Section 2.5 – Primes and Greatest Common Divisors

Primes

Definition

An integer *p* greater than 1 is called ***prime*** of the only positive factors of *p* are 1 or *p*.
A positive integer that is greater than 1 and is not prime is called composite.

Example

The integer 7 is prime because its only positive factors are 1 and 7.
The integer 9 is composite because its is divisible by 3.

Theorem – The Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Example

Find the prime factorization of 100, 641, 999, and 1024.

Solution

$$100 = 2\cdot 2\cdot 5\cdot 5 = 2^2\cdot 5^2$$

$$641 = 641$$

$$999 = 3\cdot 3\cdot 3\cdot 37 = 3^3\cdot 37$$

$$1024 = 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2 = 2^{10}$$

Trial Division

Theroem

If *n* is a composite integer, then *n* has a prime divisor less than or equal to $\sqrt{n}$

Proof

If *n* is composite, then it has a factor *a* (by definition of a composite integer) with $1 < a < n$. Hence, by the definition of a factor, we have $n = ab, \quad b\left(\textit{positive integer}\right) > 1$.

If $a > \sqrt{n} \quad \textit{and} \quad b > \sqrt{n}$, then $ab > \sqrt{n}\cdot\sqrt{n} = n$, which is a contradiction. Consequently, $a \le \sqrt{n} \ \textit{and} \ b \le \sqrt{n}$. Because both *a* and *b* are divisors of *n*, we see that *n* has a positive divisor not exceeding $\sqrt{n}$. This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, *n* has a prime divisor less than or equal to $\sqrt{n}$.

Example

Show that 101 is prime

Solution

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer). It follows that 101 is prime.

Example

Find the prime factorization of 7007

Solution

None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $\frac{7007}{7} = 1001$, and $\frac{1001}{7} = 143$, $\frac{143}{11} = 13$. Because 13 is prime, the procedure is completed.

It follows that the prime factorization is $7007 = 7^2 \cdot 11 \cdot 13$

The Sieve of *Eratosthenes*

The ***Sieve of Eratosthenes*** can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.

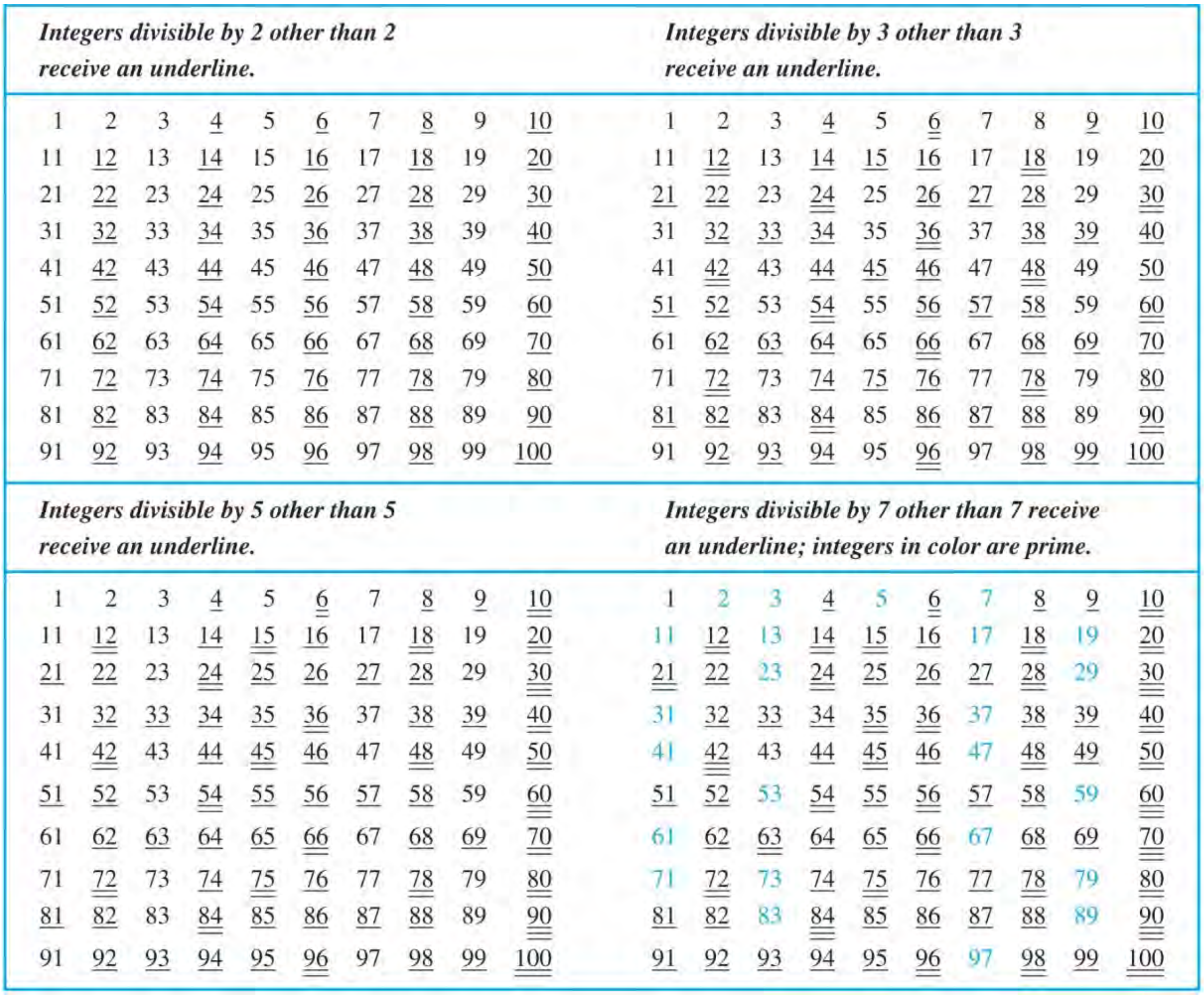
a. Delete all the integers, other than 2, divisible by 2.
b. Delete all the integers, other than 3, divisible by 3.
c. Next, delete all the integers, other than 5, divisible by 5.
d. Next, delete all the integers, other than 7, divisible by 7.
e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are: {2,3,7,11,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

