ITC8190
Mathematics for Computer Science
Elementary Number Theory

Aleksandr Lenin

October 23rd, 2018

Definition 1 (Divisibility)

Let a and b be integers with $a \neq 0$. We say a divides b, written as $a|b$, if there exists an integer c such that $b = ac$, and we call c the **quotient** of b by a. We say that a is the **divisor** or **factor** of b, and b is a **multiple** of a. If a does not divide b, we write $a \nmid b$.

Definition 2 (Trivial Divisor)

A divisor of n is called a **trivial divisor** if it is either 1 or n itself. Any other divisor d such that $d \neq 1$ and $d \neq n$ is called a **non-trivial divisor** of n.

In example, one can see that $2|6$, but $2 \nmid 7$.

Some observations:

- 0 is divisible by any integer m, since $m \cdot 0 = 0$.
- Both 1 and -1 divide any integer n.
- Any $n \neq 0$ is divided by n and $-n$.
- If $a|b$ then also $a|-b$, $-a|b$ and $-a|-b$.
- If $a|b$ and $a|c$ then $a|(b+c)$.
- If $a|b$ and $a|bc$ for any integer c.
- If $a|b$ and $b|c$ then $a|c$.
- If $a|b$ and $b|a$ then $a = \pm b$.
- If $a|b$ and $a|c$ then for all m, n we have $a|(mb+nc)$.
- If $a|b$ then $|a| \leqslant |b|$.
- Integers 1 and -1 are divisible only by 1 and -1.

Theorem 1 (Division Algorithm)

Let m and n be any positive integers. Then there exist two unique integers q and r, with $q \geqslant 0$ and $0 \leqslant r < m$, such that $n = qm + r$.

Proof.

Let T be the set of positive integers k for which $km > n$. T is not empty, since $n + 1 \in T$. Hence, T contains a least element k_0 such that $k_0 m > n$, but $(k_0 - 1)m \leqslant n$.

Define $q = k_0 - 1$. Then $(q + 1)m > n$ and $qm \leqslant n$. Subtracting qm from both sides of the equations, we get $0 \leqslant n - qm < m$. Define $r = n - qm$ and we are done.

For the proof of uniqueness of q and r see the next slide. $\square$

Theorem 2 (Division Algirthm (contd.))

Integers q and r from Theorem. 1 are unique.

Proof.

Suppose that there is another pair of integers $q' \neq 0$ and r' satisfying the conditions $n = q'm + r'$ with $0 \leqslant r' < m$.
Then we have

$$qm+r = q'm+r' \implies r-r' = (q'-q)m \implies m|(r-r') \ . \ (1)$$

From (1) it can be seen that since $0 \leqslant r - r' < m$, the only case when condition $m|(r - r')$ will not result in a contradiction is $r = r'$, and hence $q = q'$. □

Remark: the uniquely determined numbers q and r are called **quotient** and **remainder**.

Some examples

$$
\begin{aligned}
7 &= 2 \cdot 3 + 1 && n = 7, m = 3, q = 2, r = 1 \ , \\
7 &= 0 \cdot 8 + 7 && n = 7, m = 8, q = 0, r = 7 \ , \\
12 &= 4 \cdot 3 + 0 && n = 12, m = 3, q = 4, r = 0 \ .
\end{aligned}
$$

Before we prove a theorem about p-adic expansion of integers, we need a couple of specific results by the lemmas below.

Lemma 1

Let b, n be any positive integers. Then

$$(1-b)(1+b+b^2+\ldots+b^n) = 1-b^{n+1} \quad .$$

Proof.

$$\begin{aligned}(1-b)(1+b+b^2+\ldots+b^n) &= 1+b+b^2+\ldots+b^n \\ &\quad -b-b^2-b^3-\ldots-b^{n+1} \\ &= 1-b+b-b^2+\ldots+b^n-b^{n+1} \\ &= 1-b^{n+1} \quad .\end{aligned}$$

Lemma 2

Let b be any integer. Then

$$(b-1)(1+b+b^2+\ldots+b^r) < b^{r+1} \quad .$$

Proof.

