Arithmetic Derivative

Author

Novemer 29, 2025

Contents

1 Problem 484

Find the following sum:

$$\sum_{k=2}^{5\cdot 10^{15}} gcd(k, k') \tag{1.1}$$

From the bounds of gcd, our sum has to between $N = 5 \cdot 10^{15}$ and $\frac{N(N+1)}{2}$.

2 Arithmetic Derivative

The arithmetic derivative is defined as follows:

$$\begin{aligned} p' &= 1 \text{ for any prime p} \\ (ab)' &= a'b + ab' \end{aligned} \tag{2.1}$$

2.1 Arithmetic Derivative of 1

The derivative of one can be found by looking at the base case of p', take the following $(1 \cdot p)' = 1' \cdot p + p' \cdot 1 = 1$, $(1')$ must be 0.

2.2 Arithmetic Derivative of Powers of p

$$(p^n)' = np^{n-1} \tag{2.2}$$

To prove this take the base case to be $p' = 1$, and assume formula above. Now using proof by induction, show that p^{n+1} has the same form.

$$\begin{aligned} (p^{n+1})' &= (pp^n)' \\ &= p'p^n + p(p^n)' \\ &= p^n + npp^{n-1} \\ &= (n+1)p^{n+1} \end{aligned} \tag{2.3}$$

2.3 Arithmetic Derivative of a Natural Number

Let $k \in \mathbb{N}$ have a prime factorization $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where p_i is some prime and $\alpha_i \in \mathbb{N}$ is its corresponding power.

$$k' = \sum_{i=1}^{n} \alpha_i \frac{k}{p_i} \tag{2.4}$$

To prove this take the base case $(p_i^{\alpha_i})' = \alpha_i p_i^{\alpha_i - 1}$, and assume the formula above. Now using proof by induction, show that $L' = (kp_{n+1}^{\alpha_{n+1}})'$ has the same form.

$$\begin{aligned} (kp_{n+1}^{\alpha_{n+1}})' &= (p_{n+1}^{\alpha_{n+1}})'k + p_{n+1}^{\alpha_{n+1}}k' \\ &= \alpha_{n+1}p_{n+1}^{\alpha_{n+1}-1}k + p_{n+1}^{\alpha_{n+1}} \sum_{i=1}^{n} \alpha_i \frac{k}{p_i} \\ &= \alpha_{n+1}\frac{L}{p_{n+1}} + \sum_{i=1}^{n} \alpha_i \frac{L}{p_i} \\ &= \sum_{i=1}^{n+1} \alpha_i \frac{kp_{n+1}^{\alpha_{n+1}}}{p_i} \end{aligned} \tag{2.5}$$

It can be seen that k' has a factor of $p_1^{\alpha_1-1}\cdots p_n^{\alpha_n-1}$ in each part of its sum.

$$k' = p_1^{\alpha_1-1}\cdots p_n^{\alpha_n-1}\sum_{i=1}^{n}\alpha_i\frac{p_1\cdots p_n}{p_i} \tag{2.6}$$

2.4 The GCD of k and its Arithmetic Derivative

Using the closed form formula for k' we can say that the $p_1^{\alpha_1-1}\cdots p_n^{\alpha_n-1} \leq g\mathit{cd}(k,k')$. To remove the inequality, $\sum_{i=1}^{n}\alpha_i\frac{p_1\cdots p_n}{p_i}$ needs to be analyzed. If the sum has a factor of p_i then we can update $p_i^{\alpha_i-1}$ to $p_i^{\alpha_i}$ in our $g\mathit{cd}(k,k')$ calculation. So when does $p_i \mid \sum_{i=1}^{n}\alpha_i\frac{p_1\cdots p_n}{p_i}$, for all the terms $j \neq i$ there is exactly one p_i in them. Then when would $p_i|\alpha_i\frac{p_1\cdots p_n}{p_i}$? There will be at least one factor of p_i when $p_i \mid \alpha_i$. So when $\alpha_i = p_i * j \ \forall j \in \mathbb{N}$ we get an extra factor of p_i in our $g\mathit{cd}(k,k')$. We will introduce a new function $g(k) = \gcd(k,k')$ to help with readability.

$$g(k) = \gcd(k,k') = \prod_{i=1}^{n}\begin{cases} p_i^{\alpha_i-1}, & \text{if } p_i \nmid \alpha_i \\ p_i^{\alpha_i}, & \text{if } p_i \mid \alpha_i \end{cases} \tag{2.7}$$

3 Properties of g(k)

The function $g(k)$ is a multiplicative function when partitioned by the $p_i^{\alpha_i}$.

$$g(p_1^{\alpha_1}\cdots p_n^{\alpha_n}) = g(p_1^{\alpha_1})\cdots g(p_n^{\alpha_n}) \tag{3.1}$$

