

18.781: SKETCHED SOLUTIONS FOR PS1

MARTIN OLSSON

1.2 (2)

$$\begin{aligned}3587 &= 1(1819) + 1768 \\1819 &= 1(1768) + 51 \\1768 &= 34(51) + 34 \\51 &= 1(34) + 17 \\34 &= 2(17) + 0\end{aligned}$$

so $(3587, 1819) = 17$. To write

$$1819x + 3587y = 17$$

we solve the above equations “from the bottom up”. So

$$\begin{aligned}17 &= 51 - 1(34) \\&= 51 - (1768 - 34(51)) = 35(51) - 1768 \\&= 35(1819 - 1768) - 1768 = 35(1819) - 36(1768) \\&= 35(1819) - 36(3587 - 1819) = 71(1819) - 36(3587),\end{aligned}$$

so take $x = 71$ and $y = -36$.

1.2 (13)

Since $n^2 - n = n(n - 1)$, and for any integer n either n or $n - 1$ is even, it follows that $n^2 - n$ is always even.

Similarly, $n^3 - n = (n - 1)n(n + 1)$, and hence this number is divisible by 2, and also since one of any three consecutive numbers is divisible by 3, the number $n^3 - n$ is also divisible by 3. It follows that $n^3 - n$ is divisible by 6.

As for $n^5 - n$, write $n^5 - n = n(n^2 - 1)(n^2 + 1)$, and note that by the above 6 divides this number. Therefore, it suffices to show that 5 divides $n^5 - n$. If 5 divides n or $n^2 - 1$, we are done, so suppose this is not the case, and write $n = 5k + r$, for some k and $0 < r < 5$. Then $n^2 - 1 = 25k^2 + 10kr + r^2 - 1$, and if 5 does not divide $n^2 - 1$, we see that r cannot be 1 or 4 since $1^2 - 1$ and $4^2 - 1$ are both divisible by 5. Thus, r is either 2 or 3. But in this case, $n^2 + 1 = 25k^2 + 10kr + r^2 + 1$, and for either $r = 2$ or $r = 3$ we see that this is divisible by 5.

1.2 (30)

$((x, y) = g$ and $xy = b$ can be solved implies $g^2|b$) The equality $(x, y) = g$ implies that $g|x$ and $g|y$, so we can write $x = gx_0$ and $y = gy_0$, in which case $g^2x_0y_0 = b$. Thus $g^2|b$.

$(g^2|b$ implies $(x, y) = g$ and $xy = b$ can be solved) Write $b = g^2b'$. Then taking $x = g$ and $y = gb'$ we obtain a solution to the equations.

1.2 (35) By (1.9), $(a, a + 2) = (a, 2)$. Since the only divisors of 2 are 1 and 2, it follows that $(a, 2)$ is either 1 or 2.

1.2 (44) We show by induction on n that any integer n can be written uniquely in the stated form. The case $n = 1$ is clear. So assuming the result for all integers smaller than n we prove the result for n . Let 2^{j_m} be the largest power of 2 smaller than or equal to n , and write $n = 2^{j_m} + n'$. Now note that $n' < 2^{j_m}$. If not, $n' = 2^{j_m} + r$ for some r in which case $n = 2^{j_m+1} + r$, which contradicts the maximality of j_m . Now by induction, we can write n' uniquely as a sum $2^{j_1} + \cdots + 2^{j_{m-1}}$ with $j_1 < \cdots < j_{m-1}$, and since $n' < 2^{j_m}$ we must have $j_{m-1} < j_m$. Note also that the fact

$$\sum_{j=0}^r 2^j = (2^{j+1} - 1) < 2^{j+1}$$

implies that if we write n as a sum

$$2^{l_0} + \cdots + 2^{l_r}$$

with $l_0 < l_1 < \cdots < l_r$, then l_r must be equal to j_m . From this and induction the uniqueness of the expression in the exercise follows.

1.2 (47) If $2^b - 1$ divides $2^a + 1$, then $2^b - 1$ divides $(2^b - 1) + 2^a + 1 = 2^b + 2^a$. Also, a must be greater than or equal to b since $b > 2$. Therefore, $2^b + 2^a = 2^b(1 + 2^{a-b})$, and since $2^b - 1$ is odd, $(2^b - 1, 2^b) = 1$ so $2^b - 1$ must divide $1 + 2^{a-b}$. Repeating the above argument we find that $2^b - 1$ divides $1 + 2^{a-2b}$. Repeating this (using induction) we see that $2^b - 1$ divides $1 + 2^{a-nb}$ for every n . But this is impossible, for choosing n sufficiently big we find that $0 \leq a - nb < b$, which is impossible.

1.2 (50) Note that $a^2 - ab + b^2 = (a + b)^2 - 3ab$, so by (1.9),

$$(a + b, a^2 - ab + b^2) = (a + b, -3ab).$$

Now if $g = (a + b, -3ab)$, then either $g = 3$, or there exists a non-trivial common divisor of $a + b$ and ab . But no such divisor exists for if a prime p divides ab , then either p divides a or b . Say $p|a$. Then if p also divides $a + b$, we must have $p|b$ as well, which contradicts $(a, b) = 1$. Thus $(a + b, ab) = 1$ so $(a + b, -3ab) = (a + b, 3)$ which must be either 1 or 3.

