CS1231(S) Tutorial 6: Number theory 1 Solutions

National University of Singapore

2020/21 Semester 1

1. Let $a, b \in \mathbb{Z}$. Show that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

   Solution.

   1. Let $a, b \in \mathbb{Z}$ such that $a \mid b$ and $b \mid a$.
   2. Case 1: suppose $a \neq 0 \neq b$.
      2.1. Then $|a| \leqslant |b|$ and $|b| \leqslant |a|$ by Proposition 8.1.10.
      2.2. So $|a| = |b|$.
      2.3. If $a, b \geqslant 0$, then $a = |a| = |b| = b$.
      2.4. If $a, b < 0$, then $-a = |a| = |b| = -b$ and so $a = b$.
      2.5. If $a \geqslant 0$ and $b < 0$, then $a = |a| = |b| = -b$.
      2.6. If $a < 0$ and $b \geqslant 0$, then $-a = |a| = |b| = b$ and so $a = -b$.
      2.7. In all cases, we have $a = b$ or $a = -b$.
   3. Case 2: suppose $a = 0$.
      3.1. Use the definition of $a \mid b$ to find $k \in \mathbb{Z}$ such that $b = ak$.
      3.2. Then $b = ak = 0 \cdot k = 0 = a$.
   4. Case 3: suppose $b = 0$.
      4.1. Use the definition of $b \mid a$ to find $\ell \in \mathbb{Z}$ such that $a = b\ell$.
      4.2. Then $a = b\ell = 0 \cdot \ell = 0 = b$.
   5. Thus $a = b$ or $a = -b$ in all cases. □

2. Find the quotient and the remainder when

   (a) 44 is divided by 8;
   (b) 777 is divided by 21;
   (c) -123 is divided by 19;
   (d) 0 is divided by 17;
   (e) -100 is divided by 101.

   Solution.

   (a) The quotient is 5 and the remainder is 4.
   (b) The quotient is 37 and the remainder is 0.
   (c) The quotient is -7 and the remainder is 10.
   (d) The quotient is 0 and the remainder is 0.
   (e) The quotient is -1 and the remainder is 1.

3. Show that for all odd integers $n \in \mathbb{Z}$,

$$n^2 \underline{\operatorname{div}} 4 = \frac{n^2 - 1}{4}.$$

   Solution.

1. Use the hypothesis that n is odd to find $k \in \mathbb{Z}$ such that $n = 2k+1$.
2. This implies $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k) + 1$, where $0 \leqslant 1 < 4$.
3. So $n^2 \,\underline{\text{div}}\, 4 = k^2 + k$ by the uniqueness of quotients and remainders (provided by Theorem 8.1.16).
4. Line 1 also implies
$$\frac{n^2-1}{4} = \frac{(2k+1)^2-1}{4} = \frac{(4k^2+4k+1)-1}{4} = \frac{4(k^2+k)}{4} = k^2+k.$$
5. Putting lines 3 and 4 together, we see that $n^2 \,\underline{\text{div}}\, 4 = k^2 + k = (n^2-1)/4$. □

4. Is 107 prime? Is 113 prime?

   Solution. Note that $\sqrt{113} < 11$. The only primes strictly less than 11 are $2, 3, 5, 7$. Direct calculations reveal that none of these is a divisor of 107 or 113. So both 107 and 113 are prime by Proposition 8.2.6.

5. Write down an integer $n \geqslant 1231$ that shares no prime divisor with 15811090783488000. Prove that your answer is correct. Did you implicitly or explicitly use the Fundamental Theorem of Arithmetic (i.e., the fact that every positive integer greater than 1 has a unique factorization into a product of primes) in your proof? If yes, then can you avoid it (possibly by choosing a different n)?

   Solution. Let $m = 15811090783488000$ and $n = m + 1$. We claim that m and n have no common prime divisor. We prove this claim by contradiction.

