cse547/ams547 QUIZ 3 SOLUTIONS Spring 2018

QUESTION

Part 1

1. Formulate the **Euclid Algorithm** and the **Euclid Theorem**

For any $a, b \in Z^+$ and $a \geq b$,

Euclid Algorithm

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_2 r_2 + r_3$$
$$\dots \quad \dots \quad \dots$$
$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n + 0$$

Euclid Theorem

$$\text{If} \quad r_{n+1} = 0 \ \text{ then } \ r_n = (a, b) = gcd(a, b)$$

2. Use it to **prove** that for any $a, b, k \in Z$,

$$gcd(ka, kb) = k \cdot gcd(a, b).$$

Proof

$gcd(a, b) = r_n$ in the Euclid Algorithm

$$a = q_1 b + r_1$$
$$\dots \quad \dots$$
$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n + 0$$

We multiply each step by k and get

$$ka = kq_1 b + kr_1$$
$$\dots \quad \dots$$
$$kr_{n-2} = kq_n r_{n-1} + kr_n$$
$$kr_{n-1} = q_{n+1} kr_n + 0$$

This is the Euclid Algorithm for $ka,\ kb$ and hence

$$gcd(ka,kb) = k \cdot r_n = k \cdot gcd(a,b)$$

Part 2 The **Main Factorization Theorem** says: *Every composite number can be factored uniquely into prime factors.*

1. Explain its **General Form** $n = \prod_p p^{n_p}$ for $p \in P,\ n_p \geq 0$.

n_p is the multiplicity of p i.e. the number of times p occurs in the prime factorization. This is an infinite product, bur for any particular $n \in N,\ n > 1$ all but few exponents $n_p = 0$, and $p^0 = 1$. Hence for a given n, it is a finite product.

2. Use it to define a **representation** $n =< n_1,\ n_2, n_3,\ \dots\ n_k, \dots\ >$ of any $n \in N - \{0,1\}$.

We put all prime numbers in P in a 1-1 sequence

$$p_1 < p_2 < \ \dots\ p_n < \ \dots$$

$$2 < 3 < 5 < 7 < 11 < 13 < \ \dots$$

and we write the **General Form** as

$$n = \prod_{i \geq 1} p_i^{n_i} \quad \text{for } n_i \geq 0$$

Because of the uniqueness of the representation we can represent any $n \in N,\ n > 1$ as

$$n =< n_1,\ n_2, n_3,\ \dots\ n_k, \dots\ >$$

3. Find the representations of of $n = 5, 10, 12$

$5 =< 0,0,1,\ 0,\dots\ =< 0,0,1 >$

$10 == 2 \cdot 5 =< 1,0,1 >$

$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$ so $12 =< 2,1,0,0,\dots\ >=< 2,1 >$

EXTRA CREDIT

We proved the Spectrum Partition Theorem for $Spec(\sqrt{2})$ and $Spec(2+\sqrt{2})$.

1. Give 3 examples of $\alpha,\ \beta \in R - Q$ for which the **Spectrum Partition Theorem** also holds.

We also proved the following

General Spectrum Partition Theorem

Let $\alpha > 0,\ \beta > 0,\ \ \alpha,\ \beta \in R-Q$ be such that $\frac{1}{\alpha}+\frac{1}{\beta}=1$. Then the sets $Spec(\alpha)$ and $Spec(\beta)$ form a **partition** of $Z^{+}=N-\{0\}$.

HENCE the Spectrum Partition Theorem holds for any $\alpha > 0,\ \beta > 0,\ \alpha,\ \beta \in R-Q$ such that

$$\frac{1}{\alpha}+\frac{1}{\beta}=1$$

We evaluate

$$\alpha=\frac{\beta}{\beta-1}$$

Examples

E1 Take for example $\beta=\sqrt{3}$, we get $\alpha=\frac{\sqrt{3}}{\sqrt{3}-1}$

E2 Other pairs are, for example

$$\alpha=\pi \ \text{ and } \ \beta=\frac{\pi}{\pi-1}, \qquad \alpha=e^{2}sin32 \ \text{ and } \ \beta=\frac{e^{2}sin32}{e^{2}sin32-1}$$

Observe that for any number $x \in R-Q$ we have that $x-1 \neq 0$ and the number $\frac{x}{x-1} \in R-Q$.

E3 Hence any pair of numbers $x,\ \frac{x}{x-1}$ such that $x \in R-Q$ can serve an **example** of two numbers for which the **Spectrum Partition Theorem** holds, i.e. such that he sets $Spec(x)$ and $Spec(\frac{x}{x-1})$ form a **partition** of $Z^{+}=N-\{0\}$.

Part 3 Prove that there are uncountably many $\alpha,\ \beta \in R-Q$ for which it also holds.

The numbers for which Spectrum Partition Theorem holds must be irrational and must fulfill the condition $\frac{1}{\alpha}+\frac{1}{\beta}=1$. There are uncountably many irrational numbers, and so there are uncountably many pairs: $\beta,\ \frac{\beta}{\beta-1}$.