3 More on numbers

3.1 Basic exercises

2. Find the gcd of 21212121 and 12121212.

   Using Euclid's Algorithm:

$$\begin{aligned} \gcd(21212121, 12121212) &= \gcd(12121212, 9090909) \\ &= \gcd(9090909, 3030303) \\ &= 3030303 \end{aligned} \tag{1}$$

3. Prove that for all positive integers m and n, and integers k and l,

$$\gcd(m, n) | (k \cdot m + l \cdot n) \tag{2}$$

$$\begin{gathered} \forall m, n \in \mathbb{Z}^+ : \gcd(m, n) | n \iff \\ \forall m, n \in \mathbb{Z}^+ : \exists a \in \mathbb{Z} : a \cdot \gcd(m, n) = m \\ \forall m, n \in \mathbb{Z}^+ : \exists a \in \mathbb{Z} : \forall k \in \mathbb{Z} : (a \cdot k) \cdot \gcd(m, n) = k \cdot m \end{gathered} \tag{3}$$

$$\begin{gathered} \forall m, n \in \mathbb{Z}^+ : \gcd(m, n) | n \iff \\ \forall m, n \in \mathbb{Z}^+ : \exists b \in \mathbb{Z} : b \cdot \gcd(m, n) = n \iff \\ \forall m, n \in \mathbb{Z}^+ : \exists b \in \mathbb{Z} : \forall l \in \mathbb{Z} : (b \cdot l) \cdot \gcd(m, n) = l \cdot n \end{gathered} \tag{4}$$

Adding (3) and (4) gives:

$$\begin{aligned} \forall m, n \in \mathbb{Z}^+ : \exists a, b \in \mathbb{Z} : \forall k, l \in \mathbb{Z} : (a \cdot k) \cdot \gcd(m, n) + (b \cdot l) \cdot \gcd(m, n) = k \cdot m + l \cdot n \iff \\ \forall m, n \in \mathbb{Z}^+ : \exists a, b \in \mathbb{Z} : \forall k, l \in \mathbb{Z} : (a \cdot k + b \cdot l) \cdot \gcd(m, n) = k \cdot m + l \cdot n \implies \\ \forall m, n \in \mathbb{Z}^+ : \forall k, l \in \mathbb{Z} : \gcd(m, n) | k \cdot m + l \cdot n \end{aligned} \tag{5}$$

4. Find integers x and y such that $x \cdot 30 + y \cdot 22 = \gcd(30, 22)$. Now find integers x' and y' with $0 \leq y' < 30$ such that $x' \cdot 30 + y' \cdot 22 = \gcd(30, 22)$

   gcd(30, 22) = 2
   $x = 3$ and $y = -4$:

$$\begin{aligned} & x \cdot 30 + y \cdot 22 \\ =& 90 - 88 \\ =& 2 \\ =& \gcd(30, 22) \end{aligned} \tag{6}$$

   $y = 11$ and $x = -8$

$$\begin{aligned} & x \cdot 30 + y \cdot 22 \\ =& -8 \cdot 30 + 11 \cdot 22 \\ =& -240 + 242 \\ =& 2 \\ =& \gcd(30, 22) \end{aligned} \tag{7}$$

5. Prove that for all positive integers n and primes p, if $n^2 \equiv 1 (\text{mod } p)$ then either $n \equiv 1 (\text{mod } p)$ or $n \equiv -1 (\text{mod } p)$.

$$\begin{aligned}
n^2 \equiv 1(\text{mod } p) &\iff \\
n^2 - 1 \equiv 0(\text{mod } p) &\iff \\
p|n^2 - 1 &\iff \\
p|(n-1)(n+1) &\iff \\
\text{Since } p \text{ is prime: } p|(n-1) \vee p|(n+1) &\iff \\
(n-1) \equiv 0(\text{mod } p) \vee (n+1) \equiv 0(\text{mod } p) &\iff \\
n \equiv 1(\text{mod } p) \vee n \equiv -1(\text{mod } p) &\text{ as required}
\end{aligned} \tag{8}$$

