THREE PROBLEMS

PROBLEM 1: Prove that $\sqrt{2}$ is irrational.

Proof: Assume to the contrary that $\sqrt{2}$ is rational, that is $\sqrt{2} = \dfrac{a}{b}$, where a and b are integers and $b \neq 0$. Moreover, let a and b have no common divisor > 1. Then

$$2 = \frac{a^2}{b^2} \quad \Rightarrow \quad 2b^2 = a^2. \tag{1}$$

Since $2b^2$ is even, it follows that a^2 is even. Then a is also even (in fact, if a is odd, then a^2 is odd). This means that there exists $q \in \mathbb{Z}$ such that $a = 2q$. Substituting this into (1), we get $2b^2 = (2q)^2 \;\Rightarrow\; b^2 = 2q^2$. Since $2q^2$ is even, it follows that b^2 is even. Then b is also even by the arguments above. This is a contradiction. ■

THEOREM (DIVISION ALGORITHM): *For any integers a and b with $a \neq 0$ there exist unique integers q and r such that*

$$b = aq + r, \quad \textit{where} \quad 0 \leq r < |a|.$$

The integers q and r are called the **quotient** *and the* **reminder** *respectively.*

PROBLEM 2: Prove that $\sqrt{3}$ is irrational.

Proof: Assume to the contrary that $\sqrt{3}$ is rational, that is $\sqrt{3} = \dfrac{a}{b}$, where a and b are integers and $b \neq 0$. Moreover, let a and b have no common divisor > 1. Then

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

Since $3b^2$ is divisible by 3, it follows that a^2 is divisible by 3. Then a is also divisible by 3.

In fact, if a is not divisible by 3, then by the Division Algorithm there exists $q \in \mathbb{Z}$ such that

$$a = 3q + 1 \quad \text{or} \quad a = 3q + 2.$$

Suppose $a = 3q + 1$, then

$$a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(\underbrace{3q^2 + 2q}_{q'}) + 1 = 3q' + 1,$$

which is not divisible by 3. We get a contradiction. Similarly, if $a = 3q + 2$, then

$$a^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 3(\underbrace{3q^2 + 4q + 1}_{q''}) + 1 = 3q'' + 1,$$

which is not divisible by 3. We get a contradiction again.

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

PROBLEM 3: Prove that $\sqrt{101}$ is irrational.

Proof: Assume to the contrary that $\sqrt{101}$ is rational, that is $\sqrt{101} = \frac{a}{b}$, where a and b are integers and $b \neq 0$. Moreover, let a and b have no common divisor > 1. Then

$$101 = \frac{a^2}{b^2} \quad \Rightarrow \quad 101b^2 = a^2.$$

Since $101b^2$ is divisible by 101, it follows that a^2 is divisible by 101. Then a is also divisible by 101.

In fact, if a is not divisible by 101, then by the Division Algorithm there exists $q \in \mathbb{Z}$ such that

$$a = 101q + 1, \quad \text{or} \quad a = 101q + 2, \quad \ldots, \quad \text{or} \quad a = 101q + 100.$$

Suppose ...???

QUESTION: We should prove that if a^2 is divisible by 101, then a is also divisible by 101. Is it possible to prove it without using the division algorithm?

NEW IDEA

DEFINITION:

An integer $n \geq 2$ is called prime if its only positive divisors are 1 and n. Otherwise, n is called composite.

EXAMPLE: Numbers $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 \ldots$ are prime.

THEOREM (Euclid's Lemma): If p is a prime and p divides ab, then p divides a or 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.

COROLLARY: If p is a prime and p divides a^2, then p divides a.

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

Proof of Euclid's Lemma (Sketch):

Step 1: Suppose that p divides ab and p does not divide a. We prove that p divides b.

Step 2: We first prove that there exist integer numbers s and t such that

$$sp + ta = 1. \tag{3}$$

Step 3: If we multiply both sides of (3) by b, we get ..... Therefore p divides b. ■

GREATEST COMMON DIVISOR

DEFINITION:

If a and b are integers with $a \neq 0$, we say that a is a divisor of b if there exists an integer q such that $b = aq$. We also say that a divides b and we denote this by

$$a \mid b.$$

EXAMPLE: We have: $4 \mid 12$, since $12 = 4 \cdot 3$
$4 \nmid 15$, since $15 = 4 \cdot 3.75$

DEFINITION:

A common divisor of nonzero integers a and b is an integer c such that $c \mid a$ and $c \mid b$. The greatest common divisor (gcd) of a and b, denoted by (a, b), is the largest common divisor of integers a and b.

EXAMPLE: The common divisors of 24 and 84 are $\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6$, and ± 12. Hence, $(24, 84) = 12$. Similarly, looking at sets of common divisors, we find that $(15, 81) = 3,\ (100, 5) = 5,\ (17, 25) = 1, (-17, 289) = 17$, etc.

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

$$d = sa + tb, \tag{4}$$

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 (4) 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. ■

PROOF OF EUCLID'S LEMMA AND PROBLEM 3

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

$$spb + tab = b. \tag{5}$$

Since $p \mid ab$ and $p \mid spb$, it follows that $p \mid (spb + tab)$. This and (5) 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

$$p = \frac{a^2}{b^2} \quad \Rightarrow \quad pb^2 = a^2. \tag{6}$$

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 (6), 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. ■

PROBLEM 3: Prove that $\sqrt{101}$ is irrational.

Proof: Since 101 is prime, the result immediately follows from the Theorem above. ■