The assertion follows at once from Lemma 1,

$$(b-1)(1+b+b^2+\ldots+b^n) = b^{n+1}-1 \quad .$$

Hence,

$$(b-1)(1+b+b^2+\ldots+b^n) < b^{n+1} \quad .$$

Lemma 3

If $b > 1$, *then* $b^r > r$ *for* $r \geqslant 0$.

Proof.

Since $1 < b - 1$ by assumption, then for any positive integer c it holds that $c \leqslant (b-1) \cdot c$. Taking $c = 1 + b + b^2 + \ldots + b^r$, by Lemma 2 it holds that

$$1 + b + b^2 + \ldots + b^r \leqslant (b-1)(1 + b + b^2 + \ldots + b^r) < b^{r+1} \quad .$$

Every term on the left is $\geqslant 1$, and there are $r+1$ terms. It follows that

$$(b-1)(1 + b + b^2 + \ldots + b^r) \geqslant r + 1 \quad ,$$

and hence $r + 1 < b^{r+1}$ for $r \geqslant 0$. □

Theorem 3 (b-adic expansion)

Let m be a positive integer, let b be an integer greater than 1. Then there are unique integers $a_0, a_1, a_2, \ldots, a_r$ such that $m = a_0 + a_1 b + a_2 b^2 \ldots + a_r b^r$ and $0 \leqslant a_j \leqslant b - 1$ for $j = 0, \ldots, r$ with $a_r \neq 0$.

Proof.

Applying the division algorithm as shown below, we define two sequences of numbers $q_0, q_1, q_2 \ldots$ and $a_0, a_1, a_2, \ldots$ connected by the equations

$$
\begin{aligned}
m &= q_0 b + a_0 \\
q_0 &= q_1 b + a_1 \\
q_1 &= q_2 b + a_2 \\
&\ldots \\
q_{k-1} &= q_k b + a_k \\
q_k &= q_{k+1} b + a_{k+1} \\
&\ldots
\end{aligned}
$$

If we substitute q_0 into the first equation from the second, we get

$$m = (q_1\, b + a_1)\, b + a_0 = a_0 + a_1\, b + q_1\, b^2 \quad .$$

Substituting q_1 from the third equation we get

$$m = a_0 + a_1\, b + (q_2\, b + a_2)\, b^2 = a_0 + a_1\, b + a_2\, b^2 + q_2\, b^3 \quad .$$

After k such steps we obtain the result

$$m = a_0 + a_1\, b + a_2\, b^2 + a_3\, b^3 + \ldots + a_{k-1}\, b^{k-1} + a_k b^k + q_k b^{k+1} \quad .$$

$$m = a_0 + a_1 b + a_2 b^2 + a_3 b^3 + \ldots + a_{k-1} b^{k-1} + a_k b^k + q_k b^{k+1} \quad . \quad (2)$$

It can be seen that $m \geqslant q_k b^{k+1}$, since all terms on the right are $\geqslant 0$. But $b^{k+1} > k+1$ by Lemma 3. Hence,

$$m \geqslant q_k b^{k+1} > q_k(k+1) \implies m > q_k(k+1) \quad .$$

This shows that $q_k = 0$ for $k > m$. Let q_r be the first quotient which is zero. Then equation (2) takes exactly the form

$$m = a_0 + a_1 b + a_2 b^2 \ldots + a_r b^r \quad . \quad (3)$$

To show uniqueness of (3), suppose that

$$a_0 + a_1 b + a_2 b^2 \ldots + a_r b^r = m = a'_0 + a'_1 b + a'_2 b^2 \ldots + a'_s b^s$$

with $0 \leqslant a'_i < b$ for $i = 1, \ldots, s$. Then clearly a'_0 is the remainder obtained by the division of m by b, and so $a'_0 = a_0$ by the uniqueness of the division algorithm. The quotient $a'_1 + a'_2 b + \ldots + a'_s b^{s-1}$ must be the same as q_0. The remainder upon division by b is a'_1, and it must be the same as the remainder of the division of q_0 by b. That is, $a'_1 = a_1$. Continuing this way, it can be shown that the coefficients of the same powers of b in the two expressions must be equal.

The expression (3) for a positive integer m is called the **b-adic expansion of m**.

It is easy to see that the usual notation for integers is an abbreviated form of 10-adic expansion.