3.2 Core exercises

1. Prove that for all positive integers m and n, $\gcd(m, n) = m$ iff $m|n$.

   $(\Longrightarrow)$

$$\begin{aligned}
\text{Assume: } \gcd(m,n) = m &\Longrightarrow \\
\forall m, n \in \mathbb{Z} : \gcd(m,n)|n &\Longrightarrow \\
m|n &\text{ as required}
\end{aligned} \tag{9}$$

   $(\Longleftarrow)$

$$\begin{aligned}
&m|n \\
\forall m, n \in \mathbb{Z} : &\gcd(m,n)|m \\
\forall m, n \in \mathbb{Z} : &\gcd(m,n)|m \wedge m|n \Longrightarrow \\
&m|\gcd(m,n) \\
\forall m, n \in \mathbb{Z} : &m|\gcd(m,n) \wedge \gcd(m,n)|m \iff \\
&\gcd(m,n) = m
\end{aligned} \tag{10}$$

2. Let m and n be positive integers with $\gcd(m, n) = 1$. Prove that for every natural number k,

$$m|k \wedge n|k \iff m \cdot n|k$$

   $(\Longrightarrow)$

$$\begin{aligned}
m|k \wedge n|k &\iff \\
\frac{m \cdot n}{\gcd(m,n)}|k &\iff \\
\frac{m \cdot n}{1}|k &\iff \\
m \cdot n|k &\text{ as required}
\end{aligned} \tag{11}$$

   $(\Longleftarrow)$

$$\begin{aligned}
m \cdot n|k &\iff \\
\exists c \in \mathbb{Z} : c \cdot m \cdot n = k &\iff \\
\exists c \in \mathbb{Z} : (c \cdot m) \cdot n = k \wedge (c \cdot n) \cdot m = k &\iff \\
n|k \wedge m|k &\text{ as required}
\end{aligned} \tag{12}$$

3. Prove that for all positive integers a, b, c, if $\gcd(a, c) = 1$ then $\gcd(a \cdot b, c) = \gcd(b, c)$).

$$\begin{aligned}
&\gcd(a \cdot b, c)\\
=&\gcd(\gcd(a, c) \cdot b, c)\\
=&\gcd(1 \cdot b, c)\\
=&\gcd(b, c) \text{ as required}
\end{aligned} \tag{13}$$

4. Prove that for all positive integers m and n, and integers i and j:

$$n \cdot i \equiv n \cdot j (\text{mod } m) \iff i \equiv j (\text{mod } \frac{m}{\gcd(m, n)}) \tag{14}$$

($\implies$)

$$\begin{gathered}
n \cdot i \equiv n \cdot j (\text{mod } m) \iff\\
\frac{n}{\gcd(m,n)} \cdot i \equiv \frac{n}{\gcd(m,n)} \cdot j (\text{mod } \frac{m}{\gcd(m,n)}) \implies\\
\text{since } \frac{n}{\gcd(m,n)} \text{ is coprime with } \frac{m}{\gcd(m,n)}, \text{ it must have a multiplicative inverse in } \mathbb{Z}_{\frac{m}{\gcd(m,n)}} \implies\\
\frac{n}{\gcd(m,n)} \cdot \left[\frac{n}{\gcd(m,n)}\right]_m^{-1} \cdot i \equiv \frac{n}{\gcd(m,n)} \cdot \left[\frac{n}{\gcd(m,n)}\right]_m^{-1} \cdot j (\text{mod } \frac{m}{\gcd(m,n)}) \iff\\
i \equiv j (\text{mod } \frac{m}{\gcd(m,n)}) \text{ as required}
\end{gathered} \tag{15}$$

($\impliedby$)

$$\begin{gathered}
i \equiv j (\text{mod } \frac{m}{\gcd(m,n)} \implies\\
\gcd(m,n) \cdot i \equiv \gcd(m,n) \cdot j (\text{mod } m) \implies\\
\frac{n}{\gcd(m,n)} \cdot \gcd(m,n) i \equiv \frac{n}{\gcd(m,n)} \cdot \gcd(m,n) \cdot j (\text{mod } m) \implies\\
n \cdot i \equiv n \cdot j (\text{mod } m) \text{ as required}
\end{gathered} \tag{16}$$

