r or mod s, the second part of the theorem is true. $\square$

4. Euclidean Algorithm

The Euclidean Algorithm is an algorithm that is used to find the GCD of two numbers. It relies on the principle that $\gcd(a, b) = \gcd(a, b + ka)$ for any integer k (this is true because if a number divides a, then it divides b if and only if it divides $b + ka$). Similarly, $\gcd(a, b) = \gcd(a + kb, b)$. We can use this fact as in the following example (an example of the Euclidean Algorithm):

Suppose we want to find $\gcd(68, 98)$. We have

$$\gcd(68, 98) = \gcd(68, 30) = \gcd(8, 30) = \gcd(8, 6) = \gcd(2, 6) = \gcd(2, 2) = 2.$$

We can rewrite this as follows:

$$\begin{aligned} 98 &= 1 \cdot 68 + 30 \\ 68 &= 2 \cdot 30 + 8 \\ 30 &= 3 \cdot 8 + 6 \\ 8 &= 1 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

5. Extended Euclidean Algorithm

The extended Euclidean algorithm allows you, for any positive integers a and b, to find integers x and y such that $xa + yb = \gcd(a, b)$. This is essentially the Euclidean algorithm, but backwards. Here's an example: suppose we want to find x and y such that $68x + 98y = 2$. From the work we did above, we have

$$\begin{aligned} 2 &= (1)8 + (-1)6 \\ 6 = (1)30 + (-3)8 \Rightarrow 2 &= (-1)30 + (4)8 \\ 8 = (1)68 + (-2)30 \Rightarrow 2 &= (4)68 + (-9)30 \\ 30 = (1)98 + (-1)68 \Rightarrow 2 &= (-9)98 + (13)68 \end{aligned}$$

Thus, we have $x = -9$ and $y = 13$.

This lets us do some really cool things that very few people know how to do efficiently. Suppose we want to find an x such that $68x \equiv 10 \pmod{98}$. Then we have $68x = 98y + 10$ for some y, so $68x - 98y = 10$. We know that $68 \cdot 13 - 98 \cdot 9 = 2$, so $68 \cdot 65 - 98 \cdot 45 = 10$. Thus, one possible value of x is 65.

Suppose we want to find an x such that $x \equiv 5 \pmod{68}$ and $x \equiv 11 \pmod{98}$. Then we have $x = 68y + 5 = 98z + 11$, so we have $68y - 98z = 6$. One solution to this is $y = 39$ and $z = -27$. Plugging $y = 39$ into $x = 68y + 5$, we get that one value of x is 2657.

6. Euler Totient Function

The Euler Totient function, written as $\phi(n)$, takes a positive integer n and returns the number of positive integers less than or equal to n that are relatively prime to n. For

example, $\phi(6) = 2$ because there are two numbers less than 6 — namely, 1 and 5 — that are relatively prime to 6. You can evaluate $\phi(n)$ by multiplying n successively by $\frac{p-1}{p}$ for all primes p that divide n. For example, since 2 and 3 are the prime divisors of 12, we have $\phi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$. We can see that this is true because, for any $p \mid n$, if you randomly choose a number from 1 to n, inclusive, there is a probability of $\frac{p-1}{p}$ that it will not divide p. It is easy to see that these probabilities are independent for any two values of p, so we can multiply the probabilities together.

7. Mod Congruency Theorems

Theorem 7.1 (Fermat's Little Theorem)**.** *Given a prime p and a positive integer a that is relatively prime to p, $a^{p-1} \equiv 1 \pmod{p}$. (Equivalently, $a^p \equiv a \pmod{p}$.)*

Proof. Consider $\{a \pmod{p}, 2a \pmod{p}, \ldots, (p-1)a \pmod{p}\}$. We know that these are all distinct, because if ka and ma are congruent modulo p, then $(m-k)a \equiv 0 \pmod{p}$, implying that $m = k$. Furthermore, no element of the set equals 0. Thus, $\{a \pmod{p}, 2a \pmod{p}, \ldots, (p-1)a \pmod{p}\} = \{0, 1, \ldots, p-1\}$. Taking the product of the elements of each set, we get

$$\begin{aligned} a \cdot 2a \cdot \cdots \cdot (p-1)a &\equiv 1 \cdot 2 \cdot \ldots (p-1) \pmod{p} \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p}. \end{aligned}$$

(We can divide by $(p-1)!$ because clearly it isn't divisible by p and p is prime.) □

Theorem 7.2 (Euler-Fermat Theorem, Euler's Theorem)**.** *Given two relatively prime positive integers a and b, $a^{\phi(b)} \equiv 1 \pmod{b}$.*

This can be proven without too much difficulty using a similar method to the one used in the proof above, and is left as an exercise.

Theorem 7.3 (Wilson's Theorem)**.** *Given a prime p, $(p-1)! \equiv -1 \pmod{p}$.*

The easiest proof of the above theorem uses a bit of abstract algebra; you are welcome to look it up.

Theorem 7.4 (Lucas's Theorem)**.** $\binom{m}{n} \equiv \prod_i \binom{m_i}{n_i} \pmod{p}$*. In other words, m choose n is equivalent to the product of a digit in the base-p representation of m choose the corresponding digit in the base-p representation of n (mod p).*