   1. Let p be a prime number such that $p \mid m$ and $p \mid n$.
   2. Then $p \mid (n-m)$ by the Closure Lemma.
   3. In other words, we know $p \mid 1$ as $n - m = 1$.
   4. This implies $p = |p| \leqslant |1| = 1$ by Proposition 8.1.10 as $1 \neq 0$.
   5. We also know $p \geqslant 2$ since p is prime.
   6. Putting lines 4 and 5 together, we deduce that $2 \leqslant p \leqslant 1$, which is a contradiction. □

   This proof does not use the Fundamental Theorem of Arithmetic.

6.* An integer n is said to be a *perfect square* if $n = k^2$ for some $k \in \mathbb{Z}$. Prove that a positive integer n is a perfect square if and only if it has an odd number of positive divisors.

   (Hint: pair up the divisors strictly bigger than $\sqrt{n}$ and the divisors strictly smaller than $\sqrt{n}$.)

   Solution.

   1. If $d \mid n$ with $1 \leqslant d < \sqrt{n}$, then $d' \mid n$ with $\sqrt{n} < d' \leqslant n$, where $d' = n/d$.
   2. If $d' \mid n$ with $\sqrt{n} < d' \leqslant n$, then $d \mid n$ with $1 \leqslant d < \sqrt{n}$, where $d = n/d'$.
   3. Since $n/(n/d) = d$ for all divisors d of n, we see that each positive divisor d of n strictly less than $\sqrt{n}$ can be paired up with exactly one positive divisor d' of n strictly bigger than $\sqrt{n}$.
   (Formally speaking, we established here a bijection
   $$\{d \in \mathbb{Z}^+ : d \mid n \text{ and } 1 \leqslant d < \sqrt{n}\} \to \{d' \in \mathbb{Z}^+ : d' \mid n \text{ and } \sqrt{n} < d' \leqslant n\}$$
   which maps each d to n/d.)
   4. Hence the number of divisors of n that are different from $\sqrt{n}$ is even. Let this number be $2k$, where $k \in \mathbb{Z}_{\geqslant 0}$.
   5. If n is a perfect square, then $\sqrt{n}$ is also a divisor of n, and so the total number of divisors of n is $2k+1$, which is odd.
   6. Conversely, if n is not a perfect square, then $\sqrt{n} \notin \mathbb{Z}$ and so the total number of divisors of n is $2k$, which is not odd by Corollary 8.1.22. □

7. Find the binary, octal and hexadecimal expansions of 1231.

   Solution. $(1231)_{10} = (10011001111)_2 = (2317)_8 = (4\text{CF})_{16}$.

8. Find the decimal expansions of

   (a) $(1101001)_2$;

   (b) $(156)_8$;

   (c) $(74)_{16}$.

   Solution.

   (a) 105. (b) 110. (c) 116.

9.* Let $n \in \mathbb{Z}_{\geqslant 1}$ with decimal representation $(a_\ell a_{\ell-1} \dots a_0)_{10}$. Prove that $9 \mid n$ if and only if $9 \mid (a_0 + a_1 + \cdots + a_\ell)$.

   (Hint: for example,

$$\begin{aligned}
7524 &= 7 \times 1000 + 5 \times 100 + 2 \times 10 + 4 \\
&= 7 \times (999 + 1) + 5 \times (99 + 1) + 2 \times (9 + 1) + 4 \\
&= (7 \times 999 + 7) + (5 \times 99 + 5) + (2 \times 9 + 2) + 4 \\
&= (7 \times 999 + 5 \times 99 + 2 \times 9) + 7 + 5 + 2 + 4 \\
&= 9 \times (7 \times 111 + 5 \times 11 + 2 \times 1) + (7 + 5 + 2 + 4).
\end{aligned}$$

   You may use without proof the fact that

$$10^i = 9 \times 10^{i-1} + 9 \times 10^{i-2} + \cdots + 9 \times 10^0 + 1$$

   for all $i \in \mathbb{Z}_{\geqslant 0}$.)

   Solution using the summation notation.

