Homework 10

Mark Petersen

Sections 18 and 19

18. The Extended Euclidean Algorithm

Exercise 18.1. For each pair of numbers a, b below, calculate GCD (a, b) and find $x, y \in \mathbb{Z}$ such that GCD $(a, b) = ax + by$.

a) Take $a = 15$ and $b = 27$.

Using the switching algorithm we can find the GCD (a, b)

$$\begin{aligned} 27 &= 1 \cdot 15 + 12 \\ 15 &= 1 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 \end{aligned}$$

which shows that GCD $(a, b) = 3$. We can solve for x and y using the steps in the switch algorithm.

$$\begin{aligned} 3 &= 15 - 12 \\ &= 15 - (27 - 15) \\ &= 2 \cdot 15 - 1 \cdot 27 \\ &= x \cdot 15 + y \cdot 27, \end{aligned}$$

with $x = 2$ and $y = -1$.

b) Take $a = 29$ and $b = 23$.

Using the switching algorithm we can find the GCD (a, b)

$$\begin{aligned} 29 &= 1 \cdot 23 + 6 \\ 23 &= 3 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + 1, \end{aligned}$$

which shows that GCD $(a, b) = 1$. We can solve for x and y using the steps in the switch algorithm.

$$\begin{aligned} 1 &= 6 - 5 \\ &= 6 - (23 - 3 \cdot 6) \\ &= 4 \cdot 6 - 23 \\ &= 4\,(29 - 23) - 23 \\ &= 4 \cdot 29 - 5 \cdot 23 \end{aligned}$$

with $x = 4$ and $y = -5$.

c) Take $a = 91$ and $b = 133$.

Using the switching algorithm we can find the GCD (a, b)

$$\begin{aligned} 133 &= 1 \cdot 91 + 42 \\ 91 &= 2 \cdot 42 + 7 \\ 42 &= 6 \cdot 7 + 0 \end{aligned}$$

which shows that $\text{GCD}(a,b) = 7$. We can solve for x and y using the steps in the switch algorithm.

$$\begin{aligned} 7 &= 91 - 2 \cdot 42 \\ &= 91 - 2(133 - 91) \\ &= 3 \cdot 91 - 2 \cdot 133 \end{aligned}$$

with $x = 3$ and $y = -2$.

d) Take $a = 221$ and $b = 377$

Using the switching algorithm we can find the $\text{GCD}(a,b)$

$$\begin{aligned} 377 &= 1 \cdot 221 + 156 \\ 221 &= 1 \cdot 156 + 65 \\ 156 &= 2 \cdot 65 + 26 \\ 65 &= 2 \cdot 26 + 13 \\ 26 &= 2 \cdot 13 \end{aligned}$$

which shows that $\text{GCD}(a,b) = 13$. We can solve for x and y using the steps in the switch algorithm.

$$\begin{aligned} 13 &= 65 - 2 \cdot 26 \\ &= 65 - 2(156 - 2 \cdot 65) \\ &= 5 \cdot 65 - 2 \cdot 156 \\ &= 5(221 - 156) - 2 \cdot 156 \\ &= 5 \cdot 221 - 7 \cdot 156 \\ &= 5 \cdot 221 - 7(377 - 221) \\ &= 12 \cdot 221 - 7 \cdot 377 \end{aligned}$$

with $x = 12$ and $y = -7$.

Exercise 18.2. Let $a, n \in \mathbb{Z}$.Assume that $\text{GCD}(a,n) = 1$. Prove that there is some $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod n$.

