GREATEST COMMON DIVISOR

DEFINITION:

The greatest common divisor (gcd) of a and b, denoted by (a, b), is the largest common divisor of integers a and b.

THEOREM: If a and b are nonzero integers, then their gcd is a linear combination of a and b, that is there exist integer numbers s and t such that

$$sa + tb = (a, b).$$

Proof: Let d be the least positive integer that is a linear combination of a and b. We write

$$d = sa + tb, \tag{1}$$

where s and t are integers.

We first show that $d \mid a$. By the Division Algorithm we have

$$a = dq + r, \text{ where } 0 \leq r < d.$$

From this and (1) it follows that

$$r = a - dq = a - q(sa + tb) = a - qsa - qtb = (1 - qs)a + (-qt)b.$$

This shows that r is a linear combination of a and b. Since $0 \leq r < d$, and d is the least positive linear combination of a and b, we conclude that $r = 0$, and hence $d \mid a$. In a similar manner, we can show that $d \mid b$.

We have shown that d is a common divisor of a and b. We now show that d is the *greatest common divisor* of a and b. Assume to the contrary that $(a, b) = d'$ and $d' > d$. Since $d' \mid a$, $d' \mid b$, and $d = sa + tb$, it follows that $d' \mid d$, therefore $d' \leq d$. We obtain a contradiction. So, d is the greatest common divisor of a and b and this concludes the proof. ■

EUCLID'S LEMMA

THEOREM (Euclid's Lemma): If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1 a_2 \dots a_n$, then it must divide at least one of the factors a_i.

Proof: Assume that $p \nmid a$. We must show that $p \mid b$. By the theorem above, there are integers s and t with

$$sp + ta = (p, a).$$

Since p is prime and $p \nmid a$, we have $(p, a) = 1$, and so

$$sp + ta = 1.$$

Multiplying both sides by b, we get

$$spb + tab = b. \tag{2}$$

Since $p \mid ab$ and $p \mid spb$, it follows that $p \mid (spb + tab)$. This and (2) give $p \mid b$. This completes the proof of the first part of the theorem. The second part (generalization) easily follows by induction on $n \geq 2$. ■

COROLLARY: If p is a prime and $p \mid a^2$, then $p \mid a$.

Proof: Put $a = b$ in Euclid's Lemma. ■

THEOREM: Let p be a prime. Then $\sqrt{p}$ is irrational.

Proof: Assume to the contrary that $\sqrt{p}$ is rational, that is $\sqrt{p} = \dfrac{a}{b}$, where a and b are integers and $b \neq 0$. Moreover, let a and b have no common divisor > 1. Then

$$p = \frac{a^2}{b^2} \quad \Rightarrow \quad pb^2 = a^2. \tag{3}$$

Since pb^2 is divisible by p, it follows that a^2 is divisible by p. Then a is also divisible by p by the Corollary above. This means that there exists $q \in \mathbb{Z}$ such that $a = pq$. Substituting this into (3), we get $pb^2 = (pq)^2 \Rightarrow b^2 = pq^2$. Since pq^2 is divisible by p, it follows that b^2 is divisible by p. Then b is also divisible by p by the Corollary above. This is a contradiction. ■

FUNDAMENTAL THEOREM OF ARITHMETIC

THEOREM (Fundamental Theorem of Arithmetic): Assume that an integer $a \geq 2$ has factorizations

$$a = p_1 \dots p_m \quad \text{and} \quad a = q_1 \dots q_n,$$

where the p's and q's are primes. Then $n = m$ and the $q's$ may be reindexed so that $q_i = p_i$ for all i.

Proof: We prove by induction on ℓ, the larger of m and n, i. e. $\ell = \max(m, n)$.

Step 1. If $\ell = 1$, then the given equation in $a = p_1 = q_1$, and the result is obvious.

Step 2. Suppose the theorem holds for some $\ell = k \geq 1$.

