MATH10101, for supervision in week 10. Congruences — SOLUTIONS

Q18. (*warm-up*) Let a, b be integers, $d = \gcd(a, b)$, $d \neq 0$.

(i) Prove that the integers a/d and b/d are coprime.

($\star$)(ii) Write down an example of a and b where a/d is not coprime to b and a is not coprime to b/d.

Q18 - solution. (i)

Solution 1: use Bezout's Lemma to write $d = am+bn$ where $m, n \in \mathbb{Z}$. Then $(a/d)m+(b/d)n = 1$ so a/d and b/d are coprime by a question from the previous week's example sheet.

Solution 2 (without Bezout's Lemma)**:** let $e = \gcd(a/d, b/d)$, then e is a positive integer (the numbers a/d and b/d are not both zero) which divides both a/d and b/d. So $a/d = ek$, $b/d = e\ell$ for some integers k, ℓ. Then $a = dek$, $b = de\ell$ which means that de is a common divisor of a and b. But since d is the greatest common divisor and $d \neq 0$, we have $de \leq d$. Since d is positive, $e \leq 1$. Finally, since e is a positive integer, $e = 1$ and a/d, b/d are coprime, as claimed.

($\star$)(ii) For example, let $a = 12$, $b = 18$, $d = 6$. Then $a/d = 2$ is not coprime to $b = 18$ and $a = 12$ is not coprime to $b/d = 3$.

Q19. Let a, b, q, m be integers, $q, m > 0$. Prove: $qa \equiv qb \mod qm \implies a \equiv b \mod m$.

Q19 - solution. Assume that $qa \equiv qb \mod qm$. By definition of congruence, $\equiv$, this means that $qm\,|(qa - qb)$. By definition of "divides", $|$, this means that there exists an integer k such that $qa - qb = qmk$ which can equivalently be written as $q(a - b) = q(mk)$. Since q is a positive integer by assumption, $q \neq 0$, hence it follows that $a - b = mk$, so $m\,|\,a - b$ and by definition $a \equiv b \mod m$.

Q20. Jean was asked to solve the congruence $12x \equiv 7 \mod 17$. Jean wrote:

$12x \equiv 7 \mod 17$
Add 17
$12x \equiv 24 \mod 17$
Divide by 12
$x \equiv 2 \mod 17$

Is this is a well-written argument? Is the answer correct? Is the method valid? Write down a better solution.

Q20 - solution. An evaluation attempt: Jean is not using any logical connectives between the statements. Hence what Jean writes is not a mathematical argument. If, say, two statements are equivalent, one must write that explicitly. Writing one statement under the other does not imply logical links between the statements. Also, Jean does not explain the steps being made. An improved solution might look as follows — it attempts to be quite detailed:

Solution. Observe that $7 \equiv 24 \mod 17$, since $17 \,|(24-7)$. Therefore, the statement $12x \equiv 7 \mod 17$ is equivalent to the statement $12x \equiv 24 \mod 17$ by transitivity of congruence.

Now observe that $\gcd(12, 17) = 1$, since the only positive divisors of 17 are 1 and 17, and of these, only 1 is a common divisor of 12 and 17. By a result proved in the course, $12x \equiv 24 \mod 17$ implies, by dividing both sides by an integer coprime to the modulus, the congruence $x \equiv 2 \mod 17$. The two congruences are equivalent, as $x \equiv 2 \mod 17$ implies $12x \equiv 24 \mod 17$ by Modular Arithmetic.

Thus, the solution of the original congruence is $x \equiv 2 \mod 17$. **End of solution.**

Jean's approach was valid, and the final answer was correct, but the solution as given lacked detail.

Q21. Solve the following congruences for x. Your answer should be expressed as a congruence in the original modulus, 777, and given as remainder(s) mod 777.

($\star$)i) $199x \equiv -6 \mod 777$;

($\star$)ii) $6x \equiv 3 \mod 777$;

($\star$)iii) $77x \equiv 2 \mod 777$;

iv) $6x \equiv 0 \mod 777$;

v) $10101x \equiv 0 \mod 777$.

Q21 - solution. Always check your answers by substituting back into the question.