If an integer n is a composite integer, then it has a prime divisor less than or equal to $\sqrt{n}$.

To see this, note that if $n = ab$, then $a \le \sqrt{n}$ *or* $b \le \sqrt{n}$.

Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $i \le \sqrt{n}$ and see if n is divisible by i.

The Sieve of Eratosthenes



Integers divisible by 2 other than 2 receive an underline.

1	2	3	$\underline{4}$	5	$\underline{6}$	7	$\underline{8}$	9	$\underline{10}$
11	$\underline{12}$	13	$\underline{14}$	15	$\underline{16}$	17	$\underline{18}$	19	$\underline{20}$
21	$\underline{22}$	23	$\underline{24}$	25	$\underline{26}$	27	$\underline{28}$	29	$\underline{30}$
31	$\underline{32}$	33	$\underline{34}$	35	$\underline{36}$	37	$\underline{38}$	39	$\underline{40}$
41	$\underline{42}$	43	$\underline{44}$	45	$\underline{46}$	47	$\underline{48}$	49	$\underline{50}$
51	$\underline{52}$	53	$\underline{54}$	55	$\underline{56}$	57	$\underline{58}$	59	$\underline{60}$
61	$\underline{62}$	63	$\underline{64}$	65	$\underline{66}$	67	$\underline{68}$	69	$\underline{70}$
71	$\underline{72}$	73	$\underline{74}$	75	$\underline{76}$	77	$\underline{78}$	79	$\underline{80}$
81	$\underline{82}$	83	$\underline{84}$	85	$\underline{86}$	87	$\underline{88}$	89	$\underline{90}$
91	$\underline{92}$	93	$\underline{94}$	95	$\underline{96}$	97	$\underline{98}$	99	$\underline{100}$

Integers divisible by 3 other than 3 receive an underline.

