Number Theory 2023 Midterm Solutions

1. (a) What is a triangular number?

Solution

A number of the form $1 + 2 + \cdots + n$.

(b) Give a formula for the n^{th} triangular number.

Solution

$n(n+1)/2$.

(c) Fill in and prove: A number M is triangular if and only if _____ is an odd square.

Solution

...iff $\boxed{8M+1}$ is an odd square. From our formula, M is triangular if and only if $2M = n(n+1) = n^2 + n$ for some n. So if and only if $8M + 1 = 4n^2 + 4n + 1 = (2n+1)^2$ for some n.

2. (a) What does it mean that (a, b, c) is a pythagorean triple?

Solution

$a^2 + b^2 = c^2$

(b) What does it mean that it is a primitive pythagorean triple?

Solution

a, b and c have no common factors.

(c) Given a primitive pythagorean triple (a, b, c), show that exactly one of a or b must be a multiple of 3.

Solution

If both are 1 or 2 modulo 3, then their squares are 1 modulo 3. So c^2 is 2 modulo 3, but no squares are 2 modulo 3. So at least one of a or b must be 0 mod 3. They can't both be, or the triplet wouldn't be primitive.

3. (a) **I removed part (3a). So question 3 was out of 3, not out of 5.** Show that a pythagorean triple (a, b, c) is *primitive* if $\gcd(a, b) = 1$.

Solution

If p divides c and a but not b, then p^2 divides $c^2 - a^2$ but not b^2. But this contradicts $a^2 + b^2 = c^2$. So $\gcd(a, b) = 1$ implies $\gcd(a, c) = 1$. Similarily it implies $\gcd(b, c) = 1$.

(b) Fill in: We showed that any primitive triple (a, b, c) is of the form

$$a = st \qquad b = \frac{\qquad}{2} \qquad c = \frac{\qquad}{2}$$

where $s > t \geq 1$ are odd integers with $\gcd(s, t) = 1$.

Solution

$b = \frac{s^2 - t^2}{2}$ and $c = \frac{s^2 + t^2}{2}$

(c) Find a formula that describes all primitive pythagorean triples (a, b, c) such that $c = a + 2$.

Solution

Solution 1) Using that $a = st$ and $c = (s^2 + t^2)/2$, the condition $c = a + 2$ gives $(s^2 + t^2)/2 = c = a + 2 = st + 2$, from this, using that $s > t$ on the last line, we see

$$\begin{aligned} (s^2 + t^2)/2 = st + 2 \quad &\Rightarrow \quad s^2 + t^2 = 2st + 4 \\ &\Rightarrow \quad 4 = s^2 - 2st + t^2 = (s - t)^2 \\ &\Rightarrow \quad (s - t) = \pm 2 \Rightarrow s = t + 2. \end{aligned}$$

So the triples of this form are

$$(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}) = (t^2 + 2t, 2t + 2, t^2 + 2t + 2)$$

for every odd $t \geq 1$.
This answer is fine, but some might have noticed the satisfying change of variables, taking $n = t + 1$ this becomes

$$(n^2 - 1, 2n, n^2 + 1)$$

for even $n \geq 2$.

Solution 2) From $a^2+b^2 = c^2 = (a+2)^2 = a^2+4a+4$ we get that $b^2 = 4a+4 = 4(a+1)$. As b^2 is even so is b so writing $b = 2n$ we get $4n^2 = b^2 = 4a+4$ and so $n^2 = a+1$, giving that $a = n^2-1, c = a+2 = n^2+1$ and $b^2 = c^2-a^2 = 4n^2$ so $b = 2n$. Thus our triple is

$$(a, b, c) = (n^2 - 1, 2n, n^2 + 1).$$

If n is odd, this in not primitive, but if n is even, then $\gcd(n^2 - 1, 2n) = 1$ and it is. So this is for all even $n \geq 2$.

4. Use the extended Euclidean algorithm to write $\gcd(518, 399)$ as a linear combination of 518 and 399.

Solution

Step	a_i	$b_i(q_i)$	r_i	$x(518)$	$y(399)$
1	518	399(1)	119	1	-1
2	399	119(3)	42	$-3(1) = -3$	$1 - 3(-1) = 4$
3	119	42(3)	$-\boxed{7}$	$1 - 3(-3) = 10$	$-1 - 3(4) = -13$
4	42	$-7(6)$	0		

So $-7 = 518(10) - 399(13)$ or $\boxed{7 = 399(13) - 518(10)}$. I cheated, and saved a step or two by using -7 instead of 35 on that second last step. I guess this is allowed.

