

**Section 11.1**

**1)** Find the positive divisors of the following integers.

a) 72 : 1, 2, 3, 4, 6, 9, 8, 24, 36, and 72.

b) 31 : 1 and 31

c) 123 : 1, 3, 41, and 123

**2)** Prove that if  $h|m$  and  $m|n$ , then  $h|n$ .

$h|m$  means that  $ah = m$ , and  $m|n$  means  $bm = n$ , therefore  $(ab)h = b(ah) = bm = n$ , so  $h|n$ .

**3)** Show that two positive integers divide each other if and only if they are equal.

If  $m$  and  $n$  are positive integers,  $m|n$  means  $am = n$ , and  $n|m$  means  $bn = m$ , with  $a$  and  $b$  positive integers.  $am = n$  implies that  $m \leq n$ , and  $bn = m$  implies that  $n \leq m$ , therefore  $n = m$ , q.e.d.

**4)** Let  $p$  and  $q$  be two prime numbers. If  $p = q + 2$ , then  $p$  and  $q$  are called “twin prime numbers.” Find two pairs of twin prime numbers.

The first pairs of twin primes are (3, 5), (5, 7), (11, 13), (17, 19).

**5)** Prove that  $\gcd(n,m) = \gcd(m,n)$ .

The definition of  $\gcd$  does not rely in any way on the order of the numbers:  $\gcd(n,m)$  is the largest integer that divides both of them.

6) Prove that if  $m$  and  $n$  are both even, then  $\gcd(m, n) = 2 \gcd(m/2, n/2)$ .

Denote  $d = \gcd(m, n)$  and  $d' = \gcd(m/2, n/2)$ .

We have that  $d' | m/2$  and  $d' | n/2$ , so  $2d' | m$  and  $2d' | n$ , so  $2d' | d$ . (\*)

On the other hand,  $2 | m$  and  $2 | n$ , so  $2/d$ , so  $d = 2a$ . Since  $d = 2a$  divides  $2^*m/2$ ,  $a$  divides  $m/2$ , and similarly  $a$  divides  $n/2$ , so  $a$  divides  $d'$ , so  $d = 2a$  divides  $2d'$  (\*\*)

From (\*) and (\*\*) we have that  $d$  and  $d'$  are equal in absolute value. Considering in turn all possibilities for the signs of  $m$  and  $n$ , we easily prove that  $d$  and  $d'$  are actually equal.

7) Prove that if  $n \geq m > 0$ , then  $\gcd(m, n) = \gcd(m, n-m)$ .

Denote  $d = \gcd(m, n)$ , which means  $d | m$  and  $d | n$ , which means  $ad = m$  and  $bd = n$ , therefore  $(b-a)d = n-m$ , so  $d | (n-m)$ . From  $d | m$  and  $d | (n-m)$ , we have that  $d | \gcd(m, n-m)$ . Denoting  $d' = \gcd(m, n-m)$ , this is rewritten  $d | d'$ . (\*)

On the other hand,  $a'd' = m$ , and  $b'd' = n-m$ , so  $(a'+b')d' = m+n-m = n$ , so  $d' | n$ . Therefore  $d' | \gcd(m, n) = d$ . (\*\*)

From (\*) and (\*\*), we have that  $|d| = |d'|$ , and from the fact that  $n \geq m > 0$ , we have  $d = d'$ .

8) Prove that if  $p$  is a prime number and  $0 < h < p$ , then  $\gcd(p, h) = 1$ .

Proof by contradiction: assume that  $\gcd(p, h) = d > 1$ . Since  $d | h$ ,  $d \leq h < p$ , so  $d < p$ . But also  $d | p$ , which contradicts the primality of  $p$ .

9) Use Corollary 11.2 to show that the prime factorization of an integer, as discussed in Theorem 11.5, is unique.

#### ▼ Corollary 11.2

Given integers  $n$ ,  $m$ , and prime integer  $p$ , if  $p | nm$ , then  $p | n$  or  $p | m$  (inclusive).

Let  $\mathbf{n} = \mathbf{p}_1^{k_1} \dots \mathbf{p}_i^{k_i} = \mathbf{q}_1^{h_1} \dots \mathbf{q}_j^{k_j}$  be two factorizations of  $n$ . For them to be different means that:

- A. a factor  $p$  is not on the right-hand side OR
- B. a factor  $q$  is not on the left-hand side OR
- C. the factors themselves are identical, but at least one of the powers is different.

