be written as the sum of two integers, each of which is the product of at most nine primes. (In these results a prime is counted in a product according to its exponent, so 12 would be considered a product of three primes: 2, 2, and 3.) By 1940 A. Buchstab had reduced the number 9 to 4. In 1948 A. Rényi demonstrated the existence of a number $k$ such that every large even number is the sum of a prime and an integer having at most $k$ prime factors, and by 1963 the mathematician Pan had reduced $k$ to 4. This improved Selberg's 1950 result that every large even number could be expressed as $p + q$, where $pq$ had at most five prime factors. In 1965 Buchstab proved the Rényi theorem with $k = 3$. The best theorem to date along these lines is that of the Chinese mathematician Chen, announced in 1966 and published in 1973, that every sufficiently large even integer is the sum of a prime and a number that is the product of at most two primes. If 2 could be replaced by 1 the Goldbach conjecture would be essentially proved.

This little history indicates the international nature of mathematics. A conjecture made by a German who lived in Russia in a letter to a Swiss and published by an Englishman has been worked on by mathematicians of many nations, with the last word so far belonging to a Chinese.

Probably no area of mathematics has been studied more for the sheer enjoyment of its ideas and problems than the theory of numbers. The author hopes that you, the reader, will discover some of the beauty and ingenuity that past generations of number theorists, amateur and professional, have found in the subject.

Problems for Chapter 0.

1. List all primes $p < 50$ such that $p + 2$ is also prime.
2. Write each even integer $n$, $10 < n < 30$, as a sum $p + q$ of two primes with $p$ as small as possible.
3. For which integers $n$, $6 < n < 14$, is $n^2 + 1$ prime?
4. For which integers $n$, $1 < n < 14$, is $n^3 + 1$ prime?
5. Prove that if $n > 0$ and $n^2 + 1$ is prime, then $n = 1$ or $n$ is even.
6. Prove that if $n > 0$ and $n^2 + 1$ is prime, then $n = 1$.
7. What is the smallest prime number $> 31$ of the form $2^n - 1$?
8. What is the smallest prime number $> 17$ of the form $2^n + 1$?
9. What is the smallest perfect number $> 6$?
10. For which integers $n$, $7 < n < 15$, does the decimal expansion of $1/n$ repeat every $n - 1$ digits, but no smaller number of digits?
11. Show that if $n$ is any odd positive integer, and $m = (n^2 - 1)/2$, then $m^2 + n^2 = (m + 1)^2$.
12. Show that if $u$ and $v$ are any integers with $0 < v < u$, and if $x = 2uv$, $y = u^2 - v^2$, and $z = u^2 + v^2$, then $x^2 + y^2 = z^2$.
13. List all primes $< 100$ of the form $6n + 1$.
14. List all primes $< 100$ of the form $7n + 3$.
15. List all primes $< 100$ of the form $8n + 6$. 
Now \( r = m - q[a, b] \). By hypothesis \( a \mid m \), and \( a \mid [a, b] \) by the definition of the lcm. Thus \( a \mid r \) by Theorem 1.2 (with \( x = 1 \) and \( y = -q \)). The same argument shows that \( b \mid r \). We see that \( r \) is a common multiple of \( a \) and \( b \). But the inequality \( 0 < r < [a, b] \) contradicts the fact that \( [a, b] \) is the least positive common multiple of \( a \) and \( b \).

Since the assumption that \([a, b]\) does not divide \( m \) leads to a contradiction, we conclude that \([a, b]\) divides \( m \).

### Writing Proofs

The proofs of three theorems are given in this section. From them we may draw some simple lessons about how proofs are expressed.

A proof should be written in sentences. These sentences are written in the English language, even though some technical words or symbols may be used. They should start with capital letters (so a sentence should not begin with a symbol) and end with periods. Other conventional punctuation should be used as appropriate.

The most important thing to think about when writing up a proof is who is going to read it. Ivan Niven said, "a proof is something that convinces somebody." It is a communication between humans. It is not sufficient that the writer of the proof believes it; enough detail must be given so that the reader will also understand and believe. The burden of making oneself understood rests on the writer of the proof.

### Problems for Section 1.1.

**A**

1. True or false? \( 7 \mid 203, \ 16 \mid -1000, -6 \mid 3 \).
2. True or false? \( 75 \mid 3000, \ 71 \mid 0, 0 \mid -12 \).
3. Find \( d > 0 \) such that \( d \mid 18, d \nmid 12, \) and \( 36/d \nmid 10 \).
4. Find \( d > 0 \) such that \( d \mid 1000, 5 \mid d, d \mid 60, \) and \( d/2 \mid 75 \).
5. Find \([51, 34]\) and \([51, 34]\).
6. Find \([16, 81]\) and \([16, 81]\).
7. Find all \( d > 0 \) such that \( 18 \mid d \) and \( d \mid 216 \).
8. Find all \( d > 0 \) such that \( 20 \mid d \) and \( d \mid 300 \).
9. What are all the divisors of 24?
10. What are all the divisors of 30?
11. What are the multiples of 4 between \(-25\) and 25?
12. What are the multiples of 5 between \(-42\) and 42?
13. Make a table showing \( b, (a, b), [a, b], \) and \((a, b)[a, b]\) for \( a = 8 \) and \( b \) running from 1 to 9.
14. Make a table as in the problem 13 for \( a = 9 \) and \( b \) running from 1 to 10.

