~~Q A man~~

d. A man has $4.55 in change composed entirely of dimes and quarters. What are the maximum and minimum number of coins that he can have? Is it possible for the number of dimes to equal the number of quarters?

Primes and their distribution.

Definition (1): An integer $p > 1$ is called a prime number, or simply a prime, if its only positive divisors are 1 and p.

An integer greater than 1 that is not a prime is termed composite.

→ Among the first 10 positive integers, 2, 3, 5, 7 are primes and 4, 6, 8, 9, 10 are composite numbers. Note that the integer 2 is the only even prime, and according to the definition (1), the integer 1 plays a special role, being neither prime nor composite.

Note: $3 \mid 36$, and 36 can be written as

$$6 \cdot 6 = 9 \cdot 4 = 12 \cdot 3 = 18 \cdot 2$$

In each case, 3 divides at least one of the factors involved in the product.

Thm (1) If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof:- If $p \mid a$, then proved. So let us assume that $p \nmid a$. Since the only positive divisors of p are 1 and p itself, this implies $\gcd(p, a) = 1$.

Then by Euclid's lemma, we get $p \mid b$.

Corollary 1:- If p is a prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some k, where $1 \le k \le n$.

Proof:- We proceed by induction on n, no. of factors. When $n = 1$, the conclusion holds.

When $n=2$, the result follows from Theorem ①.

Suppose, by the induction hypothesis, that $n>2$ and that whenever p divides a product of less than n factors, it divides at least one of the factors..

Now, $p \mid a_1 a_2 \cdots a_n$, from Theorem ①., either $p \mid a_n$ or $p \mid a_1 a_2 \cdots a_{n-1}$.

If $p \mid a_n$, then we are done.

If $p \mid a_1 a_2 \cdots a_{n-1}$, the induction hypothesis ensures that $p \mid a_k$ for some choice of k, $1 \le k \le n-1$.

Hence p divides one of the integers $a_1, a_2, \ldots, a_n$.

Corollary 2: If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \le k \le n$.

Proof:- Using Corollary ①, we see that $p \mid q_k$, for some k, $1 \le k \le n$.

Being a prime, q_k is not divisible by any positive integer other than 1 or q_k itself.

Since $p > 1$, we are forced to conclude that $p = q_k$.

Theorem ②:- Fundamental Theorem of Arithmetic:

Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique, apart from the order in which the factor occurs.

Proof:- Either n is prime or it is composite; in the former case, there is nothing to prove.

If n is composite, then there exists an integer d satisfying d/n and $1<d<n$.

Among all such integers d, choose p_1 to be the smallest, by Well-Ordering principle.

Then p_1 must be a prime number. Otherwise, it too would have a divisor q with $1<q<p_1$.

Then we get q/p_1 and $p_1/n \Rightarrow q/n$, which contradicts the choice of p_1 as the smallest positive divisor, not equal to 1, of n.

So, we may write $n=p_1n_1$, where p_1 is prime and $1<n_1<n$.

If n_1 happens to be a prime, then we will get the representation.

On the contrary, we get to produce a second prime number p_2 such that $n_1=p_2n_2$; i.e

$$n=p_1p_2n_2 \quad , \quad 1<n_2<n_1$$

If n_2 is a prime, then it is not necessary to go further.

Otherwise, write $n_2=p_3n_3$ with p_3 as prime and

$$n=p_1p_2p_3n_3 \quad , \quad 1<n_3<n_2.$$

The decreasing sequence $n>n_1>n_2>\cdots>1$ cannot continue indefinitely, so that after finite number of steps

n_{k-1} is a prime, call it say p_k:

This leads us to the prime factorization

$$n = p_1 p_2 \cdots p_k .$$

2nd part of the proof :- Uniqueness of prime factorization:

Let us suppose that the integer n can be represented as a product of primes in two ways; say

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad , r \le s . \longrightarrow (1)$$

where the p_i and q_j are all primes, written in increasing magnitude so that

$$p_1 \le p_2 \le p_3 \cdots \le p_r \quad | \quad q_1 \le q_2 \le \cdots \le q_s .$$

Since $p_1 | q_1 q_2 \cdots q_s$, Corollary (2) of Theorem (1) gives $p_1 = q_k$ for some k, but then $p_1 \ge q_1$.

Similar reasoning gives $q_1 \ge p_1$, so we get

$$p_1 = q_1 .$$

So (1) $\Rightarrow$ $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$

Repeat the same process to get $p_2 = q_2$, and, in turn,

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s .$$

Continuing in this manner, and if the inequality $r < s$ holds, we arrive at

$$1 = q_{r+1} q_{r+2} \cdots q_s ;$$

which is not possible since $q_j > 1$. Hence $r = s$ and $p_1 = q_1$, $p_2 = q_2$, $\cdots$, $p_r = q_r$. Proof is complete □.

Note:- Several of the primes that appear in the factorisation of a given positive integer may be repeated, as in the case with $360 = 2.2.2.3.3.5$. By collecting like primes and replacing them by a single factor, we can rephrase Theorem (2) as the following Corollary.

Corollary: Any positive integer $n > 1$ can be written uniquely in a canonical form

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

where for $i = 1, 2, \ldots, r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$.

eg:- $360 = 2^3 \cdot 3^2 \cdot 5$.

$4725 = 3^3 \cdot 5^2 \cdot 7$ & $17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$

Note:- Another way of calculating gcd by prime factorization.

Suppose that $p_1, p_2, \ldots p_n$ are distinct primes that divide either of a or b.

So, $a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$, $b = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n}$

Then $\gcd(a, b) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$, where $m_i = \min(k_i, j_i)$ is the smaller of the two exponents associated with p_i in two representations.

eg:- $a = 4725$ & $b = 17460$:

Then $4725 = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7$, $17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$ & so

$\boxed{\gcd(4725, 17460) = 2^0 \cdot 3^2 \cdot 5 \cdot 7 = 315}$.