Cases A and B are easily dismissed using the Corollary: If, for instance,  $p_1$  is not found among the  $q_i$ , the Corollary implies that, nevertheless,  $p_1$  divides  $q_1^{h_1}$  or ... or  $q_j^{k_j}$ . Let's choose for example that  $p_1 | q_1^{h_1}$ ; the same corollary now implies that  $p_1 | q_1$ , which is a contradiction.

We are left then with case C:  $n = p_1^{k_1} \dots p_i^{k_i} = p_1^{h_1} \dots p_i^{h_i}$ .

Let's say that  $k_1 < h_1$ ; we simplify by dividing left and right by  $p_1^{k_1}$ , and we are left with  $p_1^{h_1 - k_1}$  on the right-hand side, whereas the left-hand side has no factors of  $p_1$ . From the Corollary, this is absurd.

**10)** Write each of the following integers as a product of prime numbers.

a)  $123 = 3^1 41^1$

b)  $375 = 3^1 5^3$

c)  $927 = 3^2 103$

**11)** Prove Theorem 11.6.

► Theorem 11.6

The  $\gcd(n, m)$  is a product of the primes that are common to  $n$  and  $m$ , where the power of each prime in the product is the smaller of its orders in  $n$  and  $m$ .

Let  $d = \gcd(n, m)$  and let  $d'$  be the product of primes in the statement of Th.11.6. Since the power of each prime in  $d'$  is the smaller of the two, that power divides both  $n$  and  $m$ , so  $d' | n$  and  $d' | m$ , therefore  $d' | \gcd(n, m) = d$ . (\*)

Conversely,  $d$  cannot have any extra factors beyond those in  $d'$ ; assuming by contradiction that it did have an extra factor  $q$ , it wouldn't divide either  $n$  or  $m$  (or both of them), therefore  $d \nmid d'$ . (\*\*)

From (\*) and (\*\*) it follows that  $|d| = |d'|$ , and an examination of all the possible sign combinations of  $n$  and  $m$  shows that actually  $d = d'$ .

**12)** Prove Theorem 11.7.

The correct statement of Th. 11.7 is:

The  $\text{lcm}(n,m)$  is a product of **all the primes that are in either  $n$  or  $m$** , where the power of each prime in the product is the larger of its powers in  $n$  and  $m$ .

Proof: Let  $M = \text{lcm}(n,m)$  and let  $M'$  be the product of primes in the statement of Th.11.7. Since the power of each prime in  $M'$  is the larger of the two,  $M'$  has all the factors of  $n$ , and all the factors of  $m$ , hence it is a multiple of  $n$  and a multiple of  $m$ , therefore it is a common multiple, so  $M|M'$ .

On the other hand, we cannot take away any of the factors  $p$  in  $M'$  and still have it be a common multiple, since then  $M'$  would not be a multiple of the number  $n$  or  $m$  in which the largest power of  $p$  occurs. Therefore,  $M'$  is the least common multiple.

**13)** Prove that for positive integers  $m$  and  $n$ ,  $\text{gcd}(m,n) = \text{lcm}(m,n)$  iff  $m = n$ .

We use the characterizations of  $\text{gcd}$  and  $\text{lcm}$  from Theorems 11.6 and 11.7.  $\text{gcd}$  and  $\text{lcm}$  are equal if and only if they have the same factors, raised to the same powers. From Th.11.7, this can happen iff that there are no uncommon prime factors for  $n$  and  $m$ . From both Th. 11.6 and 11.7, the smallest and largest power for each prime factor are equal, so the powers are identical.

**Section 11.2****14)** Illustrate the flow of Algorithm 11.1 when the top-level call is  $\text{gcd}(68, 40)$ .

$$68 \% 40 = 28$$

$$40 \% 28 = 12$$

$$28 \% 12 = 4$$

$$12 \% 4 = 0 \quad \Rightarrow \quad \text{gcd} = 4$$

**15)** Write an iterative version of Algorithm 11.1. Your algorithm should only use a constant amount of memory [i.e., the space complexity function is  $\text{in}\theta(1)$ ].

```
int gcd(int n, int m) {
    while (m > 0) {
        int q = n mod m;
        n = m;
        m = q;
    }
    return n;
}
```

**16)** Write an algorithm that uses Algorithm 11.1 to express a rational number in its lowest terms. You may assume that this rational number is given in the form of a fraction  $m/n$  where  $m$  and  $n$  are integers.

