HA2

Victor Koch-larsen and Magnus Chr. Hvidtfeldt

October 12, 2025

Exercise A.8. Prove or disprove that if $a \mid bc$, where $a, b, c \in \mathbb{Z}^+$ and $a \neq 0$ then $a \mid b$ or $a \mid c$

Assume $a \mid bc$ for some $a,\ b,\ c \in \mathbb{Z}^+$, then $bc/a = k$ for some $k \in \mathbb{Z}^+$. We will disprove this with a counter-example. Consider $a = 10,\ b = 4,\ c = 5$, then

$$\begin{aligned}\frac{bc}{a} &= \frac{4*5}{10} = 2 \in \mathbb{Z}\\ \frac{b}{a} &= \frac{4}{10} = \frac{2}{5} \notin \mathbb{Z}\\ \frac{c}{a} &= \frac{5}{10} = \frac{1}{2} \notin \mathbb{Z}\end{aligned} \tag{1}$$

Therefore, we can conclude that there exists some $a, b, c \in \mathbb{Z}^+$ s.t. if $a \mid bc$, then $a \nmid b$ and $a \nmid c$. □

Exercise A.12. Prove that if a is a positive integer, then 4 does not divide $a^2 + 2$.

We are given that $a \in \mathbb{Z}^+ \rightarrow 4 \nmid a^2 + 2$. Then $a^2 + 2 = 4c \rightarrow (a^2 + 2)/4 = c$ for some $c \in \mathbb{Z}$. We can check for all positive integers (even and odd) for some $k \in \mathbb{Z}^+$ as such. We will check first for even numbers of the form $(2k)$

$$\frac{(2k)^2 + 2}{4} = \frac{4k^2 + 2}{4} = k^2 + \frac{1}{2} \tag{2}$$

And for odd numbers of the form $(2k + 1)$

$$\frac{(2k+1)^2 + 2}{4} = \frac{4k^2 + 4k + 1 + 2}{4} = k^2 + k + \frac{3}{4} \tag{3}$$

Since for even positive integers $(2k)$ and for odd positive integers $(2k + 1)$, adding a fraction to integers will always result in a fraction. Therefore, if $a \in \mathbb{Z}^+$, 4 does not divide $a^2 + 2$. □

Exercise B.52. Write out the addition and multiplication tables for $\mathbb{Z}_6$

$\mathbb{Z}_6$ is a sequence of integers 0 or greater, reaching the numerical value 5, because 0 is also counted. Hence, the sequence is a repetition of the numbers 0,1,2,3,4,5 infinitely many times.

Example: $1 +_6 5$ for $\mathbb{Z}_6$ is equal to 0, as 6 does not exist $\in \mathbb{Z}_6$. Therefore, it returns to the next number in the sequence, which in this case is 0.

Example: $2 \cdot_6 3$ for $\mathbb{Z}_6$ is equal to the product of the number used as the placement in the sequence of numbers from 0 to 5 repeated infinitely many times.

The following is our addition table of $\mathbb{Z}_6$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(4)

The following is our multiplication table of $\mathbb{Z}_6$

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(5)

Exercise C.32. Use the Euclidean Algorithm to find the following greatest common divisors.

Let $a = bq + r$ where $\gcd(a, b) = \gcd(b, r)$. We can use this lemma (of the Euclidean Algorithm) to find the greatest common divisor. Because they share the greatest common divisors, we can reduce them and find their gcd in this way. The last remainder that we get from the Euclidean Algorithm is our greatest common divisor.

a) gcd(1,5)
We take the greater number as a and use the Euclidean Algorithm

$$5 = 1 \cdot 5 + 0 \tag{6}$$

Therefore $\gcd(1, 5) = 1$

b) gcd(100,101)
We take the greater number as a and use the Euclidean Algorithm

$$\begin{aligned} 101 &= 100 \cdot 1 + 1 \\ 100 &= 1 \cdot 100 + 0 \end{aligned} \tag{7}$$

Since the last remainder is 1, the $\gcd(100, 101) = 1$

c) gcd(123,277)
We take the greater number as a and use the Euclidean Algorithm

$$\begin{aligned} 277 &= 123 \cdot 2 + 31 \\ 123 &= 31 \cdot 3 + 30 \\ 31 &= 30 \cdot 1 + 1 \\ 30 &= 1 \cdot 30 + 0 \end{aligned} \tag{8}$$

So $\gcd(123, 277) = 1$

d) gcd(1529,14039)
We take the greater number as a and use the Euclidean Algorithm

$$\begin{aligned} 14039 &= 1529 \cdot 9 + 278 \\ 1529 &= 278 \cdot 5 + 139 \\ 278 &= 139 \cdot 2 + 0 \end{aligned} \tag{9}$$

Therefore $\gcd(1529, 14039) = 139$

e) gcd(1529,14038)
We take the greater number as a and use the Euclidean Algorithm

$$\begin{aligned} 14038 &= 1529 \cdot 9 + 277 \\ 1529 &= 277 \cdot 5 + 144 \\ 277 &= 144 \cdot 1 + 133 \\ 144 &= 133 \cdot 1 + 11 \\ 133 &= 11 \cdot 12 + 1 \\ 11 &= 1 \cdot 11 + 0 \end{aligned} \tag{10}$$

So $\gcd(1529, 14038) = 1$

f) gcd(11111,111111)
We take the greater number as a and use the Euclidean Algorithm

$$\begin{aligned} 111111 &= 11111 \cdot 10 + 1 \\ 11111 &= 1 \cdot 11111 + 0 \end{aligned} \tag{11}$$

Therefore $\gcd(11111, 111111) = 1$

Exercise C.44. Use the extended Euclidean Algorithm to express gcd(1001, 100001) as a linear combination of 1001 and 100001.

