

Selected Strayer Exercise Solutions

James K. Strayer, “Elementary Number Theory”, Waveland Press, 2002

(last updated September 30, 2007)

1.1.10(b). Let $n \in \mathbb{Z}$. Prove that $5 \mid n^5 - n$.

Solution. The result holds for $n = 1$ since $1^5 - 1 = 0$ and $5 \mid 0$. Assume that the result holds for $n = k$, where $k \geq 1$. Then $n \mid k^5 - k$. We will show that $5 \mid (k+1)^5 - (k+1)$. We calculate $(k+1)^5 - (k+1) = (k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1) - (k+1) = (k^5 - k) + 5(k^4 + 2k^3 + 2k^2 + k)$. Now 5 divides $k^5 - k$ by induction hypothesis and 5 obviously divides $5(k^4 + 2k^3 + 2k^2 + k)$, so $5 \mid (k+1)^5 - (k+1)$. By mathematical induction, $5 \mid n^5 - n$ for all integers $n \geq 1$. The result holds for $n = 0$ since $5 \mid 0^5 - 0 = 0$. Finally suppose that $n < 0$. Write $n = -m$, where m is a positive integer. Then $n^5 - n = (-m)^5 - (-m) = -(m^5 - m)$. We have proved that $5 \mid m^5 - m$, and it follows immediately that $5 \mid n^5 - n$.

1.2.25(b). Prove that no prime number can be expressed as the difference of two fourth powers of integers.

Solution. Suppose on the contrary that p is a prime number and that $p = a^4 - b^4$, where $a, b \in \mathbb{Z}$. Then $p = (a^2 + b^2)(a^2 - b^2)$. Since $|a|^2 = a^2$ and $|b|^2 = b^2$, we can assume without loss of generality that $a, b \geq 0$. We can also assume that $p > 1$, so that $a > b$. Also $b > 0$, since if $b = 0$, then $1 < p = a^4$, contradicting the assumption that p is prime. Factoring further, we get $p = (a^2 + b^2)(a + b)(a - b)$. It is easy to show that $a^2 + b^2 > a + b > a - b > 0$. [Note that $a > b > 0 \Rightarrow a > 1 \Rightarrow a^2 > a$ and that $b \geq 1 \Rightarrow b^2 \geq b$, so $a^2 + b^2 > a + b$. Also $(a + b) - (a - b) = 2b > 0$, so $a + b > a - b$.] Thus p has three distinct positive factors, contradicting the assumption that p is prime.

1.3.37. Let $a, b \in \mathbb{Z}$ with a and b not both zero and let c be a nonzero integer. Prove that $(ca, cb) = |c|(a, b)$.

Solution. METHOD 1. Set $d = (a, b)$. Since d is a common divisor of a and b , it follows that $|c|d$ is a common divisor of ca and cb . We want to show that it is the *greatest* common divisor of ca and cb . Suppose it isn't. Then $(ca, cb) = e > |c|d$. Since $|c|$ is a common divisor of ca and cb , it must divide their greatest common divisor. Thus $e = |c|f$ where $f > d$. Since $e \mid ca$ and $e \mid cb$, it follows that $f \mid a$ and $f \mid b$, contradicting our assumption that d is the greatest common divisor of a and b .

METHOD 2. Let $d = (a, b)$ and $e = (ca, cb)$. Clearly $e = (|c|a, |c|b)$, so it suffices to show that $e = cd$ when $c > 0$. Assume $c > 0$. By Proposition 1.11, there exist integers m and n such that $d = ma + nb$. Thus $cd = m(ca) + n(cb)$. Since $e \mid ca$ and $e \mid cb$, it follows that $e \mid cd$. Next we show that $cd \mid e$. Since $d \mid a$ and $d \mid b$, we can write $a = dr$ and $b = ds$ for some integers r and s . Thus $ca = (cd)r$ and $cb = (cd)s$, showing that $cd \mid ca$ and $cd \mid cb$. Hence $cd \mid e$ by the remark above Definition 10 on page 20. Since $e \mid cd$ and $cd \mid e$, we have $e = cd$ as required.

METHOD 3. We'll show that the set S of common divisors of ca and cb is the same as the set T of numbers of the form ed , where e is a divisor of c and d is a common divisor of a and b . First, $T \subseteq S$ since if e divides c and d is a common divisor of a and b , then ed divides ca and cb . To show that $S \subseteq T$, let $n \in S$ and let $k = (n, c)$. Since $n \mid ca$, we have $n/k \mid (c/k)a$. But $(n/k, c/k) = 1$ by Proposition 1.10. Hence by Proposition

1.11 there are integers r and s such that $r(n/k) + s(c/k) = 1$. Multiplying by a , we get $r(n/k)a + s(c/k)a = a$. Now n/k divides the first term and n/k divides the second term [since $n/k \mid (c/k)a$], so n/k divides a . An analogous argument starts from $n \mid cb$ and shows that n/k divides b . Hence $n = k(n/k)$, showing that n is the product of k , which divides c , and n/k , which is a common divisor of a and b . This proves that $S \subseteq T$, so $S = T$. Now (ca, cb) is defined to be the greatest element of S , so it must also be the greatest element of T . But the greatest element of T is obviously the greatest divisor of c times the greatest common divisor of a and b , so $(ca, cb) = |c|(a, b)$.