We apply Algorithm 11.1 to find the gcd, and then divide both  $m$  and  $n$  by the gcd.

**17)** Illustrate the flow of Algorithm 11.2 when the top-level call is  $\text{Euclid}(64,40,\text{gcd},i,j)$ .

We show the results in a table similar to Table 11.1:

Call	n	m	gcd	i	j
0	64	40	8	2	-3
1	40	24	8	-1	2
2	24	16	8	1	-1
3	16	8	8	0	1
4	8	0	<b>8</b>	1	0



Indeed,  $8 = 2 \cdot 64 - 3 \cdot 40$ .

**18)** Write an algorithm that uses subtraction to compute the greatest common divisor. (See Exercise 7.) Analyze your algorithm.

In Exercise 7, it was proved that, if  $n \geq m > 0$ , then  $\gcd(m, n) = \gcd(m, n-m)$ . We use this property in the following algorithm:

```
int gcd_by_sub(int n, int m) {
    if (m > n)
        swap(m, n);
    if (m == 0)
        return n;
    return gcd_by_sub(n-m, m);
}
```

Analysis: The worst case is when  $m = 1$  and  $n$  is a large number, when the number of recursive calls is  $n$ . In each call, the algorithm performs one subtraction, which needs  $\lg n$  bit manipulations, so our algorithm is  $O(n \lg n)$ .

### Section 11.3

**19)** Show that  $(S, *)$  of Example 11.21 is a group.

Proving associativity:  $x*(y*z) = (x*y)*z$ . Since this group has only 3 elements, we consider all  $3*3*3 = 27$  possible cases.

For example, take  $x = a, y = a, z = b$ : We must prove that  $a*(a*b) = (a*a)*b \Leftrightarrow a*e = b*b \Leftrightarrow a = a$ , which is true. All remaining 26 cases are solved similarly, by applying the rules given.

Proving the existence of identity element: From the fourth and fifth properties,  $e$  is the identity.

Proving the existence of an inverse for each element: From the first property,  $a$  and  $b$  are each other's inverse. From the sixth property,  $e$  is its own inverse.

**20)** Prove Theorem 11.12.

► Theorem 11.12

---

We have that  $m \equiv k \pmod n$  if and only if

$$m \bmod n = k \bmod n.$$

Proving implication " $\Rightarrow$ " By definition,  $m \equiv k \pmod n$  iff  $n \mid (m-k)$  iff an integer  $a$  exists such that  $an = m - k$ , or  $m = an + k$ . (\*)

$(m \bmod n)$  is an integer between 0 and  $n-1$  such that  $m = bn + (m \bmod n)$ . We plug in  $m$  from (\*) and we get  $an + k = bn + (m \bmod n) \Leftrightarrow k = (b-a)n + (m \bmod n)$  (\*\*)

$(k \bmod n)$  is an integer between 0 and  $n-1$  such that  $k = cn + (k \bmod n)$ . Comparing with (\*\*) and using the uniqueness of the integer division, we have that  $b - a = c$ , and  $(m \bmod n) = (k \bmod n)$ .

Proving implication " $\Leftarrow$ ". Denote  $(m \bmod n) = (k \bmod n) = R$ , with  $R$  between 0 and  $n-1$ . We have  $m = bn + R$  and  $k = cn + R$ , so  $m - k = (b-c)n$ , therefore  $n \mid (m-k)$ .

**21)** The following was left as an exercise in the proof of Theorem 11.13. Show that there exists an integer  $c$  such that  $h_1 = c \cdot n_2 n_3 \cdots n_j$ .

In the proof of Th. 11.13, we have  $h_1 n_1 = h_2 n_2 = \cdots = h_j n_j$ . Let's focus on  $h_1 n_1 = h_2 n_2$ , which implies that  $n_2 \mid h_1 n_1$ . Since  $n_2$  and  $n_1$  are relatively prime, Th. 11.4 implies that  $n_2 \mid h_1$ . In the same manner, we can show that any  $n_i \mid h_1$ . Since they're all pairwise relatively prime, each  $n_i$  is a separate factor in  $h_1$ , so  $h_1 = c \cdot n_2 n_3 \cdots n_j$ .