Proof: We suppose directly that $\text{GCD}(a,n) = 1$ with $a, n \in \mathbb{Z}$. From Thm 18.5 we know that the $\text{GCD}(a,n)$ is the smallest positive integral linear combination of a and n. Thus we can write $1 = ax + ny$ for some $x, y \in \mathbb{Z}$. Manipulating this equation yields $1 - ax = ny$. Thus we can see that $n \mid 1 - ax$ which is equivalent to $ax \equiv 1 \bmod n$. By letting $x = b$, we have shown that if the $\text{GCD}(a,n) = 1$, then there exists some $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod n$. ■

Exercise 18.3. The following exercise proves the existence and uniqueness of the lowest terms representation of a rational number.

a) Let $a, b \in \mathbb{Z}$, not both zero, and let $d = \text{GCD}(a,b)$. Prove that

$$\text{GCD}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Proof: We suppose directly that $d = \text{GCD}(a,b)$. From Thm 18.5 we can write $d = ax + by$ for some $x, y \in \mathbb{Z}$. We know d must be positive so we can divide both sides by d to get

$$1 = \frac{a}{d}x + \frac{b}{d}y.$$

Since $d \mid a$ and $d \mid b$ we know that $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Thus, using Thm 18.10 we can conclude that

$$\text{GCD}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

■

b) Prove that any rational number can be represented as a fraction $\frac{r}{s}$ with $r, s \in \mathbb{Z}$ and $s \neq 0$ and $\text{GCD}(r, s) = 1$.
Proof: Let $p_i \in \mathbb{Z}$ and $q_i \in \mathbb{Z} - \{0\}$ where $i \in \mathbb{N}$ is an indexing term. We suppose directly that m is a rational number of the form $\frac{p_1}{q_1}$. We have two cases.

Case 1. Let $\text{GCD}(p_1, q_1) = 1$, then $\frac{p_1}{q_1}$ is already in lowest terms.

Case 2. Let $\text{GCD}(p_1, q_1) = k_1$ for some $k_1 \in \mathbb{N} > 1$, then k_1 divides both p_1 and q_1 such that $p_1 = k_1 p_2$ and $q_1 = k q_2$. We can then write the rational number m as $\frac{p_2}{q_2}$. This process can be repeated until $\text{GCD}(p_n, q_n) = 1$. At this point we can write $m = \frac{p_n}{q_n}$.

■

Therefore, any rational number can be represented as a fraction $\frac{r}{s}$ such that $\text{GCD}(r, s) = 1$.

c) Prove that every rational number has a unique representation, as in part (b), with $s \in \mathbb{N}$.
Proof: We suppose by contradiction that m is a rational number that can be written as $\frac{r}{s}$ and $\frac{a}{b}$ where $r, a \in \mathbb{Z}$, $s, b \in \mathbb{N}$, $r \neq a$, $b \neq s$, $\text{GCD}(r, s) = 1$, and $\text{GCD}(a, b) = 1$. This means that $m = \frac{r}{s} = \frac{a}{b}$. This statement gives us two equations: $r = \frac{sa}{b}$ and $a = \frac{rb}{s}$. From Thm 18.10 we also know that $1 = rx + sy$ and $1 = ak + b\ell$ for some $x, y, k, \ell \in \mathbb{Z}$. We can manipulate these equations to get

$$\begin{aligned} 1 &= rx + sy \\ 1 &= \frac{sa}{b}x + sy \\ b &= s(ax + by), \end{aligned}$$

which shows that $s \mid b$. In a similar manner we get

$$\begin{aligned} 1 &= ak + b\ell \\ 1 &= \frac{rb}{s}k + b\ell \\ s &= b(rk + b\ell), \end{aligned}$$

which shows that $b \mid s$. Since $s \mid b$ and $b \mid s$ we know that $|s| = |b|$. Using this with the fact that $\frac{r}{s} = \frac{a}{b}$, we know that $|r| = |a|$. Under the assumption that $r \neq a$, $b \neq s$, this means that $r = -a$ and $s = -b$. This is a contradiction to the assumption that $s, b \in \mathbb{N}$. Thus we have shown by contradiction that every rational number has a unique representation $\frac{r}{s}$ where $r \in \mathbb{Z}$, $s \in \mathbb{N}$, and $\text{GCD}(r, s) = 1$. ■

Exercise 18.4. Let $a, b \in \mathbb{Z}$, with $b \neq 0$, and let $d = \text{GCD}(a, b)$.