1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{10}$
11	$\underline{\underline{12}}$	13	$\underline{14}$	$\underline{15}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{20}$
$\underline{21}$	$\underline{22}$	23	$\underline{\underline{24}}$	25	$\underline{26}$	$\underline{27}$	$\underline{28}$	29	$\underline{\underline{30}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	35	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{40}$
41	$\underline{\underline{42}}$	43	$\underline{44}$	$\underline{45}$	$\underline{46}$	47	$\underline{\underline{48}}$	49	$\underline{50}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	55	$\underline{56}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{60}}$
61	$\underline{62}$	$\underline{63}$	$\underline{64}$	65	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{70}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{75}$	$\underline{76}$	77	$\underline{\underline{78}}$	79	$\underline{80}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{84}}$	85	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{90}}$
91	$\underline{92}$	$\underline{93}$	$\underline{94}$	95	$\underline{\underline{96}}$	97	$\underline{98}$	$\underline{99}$	$\underline{100}$

Integers divisible by 5 other than 5 receive an underline.

1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{\underline{10}}$
11	$\underline{\underline{12}}$	13	$\underline{14}$	$\underline{\underline{15}}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{\underline{20}}$
$\underline{21}$	$\underline{22}$	23	$\underline{\underline{24}}$	$\underline{25}$	$\underline{26}$	$\underline{27}$	$\underline{28}$	29	$\underline{\underline{\underline{30}}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	$\underline{35}$	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{\underline{40}}$
41	$\underline{\underline{42}}$	43	$\underline{44}$	$\underline{\underline{45}}$	$\underline{46}$	47	$\underline{\underline{48}}$	49	$\underline{\underline{50}}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	$\underline{55}$	$\underline{56}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{\underline{60}}}$
61	$\underline{62}$	$\underline{63}$	$\underline{64}$	$\underline{65}$	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{\underline{70}}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{\underline{75}}$	$\underline{76}$	77	$\underline{\underline{78}}$	79	$\underline{\underline{80}}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{84}}$	$\underline{85}$	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{\underline{90}}}$
91	$\underline{92}$	$\underline{93}$	$\underline{94}$	$\underline{95}$	$\underline{\underline{96}}$	97	$\underline{98}$	$\underline{99}$	$\underline{\underline{100}}$

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{\underline{10}}$
11	$\underline{\underline{12}}$	13	$\underline{\underline{14}}$	$\underline{\underline{15}}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{\underline{20}}$
$\underline{\underline{21}}$	$\underline{22}$	23	$\underline{\underline{24}}$	$\underline{25}$	$\underline{26}$	$\underline{27}$	$\underline{\underline{28}}$	29	$\underline{\underline{\underline{30}}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	$\underline{\underline{35}}$	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{\underline{40}}$
41	$\underline{\underline{\underline{42}}}$	43	$\underline{44}$	$\underline{\underline{45}}$	$\underline{46}$	47	$\underline{\underline{48}}$	$\underline{49}$	$\underline{\underline{50}}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	$\underline{55}$	$\underline{\underline{56}}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{\underline{60}}}$
61	$\underline{62}$	$\underline{\underline{63}}$	$\underline{64}$	$\underline{65}$	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{\underline{\underline{70}}}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{\underline{75}}$	$\underline{76}$	$\underline{\underline{77}}$	$\underline{\underline{78}}$	79	$\underline{\underline{80}}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{\underline{84}}}$	$\underline{85}$	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{\underline{90}}}$
$\underline{\underline{91}}$	$\underline{92}$	$\underline{93}$	$\underline{94}$	$\underline{95}$	$\underline{\underline{96}}$	97	$\underline{\underline{98}}$	$\underline{99}$	$\underline{\underline{100}}$

The infinitude of Primes

It has long been known that there are infinitely many primes. This means that whenever $p_1, p_2, \ldots, p_n$ are the n smallest primes, we know there is a larger.

Theorem

There are infinitely may primes.

Proof: Assume finitely many primes: $p_1, p_2, \ldots, p_n$

Let $q = p_1 p_2 \ \ldots \ p_n + 1$. Either q is prime or by the fundamental theorem of arithmetic it is a product of primes. But none of the primes p_i divides q since if $p_i \mid q$, then p_i divide $q - p_1 p_2 \ \ldots \ p_n = 1$ .Hence, there is a prime not on the list $p_1, p_2, \ldots, p_n$ It is either q, or if q is composite, it is a prime factor of *q*. This contradicts the assumption that $p_1, p_2, \ldots, p_n$ are all the primes. Consequently, there are infinitely many primes.