**22)** Prove Theorem 11.14.

Reflexivity:  $m \equiv m \pmod n$  is true, because  $m - m = 0$ , so  $n \mid 0$  (any integer divides 0).

Symmetry: Also true, because if  $n \mid (m-k)$ , then  $n$  also divides the negative  $(k-m)$ .

Transitivity: If  $n \mid (m-k)$ ,  $an = m-k$ . If  $n \mid (k-j)$ ,  $bn = k-j$ . Adding the identities, we have  $(a+b)n = m-k+k-j = m-j$ , so  $n \mid (m-j)$ .

**23)** Show that if  $s \in [m]_n$  and  $t \in [k]_n$ , then  $s \cdot t \in [m \times k]_n$ .

$s - m = an$ , and  $t - k = bn \Leftrightarrow s \cdot t = (m + an)(k + bn) = m \cdot k + n(ak + bm + abn)$ , which shown that  $s \cdot t \equiv m \cdot k \pmod n$ .

**24)** Show that if  $G=(S,*)$  is a finite group and  $a \in S$ , then there exists integers  $k, m \geq 1$  such that  $a^k = a^k a^m$ .

Consider the sequence of powers of  $a$ :  $\{a, a^2, a^3, \dots, a^n, \dots\}$  Since  $S$  is finite, let  $k$  and  $k+m$  the first pair of duplicates in the sequence.

**25)** Show that if  $S=\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$ , then  $(S,+)$  is a subgroup of  $(\mathbb{Z}_{12},+)$ .

Associativity follows from the associativity of integer addition.

The null element is  $[0]_{12}$ .

The inverse of  $[3]$  is  $[9]$ , and the inverse of  $[6]$  is itself.

The fact that  $S$  is closed under addition is easily verified, e.g.  $[9] + [6] = [9+6] = [15] = [12+3] = [3]$ .

**26)** Use Theorem 11.19 to prove Corollary 11.3.

From the theorem,  $|S'|$  divides  $|S|$ , so  $|S| / |S'|$  must equal a positive integer  $a$ .

$a$  cannot be 1, because  $S'$  is a proper subgroup, so  $a \geq 2$ , so  $|S| / |S'| \geq 2$ , or  $|S| / 2 \geq |S'|$ .

**27)** Consider the group  $(\mathbb{Z}_9^*, \times)$ . Show that  $\langle [2]_9 \rangle = \mathbb{Z}_9^*$ .

$\mathbb{Z}_9^*$  is made up of the classes of integers that are relatively prime with 9. As shown in Example 11.31, these are  $[1], [2], [4], [5], [7], [8]$ .

The powers of  $[2]$  are:  $[2], [2^2] = [4], [2^3] = [8], [2^4] = [16] = [9+7] = [7], [2^5] = [32] = [27+5] = [5]$ , and  $[2^6] = [64] = [63+1] = [1]$ . From  $[2^7]$ , the elements repeat themselves. Therefore we have obtained exactly the set of classes in  $\mathbb{Z}_9^*$ .



**Section 11.4****28)** Solve the following modular equations.

(a)  $[8]_{10} x = [4]_{10}$

$\text{Gcd}(8,10)$  is 2, and  $2|4$ , so, according to Corollary 11.6, the equation has 2 solutions. We can find them by simply multiplying the class  $[8]$ :

$2[8] = [16] = [6]$

$3[8] = [24] = [20+4] = [4]$ , so 3 is solution

$4[8] = [32] = [30+2] = 2$ ,  $5[8] = [40] = [0]$ ,  $6[8] = [48] = [8]$ ,  $7[8] = [56] = [6]$

$8[8] = [64] = [60+4] = [4]$ , so 8 is solution

The reader is encouraged to also find the solutions using Algorithm 11.3.

(b)  $[4]_{17} x = [5]_{17}$

$\text{Gcd}(4,17) = 1$ , so the equation has a unique solution. We find it by applying Algorithm 11.3:

We apply the extended Euclid's algorithm  $\text{Euclid}(n,m,d,i,j)$  to the integers 4 and 17:

Call	n	m	gcd	i	j
0	17	4	1	1	-4
1	4	1	1	0	1
2	1	0	1	1	0



Check:  $1 = 1 \cdot 17 - 4 \cdot 4$ .

