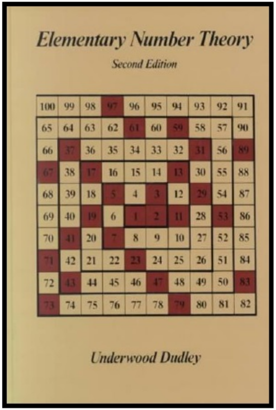
Elementary Number Theory

Section 20. $x^2 - Ny^2 = 1$—Proofs of Theorems



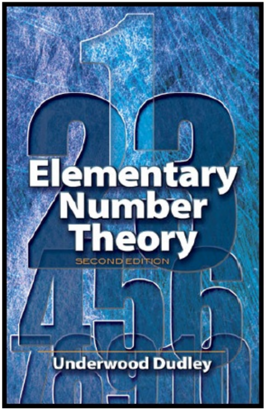


Table of contents

Lemma 20.1

Lemma 20.1. If $N > 0$ is not a square, then $x + y\sqrt{N} = r + s\sqrt{N}$ if and only if $x = r$ and $y = s$.

Proof. If $x = r$ and $y = s$, then $x + y\sqrt{N} = r + s\sqrt{N}$. For the converse, suppose that $x + y\sqrt{N} = r + s\sqrt{N}$. ASSUME $y \neq s$. Then $\sqrt{N} = \dfrac{x - r}{s - y}$ is a rational number. But N is not a square, so $\sqrt{N}$ is irrational by Note 20.B, a CONTRADICTION. So the assumption that $y \neq s$ is false, and we must have $y = s$. It then follows that $x = r$, as claimed. □

Lemma 20.1

Lemma 20.1. If $N > 0$ is not a square, then $x + y\sqrt{N} = r + s\sqrt{N}$ if and only if $x = r$ and $y = s$.

Proof. If $x = r$ and $y = s$, then $x + y\sqrt{N} = r + s\sqrt{N}$. For the converse, suppose that $x + y\sqrt{N} = r + s\sqrt{N}$. ASSUME $y \neq s$. Then $\sqrt{N} = \dfrac{x - r}{s - y}$ is a rational number. But N is not a square, so $\sqrt{N}$ is irrational by Note 20.B, a CONTRADICTION. So the assumption that $y \neq s$ is false, and we must have $y = s$. It then follows that $x = r$, as claimed. □

Lemma 20.3

Lemma 20.3. If α gives a solution of $x^2 - Ny^2 = 1$, then so does $1/\alpha$.

Proof. Let $\alpha = r + s\sqrt{N}$. Then we know that $r^2 - Ns^2 = 1$ by the definition of "gives a solution." Next,

$$\frac{1}{\alpha} = \frac{1}{r + s\sqrt{N}} \frac{r - s\sqrt{N}}{r - s\sqrt{N}} = \frac{r - s\sqrt{N}}{r^2 - Ns^2} = r - s\sqrt{N},$$

because $r^2 - Ns^2 = 1$. So $1/\alpha$ also gives a solution of $x^2 - Ny^2 = 1$, by the definition of "gives a solution," as claimed. □

Lemma 20.3

Lemma 20.3. If α gives a solution of $x^2 - Ny^2 = 1$, then so does $1/\alpha$.

Proof. Let $\alpha = r + s\sqrt{N}$. Then we know that $r^2 - Ns^2 = 1$ by the definition of "gives a solution." Next,

$$\frac{1}{\alpha} = \frac{1}{r + s\sqrt{N}} \frac{r - s\sqrt{N}}{r - s\sqrt{N}} = \frac{r - s\sqrt{N}}{r^2 - Ns^2} = r - s\sqrt{N},$$

because $r^2 - Ns^2 = 1$. So $1/\alpha$ also gives a solution of $x^2 - Ny^2 = 1$, by the definition of "gives a solution," as claimed. □

Lemma 20.4

Lemma 20.4. Let α and β give solutions of $x^2 - Ny^2 = 1$, then so does $\alpha\beta$.

