# Math 1C03 Problem Sheet 3 Solutions

1) $a \equiv b \bmod m$ if $m \mid (a-b)$.

i) $6-5=1$ and $4 \nmid 1$ so $6 \not\equiv 5 \bmod 4$

ii) $13-3=10$ and $3 \nmid 10$ so $13 \not\equiv 3 \bmod 3$

iii) $100-25=75$ and $4 \nmid 75$ so $100 \not\equiv 25 \bmod 4$

iv) $15 \mid 75$, so $100 \equiv 25 \bmod 15$

v) $1001-12345$ is an ~~odd~~ even number, so divisible by 2, so $1001 \equiv 12345 \bmod 2$

vi) $-5-5=-10$ and $3 \nmid -10$, so $-5 \not\equiv 5 \bmod 3$

vii) $4^{51}$ is even and $111\,111$ is odd, so $4^{51}-111\,111$ is odd, so $2 \nmid (4^{51}-111\,111)$. Thus $4^{51} \not\equiv 111\,111 \bmod 2$.

viii) $10!+1-9 = 10!-8$ $7 \mid 10!$ and $7 \nmid 8$, so $7 \nmid (10!-8)$. Thus $10!+1 \not\equiv 9 \bmod 7$.

ix) $10!+1-82 = 10!-81$ $9 \mid 10!$ and $9 \mid 81$, so $9 \mid (10!-81)$. Thus $10!+1 \equiv 82 \bmod 9$.

2) i) Assume $a \equiv b \bmod m$. Then $m \mid (a-b)$, that is, $a-b = mq$ for some integer $q$.

We want to show that $a^2 \equiv b^2 \bmod m$; that is, that $m \mid (a^2-b^2)$.

Now, $a^2-b^2 = (a-b)(a+b) = mq(a+b)$.

As $m \mid mq(a+b)$, so $m \mid (a^2-b^2)$, as required.

ii) Assume $a \equiv b \bmod m$. As above, $a-b = mq$.

Then $na-nb = n(a-b) = nmq$, so

$m \mid (na-nb)$, so $na \equiv nb \bmod m$.

iii) Assume that $a \equiv b \bmod m$ and $a' \equiv b' \bmod m$.

So $a-b = mq$, and $a'-b' = mq'$, where $q, q' \in \mathbb{Z}$.

~~$(a-b)(a'-b') = aa' - ba' - ab' + bb'$~~

We want to show that $aa' \equiv bb' \bmod m$.

$$\begin{aligned} aa'-bb' &= a(a'-b') + ab' - bb' \\ &= a(a'-b') + b'(a-b) \\ &= amq' + b'mq \\ &= m(aq' + b'q). \end{aligned}$$

Thus $m \mid (aa'-bb')$, as required.

3) i) $3^4 = 81 \equiv 1 \mod 80$

$111 = 4 \cdot 27 + 3$

So $3^{111} = 3^{4 \cdot 27 + 3} = (3^4)^{27} \cdot 3^3$

$\equiv 1^{27} \cdot 3^3 \mod 80$

$\equiv 27 \mod 80$

ii) $4 \equiv -1 \mod 5$ So $4^{23} \equiv (-1)^{23} \equiv -1 \mod 5$

$36 \equiv 1 \mod 5$ So $36^{11} \equiv (1)^{11} \equiv 1 \mod 5$.

Thus $4^{23} \cdot 36^{11} \equiv -1 \equiv 4 \mod 5$

4) i) there exist unique integers $q_1, r_1$ st.

$$a = q_1 m + r_1 \quad \text{and} \quad 0 \le r_1 < m$$

and there exist unique integers $q_2, r_2$ st.

$$b = q_2 m + r_2 \quad \text{and} \quad 0 \le r_2 < m.$$

ii) Assume a and b have the same remainder when divided by m. that is, $r_1 = r_2$ in the notation above. then

$$\begin{aligned} a - b &= q_1 m + r_1 - (q_2 m + r_2) \\ &= m(q_1 - q_2) + r_1 - r_2 \\ &= m(q_1 - q_2) + 0. \end{aligned}$$

thus $m \mid (a-b)$, that is, $a \equiv b \bmod m$.

iii) Assume $a \equiv b \bmod m$. so $m \mid a-b$.