5. Prove that for all positive integers m, n, p, q such that $\gcd(m, n) = \gcd(p, q) = 1$, if $q \cdot m = p \cdot n$ then $m = p$ and $n = q$.

$$\begin{gathered}
q \cdot m = p \cdot n \land \gcd(m,n) = 1 \land \gcd(p,q) = 1 \iff\\
m | p \land q | n\\
\exists i, j \in \mathbb{Z} : i \cdot m = p \land j \cdot q = n \iff\\
\exists i, j \in \mathbb{Z} : i \cdot j \cdot q \cdot m = p \cdot n \iff\\
\exists i, j \in \mathbb{Z} : i \cdot j \cdot q \cdot m = q \cdot m \iff\\
i = 1 \land j = 1 \iff\\
p = m \land n = q \text{ as required}
\end{gathered} \tag{17}$$

6. Prove that for all positive integers a and b, $\gcd(13 \cdot a + 8 \cdot b, 5 \cdot a + 3 \cdot b) = \gcd(a, b)$.

   Using Euclid's algorithm:

$$\begin{aligned}
&gcd(13 \cdot a + 8 \cdot b, 5 \cdot a + 3 \cdot b)\\
=&gcd(5 \cdot a + 3 \cdot b, 3 \cdot a + 2 \cdot b)\\
=&gcd(3 \cdot a + 2 \cdot b, 2 \cdot a + b)\\
=&gcd(2 \cdot a + b, a + b)\\
=&gcd(a + b, a)\\
=&gcd(a, b) \text{ as required}
\end{aligned} \tag{18}$$

7. Let n be an integers

   (c) Conclude that if p is a prime number greater than 3, then $p^2 - 1$ is divisible by 24.

   Take an arbitrary prime numbers $p > 3$.
   Since p is prime and $p \neq 3$: $3 \not| p \implies p^2 \equiv 1 (\text{mod } 3)$ from part (a)
   All prime numbers except 2 are odd. $p > 3 \implies p \neq 2 \implies p^2 \equiv 1 (\text{mod } 8)$ from part (b)

$$\begin{gathered} p^2 \equiv 1 (\text{mod } 3) \wedge p^2 \equiv 1 (\text{mod } 8) \iff \\ p^2 - 1 \equiv 0 (\text{mod } 3) \wedge p^2 - 1 \equiv 0 (\text{mod } 8) \iff \\ \exists i, j \in \mathbb{Z} : p = 3 \cdot i \wedge p = 8 \cdot j \iff \\ \exists i, j \in \mathbb{Z} : p^2 - 1 = 9 \cdot (8 \cdot j) - 8 \cdot (3 \cdot i) \iff \\ \exists i, j \in \mathbb{Z} : p^2 - 1 = 24 \cdot (3 \cdot j - i) \iff \\ p^2 - 1 \equiv 0 (\text{mod } 24) \iff \\ p^2 \equiv 1 (\text{mod } 24) \end{gathered} \tag{19}$$

8. Prove that $n^{13} \equiv n (\text{mod } 10)$ for all integers n.

$$\begin{gathered} \text{Using Fermat's Little Theorem :} \\ n^2 \equiv n (\text{mod } 2) \iff \\ n^{12} \equiv n^6 (\text{mod } 2) \iff \\ n^{12} \equiv n^3 (\text{mod } 2) \iff \\ n^{13} \equiv n^4 (\text{mod } 2) \iff \\ n^{13} \equiv n (\text{mod } 2) \\ n^{13} - n \equiv 0 (\text{mod } 2) \end{gathered} \tag{20}$$

$$\begin{gathered} \text{Using Fermat's Little Theorem :} \\ n^5 \equiv n (\text{mod } 5) \iff \\ n^{10} \equiv n^2 (\text{mod } 5) \iff \\ n^{13} \equiv n^5 (\text{mod } 5) \iff \\ n^{13} \equiv n (\text{mod } 5) \iff \\ n^{13} - n \equiv 0 (\text{mod } 5) \end{gathered} \tag{21}$$

$$\begin{gathered} n^{13} - n = 0 (\text{mod } 2) \wedge n^{13} - n = 0 (\text{mod } 5) \iff \\ \exists i, j \in \mathbb{Z} : 2 \cdot i = n^{13} - n \wedge 5 \cdot j = n^{13} - n \iff \\ \exists i, j \in \mathbb{Z} : n^{13} - n = 5 \cdot (2 \cdot i) - 4 \cdot (5 \cdot j) \iff \\ \exists i, j \in \mathbb{Z} : n^{13} - n = 10 \cdot (i - 2 \cdot j) \iff \\ n^{13} - n \equiv 0 (\text{mod } 10) \iff \\ n^{13} \equiv n (\text{mod } 10) \text{ as required} \end{gathered} \tag{22}$$