**B**

15. For what integers \( a \) is \( 1 \mid a \) true?
16. For what integers \( a \) is \( a \mid 0 \) true?
17. For what integers \( a \) is \( a \mid b \) true for all integers \( b \)?
1.2. THE DIVISION ALGORITHM

multiple of $a$ and $b$, from which we conclude that

$$\frac{ab}{(a,b)} \geq [a,b]. \quad [\text{Question 3: Why?} ]$$

If we could prove this inequality in the opposite direction, we would be done. Let us start over by considering $ab/[a,b]$. This is an integer. [Question 4: Why?] Also

$$\frac{a}{ab/[a,b]} = \frac{[a,b]}{b},$$

which is an integer. [Question 5: Why?] Thus $ab/[a,b]$ divides $a$. A similar proof shows that $ab/[a,b]$ divides $b$. We see that $ab/[a,b]$ is a common divisor of $a$ and $b$. Thus

$$\frac{ab}{[a,b]} \leq (a,b). \quad [\text{Question 6: Why?} ]$$

Since the two inequalities we have proved are equivalent to

$$ab \geq (a,b)[a,b] \quad \text{and} \quad ab \leq (a,b)[a,b],$$

the theorem follows. \hfill \square

Problems for Section 1.2.

Find the $q$ and $r$ guaranteed by the division algorithm for each pair $a$, $b$ in problems 1 through 12.

A

1. $a = 13$, $b = 380$
2. $a = 15$, $b = 421$
3. $a = 720$, $b = 155$
4. $a = 339$, $b = 17$
5. $a = 17$, $b = 51$
6. $a = 21$, $b = 105$
7. $a = 19$, $b = 0$
8. $a = 35$, $b = 0$
9. $a = 7$, $b = -30$
10. $a = 9$, $b = -29$
11. $a = 43$, $b = -500$
12. $a = 47$, $b = -500$

B

13. What are all the common divisors of 12 and 18?
14. What are all the common divisors of 45 and 75?
15. What are all the common multiples of 4 and 6?
16. What are all the common multiples of 27 and 18?

True-False. In the next eight problems, tell which statements are true and give counterexamples for those that are false. Assume $a$, $b$, $c$, and $d$ are arbitrary integers with $a > 0$ and $c$ and $d$ nonzero.

17. There exist integers $q$ and $r$, $0 \leq r < c$, such that $b = cq + r$.
18. There exist integers $q$ and $r$, $0 \leq r < |c|$, such that $b = cq + r$.
19. There exist integers $q$ and $r$, $|r| \leq a/2$, such that $b = aq + r$.
20. There exist integers $q$ and $r$, $|r| < a/2$, such that $b = aq + r$. 
21. The set of common divisors of \( b \) and \( c \) is the set of divisors of \( (b, c) \).
22. The set of common multiples of \( c \) and \( d \) is the set of multiples of \( [c, d] \).
23. If \( b \) is a divisor of \( c \), and \( b > (c, d) \), then \( b \) is not a divisor of \( d \).
24. If \( b \) is a multiple of \( c \), and \( b < [c, d] \), then \( b \) is not a multiple of \( d \).

The next three problems refer to the following conditions: (i) \( a \mid b \), (ii) \( 2^a \mid b^2 \), (iii) \( 2^a \leq b \).

25. Give positive integers \( a \) and \( b \) such that (i) and (ii) hold, but not (iii).
26. Give positive integers \( a \) and \( b \) such that (i) and (iii) hold, but not (ii).
27. Give positive integers \( a \) and \( b \) such that (ii) and (iii) hold, but not (i).

28. Prove that if \( ab \neq 0 \), then \( (a, b)[a, b] = |ab| \).
29. Prove that \( (a, a + 2) \) is 2 if \( a \) is even and 1 if \( a \) is odd.
30. Prove that if \( a > 0 \), then \( [a, a + 2] = a(a + 2)/2 \) if \( a \) is even and \( a(a + 2) \)
   if \( a \) is odd.
31. Prove that if \( x > 0 \), then \( (a, a + x) \) is \( (a, x) \).
32. Prove that if \( d \mid a \), \( d \mid b \), and \( d \mid c \), and if \( x, y, \) and \( z \) are any integers, then \( d \)
   divides \( ax + by + cz \).
33. Prove that if \( a \mid b \), \( b \mid c \), and \( c \mid d \), then \( a \mid d \).
34. Prove that if \( a \mid b \) and \( b \mid c \), then \( a \) divides \( ax + by + cz \) for any integers \( x, y, \) and \( z \).
35. Prove that if \( b \neq 0 \) and \( a = bx + cy \), then \( (b, c) \leq (a, b) \).
36. Prove that with the hypotheses of the last problem, \( (b, c) \mid (a, b) \).

Answers to questions in the proof of the Theorem 1.5.

1. By hypothesis \( ab > 0 \), and \( (a, b) > 0 \) since if \( d \) is a common divisor, then
   so is \(|d|\).

2. By the definition of \((a, b)\).

3. Since \(|a, b|\) is the least common multiple of \(a\) and \(b\).

4. By Theorem 1.3.

5. By the definition of \(|a, b|\).

6. Since \((a, b)\) is the greatest common divisor of \(a\) and \(b\).