a) Prove or disprove the equality $\text{GCD}(a, b/d) = 1$.
Disproof.: We will disprove the equality $\text{GCD}(a, b/d) = 1$ with a simple contradiction. Let $a = 10$, $b = 4$, then $2 = \text{GCD}(10, 4)$; however, $2 = \text{GCD}(10, 4/2)$. Hence the statement is not true. ■

b) Prove or disprove: If c is a positive common divisor of a and b, and $c = ax + by$ for some $x, y \in \mathbb{Z}$, then $c = d$.
Proof: We want to show that $c = d$ under the prescribed conditions. To this this we will first show that $d \leq c$, and then we will show that $c \leq d$.
$(d \leq c)$: We suppose directly that $a, b \in \mathbb{Z}$, $b \neq 0$, $d = \text{GCD}(a, b)$, $c \mid a$, $c \mid b$, $c \in \mathbb{N}$, and $c = ax + by$ for some $x, y \in \mathbb{Z}$. According to Thm 18.5 we know that d is the smallest positive integral linear combination of a and b. This implies that $d \leq c$.

$(c \leq d)$: We suppose by contradiction that $c \mid a$, $c \mid b$, $c = ax + by$, $d = \text{GCD}\,(a, b)$ and that $c > d$. Since $c \mid a$ and $c \mid b$, then c is a common divisor of a and b. Also since we assume that $c > d$, this means that $\text{GCD}\,(a, b) \neq d$. This is a contradiction. Therefore we know that $c \leq d$.
We have shown that $d \leq c$ and that $c \leq d$. This means that $c = d$. therefore the statement is true. ■

Exercise 18.5. Let $a, b, c, d \in \mathbb{Z}$. Assume that $\text{GCD}\,(a, b) = 1$. Prove that if $c \mid a$ and $d \mid b$, then $\text{GCD}\,(c, d) = 1$.

Proof: We suppose directly that $\text{GCD}\,(a, b) = 1$, $c \mid a$ and that $d \mid b$ with $a, b, c, d \in \mathbb{Z}$. We can write $a = ck$ and $b = d\ell$ for some $k, \ell \in \mathbb{Z}$. From Thm 18.5 we can write $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Substituting in the equalities of a, b yields

$$\begin{aligned} 1 &= ax + by \\ &= (ck)\,x + (d\ell)\,y \\ &= c\,(kx) + d\,(\ell y)\,, \end{aligned}$$

which shows that $\text{GCD}\,(c, d) = 1$ according to Thm 18.5. ■

Exercise 18.6. Let a, b be positive integers. A common multiple of a and b is an integer n such that $a \mid n$ and $b \mid n$. The least common multiple of a and b, written as $\text{LCM}\,(a, b)$, is the smallest positive common multiple of a and b.

a) Determine the LCM of 12 and 18.
   $\text{LCM}\,(12, 18) = 36$
b) Determine the LCM of 21 and 35
   $\text{LCM}\,(21, 35) = 105$
c) Prove that $\text{LCM}\,(a, b) = \frac{ab}{d}$, where $d = \text{GCD}\,(a, b)$.
   Proof: We want to show that if $d = \text{GCD}\,(a, b)$, then theLCM $(a, b) = \frac{ab}{d}$. We do this in two steps. We first show that $\text{LCM}\,(a, b) \leq \frac{ab}{d}$, and then we will show that $\text{LCM}\,(a, b) \geq \frac{ab}{d}$.
   $(\leq)$:We suppose directly that $d = \text{GCD}\,(a, b)$. Let $a' = \frac{a}{d}$ and $b' = \frac{b}{d}$ where $a', b' \in \mathbb{N}$ since $d \mid a$ and $d \mid b$. We can then write the term $\frac{ab}{d}$ as $a'b$ or ab'. From these forms we can see that $a \mid \frac{ab}{d}$ and $b \mid \frac{ab}{d}$. This shows that $\frac{ab}{d}$ is a common multiple of a and b. Thus $\text{LCM}\,(a, b) \leq \frac{ab}{d}$.
   $(\geq)$: We suppose by contradiction that $d = \text{GCD}\,(a, b)$ and $\text{LCM}\,(a, b) < \frac{ab}{d}$. Then there exists a number $m \in \mathbb{N} > 1$ such that $\text{LCM}\,(a, b) = \frac{ab}{dm} < \frac{ab}{d}$. This implies that $\frac{ab}{dm} = az$ and $\frac{ab}{dm} = bw$ for some $z, w \in \mathbb{N}$. Looking closely at the equation $\frac{ab}{dm} = az$ we can reduce it to $\frac{b}{dm} = \frac{b'}{m} = z$, and looking closely at the equation $\frac{ab}{dm} = bw$ we can reduce it to $\frac{a}{dm} = \frac{a'}{m} = w$. But this is a contradiction since it states that $m \mid a'$ and $m \mid b'$ which cant be the case since $d = \text{GCD}(a, b)$, and according to problem 18.3

