The Fundamental Theorem of Arithmetic (Applications)

Dirichlet's Theorem

A famous result of number theory deals with primes in arithmetic progressions.

THEOREM 6 (Dirichlet's Theorem on Primes in Arithmetic Progressions): Let a and b be relatively prime positive integers. Then the arithmetic progression

$$an + b, \quad n = 1, 2, 3, \ldots$$

contains infinitely many primes.

G. Lejeune Dirichlet, a German mathematician, proved this theorem in 1837. Since proofs of Dirichlet's Theorem are complicated and rely on advanced techniques, we do not present a proof here. However, it is not difficult to prove special cases of Dirichlet's theorem.

EXAMPLE: There are infinitely many primes of the form $2n + 1$, where n is a positive integer.

Proof: To prove this result, we just note that there are infinitely many prime numbers and the only even prime is 2. ■

EXAMPLE: There are infinitely many primes of the form $4n + 3$, where n is a positive integer.

Before we prove this result, we first prove a useful lemma.

LEMMA: If a and b are integers, both of the form $4n + 1$, then the product ab is also of this form.

Proof: Since a and b are both of the form $4n+1$, there exist integers r and s such that $a = 4r+1$ and $b = 4s + 1$. Hence,

$$ab = (4r + 1)(4s + 1) = 16rs + 4r + 4s + 1 = 4(4rs + r + s) + 1$$

which is again of the form $4n + 1$. ■

We now prove the desired result.

Proof: Let us assume that there are only a finite number of primes of the form $4n + 3$, say, $p_0 = 3, p_1, p_2, \ldots p_r$. Let

$$Q = 4p_1p_2 \ldots p_r + 3$$

Then there is at least one prime in the factorization of Q of the form $4n + 3$. Otherwise, all of these primes would be of the form $4n + 1$, and by the Lemma above, this would imply that Q would also be of this form, which is a contradiction. However, none of the primes $p_0, p_1, \ldots, p_n$ divides Q. The prime 3 does not divide Q, for if $3 \mid Q$, then

$$3 \mid (Q - 3) = 4p_1p_2 \ldots p_r$$

which is a contradiction. Likewise, none of the primes p_j can divide Q, because $p_j \mid Q$ implies $p_j \mid (Q - 4p_1p_2 \ldots p_r) = 3$, which is absurd. Hence, there are infinitely many primes of the form $4n + 3$. ■

Results About Irrational Numbers

THEOREM 7: Let α be a real number that is a root of the polynomial

$$x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$$

where the coefficients $c_0, c_1, \ldots, c_{n-1}$ are integers. Then α is either an integer or an irrational number.

Proof: Suppose that α is rational. Then we can write $\alpha = a/b$, where a and b are relatively prime integers with $b \neq 0$. Because α is a root of $x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$, we have

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \ldots + c_1(a/b) + c_0 = 0$$

Multiplying by b^n, we find that

$$a^n + c_{n-1}a^{n-1}b + \ldots + c_1 ab^{n-1} + c_0 b^n = 0$$

Because

$$a^n = b(-c_{n-1}a^{n-1} - \ldots - c_1 ab^{n-2} - c_0 b^{n-1})$$

we see that $b \mid a^n$. Assume that $b \neq \pm 1$. Then b has a prime divisor p. Because $p \mid b$ and $b \mid a^n$, we know that $p \mid a^n$ by Theorem 1 from Section 1.5. Hence, by the Corollary to Theorem 2, we see that $p \mid a$. However, because $(a, b) = 1$, this is a contradiction, which shows that $b = \pm 1$. Consequently, if α is rational then $\alpha = \pm a$, so that α must be an integer. ■

EXAMPLE: $\sqrt{2}$ is irrational.

