ARML Lecture VII - Number Theory

VMT Math Team

March 18, 2004

Number theory encompasses anything relating to properties of integers. In contests, we typically encounter problems involving divisibility and factorization. In this lecture we will let $p_1, p_2, \ldots$ represent the prime numbers in ascending order so that p_n is the nth prime number. We let $gcd(p, q)$ represent the greatest common denominator and let $lcm(p, q)$ the least common multiple of integers p and q.

1 Divisibility and Factoring

The Fundamental Theorem of Arithmetic says that any positive integer n can be represented in exactly one way as the product of prime numbers, so that the factorizations of p and q are identical if and only if $p = q$.

The number f divides n if and only if none of the powers of the primes in the factorization of f are greater than those of n. Specifically, f divides n k times if and only if there is no prime p is the factorization of f that appears more than $\frac{1}{k}$ times as often as it appears in the factorization of n.

On a related note, if some integer f divides integers p and q, then f divides $mp + nq$, where m and n are *any* integers.

Quick question: How many times does 3 divide 28!?

We reason that the answer is the sum of how many times 3 divides each of $1, 2, \ldots, 28$. Of the numbers 1 through 28, exactly $\lfloor \frac{28}{3} \rfloor$ a multiples of 3, $\lfloor \frac{28}{3^2} \rfloor$ are multiples of 3^2, etc. (where $\lfloor x \rfloor$ is the *floor function* and represents the greatest integer less than or equal to x). To count the total number of p's appearing in their factorizations, we compute $9+3+1+0+0+0+\cdots = 13$. The generalized result:

$$\text{Theorem}: \quad \text{A prime number } p \text{ divides } n! \text{ exactly } \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \text{ times.}$$

This fact enables us to determine how many 0's appear at the end of $n!$. Because there are more 2's than 5's in the factorization of $n!$, the number of 0's at the end of $n!$ is the

number of 5's in its factorization.

Quick question: How many factors does 120 have?

We factor 120 and find that $120 = 2^3 \cdot 3^1 \cdot 5^1$. Therefore, any $m = 2^{m_1} \cdot 3^{m_2} \cdot 5^{m_3}$ that divides 120 must satisfy $0 \leq m_1 \leq 3, 0 \leq m_2 \leq 1, 0 \leq m_3 \leq 1$. There are 4 possible m_1, 2 possible m_2, and 2 possible m_3, meaning that there are $4 \cdot 2 \cdot 2 = 16$ positive integers that divide 120. Moreover:

$$\text{Theorem}: \quad n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \text{ has } (n_1+1)(n_2+1)\cdots(n_k+1) \text{ factors.}$$

The greatest common divisor of m and n is defined to be the largest integer that divides both m and n. Two numbers whose largest common divisor is 1 are called *relatively prime* even though neither m nor n is necessarily prime. There are two notable ways to compute $gcd(m, n)$.

- *Factoring* - Let $m = p_1^{m_1} \cdot p_2^{m_2} \cdots$ and $n = p_1^{n_1} \cdot p_2^{n_2} \cdots$ such that $m_1, m_2, \ldots, n_1, n_2, \ldots \geq 0$. Then $gcd(m, n)$ is the positive integer whose prime factorization contains p_i exactly $min(m_i, n_i)$ times for all positive integers i. Remark - This is useful if the factorizations of m and n are readily available, but if m and n are large numbers such as 4897, they will be difficult to factor.

- *Euclidean Algorithm* - Let $n > m$. If m divides n, then $gcd(m, n) = m$. Otherwise, $gcd(m, n) = gcd(m, n - m \cdot \lfloor \frac{n}{m} \rfloor)$. Remark - This is useful when factoring fails. For example, finding $gcd(4897, 1357)$. 1357 does not divide 4897, so $\lfloor \frac{4897}{1357} \rfloor = 3$, $4897 - 3 \cdot 1357 = 826$ and $gcd(4897, 1357) = gcd(1357, 826)$. 826 does not divide 1357, so $gcd(1357, 826) = gcd(826, 531)$. 531 does not divide 826 so $gcd(862, 531) = gcd(531, 295)$. Continuing this process, $gcd(531, 295) = gcd(295, 236) = gcd(236, 59) = 59$.