Proof. By the definition of "give a solution," we know that $\alpha = a + b\sqrt{N}$ and $\beta = c + d\sqrt{N}$ for some a, b, c, d with $a^2 - Nb^2 = 1$ and $c^2 - Nd^2 = 1$. Then (by FOIL)

$$\alpha\beta = (a + b\sqrt{N})(c + d\sqrt{N}) = (ac + Nbd) + (ad + bc)\sqrt{N},$$

and from Lemma 20.2,

$$\begin{aligned} (ac + Nbd)^2 - N(ad + bc)^2 &= (a^2 - Nb^2)(c^2 - Nd^2) \text{ by Lemma 20.2} \\ &= (1)(1) = 1 \text{ since } \alpha \text{ and } \beta \text{ give solutions.} \end{aligned}$$

So by definition, $\alpha\beta$ gives a solution, as claimed. □

Lemma 20.4

Lemma 20.4. Let α and β give solutions of $x^2 - Ny^2 = 1$, then so does $\alpha\beta$.

Proof. By the definition of "give a solution," we know that $\alpha = a + b\sqrt{N}$ and $\beta = c + d\sqrt{N}$ for some a, b, c, d with $a^2 - Nb^2 = 1$ and $c^2 - Nd^2 = 1$. Then (by FOIL)

$$\alpha\beta = (a + b\sqrt{N})(c + d\sqrt{N}) = (ac + Nbd) + (ad + bc)\sqrt{N},$$

and from Lemma 20.2,

$$\begin{aligned} (ac + Nbd)^2 - N(ad + bc)^2 &= (a^2 - Nb^2)(c^2 - Nd^2) \text{ by Lemma 20.2} \\ &= (1)(1) = 1 \text{ since } \alpha \text{ and } \beta \text{ give solutions.} \end{aligned}$$

So by definition, $\alpha\beta$ gives a solution, as claimed. □

Lemma 20.5

Lemma 20.5. If α gives a solution of $x^2 - Ny^2 = 1$, then so does α^k for any integer k, positive, negative, or zero.

Proof. If α gives a solution, then from Lemma 20.4 and induction α^k gives a solution for all integers $k >\geq 1$. From Lemma 20.3, $1/\alpha = \alpha^{-1}$ gives a solution and, again, by Lemma 20.4 and induction $(\alpha^{-1})^k = \alpha^{-k}$ gives a solution for all integers $-k \leq -1$. Finally, with $k = 0$ we have that $\alpha^0 = 1$ and this gives a solution (namely, the trivial solution $x = 1$ and $y = 0$). That is, α^k gives a solution for all integers k, as claimed. □

Lemma 20.5

Lemma 20.5. If α gives a solution of $x^2 - Ny^2 = 1$, then so does α^k for any integer k, positive, negative, or zero.

Proof. If α gives a solution, then from Lemma 20.4 and induction α^k gives a solution for all integers $k >\geq 1$. From Lemma 20.3, $1/\alpha = \alpha^{-1}$ gives a solution and, again, by Lemma 20.4 and induction $(\alpha^{-1})^k = \alpha^{-k}$ gives a solution for all integers $-k \leq -1$. Finally, with $k = 0$ we have that $\alpha^0 = 1$ and this gives a solution (namely, the trivial solution $x = 1$ and $y = 0$). That is, α^k gives a solution for all integers k, as claimed. □

Lemma 20.6

Lemma 20.6. Suppose that a, b, c, d are nonnegative and that $\alpha = a + b\sqrt{N}$ and $\beta = c + d\sqrt{N}$ give solutions of $x^2 - Ny^2 = 1$. Then $\alpha < \beta$ if and only if $a < c$.

Proof. First, suppose $a < c$. Then $a^2 < c^2$. Since $\alpha = a + b\sqrt{N}$ and $\beta = c + d\sqrt{N}$ give solutions, then by the definition of "give solutions" we have $a^2 = 1 + Nb^2$ and $c^2 = 1 + Nd^2$. Hence, $Nb^2 < Nd^2$. Because none of b, d, N are negative, then $b < d$. Therefore, $\alpha = a + b\sqrt{N} < c + d\sqrt{N} = \beta$, as claimed.

Lemma 20.6

Lemma 20.6. Suppose that a, b, c, d are nonnegative and that $\alpha = a + b\sqrt{N}$ and $\beta = c + d\sqrt{N}$ give solutions of $x^2 - Ny^2 = 1$. Then $\alpha < \beta$ if and only if $a < c$.

Proof. First, suppose $a < c$. Then $a^2 < c^2$. Since $\alpha = a + b\sqrt{N}$ and $\beta = c + d\sqrt{N}$ give solutions, then by the definition of "give solutions" we have $a^2 = 1 + Nb^2$ and $c^2 = 1 + Nd^2$. Hence, $Nb^2 < Nd^2$. Because none of b, d, N are negative, then $b < d$. Therefore, $\alpha = a + b\sqrt{N} < c + d\sqrt{N} = \beta$, as claimed.

