MTH 4104 Example Sheet I Solutions Shu SASAKI

I-1.

$$\begin{aligned} 186 &= 132 \cdot 1 + 54 \\ 132 &= 54 \cdot 2 + 24 \\ 54 &= 24 \cdot 2 + 6 \\ 24 &= 6 \cdot 4 + 0 \end{aligned}$$

hence $\gcd(186, 24) = 6$.

$$\begin{aligned} 6 &= 54 + (-2) \cdot 24 \\ &= 54 + (-2)(132 - 2 \cdot 54) \\ &= 5 \cdot 54 + (-2) \cdot 132 \\ &= 5 \cdot (186 - 1 \cdot 132) + (-2) \cdot 132 \\ &= 5 \cdot 186 + (-7) \cdot 132 \end{aligned}$$

hence $(x, y) = (5, -7)$ does the job.

I-2. (a) By Euclid's algorithm, $\gcd(272, 200) = 8$. Also $272 \cdot (-11) + 200 \cdot 15 = 8$. Multiplying the equation through by 2, we get $272 \cdot (-22) + 200 \cdot 30 = 16$. So $(-22, 30)$ is a solution. (b) Suppose that (x, y) is a pair of integers satisfying $272x + 200y = 4$. By definition, $\gcd(272, 200)$ divides the LHS, therefore it divides the RHS, i.e. 4. However, 8 does not divide 4 (in $\mathbb{Z}$). Therefore no such pair (x, y) exists.

I-3.

$$\begin{aligned} 206 &= 64 \cdot 3 + 14 \\ 64 &= 14 \cdot 4 + 8 \\ 14 &= 8 \cdot 1 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

hence $\gcd(206, 64) = 2$.

$$\begin{aligned} 2 &= 8 - 1 \cdot 6 \\ &= 8 - 1 \cdot (14 - 1 \cdot 8) \\ &= 2 \cdot 8 - 1 \cdot 14 \\ &= 2 \cdot (64 - 4 \cdot 14) - 1 \cdot 14 \\ &= 2 \cdot 64 - 9 \cdot 14 \\ &= 2 \cdot 64 - 9 \cdot (206 - 3 \cdot 64) \\ &= (-9) \cdot 206 + 29 \cdot 64 \end{aligned}$$

hence $(x, y) = (-9, 29)$ is one solution. To find another, we solve $206x + 64y = 0$ (you will see why). Since $206x = -64y$, dividing both sides by 2, we get $103x = -32y$. Therefore $(x, y) = (32r, -103r)$, as r ranges over $\mathbb{Z}$, defines a solution for $206x + 64y = 0$ for any r.

Let (x, y) be another solution for $206x + 64y = 2$. By Euclid's algorithm, we have found $206 \cdot (-9) + 29 \cdot 64 = 2$. Subtracting the latter from the former, we see that $206(x+9) + 64(y-29) = 0$, i.e., $(x + 9, y - 29)$. By the analysis above, we then know that $(x + 9, y - 29) = (32r, -103r)$ for some integer r. In other words, $(x, y) = (-9 + 32r, 29 - 103r)$.

When $r = 0$, we recover $(-9, 29)$. When $r = 1$, we get another solution $(23, -74)$.

I-4. (a)

$$\begin{aligned} 61 &= 18 \cdot 3 + 7 \\ 18 &= 7 \cdot 2 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \end{aligned}$$

Using this, we see

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ &= 4 - (7 - 1 \cdot 4) \\ &= 2 \cdot 4 - 7 \\ &= 2 \cdot (18 - 2 \cdot 7) - 7 \\ &= 2 \cdot 18 - 5 \cdot 7 \\ &= 2 \cdot 18 - 5 \cdot (61 - 3 \cdot 18) \\ &= 17 \cdot 18 - 5 \cdot 61 \end{aligned}$$

and therefore $(x, y) = (-5, 18)$ is a solution.

(b) Let x and y be a solution for $61x + 18y = 0$. In this case, $61x = -18y$. Since 61 divides the LHS, it divides the LHS. But $\gcd(61, 18) = 1$, so 61 divides y. Let $y = 61r$ for some integer r. Similarly 18 divides the RHS and $\gcd(61, 18) = 1$, it also divides x. Combining with $y = 61r$, we deduce that $x = -18r$. In summary, if (x, y) is a solution for $61x + 18y = 1$, then it is of the form $(-18r, 61r)$ for some integer r. Conversely, any pair of the form $(-18r, 61r)$ defines a solution for the equation $61x + 18y = 1$. In conclusion, the solutions for $61x + 18y = 1$ are $(-18r, 61r)$ as° ranges over $\mathbb{Z}$.

(c) Let (x, y) be a pair of integers satisfying $61x + 18y = 1$. Subtracting $61 \cdot (-5) + 18 \cdot 17 = 1$ from it, we see that $61(x + 5) + 18(y - 17) = 0$. As we know that $(x + 5, y - 17) = (-18r, 61r)$ for some integer r, $(x, y) = (-5 - 18r, 17 + 61r)$. Conversely, any pair of integers of the form $(-5 - 18r, 17 + 61r)$, where r ranges over $\mathbb{Z}$ defines a solution for the equation $61x + 18y = 1$.

