Competitive Programming and Mathematics Society

Mathematics Workshop

Number Theory

Cyril and Zac

Table of contents

CPMSOC

Arc CLUBS SUPPORTED BY Arc INDEPENDENTLY RUN

Welcome

- Join our subcom!
- Mathematics workshops will (probably) run every odd-numbered week (1, 3, 5, ...)
- Programming ones are every other week
- Slides will be uploaded on website (unswcpmsoc.com)
- Competitive maths ain't so competitive!

Attendance form

pixels

CPMSOC

Fundamental theorem of arithmetic

CPMSOC

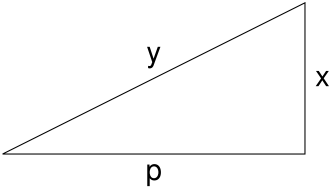
- Every positive integer has a unique prime factorisation!
- $x = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$, where $p_1, \dots, p_n$ are prime
- Very simple property that proves to be incredibly important

Definition

Two integers are coprime if they share no prime factors in their prime factorisations

Example problem

Let p be some prime number. The following right-angled triangle has integer sides x, y, p:



Find all possible values of x and y.

Example problem - solution

CPMSOC

Arc CLUBS SUPPORTED BY Arc INDEPENDENTLY RUN

Solution: Using the Pythagorean theorem, we can write $p^2 + x^2 = y^2$. Rearranging, we obtain

$$p^2 = (y - x)(y + x).$$

Since p^2 has only one prime factorisation, namely $p \times p$, we have two cases:

- $y - x = p$ and $y + x = p$. However, this would imply $x = 0$, which it cannot be as the triangle has non-zero side lengths.
- $y - x = 1$ and $y + x = p^2$. Solving these simultaneous equations, we obtain $y = \frac{p^2+1}{2}$ and $x = \frac{p^2-1}{2}$.

Modular Arithmetic

CPMSOC

- Number systems where we could have $3 = 1$?
- We can make abstract concepts of equality, as long as "$=$" obeys:
  - Reflexivity: $x = x$
  - Symmetry: $x = y \implies y = x$
  - Transitivity: $x = y$ and $y = z \implies x = z$
- Modular arithmetic is one way of doing this with integers, such that things that are equal have the same remainder, or residue, after division by a modulus. In above example, $3 = 1 \mod 2$ because both have residue 1 after division by 2.
- Traditionally, we use a three-line equal sign ($\equiv$).

Modular Arithmetic

- Amazingly, in modular arithmetic addition and multiplication are still nicely defined (e.g. $3 \times 4 = 12 = 0 \bmod 2$, and $1 \times 2 = 2 = 0 \bmod 2$ (replaced 3 and 4)).
- Proof: each number modulo m in residue classes i, j can be represented by $nm + i$.

$$(nm + i) + (pm + j) = (n + p)m + (i + j)$$

has a remainder of $i + j$.

$$(nm + i)(pm + j) = npm^2 + nmj + pmi + ij = m(npm + nj + pi) + ij$$

has a remainder of ij

Example problem

CPMSOC

- Show that if the alternating sum of a numbers digits is divisible by 11, so is that number. Hint: think about representing numbers as negatives in mod 11.

Example problem - solution

- Show that if the alternating sum of a numbers digits is divisible by 11, so is that number. Hint: think about representing numbers as negatives in mod 11.

$$\sum_{i=1}^{n-1} 10^i x_i = \sum_{i=1}^{n-1} (-1)^i x_i \bmod 11$$

Example Problem

- Prove there are infinitely many primes.

Example Problem - solution

- Prove there are infinitely many primes.
- Assume the contrary, that there are finitely many primes $p_1, p_2, ..., p_n$. Then $p_1 p_2 ... p_n + 1 = 1$ for all modulos $p_1, p_2, ..., p_n$, so is divisible by none of them ($\neq 0 \bmod p_i$), and hence a new prime. Thus there cannot be a finite list of primes.