According to Th. 11.24 / Alg. 11.3, the solution is  $[jk/d]_n = [-4 \cdot 5 / 1]_{17} = [-20]_{17} = [-3]_{17} = [14]_{17}$ . Check:  $[14 \cdot 4]_{17} = [56]_{17} = [3 \cdot 17 + 5]_{17} = [5]_{17}$ .

**29)** Implement Algorithm 11.3 and run it on various problem instances.

Implementations will vary.

**30)** Find all solutions to the equations:


$$[1]_7 x = [3]_7$$

$\text{Gcd}(1,7) = 1$ , so there is a unique solution. It is obvious that the solution is  $x = [3]_7$ .

$$[12]_9 x = [6]_9$$

$\text{Gcd}(12,9) = 3$ , so there are 3 solutions. First we find the integers  $i$  and  $j$  using Euclid's algorithm:

Call	n	m	gcd	i	j
0	12	9	3	1	-1
1	9	3	3	0	1
2	3	0	3	1	0



Check:  $3 = 1 \cdot 12 - 1 \cdot 9$ .

According to Th. 11.24 / Alg. 11.3, the solutions are:

- $[-1 \cdot 12/3 + 0 \cdot 9/3]_9 = [-4 + 0]_9 = [-4]_9 = [5]_9$ . Check:  $[12 \cdot 5]_9 = [60]_9 = [9 \cdot 6 + 6]_9 = [6]_9$ .
- $[-1 \cdot 12/3 + 1 \cdot 9/3]_9 = [-4 + 3]_9 = [-1]_9 = [8]_9$ . Check:  $[12 \cdot 8]_9 = [96]_9 = [9 \cdot 10 + 6]_9 = [6]_9$ .
- $[-1 \cdot 12/3 + 2 \cdot 9/3]_9 = [-4 + 6]_9 = [2]_9$ . Check:  $[12 \cdot 2]_9 = [24]_9 = [9 \cdot 2 + 6]_9 = [6]_9$ .

## Section 11.5

**31)** Compute  $([3]_{73})^{12}$  by raising 3 to the 12th power.

$$([3]_{73})^{12} = [1]_{73}.$$

**32)** Compute  $([7]_{73})^{15}$  by raising 7 to the 15th power.

$$([7]_{73})^{15} = [22]_{73}.$$

**33)** Use Algorithm 11.4 to compute  $([3]_{73})^{12}$ .

12 is 1100 in binary. We use a table similar to Table 11.2:

i	3	2	1	0
<b>b<sub>i</sub></b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>0</b>
k <sub>i</sub>	1	3	6	12
a	$[3]_{73}$	$[9 \cdot 3]_{73} = [27]_{73}$	$[72]_{73}$	<b><math>[1]_{73}</math></b>

**34)** Use Algorithm 11.4 to compute  $([7]_{73})^{15}$ .

15 is 1111 in binary. We use a table similar to Table 11.2:

i	3	2	1	0
<b>b<sub>i</sub></b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>
k <sub>i</sub>	1	3	6	12
a	$[7]_{73}$	$[343]_{73} = [51]_{73}$	$[30]_{73}$	<b><math>[22]_{73}</math></b>

**35)** Implement Algorithm 11.4, and run it on various problem instances.

Implementations will vary.

## Section 11.6

**36)** Find the number of prime numbers that are less than or equal to 100.

There are 25 primes less than or equal to 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.

**37)** If an integer between 1 and 10,000 is randomly chosen according to the uniform distribution, approximately what is the probability of it being prime?

From Theorem 11.27, there are approximately  $10000/\ln 10000 \approx 1085$  primes less than or equal to 10000. Randomly choosing an integer according to the uniform distribution gives  $P(\text{prime}) = 1/\ln 10\,000 \approx 0.1085$ .

**38)** Suppose we randomly choose 100 numbers between 1 and 10,000 according to the uniform distribution. Approximately, what is the probability of all of them not being prime?

We shall also assume that the numbers are chosen independently of each other, so each has an independent probability of being prime or not prime.  $p = P(\text{prime})$  was calculated in the exercise above to be  $\approx 0.1085$ , so  $P(\text{not prime})$  is the complementary probability  $q = 1 - p \approx 0.8914$ . The probability of all of them not being prime is  $q^{100} \approx 10^{-5}$ .

**39)** Show that if  $n$  is prime and  $1 < k \leq n-1$ , then  $B(n,k) \equiv 0 \pmod n$ , where  $B(n,k)$  denotes the binomial coefficient.