$$\text{GDC}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{GDC}\,(a', b') = 1.$$

   Therefore, $\text{LCM}\,(a, b) \geq \frac{ab}{d}$.
   BecauseLCM $(a, b) \leq \frac{ab}{d}$ and $\text{LCM}\,(a, b) \geq \frac{ab}{d}$, $\text{LCM}\,(a, b) = \frac{ab}{d}$ if a, b are positive integers, and $b = \text{GCD}\,(a, b)$. ■

19. Prime Numbers

Exercise 19.1. For each of the following integers n, give its canonical prime factorization.

a) $n = 27$.
   $27 = 3 \cdot 3 \cdot 3 = 3^3$
b) $n = 3072$.
   $3072 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^{10} \cdot 3$
c) $n = 60$.
   $60 = 2 \cdot 2 \cdot 5 \cdot 3$

Exercise 19.2. Let p be a prime number, $n \in \mathbb{N}$, and $a_1, \ldots, a_n \in \mathbb{Z}$. Prove that if

$$p \mid a_1 a_2 \cdots a_n$$

then $p \mid a_i$ for some $1 \leq i \leq n$.

Proof: We want to show that the open sentence

$$P(n) : \text{ if } p \mid a_1 a_2 \cdots a_n \text{ then p}|\ a_i \text{ for some } 1\text{≤i≤n}$$

is true with p a prime number, $n \in \mathbb{N}$, and $a_1, \ldots, a_n \in \mathbb{Z}$. We work this by induction.

Base Case: We verify $P(1)$ and $P(2)$. For $P(1)$ we have that if $p \mid a_1$ then $p \mid a_i$for some $1 \leq i \leq n$. Since we only have one a, then $p \mid a_1$. The statement $P(2)$ was proven in Thm 19.5 of the book.

Induction Step: We suppose that $k \in \mathbb{N}$, and that $P(k)$ is true. We want to show that $P(k+1)$ is true which is the statement: if $p \mid a_1 \cdots a_{k+1}$, then $p \mid a_i$ for some $1 \leq i \leq k+1$. Let $b = a_1 \cdots a_k$ such that we can write $p \mid ba_{k+1}$. We know from Thm 19.5 that if $p \mid ba_{k+1}$, then $p \mid b$ or $p \mid a_{k+1}$. This gives us two cases.

Case 1. If $p \mid a_{k+1}$, then were done.
Case 2. If $p \mid b$, then since we suppose $P(k)$ to be true, we know that $p \mid a_i$ for some $1 \leq i \leq k$.

Hence $P(k+1)$ is true. Therefore the open sentence $P(n)$ is true.

■

Exercise 19.3. Let $n > 1$ be a natural number. Prove that the smallest divisor d of n that is greater than 1 is prime.

Proof: We suppose directly that $n > 1$ is a natural number. Any composite divisor m of n can be factored into primes according to fundamental theorem of arithmetic. Since the prime factors of m are always less than m, we know that the a composite number cannot be the smallest divisor greater than 1 of n. Therefore, we only need to look at the unique prime factorization of n, which is

$$n = p_1 p_2 \cdots p_k$$

where $p_1 \leq p_2 \leq \cdots \leq p_k$ are prime numbers, and take the smallest prime number p_1. Hence the smallest divisor d of n that is greater than 1 is prime. ■

Exercise 19.4. The goal of this exercise is to prove that there are infinitely many primes which are congruent to -1 modulo 3. We will do this in a series of steps.

a) Prove that, with only one exception, every prime number is congruent to either 1 or -1 modulo 3.