Second, suppose $\alpha < \beta$. ASSUME $a \geq c$. Then $a^2 \geq c^2$. As above, this implies $Nb^2 \geq Nd^2$, or $b^2 \geq d^2$. But then $\alpha = a + b\sqrt{N} \geq c + d\sqrt{N} = \beta$, a CONTRADICTION. So the assumption that $a \geq c$ is false, and we must have $a < c$, as claimed. □

Lemma 20.6

Lemma 20.6. Suppose that a, b, c, d are nonnegative and that $\alpha = a + b\sqrt{N}$ and $\beta = c + d\sqrt{N}$ give solutions of $x^2 - Ny^2 = 1$. Then $\alpha < \beta$ if and only if $a < c$.

Proof. First, suppose $a < c$. Then $a^2 < c^2$. Since $\alpha = a + b\sqrt{N}$ and $\beta = c + d\sqrt{N}$ give solutions, then by the definition of "give solutions" we have $a^2 = 1 + Nb^2$ and $c^2 = 1 + Nd^2$. Hence, $Nb^2 < Nd^2$. Because none of b, d, N are negative, then $b < d$. Therefore, $\alpha = a + b\sqrt{N} < c + d\sqrt{N} = \beta$, as claimed.

Second, suppose $\alpha < \beta$. ASSUME $a \geq c$. Then $a^2 \geq c^2$. As above, this implies $Nb^2 \geq Nd^2$, or $b^2 \geq d^2$. But then $\alpha = a + b\sqrt{N} \geq c + d\sqrt{N} = \beta$, a CONTRADICTION. So the assumption that $a \geq c$ is false, and we must have $a < c$, as claimed. □

Theorem 20.1

Theorem 20.1. If θ is the generator for $x^n - Ny^2 = 1$, then all nontrivial solutions of the equation with x and y positive are given by θ^k, $k = 1, 2, \ldots$. That is, if $x = r$, $y = s$ is a solution then $\alpha = r + s\sqrt{N}$ is some positive power of θ.

Proof. Let $x = r$ and $y = s$ be any nontrivial solution of $x^2 - Ny^2 = 1$ with $r > 0$ and $s > 0$. Let $\alpha = r + s\sqrt{N}$. We have $\alpha \geq \theta$ by the choice of generator θ. So there is some positive integer k such that $\theta^k \leq \alpha < \theta^{k+1}$. Thus $1 \leq \theta^{-k}\alpha < \theta$. By Lemma 20.5, θ^{-k} gives a solution of $x^2 - Ny^2 = 1$ and then, by Lemma 20.4, $\theta^{-k}\alpha$ also gives a solution. But $1 \leq \theta^{-k}\alpha < \theta$ and θ is the smallest nontrivial solution, so it must be that $1 = \theta^{-k}\alpha$, or $\alpha = \theta^k$. That is, α is an arbitrary real number that gives solutions and $\alpha = \theta^k$ for some k, as claimed. □

Theorem 20.1

Theorem 20.1. If θ is the generator for $x^n - Ny^2 = 1$, then all nontrivial solutions of the equation with x and y positive are given by θ^k, $k = 1, 2, \ldots$. That is, if $x = r$, $y = s$ is a solution then $\alpha = r + s\sqrt{N}$ is some positive power of θ.

Proof. Let $x = r$ and $y = s$ be any nontrivial solution of $x^2 - Ny^2 = 1$ with $r > 0$ and $s > 0$. Let $\alpha = r + s\sqrt{N}$. We have $\alpha \geq \theta$ by the choice of generator θ. So there is some positive integer k such that $\theta^k \leq \alpha < \theta^{k+1}$. Thus $1 \leq \theta^{-k}\alpha < \theta$. By Lemma 20.5, θ^{-k} gives a solution of $x^2 - Ny^2 = 1$ and then, by Lemma 20.4, $\theta^{-k}\alpha$ also gives a solution. But $1 \leq \theta^{-k}\alpha < \theta$ and θ is the smallest nontrivial solution, so it must be that $1 = \theta^{-k}\alpha$, or $\alpha = \theta^k$. That is, α is an arbitrary real number that gives solutions and $\alpha = \theta^k$ for some k, as claimed. □