5. Show that for odd integers s and t, with $\gcd(s, t) = 1$, the numbers st and $\frac{s^2-t^2}{2}$ are relatively prime.

Solution

Assume that st and $\frac{s^t-t^2}{2}$ are not relatively prime. So there is some prime p dividing both st and $\frac{s^2-t^2}{2}$. As st is odd, this p is odd, and so it not only divides $\frac{s^2-t^2}{2}$, but it divides s^2-t^2. So p divides $s^2-2st-t^2=(s-t)^2$, and as it is prime, divides $(s-t)$. As $p|st$ wa may also assume that $p|t$, and so $p|(s-t)+t=s$. This contradicts the fact that $\gcd(s,t)=1$.

6. For which of $d \in \{35, 36, 37\}$ does the congruence

$$399x \equiv_{518} d$$

have a solution? Find all (non-congruent) solutions.

Solution

We saw in a previous question that $\gcd(518, 399) = 7$ so of the given values of d this congruence only has solutions for $d = 35$, which is divisible by 7. We also saw that $399(13) - 518(10) = 7$. So $x = 13$ is a solution to $399x \equiv_{518} 7$; and so $x = 65$ is a solution to $399x \equiv_{518} 35$. Adding $518/7 = 74$ gives another solution so the non-congruent solutions are $x = 65 + k74$ for $k = 0, 1, \ldots, 6$.

7. For distinct primes p and q, what is the maximum possible number of solutions to $x^2 \equiv_{pq} a$.

Solution

If $x^2 \equiv_{pq} a$, then $x^2 \equiv_p a$ and $x^2 \equiv_q a$. We know that there are at most two solutions to $x^2 \equiv_p a$ and at most two to $x^2 \equiv_q a$. Now if two solutions modulo pq reduce to the same solution modulo p, they differ by a multiple of p, so they cannot reduce to the same solution modulo q. Thus at most two solutions modulo pq reduce to any one solution modulo p. This means there are at most 4 solutions modulo pq.

8. Let $p \geq 3$ be a prime number.

   (a) Assume that $a^2 \equiv_p b^2$ for integers a and b in $\{1, 2, \ldots, p-1\}$. Show that $b \equiv_p a$ or $b \equiv_p -a$.

Solution

If $a^2 \equiv_p b^2$ then $p|(a^2 - b^2) = (a - b)(a + b)$. As p is prime, this means that $p|(a - b)$ or $p|(a + b)$ which means that $b \equiv_p a$ or $b \equiv_p -a$.

(b) What are the numbers a such that $a^2 \equiv_p 1$?

Solution

By part (a) they are 1 and -1.

(c) Show that $(p-1)! \equiv_p p-1$ for any prime p.

Solution

As p is prime, every integer $a \in \{1, 2, \ldots, p-1\}$ has a unique multiplicative inverse: an integer $1/a$ in $\{1, 2, \ldots, p-1\}$ such that $a \cdot 1/a = 1$. As by part (b) the element 1 has only two square roots 1 and -1, only 1 and -1 are their own inverses. All other numbers have a unique inverse different from themselves. We take the product $(p-1)!$ every number cancels with its inverse except 1 and -1. So

$$(p-1)! = 1 \cdot (2 \cdot 3 \cdot \cdots \cdot p-2) \cdot p-1 \equiv_p 1 \cdot (1) \cdot -1 = -1.$$

9. Use the Chinese Remainder Theorem Algorithm to find a number n such that $n \equiv_9 7$ and $n \equiv_{23} 5$.

Solution

We use the Chinese Remainder Theorem Algorithm. As $n \equiv_9 7$ we have that $n = 7 + c \cdot 9$ for some c. Plugging this into $n \equiv_{23} 5$ we get that

$$7 + c \cdot 9 \equiv_{23} 5 \Rightarrow c \equiv_{23} 21/9.$$

Though we would use EEA if it were harder, we see that $9 * (-5) \equiv_{23} 1$, so see $-5 \equiv_{23} 18$ is the multiplicative inverse of 9 modulo 23. Thus $c \equiv_{23} 21 \cdot (-5) \equiv_{23} -13 \equiv_{23} 10$. We conclude that $n = 7 + 10 \cdot 9 = 97$ is such an n.

10. (a) What is a Mersenne prime?

Solution

A prime of the form $2^p - 1$ for prime p.

(b) What is a perfect number?

Solution

A number that is the sum of its proper divisors.

(c) State and prove one of: Euclid's Perfect Number Formula or Euler's Perfect Number Theorem. (If you prove Euler, you can assume the multiplicativity of σ.)

Solution

See text