I-5. (a) Let (x, y) be a pair of integers satisfying $ax + by = 0$. Then $x = -by/a$. The RHS defines an integer if and only if $a/\gcd(a, b)$ divides y. In other words, there exists an integer c such that $y = (-c)a/\gcd(a, b)$. Plugging this back into the equation, we get $x = cb/\gcd(a, b)$. (b) Subtracting $ar + bs = \gcd(a, b)$ from $ax + by = \gcd(a, b)$, we obtain $a(x - r) + b(y - s) = 0$. Using (a), we deduce $(x - r, y - s) = (cb/\gcd(a, b), -ca/\gcd(a, b))$, i.e. $(x, y) = (r + cb/\gcd(a, b), s - ca/\gcd(a, b))$.

I-6. By definition, $\gcd(b, c)$ divides b, and c, hence $a\gcd(b, c)$ divides ab and ac. In other words, $a\gcd(b, c)$ (resp. $-a\gcd(b, c)$) is a common divisor of ab and ac if $a \geqslant 0$ (resp. $a < 0$). By definition, $a\gcd(b, c) \leqslant \gcd(ab, ac)$ (resp. $-a\gcd(b, c) \leqslant \gcd(ab, ac)$).

To prove the converse, observe firstly that $\gcd(ab, ac)$ divides ab and ac. On the other hand, Bezout's identity proves that there exist integers x and y such that $bx + cy = \gcd(b, c)$. Multiplying both sides by a, we obtain $abx + acy = a\gcd(b, c)$. Since $\gcd(ab, ac)$ divides the LHS, it also divides the RHS. Hence $\gcd(ab, ac) \leqslant a\gcd(b, c)$ (resp. $\gcd(ab, ac) \leqslant -a\gcd(b, c)$) if $a \geqslant 0$ (resp. $a < 0$).

I-7. Suppose that there exists a pair of integers (x, y) satisfying $ax + by = c$. Since $\gcd(a, b)$ divides both a and b, it divides the RHS of $ax + by = c$. It therefore follows that it also divides the RHS, i.e. c. Conversely, suppose that $\gcd(a, b)$ divides c. By Bezout's identity, there exists a pair of integers (r, s) such that $ar + bs = \gcd(a, b)$. Hence $(x, y) = (rc/\gcd(a, b), bc/\gcd(a, b))$ defines an integer solution for $ax + by = c$.

I-8. (a) Let a and b be positive integers. By the fundamental theorem of arithmetic, we may write $a = \prod_p p^{r_p(a)}$ and $b = \prod_p p^{r_p(b)}$ where p ranges over the set of prime numbers, and $r_p(a)$ and $r_p(b)$ are non-negative integers and are 0 for all but finitely many p. Then $\mathrm{lcm}(a, b) = \prod_p p^{\max(r_p(a), r_p(b))}$. (b) By comparison, $\gcd(a, b) = \prod_p p^{\min(r_p(a), r_p(b))}$, hence $\gcd(a, b)\mathrm{lcm}(a, b) = \prod_p p^{\max(r_p(a), r_p(b)) + \min(r_p(a), r_p(b))} = \prod_p p^{r_p(a) + r_p(b)} = \prod_p p^{r_p(a)} \prod_p p^{r_p(b)} = ab$. (c) Use euclid's algorithm to compute $\gcd(a, b)$. Compute $\mathrm{lcm}(a, b)$ by $ab/\gcd(a, b)$.

I-9. Let p be a prime number. We know: if p divides ab, then p divides either a or b. Repeatedly apply this to the product of primes in S.

I-10. (a) If N were a prime number, then it follows from $N \equiv -1 \bmod 4$ that N would define an element of S. However, N is defined to be clearly bigger than any element of S. Contradiction. (b) If it were, N would be even. However, $N \equiv -1 \bmod 4$, hence $N \equiv -1 \equiv 1 \bmod 2$. (c) Suppose that a prime number p in S divides N. Then $N \equiv 0 \bmod p$. However, by definition, $N_S \equiv 0 \bmod p$, hence $N = 4N_S - 1 \equiv 4 \cdot 0 - 1 \equiv -1 \bmod p$. Contradiction. (d) We have established in (c) that every prime factor p of N is NOT congruent to $-1 \bmod 4$. This means it is congruent to either 0, 1 or 2, mod 4. The case $p \equiv 0 \bmod 4$ can not occur (as it would mean that p is divisible by 4 but p is a prime number), while $p \equiv 2 \bmod 4$ would force $p = 2$ and we have excluded this case in (b). (e) Since the product of prime numbers $\equiv 1 \bmod 4$ is again congruent to $1 \bmod 4$, it follows from (d) that $N \equiv 1 \bmod 4$. However, $N \equiv -1 \bmod 4$ by definition. Contradiction. It therefore follows that the running assumption that S is finite is false, i.e. S is infinite, i.e. there are infinitely many prime numbers congruent to $-1 \bmod 4$.