Some Number Theory

Chuck Garner, Ph.D.

Department of Mathematics
Rockdale Magnet School for Science and Technology

May 25, 2009 / Georgia ARML Practice

Outline

Outline

Warm-Up Problem

Problem

Find all positive n such that $n^2 - 19n + 99$ is a perfect square.

Warm-Up Problem

Solution.

Let $n^2 - 19n + 99 = k^2$ for some integer k. Solve $n^2 - 19n + 99 - k^2 = 0$ using the quadratic formula to get $n = \frac{1}{2}\left(19 \pm \sqrt{19^2 - 4(99 - k^2)}\right)$. We want n to be an integer so the discriminant must be an integer. Thus, $19^2 - 4(99 - k^2) = j^2$ for some integer j. 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. 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 $n = 1, 9, 10, 18$. □

Fundamental Theorem of Arithmetic

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 $p = q$.

Fundamental Theorem of Arithmetic

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 $p = q$.

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.

Another problem

Problem

How many times does 3 divide 28!?

Another problem

Problem

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. To count the total number of 3's appearing in their factorizations, we compute

$9 + 3 + 1 + 0 + 0 + 0 + \cdots = 13.$ □

A Generalization

Theorem

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

Yet Another Problem

Problem

How many factors does 120 have?

Yet Another Problem

Problem

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. $\square$

Theorem of Factors

Theorem

$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ has $(n_1+1)(n_1+2)\cdots(n_k+1)$ factors.

Common Definitions

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.

Euclidean Algorithm

Theorem (Euclidean algorithm version 1)

Let $n > m$. If m divides n, then $\gcd(m, n) = m$. Otherwise, $\gcd(n, m) = \gcd(m, n - m \cdot \lfloor \frac{n}{m} \rfloor)$.

Euclidean Algorithm

Theorem (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 (Euclidean algorithm version 2)

For any positive integers m *and* n, *there exists integers* q *and* r *such that* $0 \leq r < n$ *and* $m = nq + r$.

Finding the GCD

Problem

Find $\gcd(4897, 1357)$.

Finding the GCD

Problem

Find $\gcd(4897, 1357)$.

Solution.

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 $\gcd(4897, 1357) = 59$. □

Another Definition

The most useful definition of the least common multiple is

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

Euler's phi-function

The Euler phi-function $\varphi(n)$, denotes the number of positive integers less than or equal to n that are relatively prime to n.

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

Outline

Modulo Properties

Theorem

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

Modulo Properties

Theorem

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

Theorem

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

Modulo Properties

Theorem

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

Theorem

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

Theorem (Fermat's Little Theorem)

$a^{p-1} \equiv 1 \mod p$ *for relatively prime integers a and p, where p is prime.*

Modulo Properties

Theorem

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

Theorem

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

Theorem (Fermat's Little Theorem)

$a^{p-1} \equiv 1 \mod p$ *for relatively prime integers a and p, where p is prime.*

Theorem (Euler's Theorem)

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

Modulo Properties

Theorem

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

Theorem

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

Theorem (Fermat's Little Theorem)

$a^{p-1} \equiv 1 \mod p$ *for relatively prime integers a and p, where p is prime.*

Theorem (Euler's Theorem)

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

Theorem (Wilson's Theorem)

$(p-1)! \equiv -1 \mod p$*, where p is prime.*

Modulo Arithmetic

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.

Modulo Arithmetic

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.

Modulo Arithmetic

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.

Modulo Arithmetic

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.
4. When solving for integer solutions in modulo n, any integer multiple of n can be added to or subtracted from any number.

Modulo Arithmetic

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.
4. When solving for integer solutions in modulo n, any integer multiple of n can be added to or subtracted from any number.
5. All other operations behave normally according to the standard rules of algebra over the integers.

Another Problem!

Problem

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

Another Problem!

Problem

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. □

Outline

A Theorem

Theorem

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*.*

Oh Joy! Another Problem!

Problem

Characterize the solutions to $7x + 3y = 8$. How many positive integer solutions are there?

Oh Joy! Another Problem!

Problem

Characterize the solutions to $7x + 3y = 8$. How many positive integer solutions are there?

Solution.

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.

For positive integer solutions, we must have both $8 - 3t > 0$ and $-16 + 7t > 0$. But this implies $t < \frac{8}{3}$ and $t > \frac{16}{7}$, which no integer t satisfies. Hence, there are no positive integer solutions. $\square$

Two Problems in a Row!

Problem

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.

Two Problems in a Row!

Solution.

Write $n = 8a + b$ where a and b are integers with $0 \le a, b < 8$. 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 $0 \le i < a - 1$. 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 $b = 7$. This gives $64 \cdot 8 + 7 = 519$. $\square$

Outline

Suggested Resources

104 Number Theory Problems,
Andreescu, Andrica, Feng;
Birkhäuser 2007.

Number Theory Through Inquiry,
Marshall, Odell, Starbird;
Mathematical Association of America 2007.