$B(n,k) \equiv 0 \pmod n$  means that  $B(n,k)$  is divisible by  $n$ . By definition,  $B(n,k) = n! / (k!(n-k)!) = n \cdot [(n-1)! / (k!(n-k)!)]$ . Since  $n$  is prime, the number in brackets is an integer, so  $B(n,k) = n \cdot a$ , therefore divisible by  $n$ .

**40)** Show that if  $q$  is a factor of  $n$  and  $k$  is the order of  $q$  in  $n$ , then  $q^k \mid B(n,q)$ , where  $B(n,q)$  denotes the binomial coefficient.

$B(n,q) = n! / (q!(n-q)!)$ , and, after simplifying  $(n-q)!$ , we obtain  $\frac{(n-q)(n-q+1)\dots(n-1)n}{1 \cdot 2 \cdot 3 \cdot \dots \cdot (q-1) \cdot q}$ .

Writing  $n = a \cdot q^k$ , with  $k > 0$ , we can factor out  $q$  in the first and last factor of the numerator:

$\frac{q(aq^{k-1}-1)(n-q+1)\dots(n-1)aq^k}{1 \cdot 2 \cdot 3 \cdot \dots \cdot (q-1) \cdot q} = \frac{(aq^{k-1}-1)(n-q+1)\dots(n-1)aq^k}{1 \cdot 2 \cdot 3 \cdot \dots \cdot (q-1)}$ . Since  $q$  is prime, none of the factors in the denominator can divide  $q^k$ , so we write  $\frac{(aq^{k-1}-1)(n-q+1)\dots(n-1)a}{1 \cdot 2 \cdot 3 \cdot \dots \cdot (q-1)} = b$  is an integer, and  $B(n,q) = bq^k$ , which proves the result.

**41)** Are  $9x^3+2x$  and  $x^2-4$  congruent modulo 2?

The coefficients of  $x^3$  in the two polynomials are 9 and 0, which are not congruent modulo 2 (9-0 is not divisible by 2), therefore the polynomials aren't either.

**42)** Show that  $(x-9)^4$  is not congruent to  $(x^4-9)$  modulo 4.

$$(x-9)^4 = ((x-9)^2)^2 = (x^2 - 18x + 81)^2 = x^4 - 36x^3 + 486x^2 - 2916x + 81^2$$

486 is not congruent with 0 modulo 4, because 486 is not divisible by 4.

**43)** Show that  $(x-5)^3$  is congruent to  $(x^3-5)$  modulo 3.

This must be so by Theorem 11.28, since 3 is prime.

We can also prove it directly, by expanding  $(x-5)^3 = x^3 - 15x^2 + 75x - 125$ , whose coefficients are all congruent with the respective coefficients in  $(x^3-5)$  modulo 3. For example,  $-15 = (-5)3 \equiv 0 \pmod{3}$ .

**44)** Prove Theorem 11.29.

► Theorem 11.29

Suppose  $n$  and  $r$  are prime. Then for all integers  $m$ ,

$$(x-m)^n \equiv (x^n-m) \pmod{(x^r-1, n)}.$$

A useful re-statement of this congruence modulo  $(x^r-1, n)$  is to say that

$$(x-m)^n - (x^n-m) = nP(x) + (x^r-1)Q(x), \quad (*)$$

where  $P$  and  $Q$  are polynomials in  $x$ . From Lemma 11.2, we have that  $(x-m)^n - (x^n-m) = nP(x)$ , so in  $(*)$  we simply take  $Q(x) = 0$ .

**45)** Implement Algorithm 11.5 and run it on different problem instances.

Implementations will vary.

**46)** Use Lemma 11.3 to prove Lemma 11.4.

**▲ Lemma 11.4**

Suppose  $g(x)$  is a polynomial with integer coefficients, and  $n$  and  $r$  are prime. Then

$$[g(x)]^n \equiv g(x^n) \pmod{(x^r - 1, n)}.$$

A useful re-statement of this congruence modulo  $(x^r - 1, n)$  is to say that

$$[g(x)]^n - g(x^n) = nP(x) + (x^r - 1)Q(x), \quad (*)$$

where  $P$  and  $Q$  are polynomials in  $x$ . From Lemma 11.3, we have that  $[g(x)]^n - g(x^n) = nP(x)$ , so in  $(*)$  we simply take  $Q(x) = 0$ .