Step 3. We prove it for $\ell = k + 1$. Let

$$a = p_1 \dots p_m = q_1 \dots q_n, \tag{4}$$

where

$$\max(m, n) = k + 1. \tag{5}$$

From (4) it follows that $p_m \mid q_1 \dots q_n$, therefore by Euclid's Lemma there is some q_i such that $p_m \mid q_i$. But q_i, being a prime, has no positive divisors other than 1, therefore $p_m = q_i$. Reindexing, we may assume that $q_n = p_m$. Canceling, we have $p_1 \dots p_{m-1} = q_1 \dots q_{n-1}$. Moreover, $\max(m-1, n-1) = k$ by (5). Therefore by step 2 q's may be reindexed so that $q_i = p_i$ for all i; plus, $m - 1 = n - 1$, hence $m = n$. ■

COROLLARY: If $a \geq 2$ is an integer, then there are unique distinct primes p_i and unique integers $e_i > 0$ such that

$$a = p_1^{e_1} \dots p_n^{e_n}.$$

Proof: Just collect like terms in a prime factorization. ■

EXAMPLE: $120 = 2^3 \cdot 3 \cdot 5$.

PROBLEM: Prove that $\log_3 5$ is irrational.

EUCLIDEAN ALGORITHM

THEOREM (Euclidean Algorithm): Let a and b be positive integers. Then there is an algorithm that finds (a, b).

LEMMA: If a, b, q, r are integers and $a = bq + r$, then $(a, b) = (b, r)$.

Proof: We have $(a, b) = (bq + r, b) = (b, r)$. ■

Proof of the Theorem: The idea is to keep repeating the division algorithm. We have:

$$\begin{aligned}
a &= bq_1 + r_1, \quad (a, b) = (b, r_1) \\
b &= r_1q_2 + r_2, \quad (b, r_1) = (r_1, r_2) \\
r_1 &= r_2q_3 + r_3, \quad (r_1, r_2) = (r_2, r_3) \\
r_2 &= r_3q_4 + r_4, \quad (r_2, r_3) = (r_3, r_4) \\
&\dots \\
r_{n-2} &= r_{n-1}q_n + r_n, \quad (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) \\
r_{n-1} &= r_nq_{n+1}, \quad (r_{n-1}, r_n) = r_n,
\end{aligned}$$

therefore

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = (r_3, r_4) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n.$$

■

EXAMPLE: Find $(252, 198)$. By the Euclidean Algorithm we have

$$\begin{aligned}
252 &= 198 \cdot 1 + 54 \\
198 &= 54 \cdot 3 + 36 \\
54 &= 36 \cdot 1 + 18 \\
36 &= 18 \cdot 2
\end{aligned}$$

therefore

$$(252, 198) = 18.$$

PROBLEM: Find $(35, 55)$ and $(326, 78)$.

THEOREM: Let $a = p_1^{e_1} \dots p_n^{e_n}$ and $b = p_1^{f_1} \dots p_n^{f_n}$ be positive integers. Then

$$(a, b) = p_1^{\min(e_1, f_1)} \dots p_n^{\min(e_n, f_n)}.$$

EXAMPLE: Since $720 = 2^4 \cdot 3^2 \cdot 5$ and $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$, we have:

$$(720, 2100) = 2^2 \cdot 3 \cdot 5 = 60.$$

Let d be the least positive integer that is a linear combination of a and b. We write

$$d = sa + tb, \qquad (*)$$

where s and t are integers.

We first show that $d \mid a$. By the Division Algorithm we have

$$a = dq + r, \text{ where } 0 \leq r < d.$$

From this and $(*)$ it follows that

$$\begin{aligned} r = a - dq &= a - q(sa + tb) \\ &= a - qsa - qtb \\ &= (1 - qs)a + (-qt)b. \end{aligned}$$

This shows that r is a linear combination of a and b. Since $0 \leq r < d$, and d is the least positive linear combination of a and b, we conclude that $r = 0$, and hence $d \mid a$. In a similar manner, we can show that $d \mid b$.