The $\sum g(k)$ can be factored if all the arguments share the same factor of p_i and α_i

$$\begin{aligned} &g(p_1^{\alpha_1}\cdots p_n^{\alpha_n}\cdot q_1^{\beta_1}\cdots q_m^{\beta_m}) + g(p_1^{\alpha_1}\cdots p_n^{\alpha_n}\cdot r_1^{\gamma_1}\cdots r_o^{\gamma_o}) \\ &= g(p_1^{\alpha_1}\cdots p_n^{\alpha_n})[g(q_1^{\beta_1}\cdots q_m^{\beta_m}) + g(r_1^{\gamma_1}\cdots r_o^{\gamma_o})] \end{aligned} \tag{3.2}$$

4 Creating Group G(p)

To find $\sum g(k)$ we need k's prime factorization which is expensive. So we can try to build all the k's using the primes which removes the need for prime factorization.

4.1 Brute Force

The brute force method of solving our sum would require calculating the prime factorization of each k.

$$O(\sum g(k)) \propto \sum_{k=1}^{N}\sqrt{k} \approx \int_1^N \sqrt{x}dx \approx \frac{2}{3}N^{\frac{3}{2}} \tag{4.1}$$

So we must find a procedure that has a significantly lower time complexity. So we must calculate $g(k)$ in terms of some other $g(l)$ which saves the number of computations needed.

4.2 Motivation

If we have computed $g(p_1^{\alpha_1}\cdots p_n^{\alpha_n})$ then $g(q^{\alpha}\cdot p_1^{\alpha_1}\cdots p_n^{\alpha_n}) = g(q^{\alpha})g(p_1^{\alpha_1}\cdots p_n^{\alpha_n})$. So create groups G such that we can calculate all the numbers k that have a factor of q^{α}.

4.3 Building Group G(p)

Let $p^{\alpha_n} \mid k \in G(p)$. Now, does $G(p_i) \cap G(p_j) = \emptyset$ when $i \neq j$? No. There needs to be one more condition. We will require that $q \nmid k \in G(p)$ where $q < p$.

$$G(p) = \{k \quad | \quad p^{\alpha} \mid k \wedge q \nmid k \wedge 1 < k \leq N \quad q < p, \alpha \in \mathbb{N}\} \tag{4.2}$$

The union of all our groups $G(p)$ is all the values of k we need for $\sum g(k)$.

$$\sum g(k) = \sum_{p_i} \sum_{k \in G(p_i)} g(k) \tag{4.3}$$

Why is $G(p)$ useful? There are $G(p) = \{p\}$; the p's that have this property conform to the following:

$$G(p) = \{p\} \quad \text{iff} \quad p^2 \nleq N \tag{4.4}$$

The smallest element in $G(p)$ is p, the second smallest is p^2 since $p^2 < p \cdot p_{+1}$ where p_{+1} is the prime immediately after p. For our N we get $P^* = 70,710,707$.

$$\begin{aligned} \sum_{p=P^*}^{\pi(N)} G(p) &= \pi(N) - \pi(P^*) + 1 \\ &\approx \frac{N}{\log N} - \frac{P^*}{\log P^*} + 1 \\ &\approx 138,319,418,975,671 - 3,912,265 + 1 \\ &\approx 138,319,415,063,407 \end{aligned} \tag{4.5}$$

Since $\pi({}^1P^*) \approx 3,912,265$ ...?. However, there is a $G(p) = \{p, p^2\}$ (show that there is only one p that allows for this).

$$\begin{aligned} G(p) = \{p, p^2\} \quad \text{iff} \quad p \cdot p_{+1} \nleq N \\ p = {}^1P^* = 70,710,677 \\ \sum_{k \in G({}^1P^*)} g(k) = 1 + p \end{aligned} \tag{4.6}$$

4.4 Categorizing G(p) into 13 Meta-Groups

A meta group of n is a group of $G(p)$ such that $\mu(G(p)) = n$. The measure $\mu(G)$ measures the most amount of primes a value in G has. For example, $\mu(p) = 1$, $\mu(2 \cdot 3) = 2$, $\mu(2^2 \cdot 3 \cdot 5 \cdot 7) = 4$, etc... So for the $G(2)$ the product of the first 13 primes is less then N, which is also the most amount of primes in a number in G, hence $\mu(G(2)) = 13$.

$$\mu(G(p)) = \underset{k \in G(p)}{\text{argmax}} \quad \mu(k) \tag{4.7}$$

For the problem at hand we can precompute when our measure changes; see table below. The constant's ${}^nP^*$ convey that all primes below it have a measure of at least n. The can be formalized by $n < \mu(G(p))$ for $\forall p < {}^nP^*$. Combining all the relations one can derive the closed form solution to $\mu(G(p))$. The difficulty of computing the sum $\sum_{k \in G(p)} g(k)$ is related to the measure $\mu(G(p))$.

$$\begin{aligned} \mu(G(p)) = 13 \qquad &\text{iff} \quad p = 2 \\ \mu(G(p)) = n \qquad &\text{iff} \quad {}^{n-1}P^* < p \leq {}^nP^* \\ \mu(G(p)) = 1 \qquad &\text{iff} \quad {}^1P^* \leq p \end{aligned} \tag{4.8}$$

μ	${}^{n}P^{*}$
13	${}^{13}P^{*}$=2
12	${}^{12}P^{*}$=5
11	${}^{11}P^{*}$=11
10	${}^{10}P^{*}$=19
9	${}^{9}P^{*}$=37
8	${}^{8}P^{*}$=73
7	${}^{7}P^{*}$=157
6	${}^{6}P^{*}$=397
5	${}^{5}P^{*}$=1,361
4	${}^{4}P^{*}$=8,387
3	${}^{3}P^{*}$=170,957
2	${}^{2}P^{*}$=70,710,649
1	${}^{1}P^{*}$=70,710,677

5 Calculating Prime Counting Function

In the building of $G(p)$, it was shown that having $\pi(N)$ will be use full. After quick search the fastest algorithm to find the prime counting is given by M. Deleglise and J. Rivat 1996 paper.

$$\pi(N = 5 \cdot 10^{15}) = 142,377,417,196,364 \tag{5.1}$$

The ϕ function used in the paper can be used to define $G(p)$, which gives confidence that the grouping method might be on the right path.

$$\phi(p, x) = \{k \leq x; q \mid k \to q > p\} \tag{5.2}$$

$$G(p) = \bigcup_{\alpha=0}^{\lfloor log_p N \rfloor} p^{\alpha} \cdot \phi(p_+, \frac{N}{p^{\alpha}}) \tag{5.3}$$

$$\phi(p, x) = \bigcup_{\alpha=0}^{\lfloor log_{p_+} x \rfloor} p_+^{\alpha} \cdot \phi(p_+, \frac{x}{p_+^{\alpha}}) \tag{5.4}$$

6 Square Free Numbers

A square free number is a number that has at most one factor of each prime. We will define a set Q which will contain all the numbers less than x, such that the lost prime factor is greater than p and the number is square free also.

$$Q(p, x) = \{k \leq x, q \mid k \to q > p \wedge q^2 \nmid k\} \tag{6.1}$$

6.1 g(k) equivalency set using Q(p, x)

The $g(k) = 1$ iff k is a square free number. So if we are given a number of the form $p^a q^b$ where the exponents are are at least 2. The we get $g(p^a q^b) = p^{a-1} q^{b-1}$ all the numbers which we can produce the same value after apply g are just the product above time any square free number such that is doesn't share a common factor with p or q.

7 building G(p) from largest prime down to 2

For notation the subscript of prime p indicates which prime number it is. For example p_{10} is the 10 th prime number, and p_+ is the next prime after p. From the equivalency notion we care about prime numbers that have at least a power of 2.

$$p_{\pi(\sqrt{N})} = 70,710,649 \tag{7.1}$$

So all primes that are greater than $p_{\pi(\sqrt{N})}$ wont be part of our desired sum but those prime can be used as a square free number when building equivalency set under g. Lets now take a $G(p)$ that has a measure $\mu = 2$ then a subset of such group is $\{p, p^2\}$. Take the number that can be formed with p the trivial form is p time all elements of $Q(p, \frac{N}{p})$. Or we could have prime greater than p which has a power of 2, this allows for primes q in the range $[p+1, \sqrt{\frac{N}{p}}]$. The algorithm would be to select a q in the range and then fill in the product with square free numbers, and repeat the range construction for higher powers of q and then select a next prime if there exist primes in the range. The range decreases quite fast. Find the largest prime such that there cannot be q with a power higher that one. To do this we the range to be degenerate in the sense that it contains no numbers or no primes, to have no numbers will be an easier condition to test for. $p < q$ then $p^2 < q^2$. The the largest q we can have in the product $pq^2 \leq N$ is $q = p_{\pi(\sqrt{\frac{N}{p}})}$. Since we have solved for $\mu(G(p)) = 2$ and $\mu(G(p)) = 1$, lets move on to $\mu(G(p)) = 3$ the first prime to consider is ${}^3P^* = 170,957$ which gives a range of prime q that is grater and has at least a power of 2 to be $[p+1, \sqrt{\frac{N}{170,957}}] = [70,957 + 1, 265,452]$ which has 16239 primes.

8