Proof 1: Assume to the contrary that $\sqrt{2}$ is rational, that is,

$$\sqrt{2} = \frac{a}{b}$$

where a and b are integers and $b \neq 0$. Without loss of generality we can assume that a and b have no common divisor > 1 (indeed, if a and b have a common divisor, we can cancel it out). Then

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

Now we can obtain a contradiction in two different ways:

Method 1: Since $b \mid 2b^2$, it follows that $b \mid a^2$ by (1). But $(a, b) = 1$, therefore $b \mid a$ by Theorem 1. Hence a/b is an integer which gives us a contradiction, since $a/b = \sqrt{2}$ and $\sqrt{2}$ is not an integer.

Method 2: Since $2 \mid 2b^2$, it follows that $2 \mid a^2$ by (1). Then $2 \mid a$ by the Corollary to Theorem 2. This means that there exists $k \in \mathbb{Z}$ such that

$$a = 2k \tag{2}$$

Substituting (2) into (1), we get

$$2b^2 = (2k)^2 \quad \Longrightarrow \quad 2b^2 = 4k^2 \quad \Longrightarrow \quad b^2 = 2k^2$$

Since $2 \mid 2k^2$, it follows that $2 \mid b^2$. Then $2 \mid b$ by the Corollary to Theorem 2. So, both a and b are divisible by 2 which gives us a contradiction. ■

Proof 2: $\sqrt{2}$ is irrational by Theorem 7 above, since $\sqrt{2}$ is a root of $x^2 - 2$ and is not an integer. ■

REMARK: For more examples, see Appendix I.

EXAMPLE: Let a be a positive integer that is not the mth power of an integer, so that $\sqrt[m]{a}$ it not an integer. Then $\sqrt[m]{a}$ is irrational by Theorem 7 above, since $\sqrt[m]{a}$ is a root of $x^m - a$. Consequently, such numbers as $\sqrt{2}$, $\sqrt[3]{5}$, $\sqrt[10]{17}$, etc., are irrational.

EXAMPLE: $\dfrac{1}{3}\sqrt{2} + 5$ is irrational.

Proof: Assume to the contrary that $\dfrac{1}{3}\sqrt{2} + 5$ is rational, that is,

$$\frac{1}{3}\sqrt{2} + 5 = \frac{a}{b}$$

where a and b are integers and $b \neq 0$. Then

$$\sqrt{2} = \frac{3(a - 5b)}{b}$$

Since $\sqrt{2}$ is irrational by the Example above and $\dfrac{3(a-5b)}{b}$ is rational, we obtain a contradiction. ■

REMARK: One can check that $\dfrac{1}{3}\sqrt{2}+5$ is *not* a root of a polynomial $x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ with integer coefficients (in fact, it is a root of $(3x-15)^2 - 2$). Therefore we *can't directly* apply Theorem 7 above. ■

EXAMPLE: $\sqrt{2} + \sqrt{3}$ is irrational.

Proof 1: Assume to the contrary that $\sqrt{2} + \sqrt{3}$ is rational, that is,

$$\sqrt{2} + \sqrt{3} = \frac{a}{b}$$

where a and b are integers and $b \neq 0$. Then

$$\left(\sqrt{2} + \sqrt{3}\right)^2 = \frac{a^2}{b^2} \quad \Longrightarrow \quad 2 + 2\sqrt{2}\sqrt{3} + 3 = \frac{a^2}{b^2} \quad \Longrightarrow \quad 5 + 2\sqrt{6} = \frac{a^2}{b^2} \quad \Longrightarrow \quad \sqrt{6} = \frac{a^2 - 5b^2}{2b^2}$$

Since $\sqrt{6}$ is irrational (see Appendix I) and $\dfrac{a^2 - 5b^2}{2b^2}$ is rational, we obtain a contradiction. ■

Proof 2: One can check that $\sqrt{2} + \sqrt{3}$ is a root of the polynomial

$$x^4 - 10x^2 + 1$$

and is not an integer. Therefore it is irrational by Theorem 7 above. ■

EXAMPLE: $\sqrt{2}+\sqrt[3]{3}$ is irrational.