9. Prove that for all positive integers l, m and n, if $\gcd(l, m \cdot n) = 1$ then $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$.

   This is equivalent to the contrapositive:
   If $\gcd(l, m) \neq 1 \vee \gcd(l, n) \neq 1$ then $\gcd(l, m \cdot n) \neq 1$

Let $i = \gcd(l, m)$ and $j = \gcd(l, n)$.

$$\begin{gathered} i|l \wedge i|m \iff \\ i|l \wedge i|m \cdot n \iff \\ \exists k \in \mathbb{Z} : \gcd(l, m \cdot n) = k \cdot i \iff \\ (i \neq 1 \implies \gcd(l, m \cdot n) \neq 1) \\ (\gcd(l, m) \neq 1 \implies \gcd(l, m \cdot n) \neq 1) \end{gathered} \tag{23}$$

$$\begin{gathered} j|l \wedge j|n \iff \\ j|l \wedge j|m \cdot n \iff \\ \exists k \in \mathbb{Z} : \gcd(l, m \cdot n) = k \cdot j \iff \\ (j \neq 1 \implies \gcd(l, m \cdot n) \neq 1) \iff \\ (\gcd(l, n) \neq 1 \implies \gcd(l, m \cdot n) \neq 1) \end{gathered} \tag{24}$$

So $\gcd(l, n) \neq 1 \vee \gcd(l, m) \neq 1 \implies \gcd(l, m \cdot n) \neq 1$ as required.
Since the contrapositive is true, the original statement must be true.

10. Solve the following congruences:

(a) $77 \cdot x \equiv 11 (\text{mod } 40)$

$$\begin{gathered} 77 \cdot x \equiv 11 (\text{mod } 40) \iff \\ -3 \cdot x \equiv -29 (\text{mod } 40) \iff \\ 3 \cdot x \equiv 29 (\text{mod } 40) \iff \\ \exists k \in \mathbb{Z} : 3 \cdot x = 29 + 40 \cdot k \\ \text{By inspection } 3|29 + 40 \cdot 1 \iff \\ 3|69 \iff \\ x \equiv \frac{69}{3} (\text{mod } 40) \iff \\ x \equiv 23 (\text{mod } 40) \end{gathered} \tag{25}$$

(b) $12 \cdot y \equiv 30 (\text{mod } 54)$

$$\begin{gathered} 12 \cdot y \equiv 30 (\text{mod } 54) \iff \\ \exists k \in \mathbb{Z} : 12 \cdot y = 30 + 54 \cdot k \\ \text{By inspection } 12|30 + 54 \iff \\ 12|30 + 54 \iff \\ y \equiv \frac{84}{12} (\text{mod } 54) \iff \\ y \equiv 7 (\text{mod } 54) \end{gathered} \tag{26}$$

(c) $13 \equiv z (\text{mod } 21) \wedge 3 \cdot z \equiv 2 (\text{mod } 17)$

$$\begin{gathered} 13 \equiv z (\text{mod } 21) \wedge 3 \cdot z \equiv 2 (\text{mod } 17) \iff \\ \exists k \in \mathbb{Z} : z = 13 + k \cdot 21 \wedge 3 \cdot z \equiv 2 (\text{mod } 17) \iff \end{gathered} \tag{27}$$