Proof: Let q be a prime number greater than 3. This means that $3 \nmid q$. Since every 3rd natural number is a multiple of 3, we know that $3 \mid (q+1)$ or $3 \mid (q+2)$ since either $q+1$ or $q+2$ will be a multiple of 3. If $q+2$ is a multiple of three, then $q+2-3 = q-1$ is a multiple of 3. Thus $3 \mid q+1$ or $3 \mid q-1$. This is equivalent to saying that every prime number greater than 3 is congruent to either 1 or -1 modulo 3. The last two prime numbers that we need to investigate are 2 and 3. Well $2+1=3$ which implies $3 \mid 2+1$ thus $2 \equiv -1 \bmod 3$. Lastly $3 \mid 3$ which implies $3 \nmid (3 \pm 1)$ and thus 3 is not congruent to either 1 or -1 modulo 3. Thus we have shown that every prime number other than 3 is congruent to either 1 or -1 modulo 3. ■

b) Prove that for any $n \in \mathbb{N}$ and any $a_1, \ldots, a_n \in \mathbb{Z}$, if each $a_i \equiv 1 \bmod 3$, then the product $a_1 a_2 \cdots a_n \equiv 1 \bmod 3$.
Proof: We want to show that the open sentence

$$P(n): \text{ if each } a_i \equiv 1 \bmod 3 \text{ , then the product } a_1 a_2 \cdots a_n \equiv 1 \bmod 3$$

is true for any $n \in \mathbb{Z}$ and any $a_1, \ldots, a_n \in \mathbb{Z}$. We work this by induction.
Base Case: We verify $P(2)$. We assume that $a_1 \equiv 1 \bmod 3$ and that $a_2 \equiv 1 \mod 3$ which is equivalent to saying $a_1 - 1 = 3m_1$ and $a_2 - 1 = 3m_2$ for some $m_1, m_2 \in \mathbb{Z}$. Using these identities, the product $a_1 a_2$ can be written as

$$\begin{aligned} a_1 a_2 &= (3m_1 + 1)(3m_2 + 1) \\ &= 3 \cdot 3m_1 m_2 + 3m_1 + 3m_2 + 1 \\ &= 3(3m_1 m_2 + m_1 + m_2) + 1 \end{aligned}$$

which can be written as

$$a_1 a_2 - 1 = 3k,$$

where $k = 3m_1 m_2 + m_1 + m_2$. This is equivalent to saying $a_1 a_2 \equiv 1 \bmod 3$. Hence $P(2)$ is true.
Induction Step: We suppose that $P(j)$ is true for some $j \in \mathbb{N}$, and we want to show that $P(j+1)$ is true. We begin with writing the product

$$a_1 a_2 \cdots a_j a_{j+1} = b a_{j+1}.$$

Since we assume $P(j)$ to be true, we know that $b \equiv 1 \bmod 3$. This means that $b = 3y_b + 1$ and $a_{j+1} = 3y_{j+1} + 1$ for some $y_b, y_{j+1} \in \mathbb{Z}$. Taking their product we get

$$\begin{aligned} b a_{j+1} &= (3y_b + 1)(3y_{j+1} + 1) \\ &= 3(3y_b y_{j+1} + y_b + y_{j+1}) + 1 \end{aligned}$$

which can be written as

$$b a_{j+1} = 3\ell + 1$$

where $\ell = 3y_b y_{j+1} + y_b + y_{j+1}$. This is equivalent to saying $b a_{j+1} = a_1 a_2 \cdots a_j a_{j+1} \equiv 1 \bmod 3$. Hence $P(j+1)$ is true. Therefore the open sentence $P(n)$ is true for any $n \in \mathbb{N}$. ■