1.3 (4) If n is an integer, its “digits” are the integers $0 \leq a_i < 10$ which appear when we write n in base 10

$$(1) \quad n = a_0(10)^0 + a_1(10)^1 + \cdots + a_r(10)^r$$

for some r . Now notice that $10 = 3^2 + 1$, so we have

$$(2) \quad (n, 3) = (a_0(3^2 + 1)^0 + a_1(3^2 + 1)^1 + \cdots + a_r(3^2 + 1)^r, 3) = (a_0 + a_1 + \cdots + a_r, 3)$$

by 1.9. The same argument gives the result with 9 instead of 3.

1.3 (8) It suffices to prove the slightly stronger statement that if n is an integer with base 10 expansion

$$(3) \quad n = a_0(10)^0 + a_1(10)^1 + \cdots + a_r(10)^r,$$

then $(n, 7)$ is equal to

$$(a_1 + a_2(10) + \cdots + a_r(10)^{r-1} - 2a_0, 7)$$

which since $(10, 7) = 1$ is by 1.10 equivalent to showing that $(n, 7)$ is equal to

$$(10(a_1 + a_2(10) + \cdots + a_r(10)^{r-1} - 2a_0), 7).$$

But

$$10(a_1 + a_2(10) + \cdots + a_r(10)^{r-1} - 2a_0) = a_0(10)^0 + a_1(10)^1 + \cdots + a_r(10)^r - 21a_0 = n - 21a_0,$$

so the result follows from 1.9.

1.3 (9) If p is a prime of the form $3k + 1$, then p must be odd. This implies that k must be even, for otherwise $3k + 1$ is even. Thus $k = 2k'$, and we find that $p = 6k' + 1$ as desired.

1.3 (11) If x and y are odd, then $x^2 + y^2$ is even, so $2|x^2 + y^2$. Therefore, to show that $x^2 + y^2$ is not a perfect square, it suffices to show that $(x^2 + y^2, 4) = 2$. For this, write $x = 2k + 1$ and $y = 2l + 1$. Then

$$x^2 + y^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4(k^2 + k + l^2 + l) + 2.$$

By 1.9, we therefore have

$$(x^2 + y^2, 4) = (4(k^2 + k + l^2 + l) + 2, 4) = (2, 4) = 2$$

as desired.

1.3 (36) Suppose $l \in \{1, \dots, n\}$ is an integer not equal to 2^k which is divisible by 2^k . Say $n = 2^k m$ with m not equal to 1. If m is even, write $m = 2l$, and if m is odd write $m = 2l + 1$. Then $2^k(2l)$ is in $\{1, \dots, n\}$, and so 2^{k+1} is also in $\{1, \dots, n\}$ since $2^{k+1} \leq 2^{k+1}l$. This is a contradiction since k was assumed maximal.

To deduce that $\sum_{j=1}^n (1/j)$ is not an integer, let $\{p_1, \dots, p_r\}$ be the set of odd primes which appear in the prime factorization of any of the $j \in \{1, \dots, n\}$. Let $m = 2^{k-1}p_1^{a_1} \cdots p_r^{a_r}$ with the a_i chosen big enough so that for any $j \in \{1, \dots, n\}$ the power of p_i which appears in the prime factorization of j is smaller than or equal to a_i . Then it follows from the first part of the exercise, that for all j not equal to 2^k , the number m/j is an integer. It follows that

$$m\left(\sum_{j=1}^n (1/j)\right) = \frac{m}{2^k} + \text{integer},$$

and since $(m, 2^k) = 2^{k-1}$ this cannot be an integer. Hence $\sum_{j=1}^n (1/j)$ is not an integer either.

1.3 (37) Let 2^s be the highest power of 2 appearing in the prime factorization of any number in $\{k, k+1, \dots, k+n\}$. Suppose 2^s divides two distinct numbers in this set. Say $n_1 = 2^s l_1$ and $n_2 = 2^s l_2$, and without loss of generality assume that $l_1 > l_2$. Also, note that by maximality of s , the l_i are odd. But then

$$2^s l_2 < 2^s (l_2 + 1) \leq 2^s l_1,$$

so $2^s (l_2 + 1)$ is also in $\{k, \dots, k+n\}$. But since l_2 is odd, $l_2 + 1$ is even, so $2^{s+1} | (2^s (l_2 + 1))$ which is a contradiction. This proves the first part.

The second part follows from the same reasoning as above. Let p_1, \dots, p_r be the odd primes which appear in the prime factorization of the integers $\{k, \dots, k+n\}$. Then let $m = 2^{s-1}p_1^{a_1} \cdots p_r^{a_r}$ for some sufficiently big a_i . Then m/j is an integer for all but one of the elements in $\{k, \dots, k+n\}$. We conclude that m times the sum in the problem is an integer plus a fraction (with denominator 2), and hence cannot be an integer.