Greatest Common Divisor (GCD)

$\gcd(a, b)$ denotes the greatest common divisor of a and b. It may be calculated very efficiently using the Euclidean Algorithm.

Theorem

$\gcd(a, b) = \gcd(a - b, b)$ *if* $a > b$

This is because divisibility by a and b is equivalent to divisibility by $a - b$ and b:

- $a \equiv 0 \mod d$ and $b \equiv 0 \mod d \implies a - b \equiv 0 - 0 = 0 \mod d$
- $a - b \equiv 0 \mod d$ and $b \equiv 0 \mod d \implies a = a - b + b \equiv 0 + 0 = 0 \mod d$

Example: $\gcd(729, 516)$

Bezout's Identity Proof

$ax + by = \gcd(a, b)$ has solutions for integers a, b, x, y.

Theorem

If a, b are coprime integers, ax takes on all values from 0 to $b - 1$ over $0 \leq x < b \pmod{b}$

Proof.

Consider $ax \bmod b$. If $ai = aj \bmod b$, then, since a shares no factors with b, $i = j$. So, ax takes on p distinct values under mod p for $0 \leq x < b$. Since there are only b possible values $(0, 1, ..., b - 1)$, it must cover all of them. ■

Divide both sides the original equation by $\gcd(a, b)$ to reduce the problem to $ax + by = 1$ for coprime a, b. Since $ax = 1 \bmod b$ for some x, there exists $ax = 1 + by$ for some y, so $ax - by = ax + b(-y) = 1$ exists for some integers x and $-y$.

Division in modular arithmetic???

- Suppose we have coprime a and p.
- Show that there exists an integer b such that:

$$ab = 1 \text{ mod } p$$

Division... with a catch :(

- Suppose we have coprime a and p.
- Show that there exists an integer b such that:

$$ab = 1 \bmod p$$

- Proof: b exists to satisfy $ab - px = 1 \implies ab = 1 + px$, take $\bmod p \implies ab = 1$

Fermat's Little Theorem

- $a^{p-1} = 1 \bmod p$ if p is prime
- Source: https://proofwiki.org/wiki/Fermat%27s_Little_Theorem/Proof_1
- Recall that ax takes on all values in $(0, p) \bmod p$ if $\gcd(a, p) = 1$ for $0 < x < p$.
- So, $a \times 2a \times 3a \times \ \times (p-1)a = 1 \times 2 \times 3 \times ... \times (p-1) \bmod p$. Thus, $a^{p-1}(p-1)! = (p-1)! \bmod p$, $(a^{p-1} - 1)(p-1)! = 0 \bmod p$. $(p-1)! \neq 0 \bmod p$. (Because no product of non-zero residues can give a prime, or it would be composite)

Euler's Totient Function

CPMSOC

Definition

$\varphi(n)$ equals the number of positive integers $k < n$ coprime to n (i.e. $\gcd(n, k) = 1$)

- Formula: $\varphi(n) = \prod_p p_i^{e_i - 1}(p_i - 1)$ for all prime p in the prime factorisation of n:

$$n = p_1^{e_1} p_2^{e_2} ... p_i^{e_i}$$

- This can be proved by showing a multiplicative rule on the function:

$$\varphi(ab) = \varphi(a)\varphi(b), \text{ if } \gcd(a, b) = 1$$

  and

$$\varphi(p^e) = p^{e-1}(p - 1)$$

  for p prime.
- Or we can prove it by splitting n into prime factors, using the inclusion-exclusion method to count numbers sharing a factor with n, which we will cover next.