Mersenne Primes

Definition

Prime numbers of the form $2^p - 1$, where p is prime, are called ***Mersenne primes***.

Example

$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 37, \quad 2^7 - 1 = 127$ are Mersenne primes.

$2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.

There is an efficient test for determining if $2^p - 1$ is prime. The largest known prime numbers are Mersenne primes. 47 Mersenne primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.

Distribution of Primes

Mathematicians have been interested in the distribution of prime numbers among the positive integers. In the nineteenth century, the *prime number theorem* was proved which gives an asymptotic estimate for the number of primes not exceeding *x*.

Theorem – Prime Number

The ratio of the number of primes not exceeding *x* and $\frac{x}{\ln x}$ approaches 1 as *x* grows without bound. (ln*x* is the natural logarithm of *x*),

The theorem tells us that the number of primes not exceeding *x*, can be approximated by $\frac{x}{\ln x}$.

The odds that a randomly selected positive integer less than *n* is prime are approximately $(n / \ln n / n) = \frac{1}{\ln n}$

Greatest Common Divisor

Definition

Let *a* and *b* be integers, not both zero. The largest integer *d* such that *d* | *a* and also *d* | *b* is called the greatest common divisor of *a* and *b*. The greatest common divisor of *a* and *b* is denoted by gcd(*a*,*b*).

One can find greatest common divisors of small numbers by inspection.

Example

What is the greatest common divisor of 24 and 36?

Solution

gcd(24,26) = 12

Example

What is the greatest common divisor of 17 and 22?

Solution

gcd(17,22) = 1

Definition

The integers *a* and *b* are *relatively prime* if their greatest common divisor is 1.

Example 17 and 22

Definition

The integers $a_1,\ a_2,\ \ldots,\ a_n$ are *pairwise relatively prime* if $\gcd\left(a_i, a_j\right) = 1$ whenever $1 \le i \le j \le n$.

Example

Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution

Because gcd(10,17) = 1, gcd(10,21) = 1, and gcd(17,21) = 1, 10, 17, and 21 are pairwise relatively prime.

Example

Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution

Because gcd(10,24) = 2, 10, 19, and 24 are not pairwise relatively prime.

Least Common Multiple

Definition

The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*. It is denoted by lcm(*a*,*b*).

The least common multiple can also be computed from the prime factorizations.

$$lcm(a,\ b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}$$

This number is divided by both *a* and *b* and no smaller number is divided by *a* and *b*.

Example

$$lcm\left(2^3 3^5 7^2,\ 2^4 3^3\right) = 2^{\max(3,4)} \cdot 3^{\max(5,3)} \cdot 7^{\max(2,0)}$$

$$= 2^4 \cdot 3^5 \cdot 7^2$$

Theorem

Let *a* and *b* be positive integers. Then $ab = \gcd(a,b) \cdot lcm(a,b)$

Euclidean Algorithm

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(*a*,*b*) is equal to gcd(*a*,*c*) when *a* > *b* and *c* is the remainder when *a* is divided by *b*.

Lemma 1

Let $a = bq + r$, where *a, b, q*, and *r* are integers. Then $\gcd(a,b) = \gcd(b,r)$

Proof

Suppose that *d* divides both *a* and *b*. Then *d* also divides *a* − *bq* = *r*. Hence, any common divisor of *a* and *b* must also be any common divisor of *b* and *r*. Suppose that *d* divides both *b* and *r*. Then *d* also divides *bq* + *r* = *a*. Hence, any common divisor of *a* and *b* must also be a common divisor of *b* and *r*. Therefore, $\gcd(a,b) = \gcd(b,r)$.

