

1.1.5. Prove that the square of any integer  $a$  is either of the form  $3k$  or of the form  $3k + 1$  for some integer  $k$ .

[Hint: By the Division Algorithm,  $a$  must be of the form  $3q$  or  $3q + 1$  or  $3q + 2$ .]

Let  $a \in \mathbb{Z}$  be given. Then applying the Division Algorithm with  $b = 3$ , there are unique integers  $q$  and  $r$  such that

$$a = 3q + r \quad \text{and} \quad 0 \leq r < 3.$$

Since  $0 \leq r < 3$ , we have  $r = 0, 1$  or  $2$  and so  $a$  must be of the form  $3q$  or  $3q + 1$  or  $3q + 2$  for some integer  $q$ . We consider each of these cases separately. Suppose first that  $a = 3q$  for some integer  $q$ . Then

$$a^2 = (3q)^2 = 9q^2 = 3(3q^2) = 3k \quad \text{where} \quad k = 3q^2 \in \mathbb{Z}.$$

Next, suppose that  $a = 3q + 1$  for some integer  $q$ . Then

$$a^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3k + 1 \quad \text{where} \quad k = 3q^2 + 2q \in \mathbb{Z}.$$

Finally, suppose that  $a = 3q + 2$  for some integer  $q$ . Then

$$a^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1 = 3k + 1 \quad \text{where} \quad k = 3q^2 + 4q + 1 \in \mathbb{Z}.$$

Hence, in each case  $a^2$  is either of the form  $3k$  or of the form  $3k + 1$  for some integer  $k$ . ◆

1.2.14. Find the smallest positive integer in the given set:

(a)  $\{6u + 15v \mid u, v \in \mathbb{Z}\}$

By Theorem 1.3 the smallest positive integer in the set is  $(6, 15)$ , the greatest common divisor of 6 and 15. The common divisors of 6 and 15 are  $\pm 1, \pm 3$ . Hence,  $(6, 15) = 3$  is the smallest positive integer in the set. ◆

(b)  $\{12r + 17s \mid r, s \in \mathbb{Z}\}$

As above the smallest positive integer in the set is  $(12, 17)$ , the greatest common divisor of 12 and 17. The only common divisors of 12 and 17 are  $\pm 1$ . Hence,  $(12, 17) = 1$  is the smallest positive integer in the set. ◆

1.2.29. If  $c \mid ab$  and  $(c, a) = d$ , prove that  $c \mid db$ .

Suppose that  $c \mid ab$  and  $(c, a) = d$  where  $a, b, c, d \in \mathbb{Z}$ . Then  $ab = ce$  for some  $e \in \mathbb{Z}$  and by Theorem 1.3  $d = cu + av$  for some  $u, v \in \mathbb{Z}$ . Hence, we have

$$db = (cu + av)b = cub + abv = cub + cev = c(ub + ev).$$

Therefore,  $c \mid db$  since  $ub + ev \in \mathbb{Z}$ . ◆

1.3.6. If  $p$  is prime and  $p \mid a^n$ , is it true that  $p^n \mid a^n$ ? Justify your answer.

Yes. Let  $p$  be a prime and let  $a$  be an integer and suppose that  $p \mid a^n$ . Then  $p \mid a_1 a_2 \cdots a_n$  where  $a_i = a$  for  $i = 1, \dots, n$  (since  $a^n = a_1 a_2 \cdots a_n$ ). Hence, by Corollary 1.9,  $p \mid a_i$  for some  $i = 1, \dots, n$ , that is,  $p \mid a$ ; thus,  $a = pb$  for some  $b \in \mathbb{Z}$ . Since,

$$a^n = (pb)^n = p^n(b^n) \quad \text{and} \quad b^n \in \mathbb{Z},$$

it follows that  $p^n \mid a^n$ . ◆

1.3.19. If  $n \in \mathbb{Z}$  and  $n \neq 0$ , prove that  $n$  can be written uniquely in the form  $n = 2^k m$ , where  $k \geq 0$  and  $m$  is odd.

Let  $n \in \mathbb{Z}$  with  $n \neq 0$ . We first prove that such an expression must be unique. That is, we show that it can be written thus in at most one way. Suppose that

$$n = 2^{k_1} m_1 = 2^{k_2} m_2$$

for integers  $k_i \geq 0$  and  $m_i$  odd. To prove uniqueness we must show that  $k_1 = k_2$  and  $m_1 = m_2$ . By cancellation it suffices to show that  $k_1 = k_2$ . Suppose that  $k_1 \neq k_2$ ; by relabelling if necessary we may assume  $k_1 < k_2$ . After dividing both sides of the above equation by  $2^{k_1}$  we obtain  $m_1 = 2^{k_2 - k_1} m_2$ ; since  $k_2 - k_1 > 0$ ,  $m_1$  must be divisible by 2 and therefore  $m_1$  is even. This results in a contradiction since  $m_1$  is odd. Hence, the expression is unique.

Next we show that  $n$  may be written in this form. Suppose first that  $n$  is a positive integer. Then  $n$  is either odd or even. If  $n$  is odd, then we have  $n = 2^0 n$ . Suppose  $n$  is even, then  $n > 1$  and by Corollary 1.12  $n = p_1 p_2 \cdots p_r$ , where  $p_i$  are positive primes such that  $p_1 \leq p_2 \leq \cdots \leq p_r$ . Since  $n$  is even,  $2 \mid n$  and thus  $2 \mid p_i$  for some  $i$  (by Cor. 1.9); so  $p_i = 2$  for some  $i$ , since 2 itself is prime. But 2 is the smallest positive prime so there is an integer  $k$  with  $1 \leq k \leq r$  such that  $p_i = 2$  if  $1 \leq i \leq k$  and  $p_i$  is an odd prime if  $k < i \leq r$ . We set

$$m = \begin{cases} p_{k+1} \cdots p_r & \text{if } k < r \\ 1 & \text{if } k = r. \end{cases}$$

In either case  $m$  is odd and  $n = 2^k m$ . If  $n < 0$ , then by the above argument there are integers  $k, m'$  with  $k \geq 0$  and  $m'$  odd so that  $-n = 2^k m'$ . If we set  $m = -m'$ , we have  $m$  is odd and  $n = -2^k m' = 2^k m$  as required. ◆