A given linear combination is described as some $s, t \in \mathbb{Z}$ s.t. $\gcd(a, b) = sa + tb$. We use this theorem to express $\gcd(1001, 100001)$ as a linear combination. First, we find $\gcd(1001, 100001)$.

$$\begin{aligned}100001 &= 1001 \cdot 99 + 902\\ 1001 &= 902 \cdot 1 + 99\\ 902 &= 99 \cdot 9 + 11\\ 99 &= 11 \cdot 9\end{aligned} \tag{12}$$

We can also find it using a table as follows

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	100001	1001	99	902	1	0
1	1001	902	1	99	0	1
2	902	99	9	11	1	-1
3	99	11	9	0	-9	10

Hence $\gcd(1001, 100001) = 11$

We can now utilize the Extended Euclidean Algorithm to find the linear combination. We do this by going backwards from the Euclidean Algorithm, isolating the remainders, and then inserting the new remainders inside of the equations. We isolate the remainders going backwards as follows

$$\begin{aligned}11 &= 902 - 99 \cdot 9\\ 99 &= 1001 - 902\end{aligned} \tag{13}$$

Now we can insert the equation of 99 inside the equation of the remainder 11, and then write it out as a linear combination as follows

$$\begin{aligned}11 &= 902 - 9 \cdot (1001 - 902)\\ 11 &= 10 \cdot 902 - 9 \cdot 1001\end{aligned} \tag{14}$$

Therefore the linear combination is $\gcd(1001, 100001) = 11 = 10 \cdot 902 - 9 \cdot 1001$.

Exercise D.8. Show that an inverse of a modulo m, where a is an integer and m $>$ 2 is a positive integer, does not exist if gcd(a, m) $>$ 1.

Let $\neg P$ be the statement "$\gcd(a, m) > 1$", and $\neg Q$ be the statement "an inverse of a modulo m does not exist". The statement is then $\neg P \to \neg Q$.

We will prove by contraposition, i.e. $Q \to P$ (Inverse exists $\to \gcd(a, m) = 1$). Suppose an inverse of a modulo m exists where $a \in \mathbb{Z}$, $m \in \mathbb{Z}_{>2}$, then some $x \in \mathbb{Z}$ exists s.t. $ax \equiv 1 \pmod{m}$. Thus, by definition

$$\begin{aligned}&m \mid ax - 1 \leftrightarrow ax - 1 = mc, \quad c \in \mathbb{Z}\\ &\leftrightarrow ax - mc = 1 \leftrightarrow ax + m(-c) = 1\end{aligned} \tag{15}$$

Recall that by the definition of Bezout's theorem, for some $s, t \in \mathbb{Z}$ there exists a linear combination s.t. $sa + tb = \gcd(a, b)$. Thus $\gcd(a, m)$ must be 1 (statement P). Therefore by contraposition, the initial statement is proven: if $\gcd(a, m) > 1$ then an inverse of a modulo m does not exist. □

Exercise E.20. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences x ≡ 2 (mod 3), x ≡ 1 (mod 4), and x ≡ 3 (mod 5).

By the Chinese Remainder theorem proof in the book, we will define $m = 3 * 4 * 5 = 60$. Now we can find M_1, M_2, M_3 by $M_k = \frac{m}{m_k}$ as follows

$$M_1 = \frac{60}{3} = 20, \qquad M_2 = \frac{60}{4} = 15, \qquad M_3 = \frac{60}{5} = 12 \tag{16}$$

We see that the inverse of 2 mod 3 is $y_1 = 2$, since $2 * 2 \equiv 1$ mod 3. Likewise, the inverse of 3 mod 4 is $y_2 = 3$ since $3 * 3 \equiv 1$ mod 4, and the inverse of 2 mod 5 is $y_3 = 3$ since $2 * 3 \equiv 1$ mod 5. Then we can utilize from the proof

$$\begin{aligned} x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 * 20 * 2 + 1 * 15 * 3 + 3 * 12 * 3 \\ \to 80 + 45 + 108 = 233 \equiv 233 \text{ mod } 60 = 53 \equiv 53 \text{ mod } 60 \end{aligned} \tag{17}$$

Therefore all the solutions to the system of congruences are $x \equiv 53$ mod 60 and all other solutions share the same remainder 53.

Exercise E.22. Solve the system of congruence x ≡ 3 (mod 6) and x ≡ 4 (mod 7) using the method of back substitution.

We will use back substitution to solve the system of congruence

$$x \equiv 3 \pmod{6}, \qquad x \equiv 4 \pmod{7} \tag{18}$$

Then that is the same thing as writing on the form $a = bq + r$, and substituting x for the next congruence as follows

$$\begin{aligned} x = 6t + 3 \to 6t + 3 \equiv 4 \pmod{7} \to 6t \equiv 1 \pmod{7} \\ \to t \equiv 6 \pmod{7} \to t = 7v + 6 \end{aligned} \tag{19}$$

Inserting t into the original equation of x and finding the mod

$$\begin{aligned} &x = 6(7v + 6) + 3 \to 42u + 36 + 3 = 42u + 39 \\ &x \equiv 39 \pmod{42} \end{aligned} \tag{20}$$

Therefore the solved congruence is $x \equiv 39 \pmod{42}$ using back substitution.