Example

Find *gcd* (91, 287)

Solution

$287 = 91 \cdot 3 + 14$ ***Divide 287 by 91***

$91 = 14 \cdot 6 + 7$ ***Divide 91 by 14***

$14 = 7 \cdot 2 + 0$ ***Divide 14 by 7***

$gcd\ (287, 91) = 7$

Example

Find *gcd* (414, 662)

Solution

$662 = 414 \cdot 1 + 248$ ***Divide 662 by 414***

$414 = 248 \cdot 1 + 166$ ***Divide 414 by 248***

$248 = 166 \cdot 1 + 82$ ***Divide 248 by 166***

$166 = 82 \cdot 2 + 2$ ***Divide 166 by 82***

$82 = 2 \cdot 41 + 0$ ***Divide 82 by 2***

$gcd(414, 662) = 2$

Euclidean Algorithm

```
procedure gcd(a, b: positive integers)
x := a
x := b
while  y ≠ 0
    r := x mod y
    x := y
    y := r
return x {gcd(a,b) is x}
```

GCDs as Linear Combinations

Bézout's Theorem

If *a* and *b* are positive integers, then there exist integers *s* and *t* such that gcd(a,b) = $sa + tb$.

Definition

If a and b are positive integers, then integers s and t such that gcd(a,b) = $sa + tb$ are called ***Bézout coefficients*** of a and b. The equation gcd(a,b) = $sa + tb$ is called ***Bézout's identity***.

Example

Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution

First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$

ii. $198 = 3 \cdot 54 + 36$

iii. $54 = 1 \cdot 36 + 18$

iv. $36 = 2 \cdot 18$

Now working backwards, from *iii* and *i* above

$18 = 54 - 1 \cdot 36$

$36 = 198 - 3 \cdot 54$

Substituting the 2nd equation into the 1st yields:

$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$

Substituting $54 = 252 - 1 \cdot 198$ (from *i*)) yields:

$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the ***extended Euclidean algorithm***, is developed in the exercises.

Lemma 2

If a, b, and c are positive integers such that gcd(a, b) = 1 and $a \mid bc$, then $a \mid c$.

Proof

Assume gcd(a, b) = 1 and $a \mid bc$

Since gcd(a, b) = 1, by Bézout's Theorem there are integers s and t such that $sa + tb = 1$.

Multiplying both sides of the equation by c, yields $sac + tbc = c$. $a \mid tbc$ and a divides $sac + tbc$ since $a \mid sac$ and $a \mid tbc$. We conclude $a \mid c$, since $sac + tbc = c$.

Lemma 3

If p is prime and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some i.

- Lemma 3 is crucial in the proof of the uniqueness of prime factorizations.

Uniqueness of Prime Factorization

We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique.

Proof **(*by contradiction*)**

Suppose that the positive integer *n* can be written as a product of primes in two distinct ways:

$$n = p_1 p_2 \cdots p_s \text{ and } n = q_1 q_2 \cdots q_t$$

Remove all common primes from the factorizations to get

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

By Lemma 3, it follows that p_{i_1} divides q_{j_k}, for some *k*, contradicting the assumption that p_{i_1} and q_{j_k} are distinct primes.

Hence, there can be at most one factorization of *n* into primes in nondecreasing order.

Dividing Congruences by an Integer

Theorem

Let m be a positive integer and let *a*, *b*, and *c* be integers. If $ac \equiv bc \pmod{m}$ and gcd(c,m) = 1, then $a \equiv b \pmod{m}$.

Proof

Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that gcd(c,m) = 1, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$.

Exercises *Section* 2.5 – Primes and Greatest Common Divisors

1. Determine whether each of these integers is prime.

a) 21 *b)* 29 *c)* 71 *d)* 97 *e)* 111

f) 143 *g)* 19 *h)* 27 *i)* 93 *j)* 101

k) 107 *l)* 113

2. Find the prime factorization of each these integers.

a) 88 *b)* 126 *c)* 729 *d)* 1001 *e)* 1111

f) 909,090 *g)* 39 *h)* 81 *i)* 101 *j)* 143

k) 289 *l)* 899

3. Find the prime factorization of 10!

4. Show that if a^m+1 is composite if *a* and *m* are integers greater than 1 and *m* is odd. [*Hint*: Show that *x* + 1 is a factor of the polynomial a^m+1 if *m* is odd]

5. Show that if 2^m+1 is an odd prime, then $m=2^n$ for some nonnegative integer *n*. [*Hint*: First show the polynomial identity $x^m+1=\left(x^k+1\right)\left(x^{k(t-1)}-x^{k(t-2)}+\cdots-x^k+1\right)$ holds, where $m=kt$ and *t* is odd]

