# 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. Find a formula for all points on the hyperbola $x^2 - y^2 = 1$ whose coordinates are rational numbers.

**Solution**

We parametrise the points on the hyperbola $H$ by the slope $m$ of the line $L_m$ they make through the point $p_0 = (-1, 0)$. Then we show that the point is rational if and only if $m$ is rational, so this gives a formula for all rational points. For point $p_m = (x, y)$ on $H$, the line $L_m$ is $y = m(x+1)$. The points $(x, y)$ on $H$ and $L_m$ satisfy

$$x^2 - y^1 = 1 \qquad \text{and} \qquad y = m(x+1)$$

so their $x$ values satisfy

$$x^2 + 1 = y^2 = (m(x+1))^2 = m^2x^2 + 2m^2x + m^2,$$

and so are zeros of

$$(m^2 - 1)x^2 + 2m^2x + (m^2 - 1).$$

We know than $x = -1$ is one zero of this polynomial, as $(-1, 0)$ is on $H$ and $L_m$, so to get the other one we divide by $x + 1$. This gives (by polynomial long division)

$$(m^2 - 1)x + (m^2 + 1) = 0$$

which has solution $x = \frac{1+m^2}{1-m^2}$. The point $p_m$ on $H$ is thus $p_m = (\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2})$ (by plugging the $x$-value into the equation for $L_m$). This is rational if and only if $m$ is, so $p_m$ for rational $m$ defines all the rational points of $H$ except $p_0$.

4. Use the extended Euclidean algorithm to write $\gcd(441, 329)$ as a linear combination of 441 and 329.

**Solution**

| *Step* | $a_i$ | $b_i(q_i)$ | $r_i$ | $x(441)$ | $y(329)$ |
|---|---|---|---|---|---|
| 1 | 441 | 329(1) | 112 | 1 | $-1$ |
| 2 | 329 | 112(3) | $-\boxed{7}$ | $-3(1) = -3$ | $1 - 3(-1) = 4$ |
| 3 | 112 | $-7(16)$ | 0 | | |

So $-7 = 329(4) - 441(3)$ or $\boxed{\gcd(441, 329) = 7 = 441(3) - 329(4)}$. I cheated, and saved a step or two by using $-7$ instead of 105 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 $d \in \{33, 34, 35\}$ does the congruence

$$329x \equiv_{441} d$$

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

**Solution**

We saw in a previous question that $\gcd(441, 329) = 7$ so of the given values of $d$ this congruence only has solutions for $d = 35$, which is divisible by 7. We also saw that $7 = 441(3) - 329(4)$. So $x = -4$ is a solution to $329x \equiv_{441} 7$; and so $x = (-4) \cdot 35/7 = -20$ is a solution to $329x \equiv_{441} 35$. Adding $441/7 = 63$ gives another solution so the non-congruent solutions are $x = -20 + k63$ 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. Use the Chinese Remainder Theorem Algorithm to find a number $n$ such that $n \equiv_9 6$ and $n \equiv_{23} 10$.

**Solution**

We use the Chinese Remainder Theorem Algorithm. As $n \equiv_9 6$ we have that $n = 6 + c \cdot 9$ for some $c$. Plugging this into $n \equiv_{23} 10$ we get that

$$6 + c \cdot 9 \equiv_{23} 10 \Rightarrow c \equiv_{23} 4/9.$$

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 $c \equiv_{23} 4 \cdot (-5) \equiv_{23} -20 \equiv_{23} 3$. We conclude that $n = 6 + 3 \cdot 9 = 33$ is such an $n$.

9. (a) What is a composite number?

**Solution**

An integer larger than 2 that is not prime.

(b) Approximately how many composite numbers are there less than $10^6$?

**Solution**

The prime number theorem says that the number $\pi(n)$ of primes less than $n$ is about $n/ln(n)$ so $\pi(10^6)$ is about

$$10^6 - 10^6/\ln(10^6) = 10^6 - 10^6/6\ln(10) \approx 10^6(1 - 1/14).$$

(c) Find an interval of 100 consecutive composite numbers.

**Solution**

Taking $N > 101$ we have that $i|N!$ so $i|N! + i$ for all $i = 2 \ldots 101$. So $\{N! + 2, N! + 3, \ldots, N! + 101\}$ are 100 consecutve composite numbers.

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 $\sigma$.)

Solution

See text