Euler's Totient Function - second proof

CPMSOC

- Counting proof: count all positive integers $k < n$ which share a factor greater than 1 with n (i.e. $\gcd(k, n) > 1$
- Take every prime factor and count their multiples
- Then subtract this from n to get the number of coprime integers

e.g. Consider $n = 60 = 2^2 \times 3 \times 5$

Euler's Totient Function - second proof

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Euler's Totient Function - second proof

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Euler's Totient Function - second proof

CPMSOC

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Euler's Totient Function - second proof

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Euler's Totient Function - second proof

Suppose $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

Number of integers sharing a non-one factor with n:

$\frac{n}{p_1} + \frac{n}{p_2} + \frac{n}{p_3} + \cdots$

Euler's Totient Function - second proof

CPMSOC

Suppose $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

Number of integers sharing a non-one factor with n:

$$\frac{n}{p_1} + \frac{n}{p_2} + \frac{n}{p_3} + \cdots - \frac{n}{p_1 p_2} - \frac{n}{p_2 p_3} - \frac{n}{p_1 p_3} - \cdots$$

Euler's Totient Function - second proof

Suppose $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

Number of integers sharing a non-one factor with n:

$$\frac{n}{p_1} + \frac{n}{p_2} + \frac{n}{p_3} + \cdots - \frac{n}{p_1 p_2} - \frac{n}{p_2 p_3} - \frac{n}{p_1 p_3} - \cdots + \frac{n}{p_1 p_2 p_3} + \cdots$$

Euler's Totient Function - second proof

Suppose $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.
Number of integers sharing a non-one factor with n:
$\frac{n}{p_1} + \frac{n}{p_2} + \frac{n}{p_3} + \cdots - \frac{n}{p_1 p_2} - \frac{n}{p_2 p_3} - \frac{n}{p_1 p_3} - \cdots + \frac{n}{p_1 p_2 p_3} + \cdots$

Therefore, we see that

$$\begin{aligned}
\varphi(n) &= n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} - \cdots + \frac{n}{p_1 p_2} + \frac{n}{p_2 p_3} + \frac{n}{p_1 p_3} + \cdots - \frac{n}{p_1 p_2 p_3} - \cdots \\
&= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \left(\frac{p_1 - 1}{p_1}\right) \left(\frac{p_2 - 1}{p_2}\right) \cdots \left(\frac{p_n - 1}{p_n}\right) \\
&= \frac{n}{p_1 p_2 \cdots p_n} (p_1 - 1)(p_2 - 1) \cdots (p_n - 1)
\end{aligned}$$

Attendance form :D

CPMSOC

Further events

CPMSOC

Arc CLUBS SUPPORTED BY Arc INDEPENDENTLY RUN

Please join us for:

- Maths workshop in two weeks
- Social session tomorrow
- Programming workshop next week

Wait... there's more!

McDonald's chicken McNuggets$^{\text{TM}}$ in whole boxes, each one containing a nuggets or b nuggets, for two coprime integers a and b. Due to the multi-billion-dollar corporation's uncompromising nature, each box contains exactly either of these two amounts. You can buy as many boxes of each type as you wish.

Show that the minimum integer n, such that for all integers $x \geq n$, you can buy exactly x McNuggets$^{\text{TM}}$ in total, is equal to $(a-1)(b-1)$.

My unformatted ramblings

CPMSOC

also i think i got the chicken mcnugget theorem proof: $(a-1)(b-1) - 1$ ain't possible cause you get $ax + by = ab - a - b$, or $a(x+1) + b(y+1) = ab$. because a,b are coprime, $x+1 >= b$ (consider eq in mod b) and $y+1 >= a$ (consider eq in mod a)
$(a-1)(b-1) + k$ possible for $0 <= k < b$ (now just do induction for this by adding b to possible configurations for each) proof of previous theorem: for $k = b-1$, $ax + by = ab - a - b + 1 + b - 1 = ab - a$, trivial. for $0 <= k < b - 1$, $ax = k + 1 \mod b$ exists for $0 < x < b$ (bezout's identity... kinda), so $ax - by = k + 1$ exists for some $y > 0$. note, however, $ax - by > 0$, so $by < ax < ab$, thus $y < a$ $ax - by + ab - a - b = ab - a - b + 1 + k = a(x - 1) + b(a - y - 1) = (a-1)(b-1) + k$. $x - 1, a - y - 1 >= 0$