c) Suppose that $N \in \mathbb{N}$, and $N \equiv -1 \bmod 3$. Prove that N is divisible by some prime p such that $p \equiv -1 \bmod 3$.
Proof: We suppose directly that $N \in n$, and $N \equiv -1 \bmod 3$. N can be factored out into primes according to the fundamental theorem of arithmetic as

$$N = p_1 p_2 \cdots p_k.$$

From part a) we know that every prime other than 3 is congruent to either 1 or -1 modulo 3. Since $N = 3m - 1$ for some $m \in \mathbb{N}$, we know that

$3 \nmid N$ such that $3 \neq p_i$ for any $1 \leq i \leq k$. Thus all the prime factors of N are either congruent to either 1 or -1 modulo 3. Let q denote the product of all the prime factors of N that are congruent to 1 modulo 3. From part b) we know that q is congruent to 1 module 3. Hence we can write N as

$$N = qx_1x_2 \cdots x_j$$

where x_i denotes a prime that is congruent to 1 module 3 and $j \leq k$. If $j = k$, then let $q = 1$ with no loss in generality. This just means that there are no prime factors of n that are congruent to 1 modulo 3. According to lemma A.2, the product $x_1x_2 \cdots x_j$ is congruent to -1 modulo 3 if and only if j is odd. So if j is even, then $qx_1x_2 \cdots x_j$ is congruent to 1 modulo 3 according to part b), and if j is odd, then $x_1x_2 \cdots x_j$ can be written as $3\gamma - 1$. Hence

$$\begin{aligned} N &= qx_1x_2 \cdots x_j \\ &= (3m_q + 1)(3\gamma - 1) \\ &= 3(3m_q m_\gamma - m_q + \gamma) - 1, \end{aligned}$$

which is congruent to -1 modulo 3. Therefore, $N \equiv -1 \bmod 3$, then the prime factorization of N contains an odd number of primes that are congruent to -1 modulo 3, and the prime factorization of N does not contain the prime number 3. ■

d) Prove that there are infinitely many primes p that are congruent to -1 modulo 3.
Proof: We suppose directly that S is any finite nonempty set of prime numbers that are congruent to -1 modulo 3. Let

$$N = 3 \underbrace{\prod}_{p \in S} p - 1,$$

so N is divisible by some prime q that is congruent to -1 modulo 3 by Theorem 19.7 and part c) of this problem. Using the division algorithm to divide N by any prime $p \in S$ leaves a remainder of -1. So no prime in S divides N. Hence, q must be a prime that is not in S. Thus the set S cannot include the set of all primes that are congruent to -1 modulo 3. Since no finite set can contain all of the primes that are congruent to -1 modulo 3, then there must be an infinite number of these types of primes. ■

Exercise 19.5. Prove that there are infinitely many primes p such that

$$p \equiv -1 \bmod 4.$$

This proof will be broken up into steps.

a) Prove that, with only one exception, every prime number is congruent to either 1 or -1 modulo 4.
Proof: We suppose directly that q is a prime number greater than 2, then from lemma A.1 we know that q is an odd number so we can write it as

$$q = 2k + 1,$$

where $k \in \mathbb{N}$. k can be either odd or even. This presents two cases. ■

Case 1. If k is odd, then $k = 2\alpha + 1$ where $\alpha \in \mathbb{N}$. Then

$$\begin{aligned} q &= 2(2\alpha + 1) + 1 \\ &= 4\alpha + 3, \\ &= 4(\alpha + 1) - 1 \end{aligned}$$

which is equivalent to $q \equiv -1 \bmod 4$.

Case 2. If k is even, then $k = 2\alpha$. Then

$$\begin{aligned} q &= 2 \cdot 2\alpha + 1 \\ &= 4\alpha + 1 \end{aligned}$$

which is equivalent to $q \equiv 1 \bmod 4$.