   1. $$n = \sum_{i=0}^{\ell} a_i 10^i \qquad \text{as } n = (a_\ell a_{\ell-1} \dots a_0)_{10};$$

   2. $$= \sum_{i=0}^{\ell} a_i \left(\left(\sum_{j=0}^{i-1} 9 \times 10^j \right) + 1 \right) \qquad \text{by the fact provided;}$$

   3. $$= \sum_{i=0}^{\ell} a_i \sum_{j=0}^{i-1} 9 \times 10^j + \sum_{i=0}^{\ell} a_i$$

   4. $$= 9 \sum_{i=0}^{\ell} \sum_{j=0}^{i-1} a_i 10^j + \sum_{i=0}^{\ell} a_i, \qquad \text{where } \sum_{i=1}^{\ell} \sum_{j=0}^{i-1} a_i 10^j \in \mathbb{Z}.$$

      (Remember that multiplication has a higher order of precedence than addition. In addition, the empty sum is defined to be 0.)

   5. If $9 \mid n$, then

      5.1. $$9 \,\middle|\, \left(n - 9 \sum_{i=0}^{\ell} \sum_{j=0}^{i-1} a_i 10^j \right) \qquad \text{by the Closure Lemma, as } 9 \mid 9 \textstyle\sum_{i=0}^{\ell} \sum_{j=0}^{i-1} a_i 10^j;$$

      5.2. $$\therefore\ 9 \,\Big|\, \sum_{i=0}^{\ell} a_i \qquad \text{by line 4.}$$

   6. Conversely, if $9 \mid \sum_{i=0}^{\ell} a_i$, then

6.1. $9 \,\Big|\, \Big(9\sum_{i=0}^{\ell}\sum_{j=0}^{i-1} a_i 10^j + \sum_{i=0}^{\ell} a_i\Big)$ by the Closure Lemma, as $9 \mid 9\sum_{i=0}^{\ell}\sum_{j=0}^{i-1} a_i 10^j$;

6.2. $\therefore\ 9 \mid n$ by line 4.

Solution without using the summation notation.

1. $n = a_\ell 10^\ell + a_{\ell-1}10^{\ell-1} + \cdots + a_0 10^0$ as $n = (a_\ell a_{\ell-1}\ldots a_0)_{10}$;

2. $= a_\ell(9\times 10^{\ell-1} + 9\times 10^{\ell-2} + \cdots + 9\times 10^0 + 1)$
$+ a_{\ell-1}(9\times 10^{\ell-2} + 9\times 10^{\ell-3} + \cdots + 9\times 10^0 + 1)$
$+ \cdots + a_1(9\times 10^0 + 1) + a_0 1$ by the fact provided;

3. $= 9a_\ell(10^{\ell-1} + 10^{\ell-2} + \cdots + 10^0) + a_\ell$
$+ 9a_{\ell-1}(10^{\ell-2} + 10^{\ell-3} + \cdots + 10^0) + a_{\ell-1}$
$+ \cdots + 9a_1(10^0) + a_1 + a_0$

4. $= 9\big(a_\ell 10^{\ell-1} + a_\ell 10^{\ell-2} + \cdots + a_\ell 10^0$
$+ a_{\ell-1}10^{\ell-2} + a_{\ell-1}10^{\ell-3} + \cdots + a_{\ell-1}10^0$
$+ \cdots + a_1 10^0\big)$
$+ (a_0 + a_1 + \cdots + a_\ell)$

5. $= 9m + (a_0 + a_1 + \cdots + a_\ell)$,
where $m \coloneqq a_\ell 10^{\ell-1} + a_\ell 10^{\ell-2} + \cdots + a_\ell 10^0 + a_{\ell-1}10^{\ell-2} + a_{\ell-1}10^{\ell-3} + \cdots + a_{\ell-1}10^0 + \cdots + a_1 10^0 \in \mathbb{Z}$.

6. If $9 \mid n$, then

6.1. $9 \mid (n - 9m)$ by the Closure Lemma, as $9 \mid 9m$;

6.2. $\therefore\ 9 \mid (a_0 + a_1 + \cdots + a_\ell)$ by line 4.

7. Conversely, if $9 \mid (a_0 + a_1 + \cdots + a_\ell)$, then

7.1. $9 \mid \big(9m + (a_0 + a_1 + \cdots + a_\ell)\big)$ by the Closure Lemma, as $9 \mid 9m$;

7.2. $\therefore\ 9 \mid n$ by line 4.