6. Which positive integers less than 12 are relatively prime to 12?

7. Which positive integers less than 30 are relatively prime to 30?

8. Determine whether the integers in each of these sets are pairwise relatively prime.

a) 21, 34, 55 *b)* 14, 17, 85 *c)* 25, 41, 49, 64 *d)* 17, 18, 19, 23

e) 11, 15, 19 *f)* 14, 15, 21 *g)* 12, 17, 31, 37 *h)* 7, 8, 9, 11

9. We call a positive integer ***perfect*** if it equals the sum of its positive divisors other than itself

a) Show that 6 and 28 are perfect.

b) Show that $2^{p-1}\left(2^p-1\right)$ is a perfect number when 2^p-1 is prime

10. Show that if 2^n-1 is prime, then *n* is prime. *Hint*: Use the identity

$$2^{ab}-1=\left(2^a-1\right)\cdot\left(2^{a(b-1)}+2^{a(b-2)}+\cdots+2^a+1\right)$$

11. Determine whether each of these integers is prime, verifying some of Mersenne's claims

a) 2^7-1 *b)* 2^9-1 *c)* $2^{11}-1$ *d)* $2^{13}-1$

12. What are the greatest common divisors of these pairs of integers?

a) $2^2 \cdot 3^3 \cdot 5^5,\ \ 2^5 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13,\ \ 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

c) $17,\ \ 17^{17}$

d) $2^2 \cdot 7,\ \ 5^3 \cdot 13$

e) $0,\ \ 5$

f) $2 \cdot 3 \cdot 5 \cdot 7,\ \ 2 \cdot 3 \cdot 5 \cdot 7$

g) $3^7 \cdot 5^3 \cdot 7^3,\ \ 2^{11} \cdot 3^5 \cdot 5^9$

h) $11 \cdot 13 \cdot 17,\ \ 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

i) $23^{31},\ \ 23^{17}$

j) $41 \cdot 43 \cdot 53,\ \ 41 \cdot 43 \cdot 53$

k) $1111,\ \ 0$

13. What is the least common multiple of each pair

a) $2^2 \cdot 3^3 \cdot 5^5,\ \ 2^5 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13,\ \ 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

c) $17,\ \ 17^{17}$

d) $2^2 \cdot 7,\ \ 5^3 \cdot 13$

e) $0,\ \ 5$

f) $2 \cdot 3 \cdot 5 \cdot 7,\ \ 2 \cdot 3 \cdot 5 \cdot 7$

g) $3^7 \cdot 5^3 \cdot 7^3,\ \ 2^{11} \cdot 3^5 \cdot 5^9$

h) $11 \cdot 13 \cdot 17,\ \ 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

i) $23^{31},\ \ 23^{17}$

j) $41 \cdot 43 \cdot 53,\ \ 41 \cdot 43 \cdot 53$

k) $1111,\ \ 0$

14. Find gcd(1000, 625) and lcm(1000, 625) and verify that $\gcd(100,\ 625) \cdot lcm(100,\ 625) = 1000 \cdot 625$

15. Find gcd(92928, 123552) and lcm(92928, 123552) and verify that
$\gcd(92928,\ 123552) \cdot lcm(92928,\ 123552) = 92928 \bullet 123552$

16. Use the Euclidean algorithm to find

a) $\gcd(1,\ 5)$ *b)* $\gcd(100,\ 101)$ *c)* $\gcd(123,\ 277)$ *d)* $\gcd(1529,\ 14039)$

e) $\gcd(1529,\ 14038)$ *f)* $\gcd(12,\ 18)$ *g)* $\gcd(111,\ 201)$ *h)* $\gcd(1001,\ 1331)$

i) $\gcd(12345,\ 54321)$ *j)* $\gcd(1000,\ 5040)$ *k)* $\gcd(9888,\ 6060)$

17. Prove that the product of any three consecutive integers is divisible by 6.

18. Show that if *a*, *b*, and *m* are integers such that $m \geq 2$ and $a \equiv b\left(\textbf{mod } m\right)$, then $\gcd\left(a,\ m\right) = \gcd\left(b,\ m\right)$

19. Prove or disprove that $n^2 - 79n + 1601$ is prime whenever *n* is a positive integer.