Proof 1: Assume to the contrary that $\sqrt{2}+\sqrt[3]{3}$ is rational, that is,

$$\sqrt{2}+\sqrt[3]{3}=\frac{a}{b}$$

where a and b are integers and $b\neq 0$. It follows that

$$\sqrt[3]{3}=\frac{a}{b}-\sqrt{2}$$

hence

$$\begin{aligned}3=\left(\frac{a}{b}-\sqrt{2}\right)^3&=\frac{a^3}{b^3}-3\frac{a^2}{b^2}\sqrt{2}+3\frac{a}{b}\left(\sqrt{2}\right)^2-\left(\sqrt{2}\right)^3\\&=\frac{a^3}{b^3}-3\frac{a^2}{b^2}\sqrt{2}+6\frac{a}{b}-2\sqrt{2}\\&=\frac{a^3}{b^3}+6\frac{a}{b}-\sqrt{2}\left(3\frac{a^2}{b^2}+2\right)\end{aligned}$$

We can rewrite this as

$$\sqrt{2}=\frac{\dfrac{a^3}{b^3}+6\dfrac{a}{b}-3}{3\dfrac{a^2}{b^2}+2}=\frac{a^3+6ab^2-3b^3}{3a^2b+2b^3}$$

Since $\sqrt{2}$ is irrational by the Example above and $\dfrac{a^3+6ab^2-3b^3}{3a^2b+2b^3}$ is rational, we obtain a contradiction. ■

Proof 2: One can check that $\sqrt{2}+\sqrt[3]{3}$ is a root of the polynomial

$$x^6-6x^4-6x^3+12x^2-36x+1$$

and is not an integer. Therefore it is irrational by Theorem 7 above. ■

EXAMPLE: $\log_5 2$ is irrational.

Proof: Assume to the contrary that $\log_5 2$ is rational, that is,

$$\log_5 2=\frac{a}{b}$$

where a and b are integers and $b\neq 0$. Then

$$5^{a/b}=2 \quad\Longrightarrow\quad 5^a=2^b$$

Since 5^a is odd and 2^b is even, we obtain a contradiction. ■

REMARK: For more examples, see Appendix II.

Appendix I

EXAMPLE: $\sqrt{6}$ is irrational.

Proof 1: Assume to the contrary that $\sqrt{6}$ is rational, that is,

$$\sqrt{6} = \frac{a}{b}$$

where a and b are integers and $b \neq 0$. Without loss of generality we can assume that a and b have no common divisor > 1 (indeed, if a and b have a common divisor, we can cancel it out). Then

$$6 = \frac{a^2}{b^2} \quad \Longrightarrow \quad 6b^2 = a^2 \tag{1}$$

Now we can obtain a contradiction in two different ways:

Method 1: Since $b \mid 6b^2$, it follows that $b \mid a^2$ by (1). But $(a, b) = 1$, therefore $b \mid a$ by Theorem 1. Hence a/b is an integer which gives us a contradiction, since $a/b = \sqrt{6}$ and $\sqrt{6}$ is not an integer.

Method 2: Since $2 \mid 6b^2$, it follows that $2 \mid a^2$ by (1). Then $2 \mid a$ by the Corollary to Theorem 2. This means that there exists $k \in \mathbb{Z}$ such that

$$a = 2k \tag{2}$$

Substituting (2) into (1), we get

$$6b^2 = (2k)^2 \quad \Longrightarrow \quad 6b^2 = 4k^2 \quad \Longrightarrow \quad 3b^2 = 2k^2$$

Since $2 \mid 2k^2$, it follows that $2 \mid 3b^2$. Therefore $2 \mid b^2$ by Theorem 1, since $(2, 3) = 1$. Then $2 \mid b$ by the Corollary to Theorem 2. So, both a and b are divisible by 2 which gives us a contradiction. ■

Proof 2: $\sqrt{6}$ is irrational by Theorem 7, since $\sqrt{6}$ is a root of $x^2 - 6$ and is not an integer. ■

EXAMPLE: $\sqrt[3]{5}$ is irrational.

