Solutions – Problem Set #1 (Number Theory)

January 12, 2021 / Isabella B. Amaral

Question 1

Suppose that $a^2 + b^2 = c^2$ with $a, b, c \in \mathbb{Z}$. For example, $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. Assume that $(a, b) = (b, c) = (c, a) = 1$. Prove that there exist integers u and v such that $c - b = 2u^2$ and $c + b = 2v^2$ and $(u, v) = 1$ (there is no loss in generality in assuming that b and c are odd and that a is even). Consequently $a = 2uv, b = v^2 - u^2$, and $c = v^2 + u^2$. Conversely show that if u and v are given, then the three numbers $a, b,$ and c given by these formulas satisfy $a^2 + b^2 = c^2$.

Solution:

Assuming b, c odd and $a = 2uv$, such that $u, v \in \mathbb{N}$, then we have

$$a^2 = (2u\,v)^2 = c^2 - b^2 = (c - b)(c + b) = (2u^2)(2v^2)$$

such that $c - b = 2u^2$ and $c + b = 2v^2$.

Then, if u and v are given, we have $a = 2u\,v$ and then $2u^2 + 2v^2 = 2c - b + b = 2\left(u^2 + v^2\right) \implies c = u^2 + v^2$ and also $b = v^2 - u^2$ (by the same logic).

Taking the squares of a and b, summing them up and then subtracting c^2 we have

$$\left(2u\,v\right)^2 + \left(v^2 - u^2\right)^2 - \left(u^2 + v^2\right)^2 = 4u^2\,v^2 + \left(v^4 - 2u^2\,v^2 + u^4\right) - \left(u^4 + 2u^2\,v^2 + v^4\right) = 0 \implies a^2 + b^2 = c^2.$$

$\square$

Question 2

If $a^n - 1$ is a prime, show that $a = 2$ and that n is a prime. Primes of the form $2^p - 1$ are called Mersenne primes. For example, $2^3 - 1 = 7$ and $2^5 - 1 = 31$. It is not known if there are infinitely many Mersenne primes.

Solution:

By the factorization

$$a^n - 1 = (a - 1)\sum_{k=0}^{n-1} a^k = p,$$

p must have at least 2 divisors, and if $a \neq 2$ then p isn't prime.

So we have a number of the form $2^n - 1$ which must be prime. Suppose $n = \alpha\,\beta, \alpha, \beta \in \mathbb{N}$ (i.e. n is a composite number), then $2^{\alpha\,\beta} - 1 = p \implies 2 = \sqrt[\alpha]{p+1}\,\sqrt[\beta]{p+1}$ which either (1) implies (without loss of generality) that $\alpha = 1$ and β is a prime number or it implies that (2) the number 2 is composite, which is absurd.

So then we must have $2^n - 1$ with n being a prime number, as we'd like to demonstrate.

Question 3

If $a^n + 1$ is a prime, show that a is even and that n is a power of 2. Primes of the form $2^{2^t} + 1$ are called Fermat primes. For example, $2^{2^1} + 1 = 5$ and $2^{2^2} + 1 = 17$. It is not known if there are infinitely many

Fermat primes.

Solution:

If $a^n + 1$ is a prime then a must be even for if a were any odd number then a^n would also be odd, thus $a^n + 1$ would be even. As $3^1 + 1 = 4 > 2$ is the least value for this expression it couldn't be prime.

So we know that we must have $a = 2m, m \in \mathbb{N}$. Suppose, then, that $n = \alpha\,\beta, \alpha \neq \beta$, thus we'd have the factorization $2m = \sqrt[\alpha]{p-1}\,\sqrt[\beta]{p-1}$ and, without loss of generality, we could set $2 = \sqrt[\alpha]{p-1}$ and $m = \sqrt[\beta]{p-1}$, but then we'd fall in a contradiction, as $(2m)^n = 2^\alpha\, m^\beta$. Thus we conclude that α must equal β.

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$$

Now we know that $n = \gamma^k$, where γ is prime as it cannot have more than two divisors. Suppose that γ is an odd number (any prime > 2). As γ is an odd power we have the expansion

$$a^\gamma + 1 = (a+1)\sum_{k=0}^{\gamma}(-1)^{k+1}a^k$$

which is a contradiction, as $a^\gamma + 1$ should be prime. Thus, γ must be even and, as such, must be 2 (for it must also be prime).

Then we've concluded that $a = 2m$ and $n = 2^t$ so that we have $(2m)^{2^t} + 1 = p$ being a prime number.

Question 4

Prove that $1/2 + 1/3 + \cdots + 1/n$ is not an integer.

Solution:

Assume $1/2 + 1/3 + \cdots + 1/n = a, a \in \mathbb{Z}$.

