# DGD 5

MAT1348X
June 23, 2020

The first three questions are proofs that we omitted in class.

1. Let $m$ be a positive integer. Suppose that $r_1$ is the remainder when $a$ is divided by $m$, and $r_2$ is the remainder when $b$ is divided by $m$. Show that if $a - b$ is a multiple of $m$, then $r_1 = r_2$.

*Proof.* Since $a - b$ is a multiple of $m$, the remainder is 0 when $a - b$ is divided by $m$.

On the other hand, by the division algorithm, $a = q_1m + r_1$, $b = q_2m + r_2$, where $q_1$ and $q_2$ are integers, $0 \le r_1 < m$, $0 \le r_2 < m$. Without loss of generality, we may assume $r_1 \ge r_2$. Then $a - b = (q_1 - q_2)m + (r_1 - r_2)$, $0 \le r_1 - r_2 < r_1 < m$. In other words, when $a - b$ is divided by $m$, the quotient is $q_1 - q_2$ and the remainder is $r_1 - r_2$.

By the Division Algorithm, when $a - b$ divided by $m$, the remainder is unique. Hence $r_2 - r_1 = 0$ and $r_1 = r_2$.

*Remark.* Although this result looks "obvious", we see that, if we want to prove it, the proof is not so "obvious".

First, it is easy to conclude that the remainder is 0 when $a - b$ is divided by $m$. However, this does not lead directly to $r_1 - r_2 = 0$. To make this conclusion, we need to quote the uniqueness of the remainder. This requires to show that the difference of $r_1$ and $r_2$ IS the remainder of $a - b$ divided by $m$, because the remainder of a number divided by $m$ **must be non-negative and less than $m$**. This leads us to assume $r_1 \ge r_2$. We can make this assumption without loss of generality because $a - b$ is a multiple of $m$ if and only if $b - a$ is a multiple of $m$. Therefore, we can always choose the one with larger remainder to be $a$, and the one with a smaller remainder to be $b$. Under this assumption, we can show $0 \le r_1 - r_2 < m$. Then $r_1 - r_2$ IS the remainder when $a - b$ divided by $m$, and we can quote the uniqueness of the remainder to conclude $r_1 = r_2$.

2. Show that, if gcd $(a, m) > 1$, then $a$ does not have an inverse modulo $m$.

*Proof.* Suppose gcd $(a, m) = d > 1$. Then $a = sd$, and $m = td$, where $s$ and $t$ are integers. If there is an inverse $b$ of $a$ modulo $m$, then $ab \equiv 1 \pmod{m}$, i.e., $ab = qm + 1$, or $ab - qm = 1$, where $q$ is an integer. Since $a$ and $m$ are multiples of $d$, $d$ divides $ab - qm$. Since $d$ does not divide 1 on the right-hand side, this is a contradiction.

3. Suppose the congruence $ax \equiv b \pmod{m}$ has a solution and gcd $(a, m) = d > 1$. Then $b$ is a multiple of $d$. If $d$ is also a factor of $b$, then $x$ is a solution to congruence $ax \equiv b \pmod{m}$ if and only if $x$ is a solution to congruence $a_1x \equiv b_1 \pmod{m_1}$, where $a_1 = a / d$, $b_1 = b / d$, and $m_1 = m / d$.

*Proof.* Let $a = a_1d$, and $m = m_1d$, where $a_1$ and $m_1$ are integers. If this congruence has a solution $x$, then $ax = mt + b$. Since $d$ divides $a$ and $m$, $d$ divides $ax – mt = b$, i.e., $b$ is a multiple of $d$.

Integer $x$ is a solution to congruence $ax \equiv b \pmod{m}$ if and only if $ax = mt + b$, where $t$ is an integer. Dividing this equality by $d$ on both sides, $a_1x = m_1t + b_1$. This is true if and only if $a_1x \equiv b_1 \pmod{m_1}$.

4. This is a question that the students did on the second midterm:

Find the smallest positive integer of the system of congruences $x \equiv 8 \pmod{17}$, $x \equiv 2 \pmod{29}$.

*Solution.* $x = 17s + 8$. $17s + 8 \equiv 2 \pmod{29}$. $17s \equiv -6 \equiv 23 \pmod{29}$.

To solve this congruence, we need the inverse of 17 modulo 29. This inverse is given in the question. Here is how to find it:

By Euclidean algorithm,

$29 = 1 \times 17 + 12$,
$17 = 1 \times 12 + 5$,
$12 = 2 \times 5 + 2$,
$5 = 2 \times 2 + 1$.

Then $1 = 5 – 2 \times 2 = 5 – 2 \times (12 – 2 \times 5) = (-2) \times 12 + 5 \times 5 = (-2) \times 12 + 5 \times (17 – 1 \times 12)$
$= 5 \times 17 + (-7) \times 12 = 5 \times 17 + (-7) \times (29 – 1 \times 17) = (-7) \times 29 + 12 \times 17$.

Hence, $12 \times 17 \equiv 1 \pmod{29}$.

The inverse of 17 mod 29 is 12 (mod 23).

The solution to this system is $s \equiv 12 \times 23 \equiv 276 \equiv 15 \pmod{29}$, or $s = 29t + 15$. Then $x = 17s + 8 = 17(29t + 15) + 8 = 393t + 263$, and the smallest positive solution is 263.

5. Find the coefficient of $x$ in expansion $(x^3 + x^{-2})^7$.

*Solution*. The coefficient of $(x^3)^p(x^{-2})^{7-p} = x^{5p-14}$ is $C(7, p)$.

$5p - 14 = 1$. $5p = 15$, and $p = 3$. The coefficient of $x$ is $C(7, 3) = 35$.

6. There are seven men and four women in a group. How many ways can we choose three men and two women to sit in a row so that two women are not side by side?

*Solution*. There are $P(7, 3)$ ways to choose three men, and $P(4, 2)$ ways to choose two women. Then we have $C(4, 2)3!2!$ ways to arrange them to sit without two women side by side.

$P(7, 3)P(4, 2)C(4, 2)3!2! = 181440$.

7. Find the number of bit strings of length 8 that satisfies at least one of the following conditions:

$C_1$: It starts with a 0 and end with a 1,

$C_2$: It has three 1's and five 0's.

*Solution*. The number of bit strings of length 8 that satisfy condition $C_1$ is $2^6$.

The number of bit strings of length 8 that satisfy condition $C_2$ is $C(8, 3)$.

The number of bit strings of length 8 that satisfy both conditions is $C(6, 2)$.

By the inclusion-exclusion principle, the number of bit strings of length 8 that satisfy at least one of the conditions $2^6 + C(8, 3) - C(6, 2) = 105$.