Some Number Theory

Georgia ARML

May 17, 2009

Number theory encompasses anything relating to properties of integers. In contests, we typically encounter problems involving divisibility and factorization. We let $\gcd(p,q)$ represent the greatest common denominator and let $\text{lcm}\,(p,q)$ the least common multiple of integers p and q.

1 Divisibility and Factoring

Some problems can be solved by using only basic properties, such as our first problem.

Problem 1.1 Find all positive n such that $n^2-19n+99$ is a perfect square. (AIME)

Solution. Let $n^2-19n+99=k^2$ for some integer k. Then we solve $n^2-19n+99-k^2=0$ using the quadratic formula to get $n=\frac{1}{2}\left(19\pm\sqrt{19^2-4(99-k^2)}\right)$. Since we want n to be an integer, the discriminant must be an integer. Thus, $19^2-4(99-k^2)=j^2$ for some integer j. Moreover, since j plus/minus 19 must be divisible by 2, j must be odd. Expanding, we have $4k^2-35=j^2$, or $4k^2-j^2=35$. Hence, $(2k-j)(2k+j)=35$. So $2k-j$ and $2k+j$ must be integers, and since we only care about j^2, we will seek positive cases.

One case is $2k-j=1$ and $2k+j=35$, giving $j=17$, so $j^2=289$. The other case is $2k-j=5$ and $2k+j=7$, giving $j=1$, so $j^2=1$. Hence, $k^2=81$ or $k^2=9$ which implies $n=1,9,10,18$. □

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 in 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.

Problem 1.2 How many times does 3 divide 28!?

Solution. 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 $\lfloor\frac{28}{3}\rfloor$ are 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 les 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 is as follows.

Theorem 1.1. *A prime number p divides $n!$ exactly* $\displaystyle\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor$ *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.

Problem 1.3 How many factors does 120 have?

Solution. Since $120 = 2^3 \cdot 3^1 \cdot 5^1$, we consider the three sets $\{2^0, 2^1, 2^2, 2^3\}$, $\{3^0, 3^1\}$, $\{5^0, 5^1\}$. Any number formed by picking exactly one element from each of these 3 sets and multiplying them will be a divisor 120. Hence, there are $4 \cdot 2 \cdot 2 = 16$ positive integers that divide 120. □

Theorem 1.2. *$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ has $(n_1+1)(n_1+2)\cdots(n_k+1)$ 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* and the *Euclidean algorithm*.

Theorem 1.3 (Euclidean algorithm version 1). *Let $n > m$. If m divides n, then $\gcd(m,n) = m$. Otherwise, $\gcd(n,m) = \gcd(m, n - m \cdot \lfloor \frac{n}{m} \rfloor)$.*

Theorem 1.4 (Euclidean algorithm version 2). *For any positive integers m and n, there exists integers q and r such that $0 \leq r < n$ and $m = nq + r$.*

Problem 1.4 Find $\gcd(4897, 1357)$.

Solution. Note that factoring would be time consuming. We use the Euclidean algorithm.

$$\begin{aligned}
\gcd(4897,1357) &= \gcd(1357, 4897 - 3 \cdot 1357) = \gcd(1357, 826) \\
&= \gcd(826, 1357 - 1 \cdot 826) = \gcd(826, 531) \\
&= \gcd(531, 826 - 1 \cdot 531) = \gcd(531, 295) \\
&= \gcd(295, 531 - 1 \cdot 295) = \gcd(295, 236) \\
&= \gcd(236, 295 - 1 \cdot 236) = \gcd(236, 59)
\end{aligned}$$

and since 59 divides 236, we have $\gcd(4897,1357) = \gcd(236,59) = 59$. □

The most useful definition of the least common multiple is

$$\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)}.$$

The Euler phi-function $\varphi(n)$, 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, …, p_k denote all of the distinct prime number that divide n, then

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

2 Modulo Tricks

The Euclidean algorithm states that there exists integers q and r such that $0 \leq r < p$ and $n = pq + r$. We define n modulo p — or simply $m \mod p$ — to be r. That is, $r \equiv n \mod p$. There are a number of little theorems that apply to modulos.