The same number may have b-adic expansions for any $b > 1$.

It is possible to make calculations and express the same numbers in any b-adic expansion.

In example, for $m = 159$ and $b = 10$, applying the division algorithm, we have

$$\begin{aligned} 159 &= 15 \cdot 10 + 9 \\ 15 &= 1 \cdot 10 + 5 \\ 1 &= 0 \cdot 10 + 1 \\ &\dots \end{aligned}$$

All the q-s are 0 beyond q_1. Using (3) with $k = 2$, we obtain 10-adic expansion of 159, namely $159 = 1 \cdot 10^2 + 5 \cdot 10 + 9$.

Let's calculate the 4-adic expansion of 159.

$$\begin{aligned} 159 &= 39 \cdot 4 + 3 \\ 39 &= 9 \cdot 4 + 3 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 0 \cdot 4 + 2 \end{aligned}$$

The 4-adic expansion of 159 is therefore

$$159 = 2 \cdot 4^3 + 1 \cdot 4^2 + 3 \cdot 4 + 3 \ ,$$

or in abbreviated form, 2133. Hence, $159_{10} = 2133_4$.

Let's calculate the 2-adic expansion of 159.

$$
\begin{aligned}
159 &= 79 \cdot 2 + 1 \\
79 &= 39 \cdot 2 + 1 \\
39 &= 19 \cdot 2 + 1 \\
19 &= 9 \cdot 2 + 1 \\
9 &= 4 \cdot 2 + 1 \\
4 &= 2 \cdot 2 + 0 \\
2 &= 1 \cdot 2 + 0 \\
1 &= 0 \cdot 2 + 1
\end{aligned}
$$

The 2-adic expansion of 159 is therefore

$$159 = 2^7 + 2^4 + 2^3 + 2^2 + 2 + 1 \ .$$

Hencem, $159_{10} = 10011111_2$.

It is possible to make calculations and perform arithmetic operations in any b-adic system. For this, one must know the addition and multiplication tables for the "digits" of b-adic system $0, 1, \ldots, b-1$.

I.e., in 5-adic system, we have five digits that we call $0, 1, 2, 3, 4$. The addition and multiplication tables are given below.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

(a) 5-adic addition

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

(b) 5-adic multiplication

An example of 5-adic calculations is given below

$$\begin{array}{r} 4132 \\ +2124 \\ \hline 11311 \end{array} \qquad \begin{array}{r} 143 \\ \times 240 \\ \hline 12320 \\ +34100 \\ \hline 101420 \end{array}$$

Digital computers use 2-adic (binary) system.

Historical evidence shows that ancient Babylonians used 10-adic as well as 60-adic systems, the former for the average citizen.

Definition 3 (Greatest Common Divisor)

If $n_1, n_2, \ldots, n_r$ are integers different from 0, then an integer d is called their greatest common divisor (written $d = \gcd(n_1, n_2, \ldots, n_r)$) if

- $d > 0$
- d divides $n_1, n_2, \ldots, n_r$
- Any integer which divides $n_1, n_2, \ldots, n_r$ also divides d

Proposition 1

The greatest common divisor is unique.

Proof.

Let $d = \gcd(m, n) = d'$. By condition (3) above, $d|d'$ and $d'|d$. Hence, $d = d'$. □

Observe that

$$\begin{aligned}
&\gcd(m,n) > 0 \ , \\
&\gcd(m,n) \leqslant |m| \ , \\
&\gcd(m,n) \leqslant |n| \ , \\
&\gcd(m,n) = \gcd(n,m) = \gcd(-m,n) \\
&\qquad\qquad = \gcd(m,-n) = \gcd(-m,-n) \ .
\end{aligned}$$

Theorem 4

Let a, b, q, r *be integers with* $b > 0$ *and* $0 \leqslant r < b$ *such that* $a = bq + r$. *Then* $\gcd(a, b) = \gcd(b, r)$.

Proof.

Let c be the divisor of a and b. Then $a = \alpha c$ and $b = \beta c$. We have

$$\alpha c = \beta cq + r \implies r = \alpha c - \beta cq = (\alpha - \beta q)c \ ,$$

which implies that c divides r. Hence, every divisor of a and b is also the divisor of b and r. Therefore, $\gcd(a, b) = \gcd(b, r)$.