Proof 1: Assume to the contrary that $\sqrt[3]{5}$ is rational, that is,

$$\sqrt[3]{5} = \frac{a}{b}$$

where a and b are integers and $b \neq 0$. Without loss of generality we can assume that a and b have no common divisor > 1 (indeed, if a and b have a

$$5 = \frac{a^3}{b^3} \quad \Longrightarrow \quad 5b^3 = a^3 \tag{3}$$

Now we can obtain a contradiction in two different ways:

Method 1: Since $b \mid 5b^3$, it follows that $b \mid a^3$ by (3). But $(a, b) = 1$, therefore $b \mid a^2$ by Theorem 1. From this for the same reason it follows that $b \mid a$. Hence a/b is an integer which gives us a contradiction, since $a/b = \sqrt[3]{5}$ and $\sqrt[3]{5}$ is not an integer.

Method 2: Since $5 \mid 5b^3$, it follows that $5 \mid a^3$ by (3). Then $5 \mid a$ by the Corollary to Theorem 2. This means that there exists $k \in \mathbb{Z}$ such that

$$a = 5k \tag{4}$$

Substituting (4) into (3), we get

$$5b^3 = (5k)^3 \quad \Longrightarrow \quad 5b^3 = 125k^3 \quad \Longrightarrow \quad b^3 = 25k^3$$

Since $5 \mid 25k^3$, it follows that $5 \mid b^3$. Then $5 \mid b$ by the Corollary to Theorem 2. So, both a and b are divisible by 5 which gives us a contradiction. ■

Proof 2: $\sqrt[3]{5}$ is irrational by Theorem 7, since $\sqrt[3]{5}$ is a root of $x^3 - 5$ and is not an integer. ■

EXAMPLE: $\sqrt{15}$ is irrational.

Proof 1: Assume to the contrary that $\sqrt{15}$ is rational, that is,

$$\sqrt{15} = \frac{a}{b}$$

where a and b are integers and $b \neq 0$. Without loss of generality we can assume that a and b have no common divisor > 1 (indeed, if a and b have a common divisor, we can cancel it out). Then

$$15 = \frac{a^2}{b^2} \quad \Longrightarrow \quad 15b^2 = a^2 \tag{5}$$

Now we can obtain a contradiction in two different ways:

Method 1: Since $b \mid 15b^2$, it follows that $b \mid a^2$ by (5). But $(a, b) = 1$, therefore $b \mid a$ by Theorem 1. Hence a/b is an integer which gives us a contradiction, since $a/b = \sqrt{15}$ and $\sqrt{15}$ is not an integer.

Method 2: Since $3 \mid 15b^2$, it follows that $3 \mid a^2$ by (5). Then $3 \mid a$ by the Corollary to Theorem 2. This means that there exists an integer number k such that

$$a = 3k \tag{6}$$

Substituting (6) into (5), we get

$$15b^2 = (3k)^2 \quad \Longrightarrow \quad 15b^2 = 9k^2 \quad \Longrightarrow \quad 5b^2 = 3k^2$$

Since $3 \mid 3k^2$, it follows that $3 \mid 5b^2$. Therefore $3 \mid b^2$ by Theorem 1, since $(3, 5) = 1$. Then $3 \mid b$ by the Corollary to Theorem 2. So, both a and b are divisible by 3 which gives us a contradiction. ■

Proof 2: $\sqrt{15}$ is irrational by Theorem 7, since $\sqrt{15}$ is a root of $x^2 - 15$ and is not an integer. ■

REMARK: This problem was given as a Midterm Exam question in Summer of 2017.

Appendix II

EXAMPLE: $\sin 1^\circ$ is irrational.