Theorem 2.1. *$kn+c \equiv c \mod n$ for any integers k, n, and c.*

Theorem 2.2. *$(kn+c)^m \equiv c^m \mod n$ for any integers k, n, and c, and positive integer m.*

Theorem 2.3 (Fermat's Little Theorem). *$a^{p-1} \equiv 1 \mod p$ for relatively prime integers a and p, where p is prime.*

Theorem 2.4 (Euler's Theorem). *$a^{\varphi(n)} \equiv 1 \mod n$ for relatively prime integers a and n.*

Theorem 2.5 (Wilson's Theorem). *$(p-1)! \equiv -1 \mod p$, where p is prime.*

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 $\gcd(m,n)$, each of which leaves $\gcd(m,n)$ different residues.
2. When multiplying by m in modulo n, the only numbers that can result are multiples of $\gcd(m,n)$. There are $\gcd(m,n)$ distinct residues that all lead to the same number when multiplied by m.
3. Taking the square root of both sides is "normal" only in prime modulos. (For example, the solutions to $n^2 \equiv 1 \mod 8$ are not only $n \equiv \pm 1 \mod 8$ but more completely $n \equiv \pm 1, \pm 3 \mod 8$.)
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.

Problem 2.1 Find all positive integers n less than 100 such that n^2+n+31 is divisible by 43.

Solution. Of course the problem is asking us to solve $n^2+n+31 \equiv 0 \mod 43$. Using the quadratic formula, we find that $n \equiv \frac{1}{2}\left(-1 \pm \sqrt{-123}\right) \mod 43$. However, because $-123 \equiv -123+43k \mod 43$ for any integer k, we can replace -123 with $-123+43\cdot 5 = 49$ to obtain $n \equiv \frac{1}{2}(-1 \pm 7) \mod 43$. Thus, $n \equiv 3, -4 \mod 43$. Adding 43 and 86 to each of these gives all solutions: 3, 39, 46, 82, and 89. □

3 Linear Diophantine Equations

Many problems deal with simple linear equations in two variables, such as $ax+by=c$, where we are asked to find the number of integer solutions, or maybe a few particular integer solutions. This kind of thing is really a number theory problem.

Theorem 3.1. *The equation $ax+by=c$, where a, b, and c are integers, has an integer solution if and only if $\gcd(a,b)$ divides c. Moreover, if (x_0,y_0) is one such solution, then the others are given by $x = x_0+bt$ and $y = y_0+at$ for every integer t.*

Of course, the above theorem is generalizable to any number of linear variables and coefficients.

Problem 3.1 Characterize the solutions to $7x+3y=8$.

Proof. Since $\gcd(3,7)=1$ divides 8, there are solutions. From the Euclidean algorithm, we have $7=3\cdot 2+1$, or $1=7+3(-2)$. Multiplying by 8, we have $8=7\cdot 8+3(-16)$ so that $(8,-16)$ is a solution. Thus all solutions are $(8+3t,-16+7t)$ for every integer t. □

Problem 3.2 Let n be a positive integer. Suppose there are 2016 ordered triples (x,y,z) of positive integers satisfying the equation $x+8y+8z=n$. Find the maximum value of n.

Proof. Write $n=8a+b$ where a and b are integers with $0\leq a,b<8$. Since $x\equiv n\equiv b \mod 8$, the possible values of x are $b,b+8,\ldots,b+8(a-1)$. Let $x=b+8i$ where $0\leq i<a-1$. Then $8(y+z)=8(a-i)$, or $y+z=a-i$. This gives $a-i-1$ ordered pairs (y,z) of positive integer solutions: $(1,a-i-1),\ldots,(a-i-1,1)$. Hence, there are

$$\sum_{i=0}^{a-1}(a-i-1)=\sum_{i=0}^{a-1}i=\frac{a(a-1)}{2}$$

ordered triples satisfying the conditions of the problem. Solving $a(a-1)/2=2016$ we have $a=64$. Thus, the maximum value of n is obtained by setting $b=7$: $64\cdot 8+7=519$. □

4 Exercises and Problems

(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) Find $8^{83}+6^{83} \mod 49$.

(6) What are the last three digits of 3^{2009}?

(7) Compute the remainder when 2008! is divided by 2011.

(8) (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?

(9) Determine all positive integers $n\leq 100$ such that n^4-n^2+57 is divisible by 73.

(10) Find all integers n such that $8n+3$ is a perfect square.

(11) Determine all triples of integers (x,y,z) such that $3x+4y+5z=6$.

(12) (USAMO 1979) Find all non-negative integer solutions $(n_1,n_2,\ldots,n_{14})$ to

$$n_1^4+n_2^4+\cdots+n_{14}^4=1599.$$