Let c be the divisor of b and r. Then $b = \alpha c$ and $r = \beta c$. Then

$$a = \alpha c q + \beta c = c(\alpha q + \beta) \ ,$$

which implies c divides a. Hence every common divisor of b and r is also a divisor of a and b. Therefore, $\gcd(b, r) = \gcd(a, b)$. □

The Euclidean algorithm allows to calculate the greatest common divisors of the two integers a and b. Suppose that $b < a$. Apply a series of successful divisions as follows

$$
\begin{aligned}
a &= bq_0 + r_1 && 0 \leqslant r_1 < b \\
b &= r_1 q_1 + r_2 && 0 \leqslant r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 && 0 \leqslant r_3 < r_2 \\
&\dots \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k && 0 \leqslant r_k < r_{k-1} \\
r_{k-1} &= r_k q_k + 0
\end{aligned}
$$

Then $r_k = \gcd(a, b)$.

From the division algorithm we have

$$r_k < r_k - 1 < \ldots < r_2 < r_1 < b \ .$$

The successive remainders decrease steadily, and it follows that this process must lead to a zero remainder after at most b steps.

It can be seen that from the division algorithm, all the remainders r_i are positive, so the condition $r_k = d > 0$ is satisfied.

From the last equation, it can be seen that $r_k | r_{k-1}$. From next-to-last equation, we get $r_{k-1} | r_{k-2}$. Hence, $r_k | r_{k-2}$. Continuing up the list we find that r_k divides b and a. Hence, $d | a$ and $d | b$.

Let c be any common divisor of a and b. Let $a = \alpha c$ and $b = \beta c$. From the equation $a = bq_0 + r_1$, we have

$$\begin{aligned} a = bq_0 + r_1 &\implies \alpha c = \beta c q_0 + r_1 \\ &\implies r_1 = (\alpha - \beta q_0)c \implies c | r_1 \ . \end{aligned}$$

From the second equation $b = r_1 q_1 + r_2$ it follows that $c | r_2$, because c divides both a and b. From the third equation we find that $c | r_3$.

Continuing down the list we conclude that c divides all the r-s, and in particular, r_k. Hence, the third condition of the greatest common divisor is satisfied – any integer dividing a and b also divides r_k. Therefore,

$$r_k = \gcd(a, b) \ .$$

In example, let's find $\gcd(1426, 343)$. It can be seen that

$$\begin{aligned} 1426 &= 4 \cdot 343 + 54 \\ 343 &= 6 \cdot 54 + 19 \\ 54 &= 2 \cdot 19 + 16 \\ 19 &= 1 \cdot 16 + 3 \\ 16 &= 5 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

It can also be seen that

$$\begin{aligned} \gcd(1426, 343) &= \gcd(343, 54) = \gcd(54, 19) \\ &= \gcd(19, 16) = \gcd(16, 3) \\ &= \gcd(3, 1) = \gcd(1, 0) = 1 \ . \end{aligned}$$

Hence, $\gcd(1426, 343) = 1$.

We might call Euclid's method the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day.

Donald E. Knuth
The Art of Computer Programming:
Seminumerical Algorithms

It is evident that the algorithm cannot recur indefinitely, since the second argument strictly decreases in each recursive call. Therefore, the algorithm always terminates with the correct answer.

More importantly, it can perform in polynomial time. If the Euclid's algorithm is applied to a pair of positive integers a, b with $a \geqslant b$, the number of divisions required to find $\gcd(a, b)$ is $\mathcal{O}(\log b)$ – a polynomial time complexity.