Remark. Method 3 contains a (slightly disguised) solution to Exercise 1.3.44(a). Can you find it?

METHOD 4. Since $(ca, cb) = (|c|a, |c|b)$, we can rephrase the desired conclusion as $(|c|a, |c|b) = |c|(a, b)$. Thus it will suffice to prove that $(ca, cb) = c(a, b)$ when $c > 0$. But by Proposition 1.11, if $c > 0$, then

$$\begin{aligned} (ca, cb) &= \min\{m(ca) + n(cb) : m, n \in \mathbb{Z}; m(ca) + n(cb) > 0\} \\ &= \min\{c(ma + nb) : m, n \in \mathbb{Z}; ma + nb > 0\} \\ &= c \min\{ma + nb : m, n \in \mathbb{Z}; ma + nb > 0\} = c(a, b). \end{aligned}$$

1.3.38. Let a and b be relatively prime integers. Prove that $(a + b, a - b)$ is either 1 or 2.

Solution. METHOD 1. If $d = (a + b, a - b)$, then $d \mid a + b$ and $d \mid a - b$, so by Proposition 1.2, $d \mid (a + b) + (a - b) = 2a$ and $d \mid (a + b) - (a - b) = 2b$. Since $d \mid 2a$ and $d \mid 2b$, it follows from a remark in the paragraph after the proof of Proposition 1.11 that $d \mid (2a, 2b)$. By Exercise 1.3.37, $(2a, 2b) = 2(a, b) = 2 \cdot 1 = 2$. Thus $d \mid 2$. Since $d > 0$, we must have $d = 1$ or 2.

METHOD 2. As in METHOD 1, we can show that $d \mid 2a$ and $d \mid 2b$. Since $(a, b) = 1$, by Proposition 1.11 there are integers $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. Multiplying this relation by 2, we see that $m(2a) + n(2b) = 2$. Since $d \mid 2a$ and $d \mid 2b$, it follows that $d \mid 2$, so $d = 1$ or 2.

1.3.42(a). Let $a, b, c \in \mathbb{Z}$ with $(a, b) = (a, c) = 1$. Prove that $(a, bc) = 1$.

Solution. By Proposition 1.11, there are integers m and n such that $ma + nb = 1$. Similarly there are integers r and s such that $ra + sc = 1$. Multiplying these two relations, we get $(mra + msc + nrb)a + (ns)(bc) = 1$. Let $d = (a, bc)$. Then $d \mid a$ and $d \mid bc$, so by the last relation, $d \mid 1$. Therefore $d = 1$.

1.3.44(a). Let $a, b, c \in \mathbb{Z}$ with $(a, b) = 1$ and $a \mid bc$. Prove that $a \mid c$.

Solution. By proposition 1.11, there are integers m and n such that $ma + nb = 1$. Multiplying by c gives $mac + nbc = c$. Now $a \mid mac$ and $a \mid nbc$ (since $a \mid bc$), so $a \mid c$.

1.3.53. Let $n \in \mathbb{Z}$. Prove that the integers $6n - 1$, $6n + 1$, $6n + 2$, $6n + 3$, and $6n + 5$ are pairwise relatively prime.

Solution. There are ten pairs of integers to consider, but we don't need ten different proofs. First consider the pairs $(6n - 1, 6n + 1)$, $(6n + 1, 6n + 3)$, and $(6n + 3, 6n + 5)$. If a is the first number of the pair and b is the second number, then $(-1)a + (1)b = b - a = 2$, so if $d = (a, b)$, then from $d \mid a$ and $d \mid b$, we see (Proposition 1.11) that $d \mid 2$. Therefore $d = 1$ or 2. Since a and b are both odd, $d = 1$. Next consider the pairs $(6n - 1, 6n + 2)$ and $(6n + 2, 6n + 5)$ and use analogous notation. This time $b - a = 3$, so $d \mid 3$, forcing $d = 1$ or

3. Neither a nor b is a multiple of 3, so $d = 1$. Next consider the pairs $(6n - 1, 6n + 3)$ and $(6n + 1, 6n + 5)$. We have $b - a = 4$, so $d \mid 4$ and $d = 1, 2$, or 4 . Neither a nor b is even, so $d = 1$. For the pair $(6n - 1, 6n + 5)$, we have $b - a = 6$, so $d = 1, 2, 3$, or 6 . Neither a nor b is even or a multiple of 3, so $d = 1$. Finally we have the pairs $(6n + 1, 6n + 2)$ and $(6n + 2, 6n + 3)$. For these pairs, $b - a = 1$, so $d \mid 1$, showing that $d = 1$.