Book Dudley Exercises

Jason Sass

April 19, 2025

Dudley problems section 1

Exercise 1. Let $k, n \in \mathbb{Z}$.
Then $\gcd(k, n+k) = 1$ iff $\gcd(k, n) = 1$.

Proof. Suppose $\gcd(k, n) = 1$.
Then there exist integers x, y such that $xk + yn = 1$.
Thus, $1 = xk + yn = xk - yk + yk + yn = k(x-y) + y(k+n) = (x-y)k + y(n+k)$.
Since $x-y$ and y are integers and $(x-y)k+y(n+k) = 1$, then $\gcd(k, n+k) = 1$. □

Proof. Conversely, suppose $\gcd(k, n+k) = 1$.
Then there exist integers s, t such that $sk + t(n+k) = 1$.
Thus, $1 = sk + tn + tk = sk + tk + tn = (s+t)k + tn$.
Since $s+t$ and t are integers and $(s+t)k + tn = 1$, then $\gcd(k, n) = 1$. □

Exercise 2. Let $k, n \in \mathbb{Z}$.
Then $\gcd(k, n+k) = d$ iff $\gcd(k, n) = d$.

Proof. Suppose $\gcd(k, n) = d$.
Then $d \in \mathbb{Z}^+$ and $d|k$ and $d|n$ and if c is any common divisor of k and n, then $c|d$.
Since $d|n$ and $d|k$, then d divides the sum $n+k$, so $d|(n+k)$.
Since $d|k$ and $d|(n+k)$, then d is a common divisor of k and $n+k$.

Let c be any common divisor k and $n+k$.
Then $c|k$ and $c|(n+k)$, so c divides the difference $(n+k) - k = n$.
Hence, $c|n$.
Since $c|k$ and $c|n$, then c is a common divisor of k and n, so $c|d$.
Therefore, any common divisor of k and $n+k$ divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of k and $n+k$ and any common divisor of k and $n+k$ divides d, then by definition of gcd, $d = \gcd(k, n+k)$. $\square$

Proof. Conversely, suppose $\gcd(k, n+k) = d$.

Then $d \in \mathbb{Z}^+$ and $d|k$ and $d|(n+k)$ and if c is any common divisor of k and $n+k$, then $c|d$.

Since $d|k$ and $d|(n+k)$, then d divides the difference $(n+k) - k = n$.

Since $d|k$ and $d|n$, then d is a common divisor of k and n.

Let c be any common divisor of k and n.

Then $c|k$ and $c|n$, so c divides the sum $n+k$.

Since $c|k$ and $c|(n+k)$, then c is a common divisor of k and $n+k$, so $c|d$.

Hence, any common divisor of k and n divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor k and n and any common divisor of k and n divides d, then by definition of gcd, $d = \gcd(k, n)$. $\square$

Exercise 3. Let $k, n \in \mathbb{Z}$.

Then $\gcd(k, n+rk) = d$ for all $r \in \mathbb{Z}$ iff $\gcd(k, n) = d$.

Proof. Suppose $\gcd(k, n) = d$.

Then $d \in \mathbb{Z}^+$ and $d|k$ and $d|n$ and if c is any common divisor of k and n, then $c|d$.

Let $r \in \mathbb{Z}$.

Since $d|k$, then $d|rk$.

Since $d|n$ and $d|rk$, then d divides the sum $n+rk$.

Since $d|k$ and $d|(n+rk)$, then d is a common divisor of k and $n+rk$.

Let c be any common divisor of k and $n+rk$.

Then $c|k$ and $c|(n+rk)$.

Since $c|k$, then $c|rk$.

Since $c|(n+rk)$ and $c|rk$, then c divides the difference $(n+rk) - rk = n$, so $c|n$.

Since $c|k$ and $c|n$, then c is a common divisor of k and n, so $c|d$.

Hence, any common divisor of k and $n+rk$ divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of k and $n+rk$ and any common divisor of k and $n+rk$ divides d, then by definition of gcd, $d = \gcd(k, n+rk)$. $\square$

Proof. Conversely, suppose $\gcd(k, n+rk) = d$ for all $r \in \mathbb{Z}$.

Let $r = 0$.

Then $d = \gcd(k, n+rk) = \gcd(k, n+0k) = \gcd(k, n+0) = \gcd(k, n)$.

Therefore, $\gcd(k, n) = d$. $\square$

Exercise 4. Let $x \in \mathbb{R}$ and $a, b \in \mathbb{Z}$.

I. If $x^2 + ax + b = 0$ has an integer root, then the root divides b.

II. If $x^2 + ax + b = 0$ has a rational root, then the root is an integer.

Proof. We prove I.

Suppose the equation $x^2 + ax + b = 0$ has an integer root.
Let r be an integer root of $x^2 + ax + b = 0$.
Then $r \in \mathbb{Z}$ and $r^2 + ar + b = 0$, so $b = -r^2 - ar = r(-r - a)$.
Since $-r - a \in \mathbb{Z}$ and $b = r(-r - a)$, then r divides b. □

Proof. We prove II.

Suppose the equation $x^2 + ax + b = 0$ has a rational root.
Let q be a rational root of $x^2 + ax + b = 0$.
Then $q \in \mathbb{Q}$ and $q^2 + aq + b = 0$.
Since $q \in \mathbb{Q}$, then there exist integers r, s with $s \neq 0$ such that $q = \frac{r}{s}$.
Assume q is in lowest terms. That is, assume $\gcd(r, s) = 1$, so $1 = \gcd(s, r)$.
Since $(\frac{r}{s})^2 + a \cdot (\frac{r}{s}) + b = 0$ and $s \neq 0$, then $\frac{r^2}{s^2} + \frac{ar}{s} + b = 0$, so $r^2 + ars + bs^2 = 0$.
Thus, $r^2 = -ars - bs^2 = s(-ar - bs)$.
Since $s \in \mathbb{Z}$, then $s|s$, so s divides any multiple of s.
Hence, s divides $(-ar - bs)s = s(-ar - bs)$, so s divides r^2.
Since $s|r^2$ and $\gcd(s, r) = 1$, then $s|r$.
Thus, $r = st$ for some integer t, so $q = \frac{r}{s} = \frac{st}{s} = t$.
Therefore, q is an integer. □