In Complexity Theory, the big $\mathcal{O}$ notation is used to express an asymptotic upper bound of a complexity function, i.e.

$$g(n) = \mathcal{O}(f(n)) \iff \exists k > 0 \exists n_0 \forall n > n_0 : g(n) \leqslant k \cdot f(n) \quad .$$

Or in other words,

$$\lim_{n \to \infty} \sup \frac{f(n)}{g(n)} < \infty \quad .$$

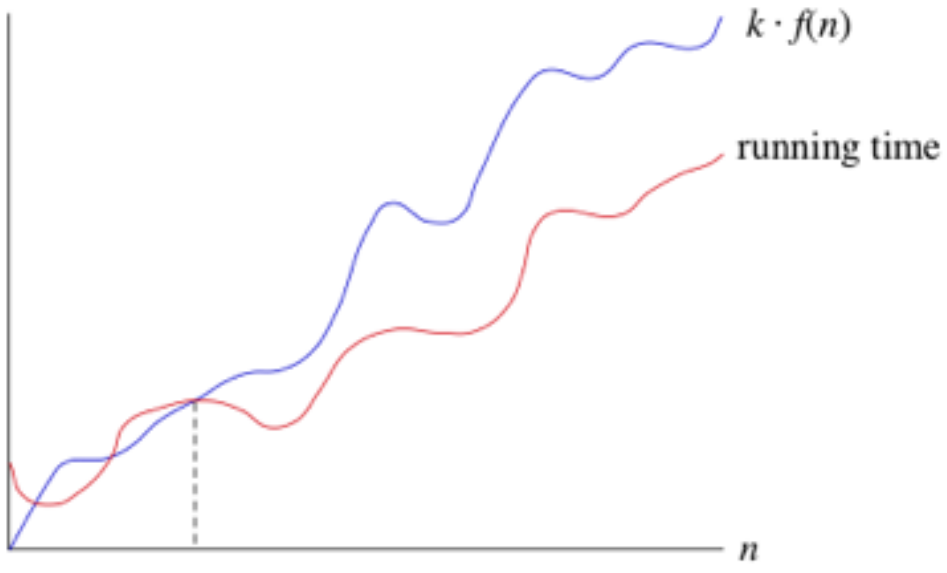

Figure: Running time $g(n)$ is asymptotically bound by $f(n)$ from above.

From the Euclidean algorithm

$$
\begin{aligned}
a &= bq_0 + r_1 & r_1 &= a - bq_0 \\
b &= r_1 q_1 + r_2 & r_{k-1} &= r_2 = b - r_1 q_1 \\
r_1 &= r_2 q_2 + r_3 & r_3 &= r_1 - r_2 q_2 \\
&\dots & &\dots \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k & r_k &= r_{k-2} - r_{k-1} q_{k-1} \\
r_{k-1} &= r_k q_k + 0
\end{aligned}
$$

it follows that the greatest common divisor of a and b – $r_k = \gcd(a, b)$ – is a linear combination of a and b.

The Bézout identity states that

$$\forall a, b > 0 \exists \alpha, \beta \in \mathbb{Z} : \alpha a + \beta b = \gcd(a, b) \ .$$

The coefficients a and b are known as Bézout coefficients, and can be obtained using the extended Euclidean algorithm.

Table: The Extended Euclidean Algorithm

26	9	a	b
8	9	a-2b	b
8	1	a-2b	b-(a-2b)=3b-a
0	1	a-2b-8(3b-a) = 9a-26b	3b-a

It can be seen that $\gcd(26, 9) = 1$, and we get two polynomials

$$9 \cdot 26 + 26 \cdot 9 = 0 \ , \qquad 3 \cdot 9 - 26 = 1 \ .$$

The second one contains our Bźout identity, with $\alpha = -1$ and $\beta = 3$. The Bezout identity is

$$-1 \cdot 26 + 3 \cdot 9 = 1 = \gcd(26, 9) \ .$$

Table: The Extended Euclidean Algorithm

12	8	a	b
4	8	a-b	b
4	0	a-b	b-2(a-b)=3b-2a

Therefore, $\gcd(12, 8) = 4$, and the Bézout identity is

$$1 \cdot 12 - 1 \cdot 8 = 4 = \gcd(12, 8) \ .$$

Definition 4 (Prime Integer)

A positive integer n is called a **prime** if its only divisors are 1 and n itself. A positive integer that has non-trivial divisors is called **composite**.

Definition 5 (Co-prime Integers)

Integers a and b are called co-prime if their only common divisors are 1 and -1.

Definition 6 (Co-prime Integers)

Integers a and b are co-prime if $\gcd(a, b) = 1$.

Proposition 2

Every composite number $m \geqslant 2$ is a product of primes.

Proof.