Now, $a - b = q_1 m + r_1 - (q_2 m + r_2)$

$= m(q_1 - q_2) + r_1 - r_2$.

Since $m \mid (a-b)$ and $m \mid (q_1 - q_2)$, also $m \mid (r_1 - r_2)$. But $0 \le r_1 < m$ and $0 \le r_2 < m$ together imply (subtracting) $-m < r_1 - r_2 < m$.

thus the only way $r_1 - r_2$ can be divisible by m is if $r_1 - r_2 = 0$ i.e. $r_1 = r_2$.

5) $p$ a fixed prime.

i) For any integer $m$ with $1 \le m < p$, $\gcd(m, p) = 1$ (as $p$ is prime and $p \nmid m$). By the euclidean algorithm, there exist integers $x$ and $y$ st.

$$mx + py = 1.$$

That is $mx - 1 = py$, or $mx \equiv 1 \bmod p$.

That is, $[mx]_p = [1]_p$, or $[m]_p[x]_p = [1]_p$.

~~Then $x$ is the value $n$ required.~~

Now write $x = qp + n$. Then $[x]_p = [n]_p$ and $1 \le n < p$, as required.

To see that $n$ is unique, suppose also $[m]_p[n']_p = [1]_p$ and $1 \le n' < p$. Then $p \mid (mn - 1)$ and $p \mid (mn' - 1)$, that is, $mn - 1 = pq$ and $mn' - 1 = pq'$.

Subtracting: $mn - mn' = pq - pq'$

$$m(n - n') = p(q - q').$$

As $p \mid$ RHS, $p \mid$ LHS. As $p$ is prime, $p \mid m$ or $p \mid (n - n')$. But $1 \le m < p$, so $p \nmid m$. And $-p < n - n' < p$, so if $p \mid (n - n')$ then $n - n' = 0$ ie. $n = n'$.

ii) $p = 5$ $\quad [(p-1)!]_p = [4 \cdot 3 \cdot 2 \cdot 1]_5 = [24]_5 = [4]_5$

for ~~$[(5-1)!]_5$~~ $(5-1)! \equiv 4 \bmod 5$

$\equiv -1 \bmod 5$.

Notice that $[4 \cdot 3 \cdot 2 \cdot 1] = [4] \cdot [3] \cdot [2] \cdot [1]$

$= [4] \cdot [1] \cdot [1] = [4]$,

as $[3] \cdot [2] = [6] = [1]$.

$p = 7$ $\quad [(p-1)!]_p = [6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1]_7$

$= [6][5][4][3][2][1]$

$= [6][15][8][1]$

$= [6][1][1][1] = [6]$

Thus $(7-1)! \equiv 6 \bmod 7 \equiv -1 \bmod 7$.

iii) $[(p-1)!] = [p-1][p-2] \cdots [2][1]$ has $p-1$ factors.

iv) We know by i) that for every integer $m$ with $1 \le m < p$ there is a unique integer $n$ with $1 \le n < p$ st. $[m]_p[n]_p = [1]_p$.

In the set of numbers $1, 2, \ldots p-2, p-1$,

each number matches with its pair, so that the product of the two is $[1]$. The only exceptions are $[1]$ (as $[1][1]=[1]$) and $[p-1]$, as $[p-1][p-1] = [p^2-2p+1] = [1]$. Thus

$$[(p-1)!] = [p-1]\underbrace{[1][1]\cdots[1]}_{\frac{p-3}{2}}[1] = [p-1].$$

Thus $[(p-1)!] = [p-1]$.

✓) Hence $(p-1)! \equiv p-1 \mod p$

$\equiv -1 \mod p$.