Substitute in $z = 13 + k \cdot 21$ into$3 \cdot z \equiv 2(\text{mod } 17)$

$$\begin{aligned}
\exists k \in \mathbb{Z} : 3 \cdot 13 + 63 \cdot k &\equiv 2(\text{mod } 17) \iff \\
63 \cdot k &\equiv 2 - 39(\text{mod } 17) \iff \\
12 \cdot k &\equiv 14(\text{mod } 17) \iff \\
\text{By inspection } 12 \cdot 4 &\equiv 14(\text{mod } 17)) \iff \\
k &\equiv 4(\text{mod } 17) \\
z &= 13 + 4 \cdot 21(\text{mod } 17) \iff \\
z &= 13 + 16(\text{mod } 17) \iff \\
z &= 12(\text{mod } 17)
\end{aligned} \tag{28}$$

11. What is the multiplicative inverse of (a) 2 in $\mathbb{Z}_7$, (b) 7 in $\mathbb{Z}_{40}$ and (c) 13 in $\mathbb{Z}_{23}$?
    (a) 4 by inspection
    (b) 23 by inspection
    (c) 16 by inspection

12. Prove that $[22^{12001}]_{175}$ has a multiplicative inverse in $\mathbb{Z}_{175}$

$$\begin{aligned}
22^{12001} &= 22 \cdot (22^4)^{3000} \iff \\
22^{12001} &\equiv 22 \cdot 1(\text{mod } 5) \iff \\
22^{12001} - 22 &\equiv 0(\text{mod } 5)
\end{aligned} \tag{29}$$

$$\begin{aligned}
22^{12001} &= 22 \cdot (22^6)^{2000} \iff \\
22^{12001} &\equiv 22 \cdot 1(\text{mod } 7) \iff \\
22^{12001} - 22 &\equiv 0(\text{mod } 7)
\end{aligned} \tag{30}$$

$$\begin{aligned}
22^{12001} - 22 \equiv 0(\text{mod } 5) \land 22^{12001} - 22 \equiv 0(\text{mod } 7) &\iff \\
\exists i, j \in \mathbb{Z} : 5 \cdot i = 22^{12001} - 22 \land 7 \cdot j = 22^{12001} - 22 &\iff \\
\exists i, j \in \mathbb{Z} : 22^{12001} - 22 \equiv 15 \cdot (7 \cdot j) - 14 \cdot (5 \cdot i) &\iff \\
\exists i, j \in \mathbb{Z} : 22^{12001} - 22 \equiv 35 \cdot (5 \cdot j - 2 \cdot i) &\iff \\
22^{12001} - 22 \equiv 0(\text{mod } 35) &\iff \\
\exists k \in \{0, 1, 2, 3, 4\} : 22^{12001} - 22 \equiv 35 \cdot k(\text{mod } 175) &\iff \\
\exists k \in \{0, 1, 2, 3, 4\} : 22^{12001} \equiv 35 \cdot k + 22(\text{mod } 175)& \\
\forall k \in \{0, 1, 2, 3, 4\} : 35 \cdot k + 22 \text{ is coprime to } 175 &\iff \\
\forall k \in \{0, 1, 2, 3, 4\} : 35 \cdot k + 22 \text{ has a multiplicative inverse in } \mathbb{Z}_m &\iff \\
22^{12001} \text{ has a multiplicative inverse in } \mathrm{Z}_m&
\end{aligned} \tag{31}$$

3.3 Optional exercises

1. Let a and b be natural numbers such that $a^2 | b \cdot (b + a)$. Prove that $a | b$.
   This is the same as the contrapositive $a \nmid b \implies a^2 \nmid b \cdot (b + a)$:

$$\begin{aligned}
a \nmid b &\iff \\
\forall i \in \mathbb{Z} : i \cdot a \neq b &\iff \\
\forall i \in \mathbb{Z} : i \cdot a^2 \neq a \cdot b&
\end{aligned} \tag{32}$$

$$\begin{aligned} a \nmid b &\iff \\ a^2 \nmid b^2 &\iff \\ \forall j \in \mathbb{Z} : j \cdot a^2 \neq b^2 & \end{aligned} \tag{33}$$

Combining (32) and (33) gives:

$$\begin{aligned} \forall i, j \in \mathbb{Z} : i \cdot a^2 + j \cdot a^2 \neq a \cdot b + b^2 &\iff \\ \forall k \in \mathbb{Z} : k \cdot a^2 \neq b \cdot (b + a) &\iff \\ a^2 \nmid b \cdot (b + a) & \text{ as required} \end{aligned} \tag{34}$$

Since we have proved the contrapositive; we have proved the original statement.