**47)** The following was left as an exercise in the proof of Lemma 11.6. Show

$$\text{ord}_r(n) \mid \text{lcm}[\text{ord}_r(p_1), \text{ord}_r(p_2), \dots, \text{ord}_r(p_k)].$$

For simplicity, we first give the proof for only two prime factors  $p_1$  and  $p_2$ , both having powers equal to 1, i.e.  $n = p_1 p_2$ :

To make the notation simpler, denote  $a = \text{ord}_r(p_1)$ , and  $b = \text{ord}_r(p_2)$ . We want to prove  $\text{ord}_r(p_1 p_2) \mid \text{lcm}(a, b)$ .

Lcm has the property of being divisible by either argument:  $a \mid \text{lcm}(a, b)$ , and  $b \mid \text{lcm}(a, b)$ , therefore

$p_1^{\text{lcm}(a, b)} \equiv 1 \pmod{r}$ , and  $p_2^{\text{lcm}(a, b)} \equiv 1 \pmod{r}$ . When we multiply these congruences, we obtain  $(p_1 p_2)^{\text{lcm}(a, b)} \equiv 1 \pmod{r}$ . (\*)

At this stage, we need a

**Lemma:** If  $n^x \equiv 1 \pmod{r}$ , then  $x$  is a multiple of  $\text{ord}_r(n)$ .

Proof of lemma: We apply the division algorithm to  $x$ :  $x = y \cdot \text{ord}_r(n) + z$ , with  $0 \leq z < \text{ord}_r(n)$ .

Therefore  $n^x = n^{y \cdot \text{ord}_r(n) + z} = [n^{\text{ord}_r(n)}]^y \cdot n^z = [1]^y \cdot n^z = n^z \equiv 1 \pmod{r}$ . But since  $0 \leq z < \text{ord}_r(n)$ , the congruence is possible iff  $z = 0$ , iff  $x = y \cdot \text{ord}_r(n)$ , which proves the lemma ■

Apply the lemma to  $(*)$  to obtain that  $\text{ord}_r(p_1 p_2) \mid \text{lcm}(a, b)$ .

The next step is to deal with arbitrary powers of the factors  $p_1$  and  $p_2$ . This is achieved by means of another

$$\text{Lemma: } \text{ord}_r(p_1)^{k_1} = \frac{\text{ord}_r p_1}{\gcd(k_1, \text{ord}_r p_1)}$$

Proof ??

The next step is to apply induction on the number of factors  $k$ .

Proof ??

**48)** Use Inequality 11.22 to obtain the inequality that follows it.

Since the numerators of the right-hand sides are the same in Inequality 11.22 and the next, we only have to prove that the second denominator is larger than the first:

$$\begin{aligned} 7(\lg(\lg n)) &\geq \lg(c_2(\lg n)^6) &\Leftrightarrow &\lg(\lg n)^7 \geq \lg(c_2(\lg n)^6) &\Leftrightarrow &(\lg n)^7 \geq c_2(\lg n)^6 \\ &\Leftrightarrow &\lg n \geq c_2, &\text{which is true if we choose } \lg N \geq c_2 \end{aligned}$$

## Section 11.7

**49)** What is the difference between a public key and a secret key?

The public key of a recipient is known to everyone, but the secret key of the recipient is only known to her/himself. Nevertheless, the recipient can use the secret key to decipher any message that was encrypted with their public key.

**50)** For an RSA cryptosystem using  $p = 7$ ,  $q = 11$ , and  $g = 13$ :

a)  $n = 7 \cdot 11 = 77$ .

b)  $\phi(n) = 6 \cdot 10 = 60$ .

c)  $h = 37$ .

**51)** Given that  $p = 23$ ,  $q = 41$ , and  $g = 3$ , then  $n = 943$ ,  $\phi(n) = 880$ , and  $h = 587$ .

The message  $[847]_{943}$  is encrypted as  $([847]_{943})^3 = [741]_{943}$ .

**52)** Using the cryptosystem in Exercise 51, the cipher  $[741]_{943}$  is decrypted as  $([741]_{943})^{587} = [847]_{943}$ .