Proof: Assume to the contrary that $\sin 1^\circ$ is rational. Then $\cos^2 1^\circ$ and $\cos 2^\circ$ are also rational, since

$$\cos^2 1^\circ = 1 - \sin^2 1^\circ \qquad \text{and} \qquad \cos 2^\circ = \cos^2 1^\circ - \sin^2 1^\circ$$

Similarly, $\cos 4^\circ$, $\cos 8^\circ$, $\cos 16^\circ$, and $\cos 32^\circ$ are rational, since

$$\cos 4^\circ = 2\cos^2 2^\circ - 1$$

$$\cos 8^\circ = 2\cos^2 4^\circ - 1$$

$$\cos 16^\circ = 2\cos^2 8^\circ - 1$$

$$\cos 32^\circ = 2\cos^2 16^\circ - 1$$

On the other hand, we have

$$\begin{aligned}
\frac{\sqrt{3}}{2} = \cos 30^\circ = \cos(32^\circ - 2^\circ) &= \cos 32^\circ \cos 2^\circ + \sin 32^\circ \sin 2^\circ \\
&= \cos 32^\circ \cos 2^\circ + 2\cos 16^\circ \sin 16^\circ \sin 2^\circ \\
&= \cos 32^\circ \cos 2^\circ + 4\cos 16^\circ \cos 8^\circ \sin 8^\circ \sin 2^\circ \\
&= \cos 32^\circ \cos 2^\circ + 8\cos 16^\circ \cos 8^\circ \cos 4^\circ \sin 4^\circ \sin 2^\circ \\
&= \cos 32^\circ \cos 2^\circ + 16\cos 16^\circ \cos 8^\circ \cos 4^\circ \cos 2^\circ \sin^2 2^\circ \\
&= \cos 32^\circ \cos 2^\circ + 64\cos 16^\circ \cos 8^\circ \cos 4^\circ \cos 2^\circ \cos^2 1^\circ \sin^2 1^\circ
\end{aligned}$$

The right-hand side is rational. One can prove that $\dfrac{\sqrt{3}}{2}$ is irrational. We obtain a contradiction. ■

EXAMPLE: The number

$$2 + \frac{1}{2!} + \frac{1}{3!} + \ldots + \frac{1}{n!} + \ldots$$

is irrational.

Proof: Assume to the contrary that this number is rational, that is,

$$\frac{a}{b} = 2 + \frac{1}{2!} + \frac{1}{3!} + \ldots + \frac{1}{n!} + \ldots,$$

where a and b are integers and $b \neq 0$. We multiply both sides by $bn!$ with

$$n > b \tag{1}$$

We get

$$\begin{aligned}
an! &= bn!\left(2+\frac{1}{2!}+\frac{1}{3!}+\ldots+\frac{1}{n!}+\ldots\right)\\
&= bn!\left(2+\frac{1}{2!}+\frac{1}{3!}+\ldots+\frac{1}{n!}\right)+bn!\left(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\frac{1}{(n+3)!}+\ldots\right)\\
&= bn!\left(2+\frac{1}{2!}+\frac{1}{3!}+\ldots+\frac{1}{n!}\right)+b\left(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\ldots\right)
\end{aligned}$$

so

$$an!-bn!\left(2+\frac{1}{2!}+\frac{1}{3!}+\ldots+\frac{1}{n!}\right)=b\left(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\ldots\right)$$

Note that $an!$ and $bn!\left(2+\frac{1}{2!}+\frac{1}{3!}+\ldots+\frac{1}{n!}\right)$ are integer. If we prove that

$$b\left(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\ldots\right)<1$$

we obtain a contradiction. To this end we observe that

$$\frac{1}{(n+1)(n+2)}<\frac{1}{(n+1)^2},\quad \frac{1}{(n+1)(n+2)(n+3)}<\frac{1}{(n+1)^3},\ldots$$

By this and a formula of geometric progression we have

$$\begin{aligned}
b\left(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\ldots\right) &< b\left(\frac{1}{n+1}+\frac{1}{(n+1)^2}+\frac{1}{(n+1)^3}+\ldots\right)\\
&= b\frac{1}{(n+1)\left(1-\frac{1}{n+1}\right)}\\
&= b\frac{1}{n+1-\frac{n+1}{n+1}}\\
&= b\frac{1}{n+1-1}\\
&= \frac{b}{n}
\end{aligned}$$

which is <1 by (1). ■