Therefore every odd prime is congruent to either 1 or -1 modulo 4. The prime number 2 is neither congruent to either 1 or -1 modulo 4 since

$$\begin{aligned} &2 \neq 4m - 1, \text{ or} \\ &2 \neq 4m + 1, \end{aligned}$$

for any $m \in \mathbb{Z}$. Therefore, every prime number except 2 is congruent to either 1 or -1 modulo 4.

b) Prove that for any $n \in \mathbb{N}$ and any $a_1, \ldots, a_n \in \mathbb{Z}$, if each $a_i \equiv 1 \bmod 4$, then the product $a_1 a_2 \cdots a_n \equiv 1 \bmod 3$.

Proof: We want to show that the open sentence

$$Q\left(n\right): \text{ if each } a_i \equiv 1 \bmod 4, \text{ then } a_1 a_2 \cdots a_n \equiv 1 \bmod 3$$

is true for any $a_1, \ldots, a_n \in \mathbb{Z}$ and any $n \in \mathbb{N}$. We work this by induction.

Base Case: We verify $Q\left(2\right)$. Let $a_1 = 4m_1 + 1$ and $a_2 = 4m_2 + 1$ since $a_i \equiv 1 \bmod 4$ with $m_1, m_2 \in \mathbb{N}$. Their product is

$$\begin{aligned} a_1 a_2 &= \left(4m_1 + 1\right)\left(4m_2 + 1\right) \\ &= 4\left(4m_1 m_2 + m_1 + m_2\right) + 1, \end{aligned}$$

which is congruent to 1 modulo 4. Hence $Q\left(2\right)$ is true.

Induction Step: Let $k \in \mathbb{N}$. We assume that $Q\left(k\right)$ is true and want to show that $Q\left(k+1\right)$ is true. We begin by writing the product

$$a_1 a_2 \cdots a_k a_{k+1} = b a_{k+1},$$

with $b = a_1 a_2 \cdots a_k$. Since we assume $Q\left(k\right)$, we know that $b = 4m_b + 1$ for some $m_b \in \mathbb{N}$. We also assume that $a_{k+1} = 4m_{k+1} + 1$ for some $m_{k+1} \in \mathbb{N}$. We can then write the product as

$$\begin{aligned} b a_{k+1} &= \left(4m_b + 1\right)\left(4m_{k+1} + 1\right) \\ &= 4\left(4m_b m_{k+1} + m_b + m_k\right) + 1, \end{aligned}$$

which is congruent to 1 modulo 4. Hence $Q\left(k+1\right)$ is true. Therefore the open sentence $Q\left(n\right)$ is true. ∎

c) Suppose that $N \in \mathbb{N}$, and $N \equiv -1 \bmod 4$. Prove that N is divisible by some prime p such that $p \equiv -1 \bmod 4$.

Proof: We suppose directly that $N \in \mathbb{N}$ and $N \equiv -1 \bmod 4$. According to the fundamental theorem of arithmetic we can write N as the product of prime

$$N = p_1 p_2 \cdots p_n,$$

we also not that since $N \equiv -1 \bmod 4$, we can write N as

$$N = 4k - 1,$$

for some $k \in \mathbb{N}$. Equating the two equations yields

$$4k - 1 = p_1 p_2 \cdots p_n,$$

which can be written as

$$4k = p_1 p_2 \cdots p_n + 1.$$

According to the division algorithm, at least one of the primes p_i with $1 \leq i \leq n$ divides $4k$ with a remainder of 1. Hence $p_i \equiv -1 \mod 4$. Therefore if $N \equiv -1 \bmod 4$, then N is divisible by some prime p such that $p \equiv -1 \bmod 4$. ■

d) Prove that there are infinitely many primes p that are congruent to -1 modulo 4.