($\star$)i) $199x \equiv -6 \mod 777$, if and only if there is an integer y such that $199x - 777y = -6$. Apply Euclid's algorithm to 777 and 199:

$$\begin{aligned}
777 &= 199 \times 3 + 180 \\
199 &= 180 \times 1 + 19 \\
180 &= 19 \times 9 + 9 \\
19 &= 9 \times 2 + 1 \\
9 &= 1 \times 9 + 0.
\end{aligned}$$

Hence $\gcd(199, -777) = \gcd(777, 199) = 1$ and since $1 \,|\, -6$, the Diophantine equation $199x - 777y = -6$ has solutions. To write 1 as an integral linear combination of 199 and 777, work back up the algorithm:

$$\begin{aligned}
1 &= 19 - 9 \times 2 = 19 - (180 - 19 \times 9) \times 2 \\
&= 180(-2) + 19 \times 19 = 180(-2) + (199 - 180) \times 19 \\
&= 199 \times 19 + 180(-21) = 199 \times 19 + (777 - 199 \times 3)(-21) \\
&= 777(-21) + 199 \times 82.
\end{aligned}$$

Thus, $199 \times 82 - 777 \times 21 = 1$.

Multiplying through by -6, we obtain $199 \times (-492) - 777 \times (-126) = -6$. Hence $(x_0, y_0) = (-492, -126)$ is a particular solution of the equation $199x - 777y = -6$. Since $\gcd(199, 777) = 1$, the general solution is $(x, y) = (-492 + 777t, -126 + 199t)$, $t \in \mathbb{Z}$.

The solution of the congruence is therefore $x \equiv -492 \mod 777$. Expressed as a remainder modulo 777, this is $\boldsymbol{x \equiv 285 \mod 777}$.

Partial check: $199 \times 285 = 56715$ and $56715 + 6 = 56721 = 777 \times 73$ which shows that 56715 is indeed congruent to -6 modulo 777.

($\star$)(ii) **Method 1:** $6x \equiv 3 \mod 777$, if and only if $6x - 777y = 3$ for some integer y. It is not difficult to see that $780 - 777 = 3$ where $780 = 6 \times 130$ is a multiple of 6. This gives a particular solution $(x_0, y_0) = (130, 1)$.

The number 6 has positive divisors $1, 2, 3, 6$ of which only 1 and 3 divide 777. Hence $\gcd(6, 777) = 3$, and the general solution of the Diophantine equation is $(x, y) = (130 + 259t, 1 + 2t)$, $t \in \mathbb{Z}$. Here $259 = \frac{777}{3}$.

The possible remainders left by $130 + 259t$, $t \in \mathbb{Z}$, when divided by 777 are 130, $130 + 259$ and $130 + 259 \times 2$. Hence the answer modulo 777 is $\boldsymbol{x \equiv 130}$, $\mathbf{389}$ or $\mathbf{648 \mod 777}$.

Method 2: the congruence can be written as $3 \times 2x \equiv 3 \times 1 \mod 3 \times 259$. Since $3 > 0$, by **Q19** we can divide both sides of the congruence **and the modulus** by 3, obtaining the equivalent congruence

$$2x \equiv 1 \mod 259.$$

Using the approach from **Q20**, rewrite this in an equivalent form as

$$2x \equiv 260 \mod 259.$$

By a result from the course, both sides can be divided by an integer coprime to the modulus. Observing that 2 is coprime to 259, we arrive at the following equivalent congruence:

$$x \equiv 130 \mod 259.$$

This is the solution of the original congruence but written modulo 259 not modulo 777. To express the answer as three remainders modulo 777, proceed as in Method 1.

($\star$)(iii) $77x \equiv 2 \mod 777$ if and only if there exists an integer y such that $77x - 777y = 2$. However, the left-hand side of this equation must be divisible by 7 hence cannot equal 2. The equation, and therefore the congruence, have **no solutions**.

(iv) $6x \equiv 0 \mod 777$ if and only if $6x - 777y = 0$ for some $y \in \mathbb{Z}$. The equation $6x - 777y = 0$ has an obvious particular solution $(0, 0)$ so the general solution is $(x, y) = (259t, 2t)$, $t \in \mathbb{Z}$. The possible remainders of $x = 259t$ modulo 777 are $\mathbf{0}$, $\mathbf{259}$ and $\mathbf{259 \times 2 = 518}$.

(v) Since $10101 = 13 \times 777$ is congruent to 0 mod 777, the congruence reads $0x \equiv 0 \mod 777$. Its solutions are **all integers**. If one were to write the answer as remainders modulo 777, it is $\{0, 1, \ldots, 776\}$, that is, all possible remainders.