Let m be the least composite number that is not a product of primes. The existence of such m is guaranteed by the well-ordering principle. Then there exist positive integers $m_1, m_2 < m$ such that $m = m_1 \cdot m_2$. Since m was the least integer that was not a product of primes, any $m' < m$ must be a product of primes. Since $m_1, m_2 < m$, they must be products of primes, and so is m, a contradiction. □

Corollary 1

Every composite integer has a prime factor.

Theorem 5 (Euclid, $\approx$ 2000 B.C.)

There are infinitely many primes.

Proof.

Suppose that $p_1, p_2, \ldots, p_k$ are all the primes. Consider the number $p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$. If it is a prime, then it is a new prime. Otherwise by Proposition 2 it has a prime factor q. If q is one of $p_1, p_2, \ldots, p_k$, then $q | (p_1 \cdot p_2 \cdot \ldots \cdot p_k)$ and $p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$, which means that q must divide the difference of these numbers, namely 1, which is impossible. So q is not one of $p_1, p_2, \ldots, p_k$ and must therefore be a new prime. $\square$

Some other results about primes (without proofs).

Theorem 6

If $n \geqslant 1$, then there exists a prime p such that $n < p \leqslant n! + 1$.

Below is the famous Bertrand–Chebyshev theorem, introduced by Joseph Bertrand in 1845 and proved by Chebyshev in 1850.

Theorem 7 (Bertrand–Chebyshev Theorem)

Given any real number $x \geqslant 1$, there exists a prime number between x and $2x$.

Theorem 8

If $n \geqslant 2$, then there are no primes between $n! + 2$ and $n! + n$.

Theorem 9

If n is a composite, then n has a prime divisor p such that $p \leqslant \sqrt{n}$.

Theorem 9 can be used to find all prime numbers up to a given positive integer x. This procedure is called the *Sieve of Eratosthenes*

Lemma 4

If $\gcd(a, n) = \gcd(b, n) = 1$, *then* $\gcd(ab, n) = 1$.

Proof.

By the Bézout identity,

$$\begin{aligned} \gcd(a, n) = 1 &\implies \exists \alpha, \beta \in \mathbb{Z} : \alpha a + \beta n = 1 \ , \\ \gcd(b, n) = 1 &\implies \exists \gamma, \delta \in \mathbb{Z} : \gamma b + \delta n = 1 \ . \end{aligned}$$

In turn, this implies that

$$\begin{aligned} 1 &= (\alpha a + \beta n)(\gamma b + \delta n) \\ &= \underbrace{(\alpha\gamma)}_{\phi} ab + \underbrace{(\alpha\delta a + \beta\gamma b + \beta\delta n)}_{\psi} \cdot n \\ &= \phi ab + \psi n \implies \gcd(ab, n) = 1 \ . \end{aligned}$$

Theorem 10 (Fundamental Theorem of Arithmetic)

Every positive integer n greater than 1 can be written uniquely as a product of primes

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i} \quad , \tag{4}$$

where $p_1, p_2, \ldots, p_k$ are distinct primes, and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are natural numbers.

The equation (4) is called the **prime power decomposition** of n, or the **standard prime factorization** of n.

Proof.

If n is prime, then it is trivially the product of a single factor. If n is not prime, by Proposition 2, n is a product of primes.

To show uniqueness of a prime factorization, suppose that the theorem is false, and let m be the least number that has two unique prime factorizations.

$$m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad ,$$

where each p_i and each q_j is prime. It can be seen that $p_i \neq q_j$, since otherwise there existed another integer $m' = \frac{m}{p_i}$ that also has two different factorizations, thus contradicting the assumption that m is least such element.

Since p_1 and $q_1 q_2 \cdots q_s$ are all primes, we have

$$\gcd(p_1, q_1) = \gcd(p_1, q_2) = \ldots = \gcd(p_1, q_s) = 1 \ .$$

By Lemma 4, this implies that

$$\gcd(p_1, \underbrace{q_1 q_2 \cdots q_s}_{m}) = \gcd(p_1, m) = 1 \ ,$$

which can never happen, since p_1 is a factor of m, and hence $p_1 | m$, a contradiction. □

THANK YOU FOR YOUR ATTENTION

ANY QUESTIONS?