We have shown that d is a common divisor of a and b. We now show that d is the *greatest common divisor* of a and b. Assume to the contrary that $(a, b) = d'$ and $d' > d$. Since $d' \mid a$, $d' \mid b$, and

$$d = sa + tb,$$

it follows that $d' \mid d$, therefore $d' \leq d$. We obtain a contradiction. So, d is the greatest common divisor of a and b and this concludes the proof. ■

THEOREM (Euclid's Lemma): If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1 a_2 \ldots a_n$, then it must divide at least one of the factors a_i.

Proof: Assume that $p \nmid a$. We must show that $p \mid b$. By the theorem above, there are integers s and t with

$$sp + ta = (p, a).$$

Since p is prime and $p \nmid a$, we have $(p, a) = 1$, and so

$$sp + ta = 1.$$

Multiplying both sides by b, we get

$$spb + tab = b. \qquad (*)$$

Since $p \mid ab$ and $p \mid spb$, it follows that $p \mid (spb + tab)$. This and $(*)$ give $p \mid b$. This completes the proof of the first part of the theorem. The second part (generalization) easily follows by induction on $n \geq 2$. ■

THEOREM: Let p be a prime. Then $\sqrt{p}$ is irrational.

Proof: Assume to the contrary that $\sqrt{p}$ is rational, that is $\sqrt{p} = \frac{a}{b}$, where a and b are integers and $b \neq 0$. Moreover, let a and b have no common divisor > 1. Then

$$p = \frac{a^2}{b^2} \quad \Rightarrow \quad pb^2 = a^2. \qquad (*)$$

Since pb^2 is divisible by p, it follows that a^2 is divisible by p. Then a is also divisible by p by the Corollary. This means that there exists $q \in Z$ such that $a = pq$. Substituting this into $(*)$, we get

$$pb^2 = (pq)^2 \;\Rightarrow\; b^2 = pq^2.$$

Since pq^2 is divisible by p, it follows that b^2 is divisible by p. Then b is also divisible by p by the Corollary. This is a contradiction. ■

Step 1. If $\ell = 1$, then the given equation in $a = p_1 = q_1$, and the result is obvious.

Step 2. Suppose the theorem holds for some $\ell = k \geq 1$.

Step 3. We prove it for $\ell = k + 1$. Let

$$a = p_1 \dots p_m = q_1 \dots q_n, \qquad (*)$$

where

$$\max(m, n) = k + 1. \qquad (**)$$

From $(*)$ it follows that $p_m \mid q_1 \dots q_n$, therefore by Euclid's Lemma there is some q_i such that $p_m \mid q_i$. But q_i, being a prime, has no positive divisors other than 1, therefore $p_m = q_i$. Reindexing, we may assume that $q_n = p_m$. Canceling, we have $p_1 \dots p_{m-1} = q_1 \dots q_{n-1}$. Moreover, $\max(m - 1, n - 1) = k$ by $(**)$. Therefore by step 2 q's may be reindexed so that $q_i = p_i$ for all i; plus, $m - 1 = n - 1$, hence $m = n$. ■

LEMMA: If a, b, q, r are integers and $a = bq + r$, then $(a, b) = (b, r)$.

Proof: We have

$$(a, b) = (bq + r, b) = (b, r). \blacksquare$$

Proof (Euclidean Algorithm): We have:

$$\begin{aligned}
a &= bq_1 + r_1, \quad (a, b) = (b, r_1) \\
b &= r_1 q_2 + r_2, \quad (b, r_1) = (r_1, r_2) \\
r_1 &= r_2 q_3 + r_3, \quad (r_1, r_2) = (r_2, r_3) \\
r_2 &= r_3 q_4 + r_4, \quad (r_2, r_3) = (r_3, r_4) \\
&\ldots \\
r_{n-2} &= r_{n-1} q_n + r_n, (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) \\
r_{n-1} &= r_n q_{n+1}, \quad (r_{n-1}, r_n) = r_n,
\end{aligned}$$

therefore $(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = (r_3, r_4) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n$. $\blacksquare$