Q22. i) Find a multiplicative inverse of 5 modulo 47.

ii) Solve the congruences: a) $5x \equiv 2 \mod 47$, b) $25x \equiv 3 \mod 47$, c) $19x \equiv 20 \mod 47$.

Q22 - solution. i) Solve $5x \equiv 1 \mod 47$: e.g., $1 \equiv 1+94 = 95 \mod 47$ so that the congruence is equivalent to $5x \equiv 95 \mod 47$; 5 is coprime to 47 hence can divide both sides by 5 to obtain an equivalent congruence $x \equiv 19 \mod 47$. Thus, 19 is the multiplicative inverse of 5 modulo 47.

ii) a) Multiply both sides by 19 to get an equivalent congruence $19 \times 5x \equiv 19 \times 2 \mod 47$, i.e. $x \equiv 38 \mod 47$.

b) Observe that $25 = 5^2$. We would like to multiply both sides by $19^2 = 361 = 47 \times 7 + 32 \equiv 32 \mod 47$. We have $19^2 \times 5^2 \equiv 1 \mod 47$ hence we obtain an equivalent congruence $x \equiv 19^2 \times 3 \equiv 32 \times 3 = 96 \equiv 2 \mod 47$.

c) Since 19 is the inverse of $5 \mod 47$, we conclude that 5 is the inverse of 19. So multiply both sides by 5 to get $5 \times 19x \equiv 5 \times 20 \mod 47$, i.e. $x \equiv 6 \mod 47$.

Q23. Find the least non-negative integer x satisfying $x \equiv 4 \mod 11$ and $x \equiv 3 \mod 13$.

Q23 - solution. Write the two congruences as $x = 4 + 11k$ and $x = 3 + 13\ell$ for integers k, ℓ. Equate to get $4 + 11k = 3 + 13\ell$. Thus we get a linear Diophantine equation $11k - 13\ell = -1$. Use Euclid's Algorithm to find $1 = 11 \times 6 - 13 \times 5$ hence $-1 = 11(-6) - 13(-5)$. This gives a particular solution $x = 4 + 11 \times (-6) = 3 + 13 \times (-5) = -62$.

Unfortunately, this particular solution is negative. By the Chinese Remainder Theorem, all solutions are obtained from -62 by adding multiples of $11 \times 13 = 143$. So we have the solution $-62 + 143 = 81$. The Chinese Remainder Theorem tells us that there is exactly one solution between 0 and 142, which must then be 81. All other solutions are either negative or greater than 142, hence $x = 81$ is the least positive solution.

($\star$)**Q24**. Find the remainders of 20^{19} and 19^{19} when divided by 13. Show that $20^{19} + 19^{19}$ is divisible by 13.

Q24 - solution. We find the residue of 20^{19} modulo 13 by the method of successive squaring. To simplify calculations, observe that $20 \equiv 7 \mod 13$. Hence by Modular Arithmetic, $20^{19} \equiv 7^{19}$. Let us find the residue of 7^{19}:

- $7^2 = 49 \equiv 10 \mod 13$, hence
- $7^4 \equiv (7^2)^2 \equiv 10^2 = 100 \equiv 9 \mod 13$, hence
- $7^8 \equiv (7^4)^2 \equiv 9^2 \equiv 3 \mod 13$, hence

- $7^{16} \equiv (7^8)^2 \equiv 3^2 \equiv 9 \mod 13$,

so that $20^{19} \equiv 7^{19} \equiv 7 \times 7^2 \times 7^{16} \equiv 7 \times 10 \times 9 = 630 \equiv 6 \mod 13$. The remainder left by 20^{19} when divided by 13 is 6.

We can of course apply the same procedure to find the remainder of 19^{19} when divided by 13. But there is a shorter way: observe that $20 + 19 = 39 \equiv 0 \mod 13$ so $19 \equiv -20 \mod 13$ and

$$19^{19} \equiv (-20)^{19} \equiv -20^{19} \equiv -6 \equiv 7 \mod 13.$$

Hence the remainder left by 19^{19} when divided by 13 is 7.

Finally, $20^{19} + 19^{19} \equiv 6 + 7 \equiv 0 \mod 13$. This shows that $20^{19} + 19^{19}$ is divisible by 13.