Proof: We suppose directly that S is any finite nonempty set of prime numbers that are congruent to -1 modulo 4. Let

$$N = 4 \underbrace{\prod}_{p \in S} p - 1,$$

so N is divisible by some prime q that is congruent to -1 modulo 4 by Theorem 19.7 and part c) of this problem. Using the division algorithm to divide N by any prime $p \in S$ leaves a remainder of -1. So no prime in S divides N. Hence, q must be a prime that is not in S. Thus the set S cannot include the set of all primes that are congruent to -1 modulo 4. Since no finite set can contain all of the primes that are congruent to -1 modulo 4, then there must be an infinite number of these types of primes. ■

Appendix

Lemma A.1. *Every prime number other than 2 is odd.*

Proof: We suppose directly that p is a prime number and let q be a prime number greater than 2. Since the only positive divisors of a prime number is itself and 1 we know that $q \neq 2m$ for some $m \in \mathbb{N}$, otherwise the prime number q would have 2 as a divisor, at which point it wouldn't be a prime number. Therefore $2 \nmid q$ thus q is odd. Since the prime number $2 = 2k$ for some $k \in \mathbb{N}$, it is even. Thus we have shown that every prime number other than 2 is odd. ∎

Lemma A.2. *Let $p_1, p_2, \ldots, p_k$ be prime numbers such that $p_i \equiv -1 \, mod \, 3$ with $1 \leq i \leq k$. The product $p_1 p_2 \cdots p_k \equiv -1 \, mod \, 3$ if and only if k is odd.*

Proof: Since this is a biconditional statement we must prove both ways.
$(\Longleftarrow)$: We want to show that the open sentence

$$Q(k) : \text{ If } k \text{ is odd, then } p_1 p_2 \cdots p_k \equiv -1 \bmod 3$$

Since we are only concerned with proving the open sentence when k is odd, we can work with the open sentence $P(n) = Q(2n-1)$ where $n \in \mathbb{N}$. We work this by induction.

Base Case: We verify $P(2)$.

$$\begin{aligned} p_1 p_2 p_3 &= \prod_{i=1}^{3} (3m_i - 1) \\ &= (3m_1 - 1)(3m_2 - 1)(3m_3 - 1) \\ &= 3(9m_1 m_2 m_3 - 3m_1 m_2 - 3m_1 m_3 - 3m_2 m_3 + m_1 + m_2 + m_3) - 1 \\ &= 3\alpha - 1, \end{aligned}$$

where $m_i \in \mathbb{N}$, which shows that $P(2)$ is true.

Induction Step: Let $j \in \mathbb{N}$. We suppose that $P(j)$ is true and we want to show that $P(j+1)$ is true. We begin with the product

$$p_1 p_2 \cdots p_{2k-1} p_{2k} p_{2(k+1)-1},$$

where $j = 2k - 1$ and $j + 1 = 2(k+1)$ by how we defined $P(n)$. Since we suppose $P(j)$, we can replace $p_1 p_2 \cdots p_{2k-1}$ with $3\gamma - 1$ with $\gamma \in \mathbb{N}$. This gives us the product

$$\begin{aligned} (3\gamma - 1) p_{2k} p_{2k+1} &= (3\gamma - 1)(3m_{2k} - 1)(3m_{2k+1} - 1) \\ &= 3(9\gamma m_{2k} m_{2k+1} - 3(\gamma m_{2k} + \gamma m_{2k+1} + m_{2k} m_{2k+1}) + \gamma + m_{2k} + m_{2k+1}) - 1 \\ &= 3\beta - 1, \end{aligned}$$

with hence $P(j+1)$ is true. Therefore the open sentence $Q(k)$ is true.

$(\Longrightarrow)$: We suppose by contradiction that $p_1 p_2 \cdots p_k \equiv -1 \bmod 3$ and k is even. Then for $k = 2$ we have

$$\begin{aligned} p_1 p_2 &= (3m_1 - 1)(3m_2 - 1) \\ &= 3(3m_1 m_2 + m_1 m_2) + 1 \\ &= 3\eta + 1, \end{aligned}$$

for some $m_1, m_2, \eta \in \mathbb{N}$. This is a contradiction since $3\eta + 1 \neq 3\xi - 1$ for some $\xi \in \mathbb{N}$. Hence if $p_1 p_2 \cdots p_k \equiv -1 \bmod 3$ then k is odd.

Since we have proven both ways, the lemma is true. ∎