The least common multiple of m and n is defined to be the least number that is divisible by both m and n. Other than listing multiples of m and n, we can determine the lcm by the formula: $lcm(m, n) = \frac{mn}{gcd(m,n)}$. Note that because $gcd(m, n) \geq 1$, we have $lcm(m, n) \leq mn$.

The Euler Phi function, $\phi(n)$, denotes the number of positive integers less than or equal to n that are relatively prime to n. If we let $p_1, p_2, \ldots, p_k$ denote all of the distinct prime numbers that divide p, then:

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

2 Modulo Trickery

The division algorithm states that when dividing n by $p \neq 0$, there is exactly one integer q such that $n = pq + r$, where $0 \leq r < |p|$. We define n modulo p (or simply m mod p) to be

r in this equation. We use the notation $r \equiv n \pmod{p}$ when solving equations. There are a number of theorems that apply to modulos, some of which are outlined here:

- $k \cdot n + c \equiv c \pmod{n}$, for any integers k, n, and c. This follows from the definition of modulos.
- $(k \cdot n + c)^m \equiv c^m \pmod{n}$, for any integers k, n, and c, and any positive integer m. This is the result of binomial expansion of the left side.
- $a^{p-1} \equiv 1 \pmod{p}$, for relatively prime integers a and p, where p is prime. A result known as *Fermat's Little Theorem*.
- $a^{\phi(n)} \equiv 1 \pmod{n}$, for any relatively prime integers a and n, where $\phi(n)$ is the Euler Phi function. This is *Euler's Generalization of Fermat's Little Theorem*.
- $(p-1)! \equiv -1 \pmod{p}$, for any prime p. This is *Wilson's Theorem*.

Whenever the word remainder appears, you should immediately think modulos. Likewise, determining the last few digits of a number should make you consider modulos.

The above theorems are merely suppliments to the algebra that can be performed on modular equations, which we outline here. The rules of *modular arithmetic* can be summarized as follows:

1. The only numbers that can be divided by m in modulo n are those that are multiples of $gcd(m, n)$.[1]
2. When multiplying by m in modulo n, the only numbers that can result are multiples of $gcd(m, n)$.[2]
3. Taking the square root of both sides is "normal" only in prime modulos. (For example, the solutions to $n^2 \equiv 1 \pmod{8}$ are not only $n \equiv \pm 1 \pmod{8}$ but more completely $n \equiv \pm 1, \pm 3 \pmod{8}$.)
4. When solving for integer solutions in modulo n, any integer multiple of n can be added to or subtracted from any number. (This includes adding multiples of n to square roots of negative numbers.)
5. All other operations behave normally according to the standard rules of algebra over the integers.

Consider, for example, solving for all positive $n \leq 100$ for which $n^2 + n + 31$ is divisible by 43. Of course we set up $n^2 + n + 31 \equiv 0 \pmod{43}$. We apply the quadratic formula and find that $n \equiv \frac{-1 \pm \sqrt{-123}}{2} \pmod{43}$. Because $-123 \equiv -123 + 43k \pmod{43}$, we replace -123 with $-123 + 5 \cdot 43 = 49$ and continue: $n \equiv \frac{-1 \pm 7}{2} \pmod{43}$, so $n \equiv 3, -4 \pmod{43}$. Therefore, all such n are 3, 39, 46, 82, and 89.

[1] Each of which leaves $gcd(m, n)$ different residues.

[2] There are $gcd(m, n)$ distinct residues that all lead to the same number when multiplied by m.

3 Practice

All of the following problems can be solved with the techniques enumerated above.

1. How many factors does 800 have?
2. How many times does 7 divide 100!?
3. What is the smallest positive integer n for which $\frac{n-6}{5n+17}$ is non-zero and reducible?
4. In Mathworld, the basic monetary unit is the Jool, and all other units of currency are equivalent to an integral number of Jools. If it is possible to make the Mathworld equivalents of \$299 and \$943, then what is the maximum possible value of a Jool in terms of dollars?
5. What are the last three digits of 3^{2004}?
6. Compute the remainder when 2000! is divided by 2003.
7. (ARML 1999) How many ways can one arrange the numbers 21, 31, 41, 51, 61, 71, and 81 such that any four consecutive numbers add up to a multiple of 3?
8. Determine all positive integers $n \leq 100$ such that $n^4 - n^2 + 57$ is divisible by 73.