**53)** In an RSA cryptosystem, show that if  $\phi(n)$  can be discovered, then the cryptosystem may be compromised.

The number  $n$  is already public, as part of the public key, so, if  $\phi(n)$  is also known, we have a system of 2 equations with the two unknowns  $p$  and  $q$ :

$$pq = n$$

$$(p-1)(q-1) = \phi(n)$$

Simple algebraic manipulations lead to the solutions  $p$  and  $q$  being the two roots of the quadratic equation  $x^2 - (n+1-\phi(n))x + n = 0$ , which is easily solved.

### Additional Exercises

**54)** Prove that there are infinitely many prime numbers.

Suppose that there are a finite number,  $n$ , of primes denoted  $p_1, p_2, \dots, p_n$ .

Let  $q = p_1 \times p_2 \times p_3 \times \dots \times p_n + 1$ . Then  $q$ , which is not prime by our initial assumption, must contain a prime factor in  $p_1$  through  $p_n$ . However, if we divide  $q$  by any of  $p_1$  through  $p_n$ , we obtain a remainder of 1, which is a contradiction. Therefore, there must be infinitely many primes.

**55)** Show that the gcd operator is associative. That is, for all integers  $m, n$ , and  $h$ , we have  $\gcd(m, \gcd(n, h)) = \gcd(\gcd(m, n), h)$ .

The simplest proof uses the characterization of gcd in terms of the prime factors (Th. 11.2 in the text):

$\gcd(m, \gcd(n, h))$  has all the prime factors common to  $m$  and  $\gcd(n, h)$ , with their lowest powers, and  $\gcd(n, h)$  has all the prime factors common to  $n$  and  $h$ , with their lowest powers. Since “common to” is an associative relation, it follows that

$\gcd(m, \gcd(n, h))$  has all the prime factors common to  $m, n$ , and  $h$ , with their lowest powers.

The second part of the last statement does not depend on the order of operation, so it's clear that  $\gcd(\gcd(m, n), h)$  can be brought to the same form.



**56)** Prove that if  $m$  is odd and  $n$  is even, then  $\gcd(m, n) = \gcd(m, n/2)$ .

We use the characterization of  $\gcd$  in terms of the prime factors (Th. 11.2 in the text):

Since  $m$  is odd,  $m$  does not have 2 as a prime factor, therefore  $\gcd(m, n)$  does not have it either, therefore it's OK to remove not just one, but all factors of 2 from  $n$ :

$\gcd(m, n) = \gcd(m, n/2^k)$ , where  $k$  is the highest power of 2 that divides  $n$ .

**57)** Prove that if  $m$  and  $n$  are both odd, then  $\gcd(m, n) = \gcd((m-n)/2, n)$ .

We already know from Exercise 7 that  $\gcd(m, n) = \gcd(m-n, n)$ . Since  $m$  and  $n$  are both odd,  $m - n$  is even, so we can apply Exercise 56.

**58)** Find the necessary condition to have equation  $mx \equiv my \pmod{n}$  imply  $x \equiv y \pmod{n}$ .

$mx \equiv my \pmod{n} \Leftrightarrow (mx - my) = an \Leftrightarrow m(x - y) = an$ . When does the last equality imply that  $x \equiv y \pmod{n} \Leftrightarrow (x - y) = bn$ ?

We substitute  $(x - y)$  into the first one:  $mbn = an$ , which, for non-zero  $n$ , implies  $mb = a$ , i.e.  $m$  is a factor of  $a$ .

**59)** Assuming that  $p$  is a prime number, find the solutions of the equation  $x^2 \equiv [1]_p$ .

$x^2 \equiv [1]_p$  means  $x^2 - 1 = kp$ , or  $(x-1)(x+1) = kp$ , therefore  $p$  divides  $x - 1$  or  $p$  divides  $x + 1$ . In the first case,  $x = ap + 1$ , and in the second,  $x = ap - 1$ . Using classes modulo  $p$ , the first solution is  $x = [1]_p$ , and the second is  $x = [-1]_p = [p-1]_p$ .

**60)** In an RSA cryptosystem, let  $p$  and  $q$  be the large primes, let  $n = pq$ , and let  $pub$  be the public key. Show that  $pub(a)pub(b)$  is congruent to  $pub(ab)$  modulo  $n$ .

$pub(a) = [a^g]_n$ , and  $pub(b) = [b^g]_n$ , so

$pub(a)pub(b) = (a^g + in)(b^g + jn) = (ab)^g + kn \equiv (ab)^g \pmod{n}$ .