2. Prove the converse of (1.3.1): For all natural numbers n and s, if there exists a natural number q such that $(2 \cdot n + 1)^2 \cdot s + t_n = t_q$, then s is a triangular number.

$$\begin{aligned} (2 \cdot n + 1)^2 \cdot s + \frac{n}{2}(n + 1) = \frac{q}{2}(q + 1) &\iff \\ (2 \cdot n + 1)^2 \cdot s = \frac{q}{2}(q + 1) - \frac{n}{2}(n + 1) &\iff \\ 2 \cdot (2 \cdot n + 1)^2 \cdot s = q^2 + q - n^2 - n &\iff \\ 2 \cdot s = \frac{(q - n) \cdot (q + n + 1)}{(2 \cdot n + 1)^2} &\iff \\ 2 \cdot s = \frac{q - n}{2 \cdot n + 1} \cdot \frac{q + n + 1}{2 \cdot n + 1} &\iff \\ s = \frac{1}{2} \cdot \frac{q - n}{2 \cdot n + 1} \cdot \left(\frac{q - n}{2 \cdot n + 1} + 1 \right) & \end{aligned} \tag{35}$$

$$\begin{aligned} s \in \mathbb{Z} &\iff \\ \frac{1}{2} \cdot \frac{q - n}{2 \cdot n + 1} \cdot \left(\frac{q - n}{2 \cdot n + 1} + 1 \right) \in \mathbb{Z} &\iff \\ \frac{q - n}{2 \cdot n + 1} \cdot \left(\frac{q - n}{2 \cdot n + 1} + 1 \right) \in \mathbb{Z} & \end{aligned} \tag{36}$$

To prove that this is a triangle number, we must prove that $\frac{q-n}{2 \cdot n+1} \in \mathbb{Z}$. I will do this by contradiction. Assume $\exists k \in \mathbb{Q} : k \cdot (k + 1) \in \mathbb{Z}$.

$$\begin{aligned} \exists k \in \mathbb{Q} : k \cdot (k + 1) \in \mathbb{Z} &\iff \\ \exists a, b \in \mathbb{Z} : \frac{b}{a} \cdot \frac{b + a}{a} \in \mathbb{Z} &\iff \\ \exists a, b \in \mathbb{Z} : \frac{b \cdot (b + a)}{a^2} \in \mathbb{Z} :&\iff \\ a^2 | b \cdot (b + a) &\implies \\ a | b \text{ from (34)} &\iff \\ \frac{b}{a} \in \mathbb{Z} & \end{aligned} \tag{37}$$

However this contradicts our original assumption that $\frac{b}{a} \in \mathbb{Q}$. So this cannot be true and hence $k \cdot (k + 1) \in \mathbb{Z} \implies k \in \mathbb{Z}$.
Since we know that $\cdot \frac{q-n}{2 \cdot n+1} \cdot \left(\frac{q-n}{2 \cdot n+1} + 1 \right) \in \mathbb{Z}$, we also know that $\frac{q-n}{2 \cdot n+1} \in \mathbb{Z}$.
This proves that s is a triangular number $(t_{\frac{q-n}{2 \cdot n+1}})$ – as required.

3. Informally justify the correctness of the following alternative algorithm for computing the gcd of two positive integers:

```
let rec gcd0(m, n) = if m = n then m
  else let p = min m n
   and q = max m n
    in gcd0(p, q - p)
```

Proof by Loop Invariant:
Case $m = n$. If $m = n$, then $\gcd(m, n) = m$. In this case, the algorithm terminates and returns m. So the algorithm is correct in this case.

Case $m > n$. If $m > n$, then the algorithm calls itself on $n, m - n$.
$m - n < m$ so the problem has been reduced in size.
$m - n > 0$ and $\gcd(m, n) = \gcd(n, m - n$ for all m, n. So the result of the algorithm is still the same.

Case $m < n$: Same argument as $(m > n)$ with m and n reversed.

Since for every case the end result of the algorithm is unchanged and the algorithm terminates in every case; it must calculate the $\gcd(m, n)$ correctly. Hence the algorithm is correct.