Adopting the summation notation, we have that

$$\sum_{k=2}^{n}\frac{1}{k} = \sum_{k=2}^{n}\frac{n!/k}{n!}$$

so that for $\sum_{k=2}^{n} 1/k$ to be an integer we must have $n! \mid \sum_{k=2}^{n} n!/k$. By the lemma that every integer a can be written as $qb + r$ we have that

$$\sum_{k=2}^{n}\frac{1}{k} = a = q\,n! + r \implies \sum_{k=2}^{n}\frac{n!}{k} = \sum_{k=2}^{n} a_k - r_k = q\,n!.$$

For $n! \mid \sum_{k=2}^{n} n!/k$ to be true we must have $n! | r$, but as each term $n!/k < n!$, then this residue must be non-zero:

$$\sum_{k=2}^{n} r_k = \sum_{k=2}^{n}(1 - 1/k) = q$$

notice that r_k is simply the opposite of what lacks for $n!/k$ to be divisible by $n!$.[1]

But as we evaluate the sum, we notice that

$$\sum_{k=2}^{n}\left(1 - \frac{1}{k}\right) = \frac{(n+2)(n-1)}{2} - \underbrace{\sum_{k=2}^{n}\frac{1}{k}}_{\text{this should be divisible by } n!}.$$

but as $(n-1)/n! = 1/n(n-2)!$ and $(n+2)/2 < n(n-2)!$ the sum cannot be divisible by $n!$. Contradiction!

Thus $1/2 + 1/3 + \cdots + 1/n$ cannot be an integer, as we'd like to show.

Question 5

If a is a nonzero integer, then for $n > m$ show that $(a^{2^n} + 1, a^{2^m} + 1) = 1$ or 2 depending on whether a is odd or even. (Hint: If p is an odd prime and $p|a^{2^m} + 1$, then $p|a^{2^n} - 1$ for $n > m$.)

Solution:

Question 6

Use the result of Exercise 4 to show that there are infinitely many primes. (This proof is due to G. Polya.)

Solution:

Question 7

For a rational number r let $[r]$ be the largest integer less than or equal to r, e.g., $[1/2] = O$, $[2] = 2$, and $[3 1/3] = 3$. Prove $\text{ord}_p n! = [n/p] + [n/p^2] + [n/p^3] + \cdots$.

Solution:

Question 8

A function on the integers is said to be multiplicative if $f(ab) = f(a)f(b)$ whenever $(a, b) = 1$. Show that a multiplicative function is completely determined by its value on prime powers.

Solution:

Question 9

If $f(n)$ is a multiplicative function, show that the function $g(n) = \sum_{d|n} f(d)$ is also multiplicative.

Solution:

Question 10

Show that $\phi(n) = n \sum_{d|n} \mu(d)/d$ by first proving that $\mu(d)/d$ is multiplicative and then using Exercises 9 and 10.

[1] i.e. $(n!/k)/n! = (n!(1/k + 1 - 1))/n! = 1 - \underbrace{(1 - 1/k)}_{r_k}$.

Solution:

Question 11

Show that

(a) $\sum_{d|n} \mu(n/d)\nu(d) = 1$ for all n.

Solution:

(b) $\sum_{d|n} \mu(n/d)\sigma(d) = n$ for all n.

Solution:

Question 12

Verify the formal identities

(a) $\zeta(s)^{-1} = \sum_{n=1}^{\infty} \mu(n)/n^s$.

Solution:

(b) $\zeta(s)^2 = \sum_{n=1}^{\infty} \nu(n)/n^s$.

Solution:

(c) $\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \sigma(n)/n^s$.

Solution:

Question 13

Show that $\sum' 1/n$, the sum being over square free integers, diverges. Conclude that $\prod_{p<N}(l + 1/p) \to \infty$ as $N \to \infty$. Since $e^x > 1 + x$, conclude that $\sum_{p<N} 1/p \to \infty$. (This proof is due to I. Niven.)

Solution:

Question 14

Mostre que a fração $\dfrac{21n+4}{14n+3}$ é irredutível para todo n natural.

Solution:

Question 15

Demonstre:

(a) se $m|a-b$, então $m|a^k-b^k$ para todo natural k.

Solution:

(b) se $f(x)$ é um polinômio com coeficientes inteiros e a e b são inteiros quaisquer, então $a-b|f(a)-f(b)$.

Solution:

(c) se k é um natural ímpar, então $a+b|a^k+b^k$.

Solution:

Question 16

Demonstrar que $(n-1)^2|n^k-1$ se, e só se, $n-1|k$.

Solution:

Question 17

Seja F_n o n-ésimo termo da sequência de Fibonacci.

(a) Encontrar dois números inteiros a e b tais que $233a+144b=1$ (observe que 233 e 144 são termos consecutivos da sequência de Fibonacci).

Solution:

(b) Mostre que $\mathrm{mdc}(F_n, F_{n+1}) = 1$ para todo $n \geqslant 0$.

Solution:

(c) Determine x_n e y_n tais que $F_n \cdot x_n + F_{n+1} \cdot y_n = 1$.

Solution:

Question 18

Demonstrar que $\mathrm{mdc}(2^a-1, 2^b-1) = 2^{\mathrm{mdc}(a,b)}-1$ para todo $a, b \in \mathbb{N}$.

Solution:

Question 19

Encontrar todas as funções $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ satisfazendo simultaneamente as seguintes propriedades

(i) $f(a, a) = a$.

Solution:

(ii) $f(a, b) = f(b, a)$.

Solution:

(iii) Se $a > b$, então $f(a, b) = \dfrac{a}{a-b} f(a-b, b)$.

Solution:

Question 20

Mostre que se n é um número natural composto, então n é divísivel por um primo p com $p \leqslant \lfloor \sqrt{n} \rfloor$.

Solution: