

1.2. Prime Numbers.

Definition 1.6. A number $p > 1$ is called a prime if it has no proper divisors (i.e., there does not exist d , $1 < d < p$ such that $d|p$.)

Theorem 1.11. *Every integer $n > 1$ can be expressed as a product of a finite number of primes. (That number can be 1.)*

Proof. If n is a prime, we are done. If n is not a prime, then $\exists d_1, d_2$ such that $a < d_1, d_2 < n$ and $d_1 d_2 = n$. If d_1 is a prime, study d_2 ; otherwise factor further. Do same for d_1 . Since a proper divisor of a number is smaller than the number, after a finite repetitions of above, we would get a process held, and the divisors are all primes. \square

“Canonical Factorization” $360 = 2^3 \cdot 3^2 \cdot 5$; This factorization is unique in \mathbb{Z} . But in algebraic number theory, unique factorization can fail.

Example 1.10. $10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$.

Theorem 1.12. *If p is a prime and $p | ab$, then $p | a$, or $p | b$. If $p | a_1 a_2 \cdots a_n$, then $p | a_i$ for some i (i.e. $p | a_1$ or $p | a_2$ or \cdots or $p | a_n$).*

Proof. Write $ab = pk$. If $p | a$, done. If $p \nmid a$, then since $(p, a) = 1$, there exist numbers x , and y such that $ax + py = 1$. Thus, $b = abx + pby = p(kx + by)$, and therefore, $p | b$. The general case is proved using induction: $n = 2$ case has been treated. Suppose the proposition holds for all $n < m$. We show that $p | a_1 a_2 \cdots a_m$ implies $p |$ some a_i . Write $a_1 a_2 \cdots a_m = (a_1 \cdots a_{m-1})a_m = ab$, say. By first part, $p | a$ or $p | b$. If $p | a_m$, we are done. Otherwise $p | a_1 \cdots a_{m-1}$. By induction hypothesis, $p | a_i$, for some $1 \leq i \leq m - 1$. \square

Theorem 1.13. (Fundamental Theorem of Arithmetic)

Factorization of any integer > 1 in primes is unique up to ordering of factors.

Proof. Suppose not. Say n had two factorizations

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t,$$

p_i, q_j are primes. Divide out any common primes that occur on both sides, so no p is a q and no q is a p . Now, $p_1 | q_1 q_2 \cdots q_t$, and so $p_1 | q_i$ for some i . Then $p_1 = q_i$, and this is a contradiction. \square

We write

$$n = \prod_p p^{\alpha(p)}, \quad \alpha = \begin{cases} 0, & \text{if } p \nmid n \\ \text{exponent of } p \text{ in factorization of } n, & \text{if } p \mid n \end{cases}$$

Example: $12 = 2^2 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \dots$

Write $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$. Then the gcd representation by prime factorization is

$$(a, b) = \prod_p p^{\min(\alpha(p), \beta(p))},$$

and the lcm representation is

$$[a, b] = \prod_p p^{\max(\alpha(p), \beta(p))}.$$

From this it is easy to show

$$a, b = |ab|.$$

We say (and write) $a = \square$ if $a = n^2$ for some n .

Example: $36 = 6^2$ is a \square . $a = \square \Leftrightarrow a = \prod_p p^{\alpha(p)}$ with all $\alpha(p)$ even.

Theorem 1.14. (Euclid) *There exist infinite number of primes.*

Proof. (Sketch) Suppose we have p_1, p_2, \dots, p_N known to be primes. Then we form $p_1 p_2 \cdots p_N + 1$. This gives rise to a new prime. \square

Proposition 1.2. *There exist arbitrarily large gaps between some consecutive primes.*

Proof. (1) From numbers

$$k! + 2, k! + 3, k! + 4, \dots, k! + k.$$

These $k - 1$ successive numbers are all composite. k can be chose arbitrarily large as we wish.

(2) Use the fact (equivalent to the Prime Number Theorem) that the N th prime p_N divided by $N \log N$ asymptotically approaches 1 as $N \rightarrow \infty$. Denote $d_n = p_n - p_{n-1}$, the distance between two consecutive primes (or size of the

gap). We have

$$\begin{aligned} p_N - 2 &= (p_N - p_{N-1}) + (p_{N-1} - p_{N-2}) + \cdots + (3 - 2) \\ &= d_N + d_{N-1} + \cdots + d_2 \\ &= \sum_{j=2}^N d_j \leq \left(\max_{2 \leq j \leq N} d_j \right) (N - 1). \end{aligned}$$

Now, $p_N - 2 \approx N \log N$, for sufficiently large N , and

$$N \log N \lesssim N \left(\max_{2 \leq j \leq N} d_j \right).$$

Therefore, we have

$$\max_{2 \leq j \leq N} d_j \geq \log N.$$

□

Theorem 1.15. *For all $y \geq 2$,*

$$\sum_{p \leq y} \frac{1}{p} > \log \log y - 1.$$

Proof. Consider the product $\prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1}$. We have

$$\left(1 - \frac{1}{p}\right)^{-1} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots,$$

a geometric series. Therefore,

$$\begin{aligned} \prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1} &= \prod_{p \leq y} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\ &= \sum_{n \in \mathcal{N}_y} \frac{1}{n} > \sum_{n \leq y} \frac{1}{n} > \log y, \end{aligned}$$

where $n \in \mathcal{N}_y$ if $n = 1$ or $(p \mid n \Rightarrow p \leq y)$. n 's occur only once in the summation due to unique factorization. The last inequality comes from

$$\sum_{n \leq y} \frac{1}{n} > \int_1^y \frac{1}{t} dt = \log y. \quad (\text{Integral Test})$$

Now, we consider the expansion

$$\begin{aligned}
 \log(1 - \epsilon) &= -\epsilon - \frac{\epsilon^2}{2} - \frac{\epsilon^3}{3} - \frac{\epsilon^4}{4} - \dots \\
 &= -\epsilon - \frac{\epsilon^2}{2} \left(1 + \frac{2\epsilon}{3} + \frac{2\epsilon^2}{4} + \frac{2\epsilon^3}{5} + \dots \right) \\
 &\geq -\epsilon - \frac{\epsilon^2}{2} (1 + \epsilon + \epsilon^2 + \epsilon^3 + \dots) \\
 &= -\epsilon - \frac{\epsilon^2}{2} (1 - \epsilon)^{-1} \geq -\epsilon - \frac{\epsilon^2}{2} \left(1 - \frac{1}{2} \right)^{-1} \\
 &= -\epsilon - \epsilon^2
 \end{aligned}$$

for ϵ is positive and sufficiently small (say, $< 1/2$) . So

$$\begin{aligned}
 \log \left[\prod_{p \leq y} \left(1 - \frac{1}{p} \right)^{-1} \right] &= (-1) \sum_{p \leq y} \log \left(1 - \frac{1}{p} \right) < \sum_{p \leq y} \frac{1}{p} + \sum_{p \leq y} \frac{1}{p^2} \\
 &\leq \sum_{p \leq y} \frac{1}{p} + 1,
 \end{aligned}$$

where we deduce the last inequality by

$$\sum_{p \leq y} \frac{1}{p^2} \leq \sum_{n=2}^{\infty} \frac{1}{n^2} < 1.$$

Thus, we arrive at

$$\sum_{p \leq y} \frac{1}{p} > \log \log y - 1.$$

□

We now can see Euclid's theorem as a corollary to this: the infinite series $\sum_{p \leq y} \frac{1}{p}$ diverges since $\log \log y$ is an increasing function of y .