Example 29. The fraction $\frac{x(x^2+2)}{3}$ is an integer for all $x \in \mathbb{Z}$.

Proof. Since we are dividing by 3, it is natural to distinguish the three cases $x=3q$, $x=3q+1$, $x=3q+2$ and to consider the remainder of $x(x^2+2)$ when dividing by 3.

If $x=3q$, then $x(x^2+2)=3q(9q^2+2)$ leaves remainder 0.

If $x=3q+1$, then $x(x^2+2)=(3q+1)(9q^2+6q+3)$ leaves remainder 0.

If $x=3q+2$, then $x(x^2+2)=(3q+1)(9q^2+12q+6)$ leaves remainder 0.

Thus, for any integer x, $x(x^2+2)$ is divisible by 3. □

2.2 Greatest common divisor

Definition 30. Let $a, b \in \mathbb{Z}$ and $a \neq 0$. We write $a|b$ (and say b is **divisible** by a) if $\frac{b}{a} \in \mathbb{Z}$.

In other words, $a|b$ if and only if there exists an integer c such that $ac=b$.

Example 31. $3|9$ but $3 \nmid 10$.

Definition 32. Let $a, b \in \mathbb{Z}$ (not both zero). The **greatest common divisor** $\gcd(a,b)$ of a and b is the largest positive integer c such that $c|a$ and $c|b$.

Example 33.

(a) $\gcd(2,4)=2$

(b) $\gcd(2,6)=2$

(c) $\gcd(15,28)=1$

(d) $\gcd(12,42)=\gcd(2^2\cdot 3, 2\cdot 3\cdot 7)=6$

(e) $\gcd(140,2016)=\gcd(2^2\cdot 5\cdot 7, 2^5\cdot 3^2\cdot 7)=2^2\cdot 7=28$

BAD?! Computing $\gcd(a,b)$ by factoring a and b is not a good approach. Though small numbers might be easy to factor, it is very hard to factor even moderately large numbers in general.

Indeed, until 2007, the NSA offered cash prizes up to 200,000 USD for factoring large numbers (20,000 USD collected in 2005 for factoring a number with 193 decimal digits; 232 decimal digits factored in 2009, larger ones remain unfactored; largest one has 617 decimal digits).

The reason the NSA, among others, is interested in factoring is that the difficulty of factoring is actually crucially used in many cryptosystems.

Lemma 34. If $a=qb+r$, then $\gcd(a,b)=\gcd(b,r)$.

Proof. Let $d \in \mathbb{N}$. We claim that $d|a$ and $d|b$ iff $d|r$ and $d|b$. [**iff** is short for "if and only if"]

"$\Longrightarrow$": $d|r$ because $\frac{r}{d}=\frac{a-qb}{d}=\frac{a}{d}-\frac{qb}{d}$ is an integer (since $d|a$ and $d|b$).

"$\Longleftarrow$": $d|a$ because $\frac{a}{d}=\frac{qb+r}{d}=\frac{qb}{d}+\frac{r}{d}$ is an integer (since $d|b$ and $d|r$). □

Example 35. Using this lemma to compute $\gcd$'s is refered to as the **Euclidean algorithm**.

(a) $\underbrace{\gcd(30,108)}_{108=3\cdot 30+18}=\underbrace{\gcd(18,30)}_{30=1\cdot 18+12}=\underbrace{\gcd(12,18)}_{18=1\cdot 12+6}=\underbrace{\gcd(6,12)}_{12=2\cdot 6+0}=\gcd(0,6)=6$

(b) $\underbrace{\gcd(15,28)}_{28=1\cdot 15+13}=\underbrace{\gcd(13,15)}_{15=1\cdot 13+2}=\underbrace{\gcd(2,13)}_{13=6\cdot 2+1}=\gcd(1,2)=1$

Armin Straub
straub@southalabama.edu

Theorem 36. (Bézout's identity) Let $a, b \in \mathbb{Z}$ (not both zero). There exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a,b) = ax + by.$$

Proof. We proceed iteratively:

$$\begin{aligned}
a &= q_1 b + r_1, \quad 0 < r_1 < b \\
b &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \quad 0 < r_3 < r_2 \\
&\vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Along the way, we have $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \ldots = \gcd(r_{n-2},r_{n-1}) = \gcd(r_{n-1},r_n) = r_n$ (why is it obvious that the last gcd is r_n?).

By the second-to-last equation, $\gcd(a,b) = r_n = r_{n-2} - q_n r_{n-1}$ is a linear combination of r_{n-2} and r_{n-1}. Then, moving one up, we replace r_{n-1} with $r_{n-3} - q_{n-1} r_{n-2}$ to write $\gcd(a,b)$ as a linear combination of r_{n-3} and r_{n-2}. Continuing in that fashion, we ultimately obtain $\gcd(a,b)$ as a linear combination of a and b. □

Corollary 37. Let $a, b \in \mathbb{Z}$ (not both zero). Then the set

$$T = \{ax + by : x, y \in \mathbb{Z}\}$$

is precisely the set of all multiples of $d = \gcd(a,b)$.

Proof. "multiples of $d \subseteq T$": Our previous theorem says that we can write $d = ax + by$, which means that $d \in T$. It also means that every multiple nd is in T because $nd = a \cdot (nx) + b \cdot (ny)$.

"$T \subseteq$ multiples of d": On the other hand, let $t = ax + by$ be any element of T. Since $d|a$ and $d|b$, we have $d|t$. That is, the element t is necessarily a multiple of d. □

Example 38. Let us revisit the previous example to illustrate how the Euclidean algorithm provides us with a way to write $\gcd(a,b)$ as an integer linear combination of a and b.

(a) $\underbrace{\gcd(30,108)}_{108=3\cdot 30+18} = \underbrace{\gcd(18,30)}_{30=1\cdot 18+12} = \underbrace{\gcd(12,18)}_{18=1\cdot 12+6} = \underbrace{\gcd(6,12)}_{12=2\cdot 6+0} = \gcd(0,6) = 6$

Trace back: $6 = \underbrace{18 - 1\cdot 12}_{12=30-18} = \underbrace{-1\cdot 30 + 2\cdot 18}_{18=108-3\cdot 30} = 2\cdot 108 - 7\cdot 30$

(b) $\underbrace{\gcd(15,28)}_{28=1\cdot 15+13} = \underbrace{\gcd(13,15)}_{15=1\cdot 13+2} = \underbrace{\gcd(2,13)}_{13=6\cdot 2+1} = \gcd(1,2) = 1$

Trace back: $1 = \underbrace{13 - 6\cdot 2}_{2=15-13} = \underbrace{-6\cdot 15 + 7\cdot 13}_{13=28-15} = 7\cdot 28 - 13\cdot 15$