October 16, 2018 8:30 AM

Theorem: (Euclid's Lemma) p: a prime

If $p \mid ab$ then $p \mid a$ or $p \mid b$

Consequences:

- If $p \mid a_1 \cdots a_n$ then $p \mid a_j$ for some j
- $\sqrt{p}$ is irrational
- Fundamental Theorem of Arithmetic

proof

By hypothesis, $p \mid ab$. Assume $p \nmid b$; need to show $p \mid a$.

Consider $S = \{k \in \mathbb{N} : k \geq 1 \text{ and } p \mid kb\}$ ($a \in S$, $b \in S$)

Take k_0 = smallest element of S ($k_0 \neq 1$)

claim: k_0 divides every element of S

$\therefore$ then $k_0 \mid p$, $k_0 \neq 1 \Rightarrow k_0 = p \nmid pa$, $k_0 \mid a$ ∎

proof of claim: Let $k \in S$, so $p \mid kb$

Want to show $k_0 \mid k$. Write

$k = k_0 q + r$ where $0 \leq r < k$ (division with remainder)

(Show $r = 0$, so that means $k_0 \mid k$).

$pkb = (k_0 q + r)b = k_0 bq + rb$ (subtract) $\Rightarrow p \mid rb$

also $p \mid k_0 b \Rightarrow p \mid k_0 bq$

* $r \geq 1$, then $r \in S$, contradicting the choice of k_0. So $r_0 = 0$

$\Rightarrow k_0 \mid k$ ∎

Fundamental Theorem of Arithmetic

Every positive integer ≥ 2 is a product of primes. Furthermore, the prime factorization is unique up to reordering.

Ex $240 = 2 \cdot 120 = 2 \cdot 2 \cdot 60 = 2^3 \cdot 30 = 2^4 \cdot 15 = 2^4 \cdot 3 \cdot 5$

$1089 = 11 \cdot 9 \cdot 11 = 3^2 \cdot 11^2$

In general, $n = \underbrace{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$ the prime factorization of n $\quad \begin{cases} p_1 < p_2 < \cdots < p_k \\ \alpha_1, \ldots, \alpha_k \geq 1 \end{cases}$

algorithm: given n, find a prime $g_1 \mid n$.

Write $n = g_1 \cdot n_1$ $\quad n > n_1 > n_2 > \ldots$

If $n_1 = 1$, done.

If $n_1 \geq 2$, repeat

Stops in finitely many steps $(\leq \log_2 n)$

proof

"existence" "uniqueness"

$P(n)$: $n \geq 2$ admits a prime factorization, unique up to reordering.

proof by strong induction:

$P(2)$: $n = 2$ is a prime factorization.

Therefore assume $P(k)$ true for $2 \leq k < n$, Want $P(n)$.

(existence) Let p: prime divisor of n.

If $n = p$, then we are done.

Else i.e. $n \neq p$, write: $\frac{n}{p}$ integer, since $p \mid n$

$n = p \cdot \frac{n}{p}$ where $2 \leq \frac{n}{p} < n$

by induction hypothesis, $\frac{n}{p} = p_1 p_2 \cdots p_k$ (p_i primes)

then $n = p p_1 p_2 \cdots p_k$ (factorization into primes).

(uniqueness) Let $n = p_1 \cdots p_k = q_1 \cdots q_\ell$ prime factorizations.

Claim: $q_1 \cdots q_\ell$ is a reordering of $p_1 \cdots p_k$. (in particular, $k = \ell$)

As $p_1 \mid n = q_1 \cdots q_\ell$, by Euclids lemma:

$p_1 \mid q_j$ for some $j = 1, \ldots, \ell$. Up to reordering/relabeling, may assume $p_1 \mid q_1$.

So $p_1 = q_1$ (divisibility of a prime). If $n = p_1 = q_1$, done. (q_1 is a prime)

Else, if $n > p_1 = q_1$ then $\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_\ell$

Then, as $2 \leq \frac{n}{p} < n$, so induction hypothesis applies.

So $q_2, \ldots, q_\ell$ is a reordering of $p_2, \ldots, p_k$.

$\Rightarrow q_1, q_2, \ldots, q_\ell$ is a reordering of $p_1, p_2, \ldots, p_k$.

Lemma: If p: prime, then $p \mid \binom{p}{k}$ for $k = 1, \dots, p-1$

October 16, 2018 9:33 AM

Application: Counting divisors

Q: How many divisors does 240 have?

$240 = 2^4 \cdot 3 \cdot 5$

Divisors of 240 have the form

$2^a \cdot 3^b \cdot 5^c$ $\begin{cases} 0 \le a \le 4 \\ 0 \le b \le 1 \\ 0 \le c \le 1 \end{cases}$ $5 \times 2 \times 2 = \boxed{20}$

Theorem Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be the prime factorization of $n \ge 2$. Then n has

$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$

divisors.

Proof Exercise.

* n^{10} has 11 divisors.

Fermat's theorem

Let p: prime. Then $p \mid a^p - a$ for every positive integer a.

Q. What is the remainder of 3^{13} upon division by 7?

A: 3

Remark 1: If $p \mid a$, then $p \mid a^p$ and $p \mid a$ both

If $p \nmid a$, then $p \mid a^p - a = a(a^{p-1} - 1)$

$\Rightarrow p \mid a^{p-1} - 1$.

Remark 2: Not true for non-primes

$4 \mid a^4 - a$ for $a = 2$

but: $n \mid a^n - a$ for all a.

↳ Fermat pseudoprimes

(besides primes, there are composite 561)

Remark 3: This is the "Little Fermat Theorem"

The "Big" Fermat Theorem is

For $n > 2$, $a^n + b^n = c^n$ has no positive integer solutions.